Teoria dei tratteggi

Simone Battagliero

4 giugno 2010

Questo libro è dedicato a tutti coloro che
sono soliti porsi domande,
rispondervi usando la ragione,
e riconoscere che questa, da sola,
non è sufficiente.

Indice

Parte I

Fondamenti di teoria dei tratteggi

Capitolo 1

Introduzione alla teoria dei tratteggi

La matematica, generalmente, risolve
problemi complessi in modo semplice;
La teoria dei tratteggi risolve
problemi semplici in modo complicato.

La teoria matematica dei tratteggi si colloca nell'ambito della teoria dei numeri. Inizialmente basata su uno studio dei numeri a un livello molto basso (nel senso informatico del termine, ossia un livello che considera tutti i minimi dettagli), si è poi evoluta giungendo a livelli più astratti. Essa è nata come strumento per la risoluzione di alcuni problemi riguardanti i numeri primi (come il calcolo dell'n-esimo numero primo e la dimostrazione della congettura di Goldbach), ma, col passare del tempo, si è sempre più configurata come teoria matematica a sé stante, pur non perdendo l'obiettivo originario.

È molto più complesso scrivere un libro che presenta una nuova teoria matematica, che scriverne uno che amplia una teoria esistente: si devono creare concetti nuovi, rendere chiare analogie e differenze tra concetti simili, porre e risolvere problemi nuovi, chiarire come problemi diversi sono in relazione tra loro, sviluppare tecniche di dimostrazione ad hoc, confrontare le soluzioni date a problemi simili, individuare possibili evoluzioni della teoria... è evidente che il lavoro è lungo e complesso, non solo dal punto di vista matematico, ma anche dal punto di vista di stesura del testo, per cui sicuramente, nonostante le continue revisioni, sono rimasti passaggi non chiari.

Anche da un punto di vista matematico credo che l'opera possa essere migliorata: infatti questo libro non è stato scritto da un matematico, per scopi di ricerca, ma da un semplice appassionato di matematica. La mancanza di un impegno professionale,

come quello di un ricercatore, aumenta la possibilità di sviste o incoerenze varie, ma in compenso questi problemi sono spesso risolti col passare del tempo.

Rispetto alla prima edizione, non pubblicata e nota solo a pochissimi, sono stati aggiunti commenti ed esempi, molte definizioni e molti teoremi sono stati generalizzati, le dimostrazioni sono state rese più formali ed alcune errate sono state corrette. Infine, ma non meno importante, per la scrittura si è usato il linguaggio LaTeX.

Molti risultati dimostrati in questo libro, e perfino alcune definizioni, possono essere generalizzati: questo sarà certamente uno dei principali obiettivi delle prossime edizioni. Per il momento, si è preferito proporre una visione globale della teoria, il più possibile organica e coerente, toccando diversi argomenti e rendendo chiare per ciascuno le possibilità di generalizzazioni future (alcune delle quali, ritenute particolarmente importanti, sono state già enunciate come congetture).

1.1 Notazioni usate

1.1.1 Notazioni fondamentali

Per quanto riguarda gli insiemi numerici, indicheremo:

- l'insieme dei numeri interi con $\mathbb{Z}$
- l'insieme dei numeri naturali (cioè degli interi maggiori o uguali a 0) con $\mathbb{N}$
- l'insieme dei numeri interi non nulli con $\mathbb{Z}^\star$
- l'insieme dei numeri naturali non nulli con $\mathbb{N}^\star$

Inoltre, useremo il simbolo $+\infty$, o semplicemente ∞, come uno speciale numero confrontabile con gli interi e tale che $x < \infty$ per ogni $x \in \mathbb{Z}$. Analogamente, useremo il simbolo $-\infty$ come uno spaciale numero tale che $-\infty < x$ per ogni $x \in \mathbb{Z}$. Non effettueremo operazioni con questi speciali numeri, ma li abbiamo introdotti solo per comodità notazionale. Ad esempio, la scrittura $\{x \in \mathbb{N} \mid 1 \leq x \leq n\}$ è un insieme finito di cardinalità n, se $n \in \mathbb{N}^\star$; se invece $n = \infty$, esso coincide con $\mathbb{N}^\star$. In questo modo abbiamo uniformità notazionale per insiemi finiti ed infiniti.
Poniamo, inoltre, $\overline{\mathbb{N}} \equiv \mathbb{N} \cup \{\infty\}$, $\overline{\mathbb{N}^\star} \equiv \mathbb{N}^\star \cup \{\infty\}$, $\overline{\mathbb{Z}} \equiv \mathbb{Z} \cup \{+\infty, -\infty\}$ e $\overline{\mathbb{Z}^\star} \equiv \mathbb{Z}^\star \cup \{+\infty, -\infty\}$.

Definiamo *intervallo* da $a \in \overline{\mathbb{Z}}$ a $b \in \overline{\mathbb{Z}}$, $a \leq b$, l'insieme $\left\{x \in \overline{\mathbb{Z}} \mid a \leq x \leq b\right\}$, e lo denoteremo col simbolo $[a, b]$. Il numero $|[a, b]| = b - a + 1$ si chiama *lunghezza* di $[a, b]$.

Come conseguenza delle notazioni precedenti, si può notare che $\mathbb{N} = [0, \infty]$ e $\mathbb{Z} = [-\infty, +\infty]$.

Useremo il simbolo $\equiv$ per indicare che il simbolo posto alla sua destra e quello posto alla sua sinistra sono due modi diversi di scrivere la stessa cosa: ogni occorrenza del primo può essere sostituita col secondo, e viceversa. Esso è utile per definire delle notazioni concise per certe espressioni; ad esempio, è noto che $|x| \equiv \begin{cases} x & \text{se } x > 0 \\ -x & \text{altrimenti} \end{cases}$.

Useremo il simbolo $=$ per indicare che l'espressione posta alla sua destra e quella posta alla sua sinistra hanno lo stesso valore. Ad esempio, $a \cdot 0 = 0$ sempre, e $4a = 12 \Leftrightarrow a = 3$.

A volte utilizzeremo la notazione lambda per definire funzioni senza nome; ad esempio $\lambda x.3x$ per indicare la funzione nella variabile x che associa ad x il valore $3x$.

Definizione 1.1. *Siano $a \in \mathbb{N}$, $b \in \mathbb{N}^\star$. Si definisce:*

- $a \bmod b \equiv$ *resto della divisione di a per b*
- $a \bmod^\star b \equiv \begin{cases} a \bmod b & \textit{se } a \bmod b > 0 \\ b & \textit{altrimenti} \end{cases}$
- $\left\lfloor \frac{a}{b} \right\rfloor \equiv$ *quoziente della divisione di a per b* $= \dfrac{a - a \bmod b}{b}$
- $\left\lceil \frac{a}{b} \right\rceil \equiv \begin{cases} \left\lfloor \frac{a}{b} \right\rfloor & \textit{se } a \bmod b = 0 \\ \left\lfloor \frac{a}{b} \right\rfloor + 1 & \textit{altrimenti} \end{cases} = \dfrac{a - a \bmod^\star b}{b} + 1$

Conveniamo di leggere i simboli appena definiti rispettivamente come "a modulo b", "a modulo star b", "parte intera di $\frac{a}{b}$" e "parte intera per eccesso di $\frac{a}{b}$". Le funzioni corrispondenti ai simboli definiti, ossia $\lambda a.\lambda b.a \bmod b$, $\lambda a.\lambda b.a \bmod^\star b$, $\lambda a.\lambda b.\left\lfloor \frac{a}{b} \right\rfloor$ e $\lambda a.\lambda b.\left\lceil \frac{a}{b} \right\rceil$, vengono chiamate rispettivamente "modulo", "modulo star", "parte intera" e "parte intera per eccesso". Le funzioni modulo e modulo star vengono chiamate entrambe *funzioni modulo*[1]; le altre due vengono chiamate *funzioni parte intera*.

Dalla definizione precedente segue che, per ogni $a \in \mathbb{N}$, $b \in \mathbb{N}^\star$:

- $0 \leq a \bmod b \leq b - 1$
- $1 \leq a \bmod^\star b \leq b$

[1] Attenzione al plurale: la funzione modulo è $\lambda a.\lambda b.a \bmod b$; le funzioni modulo sono $\lambda a.\lambda b.a \bmod b$ e $\lambda a.\lambda b.a \bmod^\star b$

Nelle espressioni, gli operatori mod e $\mathrm{mod}^\star$ hanno la stessa precedenza della moltiplicazione; ad esempio, $ab \bmod c \equiv (ab) \bmod c$ e $a + b \bmod c \equiv a + (b \bmod c)$.

Le operazioni che useremo su $\mathbb{N}$ sono:

- somma
- prodotto
- differenza
- modulo, modulo star
- parte intera, parte intera per eccesso

La differenza in $\mathbb{N}$ è definita solo quando il primo operando è maggiore o uguale al secondo. Quando la continua verifica di questa proprietà potrebbe risultare noiosa, useremo $(\mathbb{Z}, +, \cdot)$ come anello commutativo unitario, ma solo come strumento intermedio in calcoli molto lunghi.

1.1.2 Valori di verità come interi

Incontreremo molto spesso funzioni definite per casi. Spesso i casi sono solo due, quindi si ha la forma generale

$$f(x) \equiv \begin{cases} \text{espressione1}(x) & \text{se condizione1}(x) \\ \text{espressione2}(x) & \text{altrimenti} \end{cases}$$

A volte espressione1(x) e espressione2(x) sono così simili che conviene definire la funzione in una forma alternativa, utilizzando la convenzione (diffusa in alcuni linguaggi di programmazione, come il C) di trattare i valori di verità come degli interi. Un valore di verità è il risultato della valutazione di una condizione, come $a > 10$: se la condizione è falsa, il suo valore di verità è `F`; altrimenti è `V` (al posto di `F` e `V` si può usare qualsiasi coppia di simboli con gli stessi significati). Noi, come nel linguaggio C, daremo ad `F` il valore intero 0 e a `V` il valore intero 1. In questo modo potremo usare le condizioni come operandi di operazioni che normalmente si applicano su interi, valutando la condizione col valore intero associato al suo valore di verità. Ad esempio, l'espressione $2 + (b > 0)$ ha valore 3 se $b > 0$; 2 altrimenti.

Con questa notazione, la funzione di parte intera per eccesso:

$$\left\lceil \frac{a}{b} \right\rceil \equiv \begin{cases} \left\lfloor \frac{a}{b} \right\rfloor & \text{se } a \bmod b = 0 \\ \left\lfloor \frac{a}{b} \right\rfloor + 1 & \text{altrimenti} \end{cases}$$

si può scrivere anche:

$$\left\lceil \frac{a}{b} \right\rceil \equiv \left\lfloor \frac{a}{b} \right\rfloor + (a \bmod b > 0)$$

In questo caso si possono anche omettere le parentesi, perché si conviene di valutare i confronti prima di somme e differenze ma dopo prodotti, divisioni e moduli.

1.1.3 Altre notazioni

Altre notazioni usate nel corso del libro sono:

- Dom f per indicare il dominio della funzione f.
- $f(x) = \perp$, per indicare che $x \notin \text{Dom } f$ (cioè f non è definita per x).
- $f_{|X}$ per indicare la restrizione della funzione f ad X.
- $[X \to Y]$, dove X e Y sono insiemi, per indicare l'insieme delle funzioni da X in Y.
- 2^X, dove X è un insieme, per indicare l'insieme delle parti di X.
- $\max_x f(x)$ per indicare il massimo di $f(x)$ al variare di x nel dominio di f.
- $\arg\max_x f(x)$per indicare il numero x in corrispondenza del quale la funzione f assume il suo massimo valore.
- S_n per indicare il gruppo delle permutazioni di $\{1, \ldots, n\}$.
- $\sigma_k(x_1, \ldots, x_n)$ per indicare il k-esimo polinomio simmetrico elementare nelle variabili $x_1, \ldots, x_n$ (ad esempio, $\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$).
- $[f(a) \,|\, a \in \{1, \ldots, n\}]$ come abbreviazione di $[f(1), \ldots, f(n)]$.
- nA, dove $A \subseteq \mathbb{Z}$ e $n \in \mathbb{Z}$, per indicare l'insieme $\{nx \mid x \in A\}$.

1.2 Stile delle dimostrazioni

Per quanto riguarda le dimostrazioni, adotteremo uno stile molto preciso e formale. Nulla verrà lasciato all'intuizione del lettore, ogni passaggio verrà spiegato in modo che sia possibile verificarne la correttezza semplicemente applicando l'aritmetica, la

logica elementare (ad esempio, se $A \Rightarrow B$ allora $\neg B \Rightarrow \neg A$) o risultati precedentemente dimostrati. Si è scelto questo stile principalmente per poter verificare in modo semplice la correttezza di una dimostrazione.

Ogni passaggio di una dimostrazione sarà numerato univocamente. Un passaggio può essere:

- una formula che si suppone vera (come si fa ad esempio nelle dimostrazioni per assurdo)
- una formula ricavata da passaggi precedenti
- una notazione introdotta col simbolo $\equiv$

Nel primo caso, la formula è preceduta dalla parola "Se", ed i passaggi che dipendono da essa saranno indentati ad un livello superiore. Nel secondo caso, il passaggio viene spiegato tra parentesi quadre (a seconda dei casi, si possono indicare da quali passaggi precedenti deriva, quale teorema è stato applicato, se deriva banalmente dall'aritmetica di $\mathbb{N}$ o dalla logica elementare, ecc.). Nell'ultimo caso, non viene fornita alcuna spiegazione. In generale, le prime formule della dimostrazione sono quelle più vicine alla tesi (in particolare, la prima è identica alla tesi), mentre le ultime sono dettagli che vengono utilizzati a supporto di formule precedenti.

A titolo di esempio, dimostriamo nel nostro stile il famoso teorema di Euclide sui numeri primi. Denotiamo con p_n l'n-esimo numero primo, per ogni $n \in \mathbb{N}^\star$ (quindi $p_1 = 2$).

Teorema 1.1. *Esistono infiniti numeri primi.*

In altri termini, $\forall n > 0 \exists p > p_n : p$ *è primo.*

Dimostrazione.

1. $\forall n > 0 \exists p > p_n : p$ è primo [da 2., 2–(a) e 2–(b), per assurdo]
2. Sia $n > 0$ tale che $\forall p > p_n : p$ non è primo (cioè l'ultimo primo è p_n, e tutti e soli i primi sono $p_1, \ldots, p_n$)
   (a) $p_1 \ldots p_n + 1$ è primo [da 2. e i.]
      i. $\forall i \in \{1, \ldots, n\} : p_i \nmid p_1 \ldots p_n + 1$ [da ii., A. e (c), per assurdo]
      ii. Sia i tale che $p_i \mid p_1 \ldots p_n + 1$
         A. $p_i \mid 1$ [da ii. e B.]
         B. $p_i \mid p_1 \ldots p_n$
   (b) $p_1 \ldots p_n + 1 > p_n$ [da i. e (c)]

i. $p_1 \dots p_n =$
$p_1 \dots p_{n-1} p_n =$
$2^{n-1} p_n \geq$
p_n

(c) $p_i \geq 2$ per ogni i [lo prendiamo come assioma]

□

In generale, i riferimenti ad un passaggio possono essere assoluti o relativi:

- i riferimenti assoluti indicano tutto il percorso che porta al passaggio desiderato, a partire dal livello più alto, ad esempio "2.–(a)–i.–A.";
- i riferimenti relativi indicano il percorso che porta al passaggio desiderato, a partire dal passaggio corrente.

Ad esempio, al terzo rigo della dimostrazione, la spiegazione "[da 2. e i.]" contiene un riferimento assoluto ("2.") ed uno relativo ("i."). Con un percorso relativo è possibile passare ad un passaggio "padre", "figlio" o "fratello", utilizzando la terminologia degli alberi. Ciò è ambiguo in teoria, ma non in pratica, in cui ci si assicura che col buon senso sia sempre possibile individuare il passaggio a cui ci si riferisce in modo relativo.

Questo modo di procedere ha vantaggi e svantaggi. Tra i vantaggi:

- Le dimostrazioni sono comprensibili senza tanta riflessione
- È facile verificare la correttezza di una dimostrazione
- Le dimostrazioni sono scritte in modo semplice: nessun discorso contorto con molti "quindi", "perché", "infatti", ecc.
- Leggendo solo i passaggi fino ad un certo livello di indentazione (ad esempio il secondo), è possibile ottenere una versione abbreviata della dimostrazione. Infatti, i dettagli si trovano agli ultimi livelli di indentazione.

Il principale svantaggio è che le dimostrazioni sono lunghe e forse noiose. Ciò è del tutto voluto: si cercherà infatti di separare le parti noiose da quelle interessanti[2], in modo da confinare le prime nelle dimostrazioni, e le altre in definizioni, esempi, commenti, enunciati. Il lettore frettoloso può quindi saltare le dimostrazioni, con la certezza di non perdere niente di rilevante. Le dimostrazioni più significative sono comunque segnalate e commentate.

Le uniche occasioni in cui useremo lo stile di dimostrazione "classico", piuttosto che quello appena descritto, sono i risultati classificati come "osservazioni".

[2] I termini "noioso" e "interessante" sono legati a giudizi personali dell'autore.

1.3 Interi o naturali?

Nella teoria dei tratteggi si opera molto più spesso su numeri naturali, che su interi. Ciò comporta, ad esempio, che in molti contesti scritture come $2 - 3$ non hanno senso, è come scrivere $\frac{1}{0}$. In particolare, nella teoria dei tratteggi esistono funzioni che possono *restituire* interi negativi, ma mai funzioni che sono *definite* per interi negativi[3].

Si è scelto di escludere i numeri negativi[4] come argomenti di funzioni semplicemente perché, per come è attualmente concepita la teoria, non ce n'è bisogno. La teoria dei tratteggi serve principalmente a risolvere il più elementare problema matematico: quello di contare. Contare significa enumerare oggetti discreti: dire qual è il primo, qual è il secondo, qual è il terzo, e così via. Quando si conta è necessario fissare un numero iniziale (per noi sarà 0 o 1, a seconda dei casi) ed andare avanti a partire da questo. La teoria è piena di funzioni che enumerano qualcosa: è abbastanza naturale allora che queste funzioni siano definite solo per numeri positivi (che fungono da indici), sebbene gli oggetti contati possono essere dei tipi più disparati, $\mathbb{Z}$ compreso, purché ovviamente la loro totalità sia numerabile.

Qualcuno si potrebbe domandare se, pur non potendo essere argomenti di funzioni, gli interi negativi potrebbero essere utili nelle dimostrazioni, come "oggetti intermedi". Questo finora è stato praticato in maniera molto limitata, ma nulla vieta che in futuro possa diventare pratica più comune.

Qualcuno può non essere soddisfatto dalla semplice giustificazione "non ce n'è bisogno" per l'esclusione degli interi come argomento di funzioni che contano. Nulla vieta di contare avendo come indici gli interi anche negativi, o i razionali, o qualsiasi insieme numerabile: tutte queste potrebbero essere generalizzazioni della teoria. In realtà ho tentato di definire funzioni che contano definite su $\mathbb{Z}$. Ora riassumerò brevemente i risultati di questi tentativi; il resto del paragrafo comunque può essere saltato senza compromettere la comprensione del resto del libro.

L'inclusione dei negativi comporterebbe delle generalizzazioni di molte strutture che studieremo. Queste generalizzazioni, se effettuate nel modo più "naturale" possibile, introdurrebbero particolari simmetrie, dovute al fatto che gli interi negativi sono, in un certo senso, simmetrici dei positivi. Ovviamente una generalizzazione che può essere "naturale" per qualcuno può non esserlo per altri, ma, quando dico

[3] Attenzione all'espressione "funzioni della teoria dei tratteggi". Di funzioni definite su interi ne vedremo alcune, come la somma mista definita nel paragrafo successivo, ma si tratta di funzioni ausiliarie, non oggetto di studio della teoria.

[4] Dato che non si parlerà mai di numeri non interi, le espressioni "numero" e "numero intero" sono da intendersi, in questo libro, equivalenti.

che una generalizzazione è "naturale", intendo dire che sembra trovare un suo senso, una sua collocazione nel complesso della teoria e dei suoi scopi.

Fin qui, nulla di male; tuttavia, se si generalizzassero le strutture della teoria dei tratteggi, si dovrebbero generalizzare anche delle funzioni aritmetiche che ricorrono molto spesso nella teoria: mi riferisco alle funzioni che abbiamo visto poco fa: il modulo e le due varianti della parte intera. Anche queste funzioni hanno delle loro "naturali" generalizzazioni, ma qui l'aggettivo "naturale" è inteso rispetto all'aritmetica, non alla teoria dei tratteggi. Il problema è che risulterebbe davvero poco intuitivo accostare le "naturali" generalizzazioni delle strutture della teoria dei tratteggi con le "naturali" generalizzazioni delle funzioni aritmetiche: infatti queste ultime non godono delle simmetrie che la teoria dei tratteggi generalizzata vorrebbe. Ad esempio, $7 \bmod 3 = 1$ ma $-7 \bmod 3 = 2$. Ciò appare naturale a qualsiasi matematico, tuttavia un buon "teorico dei tratteggi" direbbe che $-7 \bmod 3$ dovrebbe essere, per ragioni di simmetria, -1. A questo punto, volendo privilegiare ciò che è naturale per la teoria dei tratteggi rispetto a ciò che è naturale per l'aritmetica, si dovrebbero modificare le usuali definizioni di modulo e parte intera. Questa volta $a \in \mathbb{Z}$ e $b \in \mathbb{Z}^\star$ e le definizioni sono le seguenti:

$$a \bmod b \equiv \begin{cases} \text{resto della divisione di } a \text{ per } b & \text{se } a > 0 \\ (-a) \bmod b & \text{altrimenti} \end{cases}$$

$$\left\lfloor \frac{a}{b} \right\rfloor \equiv \begin{cases} \text{quoziente della divisione di } a \text{ per } b & \text{se } a > 0 \\ -\left\lfloor \frac{-a}{b} \right\rfloor & \text{altrimenti} \end{cases}$$

$$\left\lceil \frac{a}{b} \right\rceil \equiv \begin{cases} \left\lfloor \frac{a}{b} \right\rfloor & \text{se } a \bmod b = 0 \\ \left\lfloor \frac{a}{b} \right\rfloor + \operatorname{sgn}(a) & \text{altrimenti} \end{cases}$$

Queste definizioni creano una certa simmetria tra interi positivi e negativi, come si può vedere in figura 1.1, e ciò avrebbe senso nella teoria dei tratteggi. Tuttavia esse, come già detto, non danno un grosso contributo ad una teoria il cui scopo primario, in fin dei conti, è quello di contare. Quindi, da ora in poi, useremo le definizioni date nel paragrafo precedente. Come conseguenza, le funzioni che definiremo e studieremo non saranno mai definite per numeri negativi.

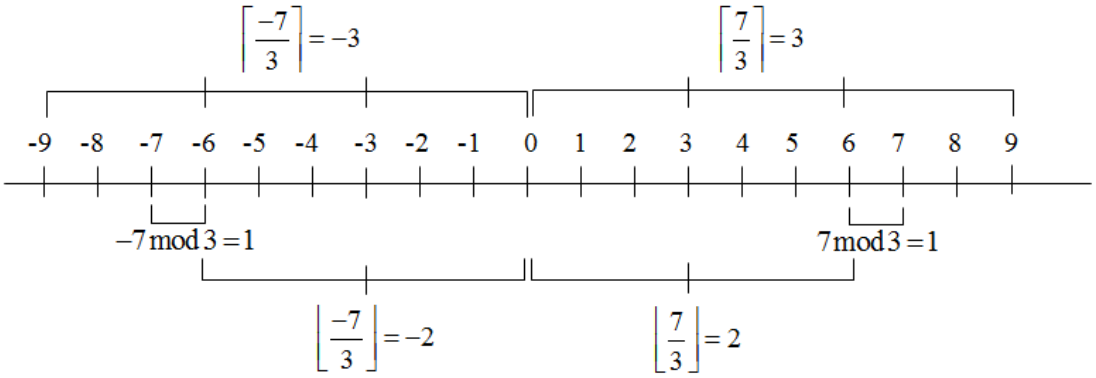

Figura 1.1: Simmetria delle definizioni alternative di modulo e parte intera

1.4 Definizioni principali

1.4.1 Da un problema concreto ai tratteggi

I tratteggi sono, in prima analisi, una formalizzazione matematica di problemi come il seguente:

Problema 1.1. *Aldo, Giovanni e Giacomo vanno regolarmente a correre. Aldo corre ogni tre giorni, di mattina; Giovanni corre ogni quattro giorni, di pomeriggio; Giacomo ogni cinque giorni, di sera. Oggi corrono tutti e tre. A partire da domani, chi sarà il decimo a correre e tra quanti giorni lo farà?*

Per risolvere questo problema, occorre tener traccia, in ordine temporale, di chi corre, in modo da scoprire chi sarà il decimo e tra quanti giorni. Posto che oggi corrono tutti e tre e i giorni si cominciano a contare a partire da domani, si ha che:

- Aldo correrà tra tre giorni, di mattina. Sarà quindi il primo a correre.
- Il quarto giorno correrà Giovanni, di pomeriggio: sarà il secondo.
- Il quinto giorno correrà Giacomo, di sera: sarà il terzo.
- La mattina del sesto giorno correrà di nuovo Aldo: sarà il quarto.
- Il pomeriggio dell'ottavo giorno correrà di nuovo Giovanni: sarà il quinto.
- La mattina del nono giorno correrà Aldo per la terza volta: sarà, complessivamente, la sesta persona a correre.
- La sera del decimo giorno correrà Giacomo: sarà il settimo a correre.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Aldo	-			-			-			-			-			-
Giovanni	-				-				-				-			
Giacomo	-					-					-					-

Tabella 1.1: Rappresentazione grafica per il problema 1.1

- Il dodicesimo giorno correranno sia Aldo, di mattina, che Giovanni, di sera: quindi Aldo sarà l'ottavo e Giovanni il nono.
- Il quindicesimo giorno, di mattina, correrà di nuovo Aldo: sarà il decimo a correre (anche Giacomo correrà lo stesso giorno, ma di sera: sarà quindi l'undicesimo).

La soluzione del problema è quindi: "Aldo, tra quindici giorni".

Un approccio grafico al problema potrebbe essere quello di disegnare una tabella come la 1.1. Le colonne rappresentano i giorni che passano a partire da quando corrono tutti e tre insieme (situazione che non è rappresentata; volendo, sarebbe il giorno 0); all'incrocio di riga e colonna si inserisce un trattino per segnare il fatto che una persona va a correre.
Non è un caso che la prima riga sia quella di Aldo, la seconda quella di Giovanni e la terza quella di Giacomo. Infatti, poiché i tre corrono, rispettivamente, di mattina, a pomeriggio e di sera, ordinando così le righe si può seguire l'ordine temporale partendo dalla prima cella della prima riga (la mattina del primo giorno) e spostandosi verso il basso e verso destra. Quindi, dalla prima cella della prima riga ci si sposta alla prima della seconda riga (il pomeriggio del primo giorno), quindi alla prima della terza riga (la sera del primo giorno), poi alla seconda della prima riga (la mattina del secondo giorno), e così via. Avendo disegnato la tabella, per rispondere al quesito posto, basta contare i trattini che si incontrano procedendo nell'ordine descritto, fermandosi al decimo. Invito i lettori a provare: troveranno che il decimo trattino sta nella quindicesima cella (quindicesimo giorno) della prima riga (quella di Aldo), da cui la soluzione cercata.

Ora formalizziamo matematicamente tutto ciò. Cominciamo col rappresentare le tre persone con dei numeri interi positivi: 1 per Aldo, 2 per Giovanni e 3 per Giacomo. Si noti che i numeri sono assegnati in modo che, se due persone corrono lo stesso giorno, chi corre prima ha il numero più basso. Ad esempio, il dodicesimo giorno corrono Aldo e Giovanni, ma Aldo (numero 1) corre la mattina, prima di Giovanni (numero 2) che corre il pomeriggio.
Una corsa è identificata univocamente da due numeri: il numero della persona che corre (es. 3 per Giacomo) ed un numero progressivo che conta tutte le volte che

va a correre quella persona. Ad esempio, la quarta corsa di Giacomo è identificata dalla coppia $\langle 3, 4\rangle$: il 3 per indicare Giacomo ed il 4 per indicare la sua quarta corsa. Ogni persona corre, nel nostro modello, infinite volte.
La corsa è formalizzata col concetto di *trattino*:

Definizione 1.2. *Si definisce* trattino *una coppia ordinata* $t \equiv \langle i, k\rangle \in \mathbb{N}^\star \times \mathbb{N}$. i *è detto* indice *del trattino, e si definisce la funzione* $\text{ind} : \mathbb{N}^\star \times \mathbb{N} \to \mathbb{N}^\star$ *come* $\text{ind}(\langle i, k\rangle) = i$.

Sia $C \subseteq \mathbb{N}^\star$. *Si pone* $\text{Tratt}_C \equiv C \times \mathbb{N}$ *(l'insieme di tutti i possibili trattini con indice in* C*).*

Ogni corsa avviene in un certo giorno, secondo una legge fissata (nel nostro caso, Aldo corre ogni tre giorni, Giovanni ogni quattro e Giacomo ogni cinque). La legge che associa una corsa al giorno in cui questa ha luogo è detta *tratteggio*. Il nostro modello impone che una persona non può correre più di una volta lo stesso giorno e che esiste un giorno iniziale, detto *origine*, in cui tutte le persone considerate vanno a correre. In termini più formali:

Definizione 1.3. *Sia* $C \subseteq \mathbb{N}^\star$, $C \neq \emptyset$. *Si definisce* tratteggio *una funzione* $T \in [\text{Tratt}_C \to \mathbb{Z}]$ *tale che:*

- $\forall \langle n, 0\rangle, \langle m, 0\rangle \in \text{Tratt}_C : T(\langle n, 0\rangle) = T(\langle m, 0\rangle) \equiv \mathcal{O}_T \equiv$ *origine di* T
- $\forall \langle n, k\rangle, \langle n, h\rangle \in \text{Tratt}_C : k < h \Rightarrow T(\langle n, k\rangle) \leq T(\langle n, h\rangle)$

Se T *è tale che, nella seconda proprietà, si può scrivere* $<$ *anziché* $\leq$*, allora* T *si dice* strettamente monotono.

C *si dice* insieme delle componenti *del tratteggio.*

$|C|$ *è detto ordine del tratteggio, e si indica con* $\text{ord}(T)$. *Se* $\text{ord}(T) = n$*, si dice che* T *è* di n-esimo ordine. *Se* $\text{ord}(T) \in \mathbb{N}$*,* T *si dice* finito*; altrimenti (cioè se* $\text{ord}(T) = \infty$*) si dice* infinito.

Chiamiamo T_1 il tratteggio che rappresenta la situazione descritta nel problema 1.1, e rappresentata nella tabella 1.1. Esso è di terzo ordine (perché si sono considerate tre persone), dunque è una funzione da $\text{Tratt}_{\{1,2,3\}}$ in $\mathbb{Z}$. La funzione deve essere tale che $T_1(\langle i, k\rangle)$ deve indicare tra quanti giorni correrà la persona i (1 per Aldo, 2 per Giovanni e 3 per Giacomo), quando correrà la k-esima volta ($k = 0$ il giorno iniziale). Stando ai dati disponibili, tale funzione è:

$$T_1(\langle i, k\rangle) = \begin{cases} 3k & \text{se } i = 1 \\ 4k & \text{se } i = 2 \\ 5k & \text{se } i = 3 \end{cases} \tag{1.1}$$

È facile verificare, riguardando la definizione precedente, che T_1 è un tratteggio, in particolare un tratteggio strettamente monotono, e che $\mathcal{O}_{T_1} = 0$.

Per convenzione, denoteremo i tratteggi con le lettere maiuscole da T in poi; i trattini, con le rispettive minuscole.

Si noti che un tratteggio è una funzione che ha insieme di arrivo in $\mathbb{Z}$. Ai fini del nostro esempio, sarebbe bastato considerare $\mathbb{N}$, perché si comincia dal giorno 0, ma la definizione più generale consente di modellare anche altri tipi di problemi, in cui si fa riferimento a ciò che accade nel passato (-1 rappresenta ieri, -2 l'altro ieri, eccetera).

Definizione 1.4. *Sia T un tratteggio e t un trattino. Se $t \in \operatorname{Dom} T$, si dice che t* appartiene *al tratteggio T e si scrive $t \in T$. Se A è un insieme di trattini, si pone $A \subseteq T \equiv A \subseteq \operatorname{Dom} T$.*

Si distinguono vari tipi di tratteggi. Ad esempio, un tratteggio T può essere:

- lineare, se $T(\langle i, k\rangle) = n_i \cdot k$, con $n_i \in \mathbb{N}^\star$ fissati
- ineare con spiazzamento, se $T(\langle i, k\rangle) = n_i \cdot k + s_i$, con $n_i \in \mathbb{N}^\star$ed $s_i \in \mathbb{Z}$ assegnati
- ...

Definizione 1.5. *Siano T un tratteggio e $t \in T$ un suo trattino. Il numero $T(t)$ si dice* valore *di t in T. $T(t)$ si può scrivere anche come $|t|_T$, o come $|t|$, se il tratteggio a cui ci si riferisce è chiaro dal contesto.*

Definizione 1.6. *Si definiscono i seguenti simboli:*

- $\mathcal{T}^k$, *con $k \in \overline{\mathbb{N}}^\star$, denota l'insieme di tutti i tratteggi di ordine k*
- $\mathcal{T}^{\mathbb{N}^\star} \equiv \bigcup_{k \in \mathbb{N}^\star} \mathcal{T}^k$ *denota l'insieme di tutti i tratteggi finiti*
- $\mathcal{T}^{\overline{\mathbb{N}}^\star} \equiv \bigcup_{k \in \overline{\mathbb{N}}^\star} \mathcal{T}^k$ *denota l'insieme di tutti i tratteggi (finiti e infiniti)*

1.4.2 Rappresentazione grafica

Come abbiamo visto, un tratteggio si può rappresentare con una tabella, avente tante righe quant'è l'ordine del tratteggio ed infinite colonne, numerate a partire da $\mathcal{O}_T$. In una cella di riga r e colonna c si disegna un trattino se e solo se $\exists t = \langle r, k\rangle \in T \ni T(t) = c$. Ad esempio, il tratteggio T_1 (equazione 1.1) si può rappresentare con la tabella 1.1. In teoria, per rappresentare l'intero tratteggio, la tabella dovrebbe

0	1	2	3	4	5	6	7
$\langle 1,0\rangle$			$\langle 1,1\rangle$			$\langle 1,2\rangle$	
$\langle 2,0\rangle$				$\langle 2,1\rangle$			
$\langle 3,0\rangle$					$\langle 3,1\rangle$		

8	9	10	11	12	13	14	15
	$\langle 1,3\rangle$			$\langle 1,4\rangle$			$\langle 1,5\rangle$
$\langle 2,2\rangle$				$\langle 2,3\rangle$			
		$\langle 3,2\rangle$					$\langle 3,3\rangle$

Tabella 1.2: Rappresentazione grafica dei trattini del tratteggio T_1 (equazione 1.1)

avere infinite colonne, ma chiaramente nella pratica ci si ferma ad un certo numero di colonna, utile per gli scopi del momento (15 in questo caso), restando sottinteso che le colonne dovrebbero continuare all'infinito.

In generale, due trattini sulla stessa riga hanno lo stesso indice: se una riga è più in basso di un'altra, vuol dire che i suoi trattini hanno un indice maggiore di quelli della riga posta più in alto. I trattini $\langle i,k\rangle$ sulla prima colonna hanno tutti $k=0$. Partendo dal trattino $\langle i,k\rangle$ e continuando a leggere la riga i verso destra, il primo trattino che si incontra è $\langle i,k+1\rangle$. Nel caso del tratteggio T_1, ciò si può visualizzare con una tabella come la 1.2. Tale rappresentazione è più completa, ma generalmente preferiamo la prima, più concisa.

1.4.3 Ordinamento temporale

Definizione 1.7. *Sia T un tratteggio. Sui suoi trattini si definisce la relazione $\leq$, detto* ordinamento temporale*, tale che* $\forall t \equiv \langle i,n\rangle \in T\, \forall t' \equiv \langle j,m\rangle \in T : t \leq t' \overset{def}{\iff} |t| < |t'| \vee (|t| = |t'| \wedge (i < j \vee (i = j \wedge n \leq m)))$.

Ad esempio, nel tratteggio T_1 si ha: $\langle 1,0\rangle \leq \langle 2,0\rangle \leq \langle 3,0\rangle \leq \langle 1,1\rangle \leq \langle 2,1\rangle \leq \langle 3,1\rangle \leq \langle 1,2\rangle \leq \langle 2,2\rangle \leq \langle 1,3\rangle \leq \langle 3,2\rangle \leq \langle 1,4\rangle \leq \langle 2,3\rangle \leq \ldots$.

Come già detto, l'ordinamento temporale si ottiene leggendo la tabella che rappresenta un tratteggio dall'alto verso il basso, da sinistra verso destra e, all'interno di una cella, per valori crescenti della seconda componente del trattino.

Si dimostra facilmente che la relazione $\leq$ è una relazione d'ordine, anche per i tratteggi non strettamente monotoni. Ad esempio, supponiamo che Aldo corra due volte la mattina del sesto giorno (tabella 1.3): il tratteggio U che modella questa situazione non è strettamente monotono, perché si ha $U(\langle 1,2\rangle) = U(\langle 1,3\rangle) = 6$ (la seconda e la terza corsa di Aldo hanno luogo entrambe nel sesto giorno). Secondo la definizione di ordinamento temporale, si ha $\langle 1,2\rangle \leq \langle 1,3\rangle$ e non $\langle 1,3\rangle \leq \langle 1,2\rangle$.

0	1	2	3	4	5	6	7
$\langle 1,0\rangle$			$\langle 1,1\rangle$			$\langle 1,2\rangle, \langle 1,3\rangle$	
$\langle 2,0\rangle$				$\langle 2,1\rangle$			
$\langle 3,0\rangle$					$\langle 3,1\rangle$		

8	9	10	11	12	13	14	15
	$\langle 1,4\rangle$			$\langle 1,5\rangle$			$\langle 1,6\rangle$
$\langle 2,2\rangle$				$\langle 2,3\rangle$			
		$\langle 3,2\rangle$					$\langle 3,3\rangle$

Tabella 1.3: Un tratteggio non strettamente monotono: Aldo corre due volte lo stesso giorno

Di conseguenza, si possono ordinare i trattini di U solo nel seguente modo: $\langle 1,0\rangle \leq \langle 2,0\rangle \leq \langle 3,0\rangle \leq \langle 1,1\rangle \leq \langle 2,1\rangle \leq \langle 3,1\rangle \leq \langle 1,2\rangle \leq \langle 1,3\rangle \leq \langle 2,2\rangle \leq \ldots$

Notiamo che il criterio per stabilire quale di due trattini è minore di un altro si semplifica molto, rispetto alla definizione 1.7, per i tratteggi di primo ordine, come si può facilmente verificare:

Proprietà 1.1. *Sia T un tratteggio di primo ordine con insieme delle componenti $\{i\}$, e siano $t \equiv \langle i,h\rangle \in T$ e $u \equiv \langle i,k\rangle \in T$. Allora $t \leq u \Leftrightarrow h \leq k$.*

È utile introdurre sin da ora dei termini che indicano l'insieme di tutti i trattini il cui valore è compreso in un certo insieme di valori (nel problema 1.1, l'insieme di tutte le "corse" (trattini) che avvengono in un insieme di giorni consecutivi fissato):

Definizione 1.8. *Siano $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, $x,y \in \mathbb{Z}$, $x \leq y$. L'insieme $\bigcup_{x\leq z\leq y} T^{-1}(z) = \{t \in T \mid x \leq |t| \leq y\}$ prende il nome di* finestra di T da x a y.

Ad esempio, La finestra di T_1 da 4 a 7 coincide con l'insieme $\{\langle 2,1\rangle, \langle 3,1\rangle, \langle 1,2\rangle\}$.

A partire dall'ordinamento temporale $\leq$ si possono definire in modo ovvio le relazioni $=, <, >$ e $\geq$:

Definizione 1.9. *Sia T un tratteggio. Sui suoi trattini si definiscono le relazioni $=, <, >$ e $\geq$ tali che per ogni $t \in T$, $t' \in T$ si ha:*

- $t = t' \overset{def}{\iff} t \leq t' \wedge t' \leq t$
- $t < t' \overset{def}{\iff} t \leq t' \wedge t' \not\leq t$
- $t > t' \overset{def}{\iff} t' < t$
- $t \geq t' \overset{def}{\iff} t' \leq t$

In particolare, riguardo alle prime due relazioni, si verifica facilmente che:

Proprietà 1.2. *Sia T un tratteggio. Per ogni $t \equiv \langle i, n\rangle \in T$, $t' \equiv \langle j, m\rangle \in T$ si ha:*

- $t < t' \Leftrightarrow |t| < |t'| \vee (|t| = |t'| \wedge (i < j \vee (i = j \wedge n < m)))$
- $t = t' \Leftrightarrow i = j \ \wedge \ n = m$

1.4.4 Sottotratteggi e sovratratteggi

Nel problema 1.1 si tratta di tre persone che vanno a correre: Aldo, Giovanni e Giacomo. Ci si può però restringere a considerare solo due delle tre persone, ad esempio Aldo e Giovanni, mantenendo le ipotesi che oggi corrono tutti e due (banalmente deducibile dal fatto che oggi corrono loro due, più Giovanni, come asserito nel problema 1.1) e che Aldo corre ogni tre giorni e Giovanni ogni cinque.
Questa nuova situazione viene modellata con la tabella 1.4.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Aldo			-			-			-			-			-
Giacomo					-					-					-

Tabella 1.4: Rappresentazione grafica per il problema 1.1, considerando solo Aldo e Giacomo

Essa corrisponde al tratteggio $T_2 : \mathrm{Tratt}_{\{1,3\}} \to \mathbb{Z}$ tale che:

$$T_2\left(\langle i, k\rangle\right) = \begin{cases} 3k & \text{se } i = 1 \\ 5k & \text{se } i = 3 \end{cases}$$

Si noti che non sono cambiati i numeri assegnati alle persone: Aldo ha sempre il numero 1 e Giacomo il numero 3.

T_2 si dice sottotratteggio di T_1. Si può notare che $T_2 = T_{1|\mathrm{Tratt}_{\{1,3\}}}$: un sottotratteggio è quindi una restrizione di un altro tratteggio.

Definizione 1.10. *Siano T e T' due tratteggi e siano C e C', rispettivamente, gli insiemi degli indici di T e di T'. Sia $C' \subseteq C$ e $T' = T_{|\mathrm{Tratt}_C}$. Allora T' viene detto* sottotratteggio *di T, e si scrive $T' \leq T$. Equivalentemente, T viene detto* sovratratteggio *di T' , e si scrive $T \geq T'$.*
Si pone inoltre $T' \equiv T\left[c_1, \ldots, c_n\right]$, dove $c_1 < \ldots < c_n$ e $C' = \{c_1, \ldots, c_n\}$.

Come abbiamo visto, un sottotratteggio T' di un tratteggio T viene rappresentato da una tabella ottenuta da quella di T eliminando zero o più righe (ma non tutte).

1.4.5 Classi e spazi

Si sarà notato, nell'analisi del problema 1.1, che alcuni giorni corrono più persone (anche se in diversi momenti della giornata), in altri giorni corre una sola persona, e in altri giorni non corre nessuno. Ad esempio, il dodicesimo giorno corrono sia Aldo che Giovanni, il terzo giorno corre solo Aldo ed il settimo giorno non corre nessuno (v. tabella 1.1). Si può semplificare questa questione, dicendo che ci sono alcuni giorni in cui corre *qualcuno* (*almeno* una persona) ed alcuni giorni in cui non corre *nessuno*. Nella terminologia della teoria dei tratteggi, i primi vengono detti *classi* ed i secondi *spazi*.

Definizione 1.11. *Si definisce* classe per valore *(o semplicemente* classe*) di un tratteggio T con insieme di indici C, una classe di equivalenza su* Tratt_C *indotta dalla relazione "avere lo stesso valore"*[5]*. Si definisce* valore *di una classe c il valore di uno dei suoi elementi, e lo si indica con $|c|_T$ o $|c|$, a seconda del contesto.*

Una classe con più di un rappresentante viene detta sovrapposizione*.*

Ad esempio, le tre classi di valore più basso in T_1 sono:

- la classe di valore 0, che è una sovrapposizione perché ha tre rappresentanti: $\langle 1, 0\rangle$, $\langle 2, 0\rangle$ e $\langle 3, 0\rangle$ (corrono Aldo, Giovanni e Giacomo, si tratta del giorno iniziale);
- la classe di valore 3, che non è una sovrapposizione, perché ha come unico rappresentante $\langle 1, 1\rangle$ (corre solo Aldo);
- la classe di valore 4, con unico rappresentante $\langle 2, 1\rangle$ (corre solo Giovanni).

Sulle classi di un tratteggio T si definisce un ordinamento, detto *ordinamento temporale* come quello dei trattini, tale che se c e d sono due classi, $c \leq d \equiv |c|_T \leq |d|_T$. Ciò permette di definire il tratteggio delle classi di T:

Definizione 1.12. *Sia T un tratteggio. Si definisce* tratteggio delle classi *di T, e si indica con $c(T)$, il tratteggio di primo ordine $c(T) : \mathrm{Tratt}_{\{1\}} \to \mathbb{Z}$ tale che, per ogni $k \in \mathbb{N}$, $c(T)(\langle 1, k\rangle)$ è il valore della k-esima classe di T nell'ordinamento temporale delle classi, considerando, come 0-esima classe, la classe di valore $\mathcal{O}_T$.*

Ad esempio, il tratteggio delle classi del tratteggio T_1, $c(T_1)$, è rappresentato dalla tabella 1.5.

[5] Formalmente, la relazione $R \subseteq \mathrm{Tratt}_C \times \mathrm{Tratt}_C$ tale che per ogni $s, t \in \mathrm{Tratt}_C$, $s\,R\,t \Leftrightarrow |s|_T = |t|_T$.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
-			-	-	-	-		-	-	-		-			-

Tabella 1.5: Tratteggio delle classi del tratteggio T_1 (equazione 1.1): $c(T_1)$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
-	-					-				-		-	-	

Tabella 1.6: Tratteggio degli spazi del tratteggio T_1 (equazione 1.1): $s(T_1)$

Si può dire che la rappresentazione del tratteggio delle classi di un tratteggio si può ottenere da quella del tratteggio "sovrapponendo" tutte le righe per formarne una sola.

Un altro concetto importante, complementare a quello di classe, è il concetto di spazio:

Definizione 1.13. *Si definisce* spazio *di un tratteggio T un intero n tale che non esistono trattini di T di valore n.*

Nella rappresentazione di un tratteggio, gli spazi sono i numeri delle colonne senza trattini. La parola "spazio" ricorda proprio questo, essendo usata nell'accezione fisica e soprattutto grafica, piuttosto che nell'accezione matematica (es. "spazio vettoriale").

Sugli spazi è già definito un ordinamento, perché si tratta di numeri interi. Si può definire, analogamente a prima, il tratteggio degli spazi:

Definizione 1.14. *Sia T un tratteggio. Si definisce* tratteggio degli spazi *di T, e si indica con $s(T)$, il tratteggio di primo ordine $s(T) : \mathrm{Tratt}_{\{1\}} \to \mathbb{Z}$ tale che, per ogni $k \in \mathbb{N}$, $s(T)(\langle 1, k\rangle)$ è il valore del k-esimo spazio di T (per $k = 0$, il più piccolo spazio di T; per $k = 1$, lo spazio successivo, ecc.).*

Ad esempio, il tratteggio $s(T_1)$ è rappresentato dalla tabella 1.6, dove si può notare la "complementarietà" col tratteggio $c(T_1)$ visualizzato in tabella 1.5.

Osserviamo che $\mathcal{O}_f$ non è uno spazio, per qualsiasi tratteggio T . In particolare, $\mathcal{O}_T$ è una classe di cardinalità pari all'ordine di T (in quanto, per ogni possibile indice i, $T(\langle i, 0\rangle) = \mathcal{O}_T$); quindi $\mathcal{O}_T$ è una classe infinita, se T è infinito.

1.4.6 Periodo e domini fondamentali

Due conceti ricorrenti in teoria dei tratteggi sono quelli di periodo e di dominio fondamentale. I due termini sono presi in prestito dalla teoria delle tassellazioni, in cui essi sono utilizzati per descrivere formalmente la ripetitività di molte decorazioni

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Aldo	-			-				-			-				-
Giovanni	-				-			-				-			-

Tabella 1.7: Aldo corre il lunedì e il giovedì mattina; Giovanni il lunedì e il venerdì pomeriggio.

o disegni di tipo geometrico (molti dei quali si possono ritrovare su piastrelle o mosaici).

Supponiamo che Aldo corra il lunedì e il giovedì, sempre di mattina, e Giovanni corra il lunedì e il venerdì, sempre di pomeriggio, e che il giorno da cui si comincia a contare sia un lunedì (tabella 1.7). Ciò corrisponde al tratteggio $T : \text{Tratt}_{\{1,2\}} \to \mathbb{Z}$ tale che per ogni $\langle i, k\rangle \in \text{Tratt}_{\{1,2\}}$:

$$T\left(\langle i,k\rangle\right) = \begin{cases} 1 + 7\frac{k}{2} & \text{se } k \text{ è pari (incluso 0)} \\ 4 + 7\frac{k-1}{2} & \text{se } k \text{ è dispari e } i = 1 \\ 5 + 7\frac{k-1}{2} & \text{se } k \text{ è dispari e } i = 2 \end{cases} \tag{1.2}$$

Questo tratteggio è "periodico", nel senso che si può individuare uno schema che si ripete: nell'arco della settimana, infatti, si ha sempre che il lunedì corrono tutti e due, il mercoledì mattina corre Aldo ed il giovedì mattina corre Giovanni, e questo accade tutte le settimane. Inoltre, non si può trovare un periodo di tempo più corto di una settimana nel quale si verifichi qualche schema ripetitivo in modo costante nel tempo (ad esempio, se suddividessimo il tempo a blocchi di sei giorni, avremmo blocchi di sei giorni in cui gli eventi accadono in tempi relativi diversi, rispetto ad altri blocchi di sei giorni). Si esprime tutto ciò dicendo che una settimana è un *dominio fondamentale* del tratteggio preso in esame. Ciò significa che possiamo considerare qualsiasi blocco di sette giorni, essendo sicuri che in tutti i successivi blocchi di sette giorni si verificheranno gli stessi eventi nello stesso ordine e negli stessi tempi relativi. Se ad esempio consideriamo un blocco che va da un lunedì a una domenica, siamo sicuri che, sia nel blocco considerato che in tutti i successivi blocchi che vanno da lunedì a domenica, accadrà che il primo giorno (lunedì) correranno sia Aldo che Giovanni, dopo tre giorni (giovedì) correrà Aldo, e dopo un ulteriore giorno (venerdì) correrà Giovanni. Possiamo anche partire da altri giorni e trovare situazioni analoghe: ad esempio in tutti i blocchi che vanno dal mercoledì al martedì successivo si ha che il secondo giorno (cioè giovedì, perché siamo partiti da mercoledì) correrà Aldo; il terzo giorno (venerdì) correrà Giovanni, il sesto giorno (lunedì) correranno entrambi.

Volendo, si può formulare il concetto di periodicità, per il tratteggio T, nel seguente

modo: preso un qualsiasi blocco di sette giorni (ad es. i giorni 1-7), se lo "tagliassimo" e lo "incollassimo" sopra il successivo blocco di sette giorni (ad es. i giorni 8-14), i due blocchi combacerebbero perfettamente.

Si può anche osservare che in tutti i domini fondamentali (blocchi di sette giorni) si ha lo stesso numero di corse, quattro, perché corre due volte Aldo e due volte Giovanni. Quindi un altro modo per dire che il tratteggio è ripetitivo è dire che ogni quattro corse complessive (cioè sia di Aldo che di Giovanni) passa una settimana. Ad esempio, l'arco di tempo che intercorre tra la prima e la quinta corsa, o tra la seconda e la sesta, o tra la quinta e la nona, è sempre di una settimana (invitiamo il lettore a verificare ciò nella tabella 1.7). In questo caso, si dice che quattro è il periodo del tratteggio, perché ogni quattro corse passa sempre uno stesso numero di giorni, ed in più quattro è il più piccolo numero con questa proprietà (ad esempio, esaminando cosa accade ogni tre corse, si nota che l'intervallo di tempo tra la prima e la terza corsa è diverso da quello tra la seconda e la quarta).

In termini formali:

Definizione 1.15. *Sia T un tratteggio finito. Se esiste un $n \in \mathbb{N}^\star$ tale che:*

$$\exists m \in \mathbb{N}^\star \, \forall t \in T : \, T(t) = T(t_n) - m \, \wedge \, \mathrm{ind}(t) = \mathrm{ind}(t_n) \tag{1.3}$$

dove t_n è l'n-esimo trattino successivo a t nell'ordinamento temporale, allora T si dice periodico*, il più piccolo n che soddisfa la (1.3) si definisce* periodo *di T e qualsiasi intervallo del tipo $[a, a+m-1]$, $a \in \mathbb{Z}$, $a \geq \mathcal{O}_T$ si chiama* dominio fondamentale *di T; altrimenti, T si dice* aperiodico*.*

Ad esempio, il tratteggio (1.5) è periodico, essendo il suo periodo $n = 4$ e la lunghezza (numero di giorni) di un suo dominio fondamentale $m = 7$. Infatti, ponendo nella (1.3) per esempio $t = \langle 1, 1 \rangle$, si può verificare che $4 = T(\langle 1, 1 \rangle) = T(t) = T(t_4) - m = T(\langle 1, 3 \rangle) - 7 = 11 - 7$, dove $t_4 \equiv \langle 1, 4 \rangle$ è il quarto (cioè l'n-esimo) trattino successivo a $\langle 1, 1 \rangle$ nell'ordinamento temporale ed è tale che $\mathrm{ind}(t) = 1 = \mathrm{ind}(t_4)$.

Seguiremo una semplice convenzione per rappresentare i tratteggi periodici: se m è la lunghezza di un dominio fondamentale, disegneremo solamente le colonne da $\mathcal{O}_T$ a $\mathcal{O}_T + m$, in modo da rappresentare un dominio fondamentale per intero (da $\mathcal{O}_T$ a $\mathcal{O}_T + m - 1$) ed una colonna in più che, come conseguenza della definizione 1.15, è uguale alla prima, per ricordare che il tratteggio è periodico. Eventualmente, aggiungeremo anche un'ulteriore colonna costituita esclusivamente da puntini. Ad esempio, una rappresentazione "convenzionale" del tratteggio in tabella 1.7 è quella della tabella 1.8.

	1	2	3	4	5	6	7	8	...
Aldo	-			-				-	...
Giovanni	-				-			-	...

Tabella 1.8: Rappresentazione "convenzionale" del tratteggio in tabella 1.7.

Un'immediata conseguenza della definizione 1.15 è:

Osservazione 1.1. *Se T è un tratteggio finito di periodo n, ogni dominio fondamentale di T contiene esattamente n trattini.*

Chiudiamo con un paio di osservazioni.

Primo, la definizione di tratteggio periodico è stata data solo per tratteggi finiti. Infatti, non è così ovvio dare una definizione analoga per i tratteggi infiniti. Inoltre, se provassimo ad applicare la definizione 1.15 ai tratteggi infiniti, scopriremmo che un tratteggio infinito strettamente monotono non è periodico, e ciò è dovuto al fatto che, come abbiamo già osservato, se T è infinito allora $\mathcal{O}_T$ è una classe infinita. Infatti, se scegliessimo $t \in T$ tale che $T(t) = \mathcal{O}_T$, anche $T(t_n) = \mathcal{O}_T$ (altrimenti $\mathcal{O}_T$ non sarebbe infinita), quindi solo per $m = 0$ si avrebbe che $T(t) = T(t_n) - m$ (e, anche per $m = 0$, $\operatorname{ind}(t)$ sarebbe diverso da $\operatorname{ind}(t_n)$), diversamente da quanto richiesto dalla definizione. Inviatiamo il lettore a completare con i dovuti dettagli questa "dimostrazione", a scopo di esercizio. Si tenga presente, comunque, che il concetto di periodicità esiste solo per i tratteggi finiti.

La seconda osservazione riguarda la condizione $\operatorname{ind}(t) = \operatorname{ind}(t_n)$ presente nell'equazione 1.15. Essa è fondamentale perché, se non ci fosse, la definizione di periodicità non corrisponderebbe al concetto intuitivo che abbiamo dato inizialmente, dello "stesso schema che si ripete". Per chiarire questo concetto, diamo la definizione di tratteggio debolmente periodico:

Definizione 1.16. *Sia T un tratteggio finito. Se esiste un $n \in \mathbb{N}^\star$ tale che:*

$$\exists m \in \mathbb{N}^\star \, \forall t \in T : \, T(t) = T(t_n) - m \tag{1.4}$$

dove t_n è l'n-esimo trattino successivo a t nell'ordinamento temporale, allora T si dice debolmente periodico*, il più piccolo n che soddisfa la (1.3) si definisce* periodo *di T e qualsiasi intervallo del tipo $[a, a + m - 1]$, $a \in \mathbb{Z}$, $a \geq \mathcal{O}_T$ si chiama* dominio fondamentale *di T.*

Per ottenere un tratteggio debolmente periodico, potremmo partire dal tratteggio T visualizzato in tabella 1.7 ed "abbassare" il terzo trattino, ottenendo la tabella 1.9. "Abbassare" il terzo trattino significa che la terza corsa, che doveva essere fatta da

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Aldo	-							-			-				-
Giovanni	-			-	-			-				-			-

Tabella 1.9: Un tratteggio debolmente periodico: Aldo corre il lunedì e il giovedì mattina; Giovanni il lunedì e il venerdì pomeriggio, tranne il quarto giorno, in cui Giovanni corre al posto di Aldo.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Aldo o Giovanni	-			-	-			-			-	-			-

Tabella 1.10: Tratteggio delle classi del tratteggio mostrato in figura 1.9

Aldo il quarto giorno, viene invece fatta da Giovanni, lo stesso giorno: Giovanni corre al posto di Aldo. Il tratteggio corrispondente è $U : \mathrm{Tratt}_{\{1,2\}} \to \mathbb{Z}$ tale che per ogni $\langle i, k\rangle \in \mathrm{Tratt}_{\{1,2\}}$:

$$U\left(\langle i,k\rangle\right) = \begin{cases} 1 & \text{se } k = 0 \\ 1 + 7\frac{k+1}{2} & \text{se } k \text{ è dispari e } i = 1 \\ 1 + 7\frac{k-1}{2} & \text{se } k > 1,\ k \text{ è dispari e } i = 2 \\ 4 & \text{se } k = 1 \text{ e } i = 2 \\ 4 + 7\frac{k}{2} & \text{se } k > 0,\ k \text{ è pari e } i = 1 \\ 5 + 7\left(\frac{k}{2} - 1\right) & \text{se } k > 0,\ k \text{ è pari e } i = 2 \end{cases} \tag{1.5}$$

Il lettore può verificare che questo tratteggio è debolmente periodico, con periodo 4 e lunghezza di un dominio fondamentale pari a 7. In esso, però, non si può ritrovare il concetto intuitivo di "schema che si ripete sempre", o si può trovarlo solo a partire dal quinto giorno (es. giorni 5-11, 12-18, 19-25, ecc.), perciò il tratteggio non rientra nella definizione di tratteggio periodico. Esso è comunque "debolmente" periodico perché una periodicità resta comunque, ma solo nel tratteggio delle classi di U, identico al tratteggio delle classi di T, come si vede in tabella 1.10.

1.5 Cosa significano i tratteggi?

Nel paragrafo precedente abbiamo visto cosa *sono* i tratteggi. Ora chiediamoci invece: cosa *significano* i tratteggi? Ossia, come possiamo interpretarli?

Come per gli altri enti matematici, a questa domanda si possono dare forse infinite risposte. Qui ne daremo solo due: un'interpretazione matematica ed una fisica, entrambe elementari.

Nell'interpretazione matematica, un tratteggio T con insieme degli indici C rappresenta una relazione tra C e l'insieme $\{n \in \mathbb{Z} | n \geq \mathcal{O}_T\}$, ossia un sottoinsieme R di $C \times \{n \in \mathbb{Z} | n \geq \mathcal{O}_T\}$. Informalmente, presi un indice i (numero di riga) ed un intero n (numero di colonna), essi sono in relazione se, nella tabella che rappresenta T, nella cella di riga i e colonna n è presente un trattino. Equivalentemente, i ed n sono in relazione se nel tratteggio T esiste un trattino di indice i e di valore n. In simboli:

$$i\,R\,n \overset{def}{\iff} \exists t \in T : \mathrm{ind}\,(t) = i \wedge |t|_T = n$$

Ad esempio, nel caso del tratteggio T_1, si ha $R \subset \{1,2,3\} \times \mathbb{N}$ e

$$i\,R\,n \Leftrightarrow$$

$$\exists t \in T_1 : \mathrm{ind}\,(t) = i \wedge |t|_T = n \Leftrightarrow$$

$$\exists t \in T_1 : \mathrm{ind}\,(t) = i \wedge T_1\,(t) = n \Leftrightarrow$$

$$\exists \langle i,k \rangle \in T_1 : T_1\,(\langle i,k \rangle) = n \Leftrightarrow$$

$$\exists \langle i,k \rangle \in T_1 : \left(\begin{cases} 3k & \text{se } i = 1 \\ 4k & \text{se } i = 2 \\ 5k & \text{se } i = 3 \end{cases} \right) = n \Leftrightarrow$$

$$i \in \{1,2,3\} \wedge \exists k \in \mathbb{N} : 3k = n \vee 4k = n \vee 5k = n \Leftrightarrow$$

$$i \in \{1,2,3\} \wedge (3 \mid n \vee 4 \mid n \vee 5 \mid n)$$

Cioè $R = \left\{ \begin{array}{l} \langle 1,0 \rangle, \langle 1,3 \rangle, \langle 1,6 \rangle, \langle 1,9 \rangle, \ldots, \\ \langle 2,0 \rangle, \langle 2,4 \rangle, \langle 2,8 \rangle, \langle 2,12 \rangle, \ldots, \\ \langle 3,0 \rangle, \langle 3,5 \rangle, \langle 3,10 \rangle, \langle 3,15 \rangle, \ldots \end{array} \right\}$.

Nell'interpretazione fisica, un tratteggio rappresenta il susseguirsi di infiniti eventi nel tempo, dove:

- Il tempo è misurato in intervalli discreti di medesima durata (ad esempio, in secondi);
- Esiste un istante iniziale ma non un istante finale;
- Esiste un insieme di eventi possibili, ognuno dei quali accade infinite volte;

- Un evento non può accadere due volte nello stesso intervallo di tempo (dove per "intervallo di tempo" si intende uno degli intervalli definiti nel primo punto); tuttavia è possibile che un evento accada una volta in un intervallo di tempo ed un'altra volta nell'intervallo successivo;

- Nell'istante iniziale accadono tutti gli eventi.

Più precisamente, dato un tratteggio T con insieme degli indici C, quest'ultimo viene interpretato come l'insieme degli eventi e l'appartenenza di un trattino $\langle i, k\rangle$ a T viene interpretata come il fatto che la k-esima volta che si verifica l'evento i è nell'istante $T(\langle i, k\rangle)$. Questa interpretazione si adatta perfettamente al problema 1.1, in cui il tempo è misurato in giorni, l'istante iniziale è oggi, i tre eventi possibili sono "Aldo va a correre", "Giovanni va a correre" e "Giacomo va a correre".

1.6 Funzioni fondamentali

La teoria dei tratteggi è basata sullo studio di alcune funzioni fondamentali, che ora definiamo. Per restare nello spirito di questo capitolo, puramente introduttivo e concettuale, non enunciamo alcuna proprietà di queste funzioni, ma diamo solo definizioni ed esempi. Alcune semplici proprietà sono discusse nel paragrafo 3.1.

Quanto alla notazione, è convenzione che tutte le funzioni relative ai tratteggi abbiano un nome che inizia con la lettera t. Inoltre, ogni funzione fondamentale è legata ad un certo tratteggio T (cioè la sua definizione è indotta da quella di T), che viene scritto in pedice nel nome della funzione, ad esempio nome_funzione_T. Quindi, se T e U sono due tratteggi diversi, nome_funzione_T e nome_funzione_U sono, in generale, due funzioni diverse. Se si scrive nome_funzione_T senza specificare qual è T, vuol dire che si sta considerando un T generico e che quindi le affermazioni che si fanno sono valide qualunque sia T. Ad esempio, se si dice che nome_funzione_T è suriettiva senza specificare T, vuol dire che, al variare di T, nome_funzione_T è sempre una funzione suriettiva.

Introduciamo ciascuna funzione con riferimento al problema 1.1. Infatti ciascuna di esse risponde ad una domanda ben precisa.

Domanda: Chi sarà l'n-esima persona a correre? Quante volte dovrà correre questa persona, per poter dire di essere l'n-esima persona a correre?

Per rispondere a questa domanda coi tratteggi, si deve cercare l'n-esimo trattino di T_1 nell'ordinamento temporale. A questo punto, l'indice del trattino trovato è il numero corrispondente alla persona, ed il secondo valore della coppia costituente il

trattino indica quante volte avrà già corso quella persona, compresa la volta in cui è l'n-esima persona a correre. Ad esempio, se $n = 10$ si torna al problema 1.1: il decimo trattino nell'ordinamento temporale è $\langle 1, 5\rangle$, che rappresenta la quinta corsa di Aldo (numero 1). Quindi Aldo sarà il decimo a correre e, può dire di esserlo quando corre per la quinta volta.

Una domanda di questo tipo richiede quindi la conoscenza dell'n-esimo trattino di un tratteggio:

Definizione 1.17. *Dato un tratteggio finito T con insieme di indici C, si definisce la funzione t_T:*

$$\mathrm{t}_T : \mathbb{N}^\star \to \mathrm{Tratt}_C \ni \mathrm{t}_T(x) \equiv \begin{cases} \min\limits_{t \in T,\, t > \mathcal{O}_T} t & \text{se } x = 1 \\ \text{trattino successivo a } \mathrm{t}_T(T, x-1) & \text{altrimenti} \end{cases}$$

dove il minimo e l'espressione "successivo" vanno intese rispetto all'ordinamento temporale dei trattini di T.

Ad esempio, $\mathrm{t}_{T_1}(1) = \langle 1, 1\rangle$, $\mathrm{t}_{T_1}(2) = \langle 2, 1\rangle$, $\mathrm{t}_{T_1}(3) = \langle 3, 1\rangle$, $\mathrm{t}_{T_1}(4) = \langle 1, 2\rangle$, $\mathrm{t}_{T_1}(5) = \langle 2, 2\rangle$, $\mathrm{t}_{T_1}(6) = \langle 1, 3\rangle$, ecc.

Si noti che t_T è definita solo se T è finito, perché in questo modo la funzione è sicuramente suriettiva (che è ciò che vogliamo, perché così ad ogni trattino è associato un numero naturale). Se invece T fosse infinito, esso potrebbe avere una classe per valore infinita c: in questo caso, un trattino t di valore maggiore del valore di c non avrebbe controimmagine. Infatti, se fosse $\mathrm{t}_T(x) = t$ per qualche x, la classe c avrebbe meno di x elementi, il che va contro l'ipotesi che c è infinita. È evidente che ciò dipende dal particolare ordinamento di trattini scelto, e che il problema non ci sarebbe se considerassimo qualche altro ordinamento dei trattini (ad esempio, un ordinamento "diagonale", alla Cantor), ma per il momento preferiamo considerare l'ordinamento per colonne, perché sembra il più naturale.

Osservazione 1.2. *Per ogni $x \in \mathbb{N}^\star$ e per ogni $T \in \mathcal{T}^1$, $\mathrm{t}_T(x) = \langle 1, x\rangle$.*

Domanda: Quando correrà colui che sarà l'n-esimo a correre?

Per rispondere a questa domanda, conviene rispondere prima alla precedente: una volta saputo chi è l'n-esima persona a correre e quante volte dovrà correre per essere l'n-esimo, il giorno in cui questo accadrà è noto dal tratteggio. Ad esempio, se sappiamo che il decimo trattino è $\langle 1, 5\rangle$ – cioè che quando Aldo corre per la quinta volta, è il decimo a correre – sappiamo anche che il valore del decimo trattino è

$T_1(\langle 1,5\rangle) = 3 \cdot 5 = 15$, cioè che la decima persona a correre corre il quindicesimo giorno.

Si può quindi pensare ad una funzione, ottenuta componendo t_{T_1} con T_1 stessa, che restituisce direttamente il valore dell'n-esimo trattino di T_1. In generale:

Definizione 1.18. *Dato un tratteggio T, si definisce la funzione* $\mathrm{t\_valore}_T$*:*

$$\mathrm{t\_valore}_T : \mathbb{N} \to \mathbb{Z} \nexists' \mathrm{t\_valore}_T(x) = \begin{cases} \mathcal{O}_T & \text{se } x = 0 \\ T(\mathrm{t}_T(x)) & \text{altrimenti} \end{cases}$$

Ad esempio, $\mathrm{t\_valore}_{T_1}(0) = 0$, $\mathrm{t\_valore}_{T_1}(1) = 3$, $\mathrm{t\_valore}_{T_1}(2) = 4$, $\mathrm{t\_valore}_{T_1}(3) = 5$, $\mathrm{t\_valore}_{T_1}(4) = 6$, $\mathrm{t\_valore}_{T_1}(5) = 8$, $\mathrm{t\_valore}_{T_1}(6) = 9$, ecc.

Domanda: Quale sarà l'n-esimo giorno in cui corre qualcuno?

I giorni in cui corre qualcuno sono i valori delle classi di T_1. Quindi, per rispondere alla domanda, bisogna cercare l'n-esima classe di T_1. In generale:

Definizione 1.19. *Dato un tratteggio T, si definisce la funzione* $\mathrm{t\_classe}_T$*:*

$$\mathrm{t\_classe}_T : \mathbb{N} \to \mathbb{Z} \nexists' \mathrm{t\_classe}_T(x) = \textit{valore della } x\textit{-esima classe di } T$$

dove come 0*-esima classe di T si considera la classe di valore $\mathcal{O}_T$.*

In alternativa, avendo definito il tratteggio delle classi $c(T)$, si può dire che $\mathrm{t\_classe}_T(x) = \mathrm{t\_valore}_{c(T)}(x)$.

Ad esempio, $\mathrm{t\_classe}_{T_1}(0) = 0$, $\mathrm{t\_classe}_{T_1}(1) = 3$, $\mathrm{t\_classe}_{T_1}(2) = 4$, $\mathrm{t\_classe}_{T_1}(3) = 5$, ecc.

$\mathrm{t\_classe}_T$ è definita anche per i tratteggi infiniti, perché è sempre suriettiva. Inoltre, come t_T ma diversamente da $\mathrm{t\_valore}_T$, è anche iniettiva.

Domanda: Quanti giorni passano tra quando corre l'n-esima persona e quando corre la $n+1$-esima?

Il modo più ovvio di fornire una risposta è calcolare quando corre l'n-esima persona, quando corre la $n+1$-esima, poi calcolare la differenza tra i due risultati. In generale:

Definizione 1.20. *Dato un tratteggio $T \equiv \langle C, f\rangle$, si definisce la funzione* $\mathrm{t\_valore\_diff}_T$*:*

$$\mathrm{t\_valore\_diff}_T : \mathbb{N}^\star \to \mathbb{N} \nexists' \mathrm{t\_valore\_diff}_T(x) \equiv \mathrm{t\_valore}_T(x) - \mathrm{t\_valore}_T(x-1)$$

Domanda: Quanti giorni passano tra l'n-esimo giorno in cui corre qualcuno e l'$n+1$-esimo giorno in cui corre qualcuno?

Come per la domanda precedente, il modo più ovvio per rispondere è calcolare separatamente quali sono l'n-esimo e l'$n+1$-esimo giorno in cui corre qualcuno e calcolarne la differenza. In generale:

Definizione 1.21. *Dato un tratteggio T, si definisce la funzione* t_classe_diff_T*:*

$$\text{t\_classe\_diff}_T : \mathbb{N}^\star \to \mathbb{N}^\star \ni' \text{t\_classe\_diff}_T(x) \equiv \text{t\_classe}_T(x) - \text{t\_classe}_T(x-1)$$

Si noti che la differenza tra i valori di due trattini consecutivi può essere nulla (ma solo se i trattini hanno indici diversi); quella tra i valori di due classi consecutive no.

Domanda: Qual è l'n-esimo giorno in cui non corre nessuno?

I giorni in cui non corre nessuno sono gli spazi di T_1, quindi la domanda concide col la richiesta dell'n-esimo spazio di T_1.

Definizione 1.22. *Dato un tratteggio $T \equiv \langle C, f \rangle$ con infiniti spazi, si definisce la funzione* t_spazio_T*:*

$$\text{t\_spazio}_T : \mathbb{N}^\star \to \mathbb{Z} \ni' \text{t\_spazio}_T(x) \equiv \begin{cases} \min\limits_{s \text{ spazio di } T,\, s > \mathcal{O}_T} s & \text{se } x = 1 \\ \min\limits_{s \text{ spazio di } T,\, s > \text{t\_spazio}_T(x-1)} s & \text{altrimenti} \end{cases}$$

In alternativa, avendo definito il tratteggio degli spazi $s(T)$, si può dire che $\text{t\_spazio}_T(x) = \text{t\_valore}_{s(T)}(x)$.

Ad esempio, $\text{t\_spazio}_{T_1}(1) = 1$, $\text{t\_spazio}_{T_1}(2) = 2$, $\text{t\_spazio}_{T_1}(3) = 7$, $\text{t\_spazio}_{T_1}(4) = 11$, ecc.

Domanda: Fino all'n-esimo giorno compreso, quanti giorni non ha corso nessuno?

Per rispondere a questa domanda, occorre contare quanti spazi di T_1 sono minori o uguali ad n o, in altri termini, qual è il massimo y tale che l'y-esimo spazio è minore o uguale ad n. In generale:

Definizione 1.23. *Dato un tratteggio T, si definisce la funzione* ${\text{t\_spazio}^{-1}}_T$*:*

$${\text{t\_spazio}^{-1}}_T : [\text{t\_spazio}_T(1), \infty] \to \mathbb{N}^\star \ni' {\text{t\_spazio}^{-1}}_T(x) \equiv \max_{\text{t\_spazio}_T(y) \leq x} y$$

Ad esempio, ${\text{t\_spazio}^{-1}}_{T_1}(1) = 1$, ${\text{t\_spazio}^{-1}}_{T_1}(2) = 2$, ${\text{t\_spazio}^{-1}}_{T_1}(3) = 2$, ${\text{t\_spazio}^{-1}}_{T_1}(4) = 2$, ${\text{t\_spazio}^{-1}}_{T_1}(5) = 2$, ${\text{t\_spazio}^{-1}}_{T_1}(6) = 2$, ${\text{t\_spazio}^{-1}}_{T_1}(7) = 3$, ecc.

Si noti che, essendo t_spazio_T iniettiva, se ne può considerare l'inversa, t_spazio_T^{-1}. Questa funzione però è diversa da ${\text{t\_spazio}^{-1}}_T$. La differenza è in primo luogo notazionale: nel secondo caso, il "-1" fa parte del nome della funzione. In secondo luogo, la funzione ${\text{t\_spazio}^{-1}}_T$ è definita in $\{n \in \mathbb{Z} | n \geq \text{t\_spazio}_T(1)\}$, mentre t_spazio_T^{-1}, essendo l'inversa di t_spazio_T, è definita sulla sua immagine, cioè sull'insieme degli spazi di T sull'insieme degli spazi di T. Tuttavia, le due funzioni sono molto simili, in quanto $\text{t\_spazio}_T^{-1} = ({\text{t\_spazio}^{-1}}_T)_{|S}$, dove S è l'insieme degli spazi di T. Si verifica facilmente che:

Osservazione 1.3. *Per ogni $x, y \in \mathbb{N}^\star$ e per ogni tratteggio T avente spazi:*

- ${\text{t\_spazio}^{-1}}_T(\text{t\_spazio}_T(x)) = x$
- $x < y \Rightarrow {\text{t\_spazio}^{-1}}_T(x) \leq {\text{t\_spazio}^{-1}}_T(y)$
- ${\text{t\_spazio}^{-1}}_T(x) = |\{s \in [1, x] \mid s \text{ è uno spazio di } T\}|$

Finora abbiamo visto varie funzioni che abbiamo chiamato "fondamentali", senza però dire in generale cosa sia una funzione fondamentale. In realtà il concetto è ancora da chiarire e la sua definizione avrebbe bisogno di una base più forte di quella che abbiamo dato in questo capitolo. Per il momento, definiamo semplicemente funzioni fondamentali una di quelle che abbiamo visto in questo paragrafo:

Definizione 1.24. *Sia $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$. Si definiscono gli insiemi:*

- $\mathcal{F} \equiv \left\{\text{t}, \text{t\_valore}, \text{t\_classe}, \text{t\_valore\_diff}, \text{t\_classe\_diff}, \text{t\_spazio}, {\text{t\_spazio}^{-1}}\right\}$
- $\mathcal{F}_T \equiv \{f_T \mid f \in \mathcal{F}\}$

Si definisce funzione fondamentale *una funzione $f_T \in \bigcup_{U \in \mathcal{T}^{\overline{\mathbb{N}}^\star}} \mathcal{F}_U$, se questa è definita*[6].

Sia $f \in \mathcal{F}$. Si noti che tutte le funzioni fondamentali in $\left\{f_T \mid T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}\right\}$ hanno lo stesso dominio, ossia il dominio di una funzione fondamentale f_T dipende solo da f, non da T. Per ricordarlo, evitando confusione, introduciamo la seguente notazione:

Notazione 1.1. *Siano $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$ e $f_T \in \mathcal{F}_T$. Si pone Dom $f \equiv$ Dom f_T.*

[6] Il motivo di questa precisazione è che non tutte le funzioni fondamentali hanno senso per tutti i tratteggi di $\mathcal{T}^{\overline{\mathbb{N}}^\star}$, ad esempio t_valore_T è definita solo se T è finito.

1.7 Upcast e downcast

Due concetti fondamentali della teoria dei tratteggi sono quelli di upcast e downcast. Come i precedenti concetti, li spiegheremo partendo da problemi concreti. Poiché tutti i problemi che vedremo condividono le stesse ipotesi, li scriviamo una volta per tutte nella seguente:

Assunzione 1.1. *Aldo, Giovanni e Giacomo vanno regolarmente a correre. Aldo corre ogni tre giorni, di mattina; Giovanni corre ogni quattro giorni, di pomeriggio; Giacomo ogni cinque giorni, di sera. Oggi corrono tutti e tre. I giorni si contano a partire da domani.*

1.7.1 Upcast e up-conservatività

Consideriamo il seguente problema:

Problema 1.2. *Quando Aldo e Giovanni avranno corso complessivamente sette volte, quante volte avranno corso complessivamente tutti e tre?*

Per rispondere a questa domanda, è possibile analizzare la tabella che rappresenta solo le corse di Aldo e Giovanni, senza considerare Giacomo (figura 1.4). Questa rappresenta un nuovo tratteggio, sottotratteggio di T_1, che, con le notazioni del paragrafo 1.4, si può indicare con $T_1[1,2]$. La settima corsa di Aldo e Giovanni è rappresentata dal settimo trattino di $T_1[1,2]$, cioè $\langle 1,5\rangle$. Tuttavia, in T_1 questo trattino non è il settimo, ma il decimo (come abbiamo visto all'inizio del paragrafo 1.6). Allora si ha l'equazione:

$$\mathrm{t}_{T_1[1,2]}(7) = \langle 1,5\rangle = \mathrm{t}_{T_1}(10)$$

che implica:

$$\mathrm{t}_{T_1[1,2]}(7) = \mathrm{t}_{T_1}(10) \tag{1.6}$$

leggibile come: "Quando Aldo e Giovanni hanno corso complessivamente sette volte, tutti e tre hanno corso complessivamente dieci volte", che è anche la risposta al problema 1.2.

Possiamo pensare, leggendo la (1.6), che esista una funzione che associ al numero 7 il numero 10, dati T_1 e $T_1[1,2]$. Più formalmente, potremmo cercare una funzione $g : \mathbb{N}^\star \to \mathbb{N}^\star$ tale che per ogni $x \in \mathbb{N}^\star$:

$$\begin{cases} g(x) = y \Rightarrow \mathrm{t}_{T_1[1,2]}(x) = \mathrm{t}_{T_1}(y) \\ g(x) = \bot \Rightarrow \neg\exists y \in \mathbb{N}^\star : \mathrm{t}_{T_1[1,2]}(x) = \mathrm{t}_{T_1}(y) \end{cases} \tag{1.7}$$

Oppure, equivalentemente, ponendo $\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t}) \equiv \left\{y \in \mathbb{N}^\star \mid \mathrm{t}_{T_1[1,2]}(x) = \mathrm{t}_{T_1}(y)\right\}$:

$$\begin{cases} g(x) \in \mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t}) & \text{se } \mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t}) \neq \emptyset \\ g(x) = \bot & \text{altrimenti} \end{cases} \tag{1.8}$$

Nel nostro esempio, è possibile verificare che:

- $\begin{aligned} \mathrm{Up}_1^{T_1[1,2]\to T_1}(\mathrm{t}) &\equiv \left\{y \in \mathbb{N}^\star \mid \mathrm{t}_{T_1[1,2]}(1) = \mathrm{t}_{T_1}(y)\right\} \\ &= \left\{y \in \mathbb{N}^\star \mid \langle 1,1\rangle = \mathrm{t}_{T_1}(y)\right\} = \{1\} \end{aligned}$
- $\mathrm{Up}_2^{T_1[1,2]\to T_1}(\mathrm{t}) \equiv \left\{y \in \mathbb{N}^\star \mid \langle 2,1\rangle = \mathrm{t}_{T_1}(y)\right\} = \{2\}$
- $\mathrm{Up}_3^{T_1[1,2]\to T_1}(\mathrm{t}) \equiv \left\{y \in \mathbb{N}^\star \mid \langle 1,2\rangle = \mathrm{t}_{T_1}(y)\right\} = \{4\}$
- ...

Quindi la g che cerchiamo è tale che $g(1) = 1$, $g(2) = 2$, $g(3) = 4$, eccetera.

Possiamo notare che $\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t})$ non è mai vuoto, per ogni x (intuitivamente, ciò accade perché i trattini di $T_1[1,2]$ sono anche trattini di T_1). Ciò comporta che la seconda condizione del sistema 1.12 ($g(x) = \bot$ se $\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t}) = \emptyset$) non si verifica mai: dunque le funzioni g che soddisfano il sistema 1.12 sono tutte totali. In generale si ha che, per ogni $x \in \mathbb{N}^\star$, $\left|\mathrm{Up}_x^{T\to T'}(\mathrm{t})\right| \geq 1$: si esprime questo fatto dicendo che t è *up-conservativa*.

Abbiamo detto che nel nostro esempio $\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t})$ non è mai vuoto. Possiamo in realtà precisare quest'affermazione dicendo che $\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t})$ contiene sempre un singolo elemento, ossia, per ogni x, $\left|\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t})\right| = 1$. Ciò comporta che esiste un'unica g che soddisfa le condizioni 1.12. Infatti, se fosse, per esempio, $\mathrm{Up}_3^{T_1[1,2]\to T_1}(\mathrm{t}) = \{4,5\}$ anziché $\{4\}$, ci sarebbero almeno due funzioni soddisfacenti le condizioni date: una g_1 tale che $g_1(1) = 1$, $g_1(2) = 2$, $g_1(3) = 4$, ... ed una g_2 tale che $g_2(1) = 1$, $g_2(2) = 2$, $g_2(3) = 5$, ... In generale, maggiori sono le x per cui $\left|\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t})\right| > 1$, più funzioni diverse soddisfano le condizioni 1.12. Nel nostro caso invece, essendo $\left|\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t})\right| = 1$ per ogni x, esiste una sola soluzione del sistema 1.12. In generale, si può dimostrare che per ogni tratteggio T e per ogni $T' \geq T$ si ha che $\left|\mathrm{Up}_x^{T\to T'}(\mathrm{t})\right| = 1$: per esprimere ciò, si dice che t è *upcast-sicura*.

Ciò che abbiamo detto per la funzione t può estendersi a tutte le funzioni fondamentali, nel modo seguente:

Definizione 1.25. *Siano $f \in \mathcal{F}$, T' un tratteggio, $T \leq T'$ e $x \in Dom\ f$. Si definisce* upcast di f da T a T' rispetto ad x *l'insieme:*

$$\mathrm{Up}_x^{T\to T'}(f) \equiv \{y \in Dom\ f \mid f_T(x) = f_{T'}(y)\}$$

Definizione 1.26. *Siano $f \in \mathcal{F}$, T' un tratteggio e $T \leq T'$. Si definisce* upcast di f da T a T' *il seguente insieme di funzioni da Dom f in Dom f:*

$$\mathrm{Up}^{T\to T'}(f) \equiv \left\{ \begin{array}{l} g \in [Dom\ f \to Dom\ f] \mid \\ \forall x \in Dom\ f : \begin{cases} g(x) \in \mathrm{Up}_x^{T\to T'}(f) & se\ \mathrm{Up}_x^{T\to T'}(f) \neq \emptyset \\ g(x) = \bot & altrimenti \end{cases} \end{array} \right\}$$

In altri termini, $\mathrm{Up}^{T\to T'}(f)$ è l'insieme delle soluzioni del sistema:

$$\left\{ \begin{array}{l} g(x) = y \Rightarrow f_T(x) = f_{T'}(y) \\ g(x) = \bot \Rightarrow \neg\exists y \in \mathbb{N}^\star : f_T(x) = f_{T'}(y) \end{array} \right. \tag{1.9}$$

Definizione 1.27. *Una funzione fondamentale f_T si definisce* up-conservativa *se, per ogni tratteggio T e per ogni $T' \geq T$, $\mathrm{Up}^{T\to T'}(f)$ contiene solo funzioni totali.*

Si osservi che $\mathrm{Up}^{T\to T'}(f)$ contiene solo funzioni totali $\Leftrightarrow \forall x \in \mathrm{Dom}\ f : \mathrm{Up}_x^{T\to T'}(f) \neq \emptyset \Leftrightarrow \forall x \in \mathrm{Dom}\ f\ \exists y \in \mathrm{Dom}\ f\ \ni' f_{T'}(y) = f_T(x)$.

Non tutte le funzioni fondamentali sono up-conservative. Consideriamo ad esempio il seguente problema:

Problema 1.3. *Il quinto giorno in cui non corrono né Aldo, né Giovanni, correrà Giacomo?*

Questo problema ci porta a considerare gli spazi del tratteggio $T_1[1,2]$, mostrato in figura 1.4. Infatti, il quinto giorno in cui non corrono né Aldo, né Giovanni è, con le notazioni della teoria dei tratteggi, $\mathrm{t\_spazio}_{T_1[1,2]}(5)$, che è pari a 10. Nel decimo giorno, però, Giacomo corre. Quindi la risposta al problema è negativa. Ciò significa che la funzione $\mathrm{t\_spazio}_T$ non è up-conservativa, perché non esiste un $y \in \mathbb{N}^\star$ tale che $\mathrm{t\_spazio}_{T_1[1,2]}(5) = \mathrm{t\_spazio}_{T_1}(y)$, dunque $\mathrm{Up}_5^{T_1[1,2]\to T_1}(\mathrm{t\_spazio}) = \emptyset$.

Il fatto che $\mathrm{Up}_5^{T_1[1,2]\to T_1}(\mathrm{t\_spazio}) = \emptyset$ non significa che $\mathrm{Up}_x^{T_1[1,2]\to T_1}(\mathrm{t\_spazio}) = \emptyset$ per ogni x. Ad esempio, ciò non è vero per $x = 6$: se avessimo chiesto se Giacomo corre nel *sesto* giorno in cui non corrono né Aldo, né Giovanni, la risposta sarebbe stata negativa. In sintesi, il quinto spazio di $T_1[1,2]$ non è uno spazio di T_1, ma il sesto lo è.

In generale, per le funzioni non up-conservative, ha senso chiedersi, per un fissato elemento x del dominio, se $\mathrm{Up}_x^{T\to T'}(f)$ è vuoto o meno. A questa domanda risponde la *funzione di up-conservatività*:

Definizione 1.28. *Siano $f \in \mathcal{F}$ e $T, T' \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, con $T \leq T'$. Si definisce la funzione* $\mathrm{UpCons}^{T\to T'}(f) \in [Dom\ f \to \{0,1\}]$ *tale che:*

$$\mathrm{UpCons}^{T\to T'}(f)(x) = \left(\mathrm{Up}_x^{T\to T'}(f) \neq \emptyset\right)$$

Essa viene detta funzione di up-conservatività *di f da T a T'.*

Ovviamente, per le funzioni fondamentali up-conservative, la funzione di up-conservatività assume sempre valore 1.
Si può verificare facilmente che le funzioni fondamentali up-conservative per ogni T sono t_T, $\mathrm{t\_valore}_T$, $\mathrm{t\_classe}_T$, $\mathrm{t\_spazio}_T^{-1}$.

Una funzione up-conservativa può essere anche *upcast-sicura*:

Definizione 1.29. *Una funzione fondamentale f_T si definisce* upcast-sicura *se, per ogni tratteggio T e per ogni $T' \geq T$, $\mathrm{Up}^{T\to T'}(f) = \{g\}$, con g totale.*

Si osservi che $\mathrm{Up}^{T\to T'}(f) = \{g\}$, con g totale $\Leftrightarrow \forall x \in \mathrm{Dom}\ f : \left|\mathrm{Up}_x^{T\to T'}(f)\right| = 1$ $\Leftrightarrow \forall x \in \mathrm{Dom}\ f : \exists \mid y \in \mathrm{Dom}\ f \ni' f_{T'}(y) = f_T(x)$.

Ovviamente, se una funzione fondamentale è upcast-sicura, è anche up-conservativa, ma il viceversa può non essere vero. Ad esempio, consideriamo il seguente problema:

Problema 1.4. *Quante volte dovrebbero correre complessivamente i tre perché l'ultimo a correre corra nello stesso giorno in cui corre Aldo la quarta volta?*

Consideriamo $T_1[1]$, ossia il sottotratteggio di T_1 contenente solo i trattini di indice 1, il numero che rappresenta Aldo. Il giorno in cui corre Aldo la quarta volta è $\mathrm{t\_valore}_{T_1[1]}(4) = |\langle 1,4\rangle|_{T_1[1]} = 3\cdot 4 = 12$. Il problema chiede qual è il numero y tale che $\mathrm{t\_valore}_{T_1}(y) = \mathrm{t\_valore}_{T_1[1]}(4) = 12$. Infatti, se è vera questa condizione, significa che, se i tre corrono complessivamente y volte, l'ultimo (l'y-esimo) corre il dodicesimo giorno, lo stesso in cui Aldo corre per la quarta volta. Esaminando la tabella in figura 1.1, si evince che esistono due y che soddisfano la condizione: 8 e 9. Infatti, l'ottava persona a correre, tra Aldo, Giovanni e Giacomo, è Aldo, che corre il dodicesimo giorno (come sapevamo), ma anche Giovanni, che è il nono, corre lo stesso giorno. Dunque si ha:

$$\mathrm{t\_valore}_{T_1}(8) = \mathrm{t\_valore}_{T_1}(9) = \mathrm{t\_valore}_{T_1[1]}(4) = 12$$

o, più sinteticamente:

$$\mathrm{Up}_4^{T_1[1]\to T_1}(\mathrm{t\_valore}) = \{8,9\} \tag{1.10}$$

dunque la funzione $\mathrm{t\_valore}_T$ non è upcast-sicura, pur essendo up-conservativa, come è facile dimostrare.

Una conseguenza della 1.10 è che $\mathrm{Up}^{T_1[1]\to T_1}$ contiene alcune funzioni g tali che $g(4) = 8$ ed altre g per cui $g(4) = 9$.

Un problema fondamentale della teoria dei tratteggi è trovare almeno un elemento di $\mathrm{Up}^{T\to T'}(f)$, dati f, T e T'. Ciò è complicato dalla presenza, in $\mathrm{Up}^{T\to T'}(f)$, di funzioni parziali (a meno che f sia up-conservativa, cosa che non si suppone in generale). Risulta invece più semplice trovare una funzione g' che non è esattamente uguale ad un elemento g di $\mathrm{Up}^{T\to T'}(f)$, ma è molto simile, nel senso che:

- se $g(x)$ è definita, $g(x) = g'(x)$
- se $g(x) = \bot$, non c'è nessun vincolo su $g'(x)$ (g' può assumere qualsiasi valore in x o essere indefinita)

Ciò si può sintetizzare dicendo che $g'_{|\mathrm{Dom}\ g} = g$. Formalizziamo questo concetto quanto basta per i nostri scopi.

Definizione 1.30. *Siano $f, g \in [D \to C]$, con D e C insiemi qualsiasi non vuoti. Si dice che f è una* specializzazione *di g, e si scrive $f \leq g$, se $f_{|Dom\ g} = g$.*

Definizione 1.31. *Siano D, C e X insiemi non vuoti e $X \subseteq [D \to C]$.*
Si chiama insieme delle specializzazioni *di X, e si indica con Spec X, l'insieme* $\{f \in [D \to C] \mid \exists g \in X : f \leq g\}$.

Uno dei nostri problemi sarà quello di cercare, dati f, T e T', un elemento di Spec $\mathrm{Up}^{T\to T'}(f)$. Se $g \in \mathrm{Spec}\ \mathrm{Up}^{T\to T'}(f)$, vuol dire che esiste una funzione $h \in \mathrm{Up}^{T\to T'}(f)$ tale che g si comporta come h quando h è definita. Ma, per definizione di upcast di f, $h(x) \in \mathrm{Up}_x^{T\to T'}(f)$. Quindi, se $\mathrm{Up}_x^{T\to T'}(f) \neq \emptyset$, h è definita per x e quindi $g(x) = h(x) \in \mathrm{Up}_x^{T\to T'}(f)$; altrimenti, nulla si può dire su g. Riassumendo:

Osservazione 1.4.

$$g \in \mathit{Spec}\ \mathrm{Up}^{T\to T'}(f) \Leftrightarrow$$

$$\forall x \in \mathit{Dom}\ f : \mathrm{Up}_x^{T\to T'}(f) \neq \emptyset \Rightarrow g(x) \in \mathrm{Up}_x^{T\to T'}(f) \Leftrightarrow$$

$$\forall x \in \mathit{Dom}\ f : (\exists y \in \mathit{Dom}\ f : f_T(x) = f_{T'}(y)) \Rightarrow f_T(x) = f_{T'}(g(x))$$

Osserviamo che, se $g \in \mathrm{Spec}\ \mathrm{Up}^{T\to T'}(f)$, possiamo trovare una funzione $g' \in \mathrm{Up}^{T\to T'}$, soluzione del sistema 1.9, ponendo:

$$g'(x) = \begin{cases} g(x) & \text{se } \mathrm{UpCons}^{T\to T'}(f)(x) = 1 \\ \bot & \text{altrimenti} \end{cases}$$

per ogni $x \in \mathrm{Dom}\ f$.

1.7.2 Downcast e down-conservatività

I concetti di downcast e down-conservatività sono analoghi a quelli di upcast e up-conservatività ed, in un certo senso, inversi. Infatti, potremmo considerare dei problemi analoghi a quelli visti per l'upcast, ma invertendo dati e soluzioni. Ad esempio, invertendo così il problema 1.2, si ottiene il seguente:

Problema 1.5. *Quando Aldo, Giovanni e Giacomo avranno corso complessivamente dieci volte, quante volte avranno corso complessivamente Aldo e Giovanni?*

L'equazione che permette di risolvere il problema è sempre la 1.6, che per comodità riportiamo:

$$\mathrm{t}_{T_1[1,2]}(7) = \mathrm{t}_{T_1}(10)$$

Tuttavia, mentre prima cercavamo una funzione che a 7 associa 10, ora cerchiamo una funzione che a 10 associa 7. In generale, cerchiamo una funzione $g' : \mathbb{N}^\star \to \mathbb{N}^\star$ tale che per ogni $y \in \mathbb{N}^\star$:

$$\begin{cases} g'(y) = x \Rightarrow \mathrm{t}_{T_1}(y) = \mathrm{t}_{T_1[1,2]}(x) \\ g'(y) = \bot \Rightarrow \neg\exists x \in \mathbb{N}^\star : \mathrm{t}_{T_1}(y) = \mathrm{t}_{T_1[1,2]}(x) \end{cases} \tag{1.11}$$

Oppure, equivalentemente, definendo $\mathrm{Down}_y^{T_1 \to T_1[1,2]}(\mathrm{t}) \equiv \left\{x \in \mathbb{N}^\star \mid \mathrm{t}_{T_1}(y) = \mathrm{t}_{T_1[1,2]}(x)\right\}$:

$$\begin{cases} g'(y) \in \mathrm{Down}_y^{T_1 \to T_1[1,2]}(\mathrm{t}) & \text{se } \mathrm{Down}_y^{T_1 \to T_1[1,2]}(\mathrm{t}) \neq \emptyset \\ g'(y) = \bot & \text{altrimenti} \end{cases} \tag{1.12}$$

Si noti che nella definizione di questa g', rispetto all'equazione 1.12 che definiva la funzione g che permette di risolvere il problema dell'upcast, si sono solo scambiati i tratteggi T_1 e $T_1[1,2]$ (e, per comodità di confronto, anche i simboli x e y).
g' è proprio l'inversa di g; infatti:

$g'(y) = x \Leftrightarrow$ [dalla 1.11]
$\mathrm{t}_{T_1}(y) = \mathrm{t}_{T_1[1,2]}(x) \Leftrightarrow$
$\mathrm{t}_{T_1[1,2]}(x) = \mathrm{t}_{T_1}(y) \Leftrightarrow$ [dalla 1.7]
$g(x) = y$

Inoltre:

$g'(y) = \bot \Leftrightarrow$ [dalla 1.11]
$\neg\exists x \in \mathbb{N}^\star : \mathrm{t}_{T_1}(y) = \mathrm{t}_{T_1[1,2]}(x) \Leftrightarrow$ [dalla 1.7]
$\neg\exists x \in \mathbb{N}^\star : g(x) = y \Leftrightarrow$

$y \notin \operatorname{Im} g \Leftrightarrow$
$g^{-1}(y) = \bot$

Quindi stiamo parlando, in questo paragrafo, degli stessi concetti del paragrafo precedente, ma visti dall'ottica opposta. Se l'upcast permette di passare da un tratteggio (ad esempio $T_1[1,2]$) ad un suo sovratratteggio (T_1), il downcast permette di passare da un tratteggio (come T_1) ad un suo sottotratteggio ($T_1[1,2]$). Segue quindi un elenco di definizioni riguardanti il downcast e la down-conservatività, ottenute da quelle del paragrafo precedente sostituendo in ciascuna $T \leq T'$ con $T' \leq T$.

Definizione 1.32. *Siano $f \in \mathcal{F}$, T'un tratteggio, $T' \leq T$ e $x \in Dom\ f$. Si definisce* downcast di f da T a T' rispetto ad x *l'insieme:*

$$\mathrm{Down}_x^{T \to T'}(f) \equiv \{y \in Dom\ f \mid f_T(x) = f_{T'}(y)\}$$

Definizione 1.33. *Sia $f \in \mathcal{F}$, T' un tratteggio e $T \geq T'$. Si definisce* downcast di f da T a T' *il seguente insieme di funzioni da Dom f in Dom f:*

$$\mathrm{Down}^{T \to T'}(f) \equiv \left\{ \begin{array}{l} g \in [Dom\ f \to Dom\ f] \mid \\ \forall x \in Dom\ f : \begin{cases} g(x) \in \mathrm{Down}_x^{T \to T'}(f) & se\ \mathrm{Down}_x^{T \to T'}(f) \neq \emptyset \\ g(x) = \bot & altrimenti \end{cases} \end{array} \right\}$$

Definizione 1.34. *Una funzione fondamentale f_T si definisce* down-conservativa *se, per ogni tratteggio T e per ogni $T' \leq T$, $\mathrm{Down}^{T \to T'}(f)$ contiene solo funzioni totali.*

Definizione 1.35. *Siano $f \in \mathcal{F}$ e $T, T' \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, con $T \geq T'$. Si definisce la funzione* $\mathrm{DownCons}^{T \to T'}(f) \in [Dom\ f \to \{0,1\}]$ *tale che:*

$$\mathrm{DownCons}^{T \to T'}(f)(x) = \left(\mathrm{Down}_x^{T \to T'}(f) \neq \emptyset\right)$$

Essa viene detta funzione di down-conservatività *di f da T a T'.*

Definizione 1.36. *Una funzione fondamentale f_T si definisce* downcast-sicura *se, per ogni tratteggio T e per ogni $T' \leq T$, $\mathrm{Down}^{T \to T'}(f) = \{g\}$, con g totale.*

1.7.3 Alcune semplici proprietà

Vediamo alcune proprietà delle funzioni fondamentali legate all'upcast e al downcast:

Proprietà 1.3. *Dato un tratteggio T ed una funzione fondamentale f_T:*

- *$f_{T'}$ iniettiva per ogni $T' \geq T$ e f_T up-conservativa $\Rightarrow f_T$ upcast-sicura*
- *f_T iniettiva $\wedge$ f_T down-conservativa $\Leftrightarrow$ f_T downcast-sicura*

Dimostrazione. Dimostriamo le diverse implicazioni:

- $f_{T'}$ iniettiva per ogni $T' \geq T$ e f_T up-conservativa $\Rightarrow f_T$ upcast-sicura [da 1., 1.–(a) e 1.–(a)–i.]

  1. Supponiamo $\forall T' \geq T \, \forall x \in \mathrm{Dom}\, f \, \exists y \in \mathrm{Dom}\, f \ni' f_{T'}(y) = f_T(x)$ [f_T è up-conservativa]
     (a) Supponiamo $f_{T'}$ iniettiva per ogni T'
        i. f_T è upcast-sicura [da ii.]
        ii. $\forall T' \geq T \, \forall x \in \mathrm{Dom}\, f \, \exists \mid y \in \mathrm{Dom}\, f \ni' f_{T'}(y) = f_T(x)$ [da iii., iii.–A. e 1.]
        iii. Sia $z \in \mathrm{Dom}\, f$ tale che $f_{T'}(y) = f_{T'}(z)$
           A. $y = z$ [da (a)]

- f_T iniettiva $\wedge$ f_T down-conservativa $\Rightarrow$ f_T downcast-sicura

  1. Supponiamo $\forall T' \leq T \forall x \in \mathrm{Dom}\, f \exists y \in \mathrm{Dom}\, f \ni' f_{T'}(y) = f_T(x)$ [f_T è down-conservativa]
     (a) Supponiamo $f_{T'}$ iniettiva per ogni T'
        i. f_T è downcast-sicura [da ii.]
        ii. $\forall T' \leq T \, \forall x \in \mathrm{Dom}\, f \, \exists \mid y \in \mathrm{Dom}\, f \ni' f_{T'}(y) = f_T(x)$ [da iii., iii.–A. e 1.]
        iii. Sia $z \in \mathrm{Dom}\, f$ tale che $f_{T'}(y) = f_{T'}(z)$
           A. $y = z$ [da (a)]

- f_T downcast-sicura $\Rightarrow$ f_T iniettiva $\wedge$ f_T down-conservativa [da 1., 1.–(a) e 1.–(b)]

  1. Supponiamo $\forall T' \leq T \, \forall x \in \mathrm{Dom}\, f \, \exists \mid y \in \mathrm{Dom}\, f \ni' f_{T'}(y) = f_T(x)$ [f_T è downcast-sicura]
     (a) f_T è down-conservativa [da 1.]
     (b) f_T è iniettiva [da i.]

i. $\forall x \in \text{Dom } f \, \exists \mid y \in \text{Dom } f \ni' f_T(y) = f_T(x)$ [da 1., ponendo $T' = T$]

□

Si noti che per la prima proprietà non vale l'implicazione inversa "f_T upcast-sicura⇒$f_{T'}$ iniettiva per ogni $T' \geq T$ e f_T up-conservativa", perché in particolare non vale che "f_T upcast-sicura⇒$f_{T'}$ iniettiva per ogni T'". Infatti, supponiamo che esista un tratteggio $T' \geq T$ ed esistano x ed y in Dom f distinti, tali che $f_{T'}(x) = f_{T'}(y) \equiv h$. In questo caso, $f_{T'}$ non è iniettiva, ma ciò non esclude che f_T sia upcast-sicura: basta che non esista nessun valore z tale che $f_T(z) = h$.

Più formalmente, se vale che $\forall T' \geq T \, \forall x, y \in \text{Dom } f : (x \neq y \wedge f_{T'}(x) = f_{T'}(y) \equiv h) \Rightarrow \neg\exists z \in \text{Dom } f : f_T(z) = h$, si può dimostrare che f_T è upcast-sicura, anche qualora $f_{T'}$ non fosse iniettiva. Potevamo scrivere quest'ultima formula al posto di "$f_{T'}$ iniettiva per ogni $T' \geq T$" nella proprietà, e sostituire l'implicazione con una doppia implicazione, ma non lo abbiamo fatto per non appesantire l'enunciato.

Sembra quindi che l'upcast crei più complicazioni del downcast; infatti alcune proprietà, come l'iniettività, se valgono per f_T valgono anche per ogni $f_{T'}$ con $T' \leq T$, ma non è detto che valgano per ogni $f_{T'}$ con $T' \geq T$. Ciò intuitivamente accade perché un sovratratteggio di T ha, in generale, trattini che T non ha, a differenza dei sottotratteggi di T, i cui trattini appartengono tutti anche a T.

Poco fa abbiamo osservato che esistono funzioni fondamentali sempre up-conservative, o sempre down-conservative. Applicando le proprietà appena dimostrate sulla base di quelle osservazioni si conclude:

Proprietà 1.4.

- t_T *è sempre upcast-sicura, ma non sempre downcast-sicura*
- t_valore_T *non è sempre né upcast-sicura, né downcast-sicura*
- t_spazio_T *è sempre downcast-sicura, ma non sempre upcast-sicura*
- $\text{t\_spazio}^{-1}{}_T$ *non è sempre né upcast-sicura, né downcast-sicura*
- t_classe_T *è sempre sia upcast-sicura che downcast-sicura*
- t_valore_diff_T *non è sempre né upcast-sicura, né downcast-sicura*
- t_classe_diff_T *non è sempre né upcast-sicura, né downcast-sicura*

Abbiamo osservato poc'anzi che, se $\mathrm{Up}_x^{T\to T'}(f) \neq \emptyset$, $g(x) \in \mathrm{Up}_x^{T\to T'}(f)$, dove $g \in \mathrm{Spec}\ \mathrm{Up}^{T\to U}(f)$. Ora lo dimostriamo formalmente, in modo da far pratica con le definizioni di questo paragrafo.

Proprietà 1.5. *Siano* $f \in \mathcal{F}$ *e* $T, U \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, *con* $U \geq T$, $u \in$ *Spec* $\mathrm{Up}^{T\to U}(f)$, $d \in$ *Spec* $\mathrm{Down}^{U\to T}(f)$ *e* $x \in$ *Dom* f.

- *Se* $\mathrm{UpCons}^{T\to U}(f)(x) = 1$, $u(x) \in \mathrm{Up}_x^{T\to U}(f)$
- *Se* $\mathrm{DownCons}^{U\to T}(f)(x) = 1$, $d(x) \in \mathrm{Down}_x^{U\to T}(f)$

Dimostrazione. Dimostriamo il secondo punto:

1. $\mathrm{DownCons}^{U\to T}(f)(x) = 1 \Rightarrow d(x) \in \mathrm{Down}_x^{U\to T}(f)$ [da (c) e (c)–i.]
2. Sia $d' \in \mathrm{Down}^{U\to T}(f) : d \leq d'$ [d' esiste perché $d \in \mathrm{Spec}\ \mathrm{Down}^{U\to T}(f)$]
   (a) $d'(x) \neq \bot \Rightarrow d(x) = d'(x)$ [da 2. (in particolare, da $d \leq d'$)]
   (b) $d'(x) \in \mathrm{Down}_x^{U\to T}(f)$ [da 2. (in particolare, da $d' \in \mathrm{Down}^{U\to T}(f)$)]
   (c) Se $\mathrm{DownCons}^{U\to T}(f)(x) = 1$
      i. $d(x) \in \mathrm{Down}_x^{U\to T}(f)$ [da (b) e ii.]
      ii. $d(x) = d'(x)$ [da (a) e iii.]
      iii. $d'(x) \neq \bot$ [da (b) e iv.]
      iv. $\mathrm{Down}_x^{U\to T}(f) \neq \emptyset$ [da 2.]

La prima parte si dimostra in maniera analoga, basta sostituire $\mathrm{Down}^{U\to T}(f)$ con $\mathrm{Up}^{U\to T}(f)$, $\mathrm{Down}_x^{U\to T}(f)$ con $\mathrm{Up}_x^{U\to T}(f)$, $\mathrm{DownCons}^{U\to T}(f)$ con $\mathrm{UpCons}^{U\to T}(f)$ e d con u.

□

La seguente proposizione esprime un legame tra upcast e downcast.

Proposizione 1.1. *Siano* $f \in \mathcal{F}$ *e* $T, U \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, *con* $U \geq T$, $u \in$ *Spec* $\mathrm{Up}^{T\to U}(f)$, $d \in$ *Spec* $\mathrm{Down}^{U\to T}(f)$ *e* $x, y \in$ *Dom* f.

- *Se* f_T *è upcast-sicura e* $\mathrm{DownCons}^{U\to T}(f)(x) = 1$, *allora* $y = d(x) \Rightarrow x = u(y)$
- *Se* f_U *è downcast-sicura e* $\mathrm{UpCons}^{T\to U}(f)(x) = 1$, *allora* $y = u(x) \Rightarrow x = d(y)$

Dimostrazione.

1. Se f_T è upcast-sicura e $\text{DownCons}^{U\to T}(f)(x) = 1$

   (a) $\text{Down}_x^{U\to T}(f) \neq \emptyset$ [da 1. (in particolare, da $\text{DownCons}^{U\to T}(f)(x) = 1$)]

   (b) $\text{Down}_x^{U\to T}(f) = \{z \in \text{Dom } f_T \mid f_U(x) = f_T(z)\}$

   (c) $d(x) \in \text{Down}_x^{U\to T}(f)$ [da 1. (in particolare, da $\text{DownCons}^{U\to T}(f)(x) = 1$), per la proprietà 1.5]

   (d) Sia $y = d(x)$

      i. $x = u(y)$ [da ii. e iii.]

      ii. $u(y) \in \text{Up}_y^{T\to U}(f)$ [da $u \in \text{Spec Up}^{T\to U}(f)$, per la proprietà 1.5]

      iii. $\text{Up}_y^{T\to U}(f) = \{x\}$ [da A. e B.]

         A. $x \in \text{Up}_y^{T\to U}(f)$ [da C.]

         B. $\left|\text{Up}_y^{T\to U}(f)\right| = 1$ [da 1. (in particolare, perché f_T è upcast-sicura)]

         C. $f_U(x) = f_T(y)$ [da (b), (c) e (d)]

La seconda parte si dimostra in maniera analoga, basta sostituire $\text{Down}^{U\to T}(f)$ con $\text{Up}^{U\to T}(f)$, $\text{Down}_x^{U\to T}(f)$ con $\text{Up}_x^{U\to T}(f)$, $\text{DownCons}^{U\to T}(f)$ con $\text{UpCons}^{U\to T}(f)$ e d con u.

□

1.8 Cosa studia la teoria dei tratteggi?

Finora abbiamo introdotto le notazioni e le definizioni fondamentali della teoria dei tratteggi; ora vediamo quali sono i principali problemi oggetto del suo studio.

Posto $f \in \mathcal{F}$, esistono due generalissimi problemi:

- Noto un tratteggio T, calcolare la funzione fondamentale f_T;
- Noto un tratteggio T ed un suo sottotratteggio T', calcolare una funzione qualsiasi appartenente a $\text{Spec Up}^{T'\to T}(f)$ o a $\text{Spec Down}^{T\to T'}(f)$.

Da un certo punto di vista, si tratta di problemi molto semplici: si possono formulare, infatti, semplici algoritmi per risolverli. Ad esempio:

- supponiamo di avere un tratteggio $T \in \mathcal{T}^1$, con insieme delle componenti $\{1\}$, $x \in \mathbb{N}^\star$ e di voler calcolare $\text{t\_spazio}_T(x)$: il problema può essere risolto con l'algoritmo 1.1

- supponiamo di voler calcolare una funzione appartenente a Spec $\mathrm{Up}^{T[1]\to T}$ (t_valore), con $T \in \mathcal{T}^2$ avente insieme delle componenti $\{1,2\}$: possiamo farlo con l'algoritmo 1.2

Algoritmo 1.1 Calcolo di $y = \mathrm{t\_spazio}_T(x)$ con T di primo ordine

Input $T \in \mathcal{T}^1$, $x \in \mathbb{N}^\star$
Output $y = \mathrm{t\_spazio}_T(x)$
  cont_spazi $\leftarrow 0$
  $k \leftarrow 1$
  valore_trattino_precedente $\leftarrow \mathcal{O}_T$
  mentre cont_spazi $< x$ **esegui**
    cont_spazi $\leftarrow$ cont_spazi $+ (|\langle 1,k\rangle|_T -$ valore_trattino_precedente $- 1)$
    valore_trattino_precedente $\leftarrow |\langle 1,k\rangle|_T$
    $k \leftarrow k+1$
  fine mentre
  $y \leftarrow$ valore_trattino_precedente $-$ (cont_spazi $- x + 1$)

Algoritmo 1.2 Calcolo di un $y \in \mathrm{Up}_x^{T[1]\to T}$ (t_valore) con T di secondo ordine

Input $T \in \mathcal{T}^2$, $x \in \mathbb{N}^\star$, $\mathrm{UpCons}^{T[1]\to T}$ (t_valore) $(x) = 1$
Output $y \in \mathrm{Up}_x^{T[1]\to T}$ (t_valore)
  da_trovare $\leftarrow \mathrm{t\_valore}_{T[1]}(x)$
  $y \leftarrow 0$
  trovato $\leftarrow$ F
  mentre non trovato **esegui**
    $y \leftarrow y+1$
    trovato $\leftarrow (\mathrm{t\_valore}_T(y) =$ da_trovare$)$
  fine mentre

Come si evince dagli esempi, è semplice risolvere i problemi della teoria dei tratteggi con degli algoritmi. Ciò che è difficile, ed è lo scopo primario della teoria, è risolverli con *formule non ricorsive, calcolabili in tempo costante.* (si intende costante rispetto alla variabile di interesse per il problema, ad esempio rispetto ad x se si vuole calcolare $\mathrm{t\_spazio}_T(x)$).

Consideriamo l'esempio del calcolo di $\mathrm{t\_spazio}_T(x)$, che abbiamo risolto con l'algoritmo 1.1. Supponiamo che $T \in \mathcal{L}^1$ e che, per ogni $x \in \mathbb{N}$, $T(\langle 1,x\rangle) = cx$, con $c \in \mathbb{N}^\star$. Dimostreremo (teorema 8.1) che:

$$\mathrm{t\_spazio}_T(x) = \left\lfloor \frac{cx-1}{c-1} \right\rfloor$$

Il valore così determinato coincide esattamente con quello calcolato dall'algoritmo. Rispetto a quest'ultimo, la formula:

- Permette di ottenere il risultato in tempo costante rispetto al valore di x;
- È trattabile da un punto di vista matematico: se ne possono studiare le proprietà.

L'algoritmo invece fornisce la risposta in tempo lineare rispetto ad x, ed è difficile studiarne le proprietà.

Lo scopo primario della teoria dei tratteggi, quindi, è trovare formule per calcolare, in tempo costante, ciò che è calcolabile in tempo lineare attraverso dei semplici algoritmi. Le formule ottenute poi, oltre ad essere semplicemente usate, possono essere oggetto di studio ulteriore.

L'unico vantaggio rilevante degli algoritmi rispetto alle formule è la generalità. Infatti, le formule cambiano a seconda della classe di tratteggi considerata; gli algoritmi no. Se si vuole seguire l'approccio basato su formule, quindi, bisogna fissare una particolare classe di tratteggi e risolvere i vari problemi per quella specifica classe di tratteggi; se si cambia classe di tratteggi, bisogna sostanzialmente ricominciare lo studio daccapo.

1.9 Cosa *non* studia (ma potrebbe studiare) la teoria dei tratteggi

I problemi che presenteremo in questo paragrafo potrebbero dar luogo ad estensioni della teoria: non li tratteremo in questo libro.

Abbiamo detto che il problema di calcolare, senza algoritmi, una funzione fondamentale dipende dalla classe di tratteggi considerata. Ci si può chiedere se esiste qualche funzione in grado di calcolare una funzione fondamentale a prescindere dalla classe di tratteggi. Ad esempio, considerando t_spazio_T come funzione fondamentale, potremmo richiedere:

- Una funzione $\Phi : \mathcal{T}^{\overline{\mathbb{N}}^\star} \to [\mathbb{N}^\star \to \mathbb{Z}]$ tale che per ogni $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$ sia $\Phi(T) = \text{t\_spazio}_T$
- Una funzione $\Phi_{\text{down}} : \mathcal{T}^{\overline{\mathbb{N}}^\star} \times \mathcal{T}^{\overline{\mathbb{N}}^\star} \to 2^{[\mathbb{N}^\star \to \mathbb{N}^\star]}$ tale che per ogni $T, T' \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, con $T' \leq T$, sia $\Phi_{\text{down}}(T, T') \in \text{Spec Down}^{T \to T'}(\text{t\_spazio})$
- Una funzione $\Phi_{\text{up}} : \mathcal{T}^{\overline{\mathbb{N}}^\star} \times \mathcal{T}^{\overline{\mathbb{N}}^\star} \to 2^{[\mathbb{N}^\star \to \mathbb{N}^\star]}$ tale che per ogni $T, T' \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, con $T' \geq T$, sia $\Phi_{\text{up}}(T, T') \in \text{Spec Up}^{T \to T'}(\text{t\_spazio})$

Trovare simili funzioni porterebbe la teoria su un piano decisamente più astratto: dallo studio delle funzioni fondamentali per una specifica classe di tratteggi allo

studio delle funzioni fondamentali per classi di tratteggi generiche. In questo libro studieremo diverse classi di tratteggi: se si risolvessero problemi come quelli di sopra, tali studi verrebbero unificati. Tale unificazione comunque non sembra facile, a guidicare dalla diversità (almeno apparente) delle formule che esprimono le funzioni $\Phi(T)$, $\Phi_{\text{down}}(T, T')$ e $\Phi_{\text{up}}(T, T')$ per classi di tratteggi anche molto simili: troveremo esempi di questo fenomeno nel corso del libro.

Capitolo 2

Proprietà del modulo e della parte intera

Una buona teoria matematica è come un buon software:
i servizi di base sono separati da tutto il resto.

Nella teoria dei tratteggi si usano molto spesso le funzioni modulo e parte intera, definite nel capitolo precedente. Perciò, prima di entrare nel vivo della teoria, è opportuno conoscerle meglio. Questo capitolo raccoglie varie proprietà di dette funzioni, che verranno utilizzate nel seguito.

Nel leggere le varie proprietà, è importante ricordarsi che si sta lavorando in $\mathbb{N}$, quindi non esistono inversi rispetto all'addizione. Si può usare l'operazione di sottrazione $a - b$, ma bisogna ricordarsi di controllare sempre che a sia maggiore o uguale di b.

Un'altra cosa che può non sembrare naturale è che i resti delle divisioni, ossia i risultati delle funzioni modulo, sono dei numeri naturali, non delle classi di resto. Bisogna far attenzione a non credere che ciò che vale per le classi di resto vale anche quando si usano le funzioni modulo. Ad esempio, per le classi di resto vale la proprietà:

$$\forall a, k \in \mathbb{N} \forall n \in \mathbb{N}^\star : [a + k]_n = [a]_n + [k]_n$$

Si può essere tentati di credere che per le funzioni modulo valga l'analoga proprietà:

$$\forall a, k \in \mathbb{N} \forall n \in \mathbb{N}^\star : (a + k) \bmod n = (a \bmod n) + (k \bmod n)$$

Ma ciò non è affatto vero. Per verificarlo, basta prendere 3, 4 e 5 come valori di a, k ed n: $(3 + 4) \bmod 5 = 7 \bmod 5 = 2$, ma $(3 \bmod 5) + (4 \bmod 5) = 3 + 4 = 7$.

La proprietà corretta è invece la seguente:

$$\forall a, k \in \mathbb{N} \forall n \in \mathbb{N}^\star : (a + k) \bmod n = ((a \bmod n) + (k \bmod n)) \bmod n$$

Situazioni come questa si verificano molto spesso. Conviene dimenticare le classi di resto e ricordarsi che si sta lavorando con numeri naturali.

2.1 Proprietà del modulo

Vediamo ora alcune proprietà delle funzioni modulo. Nella scelta delle proprietà si è cercato di mantenere un livello di generalità accettabile e di includere, ove possibile, per ogni proprietà una sua "simmetrica" rispetto al qualche criterio (ad esempio l'uso di mod invece di mod*).

Proprietà 2.1. *$\forall a \in \mathbb{N}$, $\forall k \in \mathbb{Z}$, $\forall n \in \mathbb{N}^\star$: $a+kn \geq 0 \Rightarrow a \bmod n = (a + kn) \bmod n$.*

Dimostrazione. La proprietà segue direttamente dalla definizione di modulo. □

Proprietà 2.2. *$\forall a, k \in \mathbb{N}$, $\forall n \in \mathbb{N}^\star$: $(a + k) \bmod n = ((a \bmod n) + k) \bmod n$.*

Dimostrazione.

1. $(a + k) \bmod n =$ [divisione di a per n in $\mathbb{N}$]
   $\left(\left\lfloor \frac{a}{n} \right\rfloor n + a \bmod n + k\right) \bmod n =$ [per la proprietà 2.1]
   $((a \bmod n) + k) \bmod n$

□

Proprietà 2.3. *$\forall k \in \mathbb{N}$, $\forall b, n \in \mathbb{N}^\star$: $b\,(k \bmod n) = bk \bmod bn$.*

Dimostrazione.

1. $b\,(k \bmod n) = bk \bmod bn$ [da (a) e (b), per la divisione in $\mathbb{N}$]

   (a) $bk = bn \left\lfloor \frac{k}{n} \right\rfloor + b\,(k \bmod n)$ [da i., moltiplicando per b]

      i. $k = n \left\lfloor \frac{k}{n} \right\rfloor + (k \bmod n)$ [divisione di k per n in $\mathbb{N}$]

   (b) $b\,(k \bmod n) < bn$ [perché $k \bmod n < n$ e $b > 0$]

□

Nella dimostrazione di questa proprietà si è usata per la prima volta una tecnica che ricorrerà spesso in seguito, in contesti più complessi. Dati qualsiasi $x \in \mathbb{N}$ e $y \in \mathbb{N}^\star$, se dobbiamo dimostrare che un numero $r \in \mathbb{N}$ è il resto della divisione di x per y, cioè se dobbiamo dimostrare che $r = x \bmod y$, dobbiamo provare due cose:

- x si può scrivere nella forma $yq + r$
- $r < x$

Per la definizione di resto, ciò garantisce che $r = x \bmod y$. Nel caso della proprietà precedente, ponendo $x \equiv bk$, $y \equiv bn$ e $r \equiv b\,(k \bmod n)$, si può trovare la corrispondenza di quanto appena detto con la dimostrazione.

Proprietà 2.4. *$\forall a, k \in \mathbb{N}$, $\forall n \in \mathbb{N}^\star$: $(a + k) \bmod n \leq (a \bmod n) + (k \bmod n)$. In particolare:*

- $(a \bmod n) + (k \bmod n) < n \Rightarrow (a + k) \bmod n = (a \bmod n) + (k \bmod n)$
- $(a \bmod n) + (k \bmod n) \geq n \Rightarrow (a + k) \bmod n = (a \bmod n) + (k \bmod n) - n$

Dimostrazione.

1. Se $(a \bmod n) + (k \bmod n) < n$:
   (a) $(a + k) \bmod n = (a \bmod n) + (k \bmod n)$ [da 1., (b), 3. e $0 \leq (a + k) \bmod n < n$]
   (b) $(a \bmod n) + (k \bmod n) - n < 0$
2. Se $(a \bmod n) + (k \bmod n) \geq n$:
   (a) $(a + k) \bmod n = (a \bmod n) + (k \bmod n) - n$ [da 2., 3. e $0 \leq (a + k) \bmod n < n$]
3. $(a + k) \bmod n \in \{(a \bmod n) + (k \bmod n), (a \bmod n) + (k \bmod n) - n\}$ [equivalente a (a)]
   (a) $a \bmod n + k \bmod n - (a + k) \bmod n \in \{0, n\}$ [da i., ii. e iii.]
      i. $a \bmod n + k \bmod n - (a + k) \bmod n < 2n$ [da A.]
         A. $a \bmod n + k \bmod n < 2n$ [perché entrambi gli addendi sono minori di n]

ii. $(a \bmod n + k \bmod n - (a+k) \bmod n) \bmod n =$ [per la proprietà 2.1]
$\left(a \bmod n + n \left\lfloor \frac{a}{n} \right\rfloor + k \bmod n + n \left\lfloor \frac{k}{n} \right\rfloor - (a+k) \bmod n - n \left\lfloor \frac{a+k}{n} \right\rfloor\right) \bmod n =$
[per la divisione in $\mathbb{N}$]
$(a + k - (a+k)) \bmod n =$
$0 \bmod n =$
0

iii. $a \bmod n + k \bmod n - (a+k) \bmod n \geq 0$ [equivalente a A.]
Quindi ha senso considerare la sottrazione $a \bmod n + k \bmod n - (a+k) \bmod n$.

A. $(a+k) \bmod n =$ [divisione di a e k per n in $\mathbb{N}$]
$\left(a \bmod n + k \bmod n + n \left\lfloor \frac{a}{n} \right\rfloor + n \left\lfloor \frac{k}{n} \right\rfloor\right) \bmod n =$ [per la proprietà 2.1]
$(a \bmod n + k \bmod n) \bmod n \leq$
$a \bmod n + k \bmod n$

□

Proprietà 2.5. $\forall a, k \in \mathbb{N}, \forall n \in \mathbb{N}^\star$: $(a+k) \bmod n = 0 \wedge a \bmod n > 0 \Rightarrow a \bmod n + k \bmod n = n$

Dimostrazione.

1. $a \bmod n + k \bmod n = n$
[da (a) e (b), perché n è l'unico multiplo di n compreso tra 1 e $2n-2$]

(a) $n \mid a \bmod n + k \bmod n$ [da i., per definizione]

i. $0 =$ [per ipotesi]
$(a+k) \bmod n =$ [per la proprietà 2.2]
$(a \bmod n + k) \bmod n =$ [per la proprietà 2.2]
$(a \bmod n + k \bmod n) \bmod n$

(b) $1 \leq a \bmod n + k \bmod n \leq 2n-2$ [da i. e ii., per la compatibilità di $\leq$ rispetto alla somma]

i. $0 \leq k \bmod n \leq n-1$

ii. $1 \leq a \bmod n \leq n-1$ [per definizione e dall'ipotesi $a \bmod n > 0$]

□

Proprietà 2.6. $\forall a, k \in \mathbb{N}, \forall n \in \mathbb{N}^\star$: $ak \bmod n = a\,(k \bmod n) \bmod n$.

Dimostrazione.

1. $ak \bmod n = a\,(k \bmod n) \bmod n$ [da 2., e da $ak \bmod n < n$, per la divisione in $\mathbb{N}$]
2. $a\,(k \bmod n) = n\left(\left\lfloor \frac{ak}{n} \right\rfloor - a \left\lfloor \frac{k}{n} \right\rfloor\right) + ak \bmod n$ [da 3., con calcoli algebrici]
3. $0 = n\left(\left\lfloor \frac{ak}{n} \right\rfloor - a \left\lfloor \frac{k}{n} \right\rfloor\right) + (ak \bmod n - a\,(k \bmod n))$ [sottraendo (b) da (a)]
   (a) $ak = n \left\lfloor \frac{ak}{n} \right\rfloor + ak \bmod n$ [divisione di ak per n in $\mathbb{N}$]
   (b) $ak = na \left\lfloor \frac{k}{n} \right\rfloor + a\,(k \bmod n)$ [da i., moltiplicando per a]
      i. $k = n \left\lfloor \frac{k}{n} \right\rfloor + k \bmod n$ [divisione di k per n in $\mathbb{N}$]

□

Proprietà 2.7. $\forall a, c \in \mathbb{N},\ a \geq c,\ \forall b \in \mathbb{N}^\star$:

$$(a-c) \bmod b = \begin{cases} a \bmod b - c \bmod b & \text{se } a \bmod b \geq c \bmod b \\ b - (c \bmod b - a \bmod b) & \text{se } b - (c \bmod b - a \bmod b) \end{cases}$$

Dimostrazione.

1. $(a-c) \bmod b =$ [divisione di a per b]
   $\left(b \left\lfloor \frac{a}{b} \right\rfloor + a \bmod b - c\right) \bmod b =$ [divisione di c per b]
   $\left(b \left\lfloor \frac{a}{b} \right\rfloor + a \bmod b - b \left\lfloor \frac{c}{b} \right\rfloor - c \bmod b\right) \bmod b =$ [da (a), (a)–i., (b) e (b)–i.]
   $\begin{cases} a \bmod b - c \bmod b & \text{se } a \bmod b \geq c \bmod b \\ b - (c \bmod b - a \bmod b) & \text{se } b - (c \bmod b - a \bmod b) \end{cases}$
   (a) Se $a \bmod b \geq c \bmod b$:
      i. $\left(b \left\lfloor \frac{a}{b} \right\rfloor + a \bmod b - b \left\lfloor \frac{c}{b} \right\rfloor - c \bmod b\right) \bmod b =$
      $\left(b \left(\left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor\right) + a \bmod b - c \bmod b\right) \bmod b =$ [per la proprietà 2.1]
      $(a \bmod b - c \bmod b) \bmod b =$ [da ii.]
      $a \bmod b - c \bmod b$
      ii. $0 \leq$ [da (a)]
      $a \bmod b - c \bmod b \leq$ [perché $c \bmod b \geq 0$]
      $a \bmod b <$
      b
   (b) Se $a \bmod b < c \bmod b$:
      i. $\left(b \left\lfloor \frac{a}{b} \right\rfloor + a \bmod b - b \left\lfloor \frac{c}{b} \right\rfloor - c \bmod b\right) \bmod b =$
      $\left(b \left(\left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor - 1\right) + (b - (c \bmod b - a \bmod b))\right) \bmod b =$ [per la proprietà 2.1]
      $((b - (c \bmod b - a \bmod b))) \bmod b =$ [da ii.]
      $b - (c \bmod b - a \bmod b)$

ii. $0 <$ [perché $c \bmod b < b$]
$b - c \bmod b \leq$ [perché $a \bmod b \geq 0$]
$b - (c \bmod b - a \bmod b) \leq$ [da (b)]
$b - 1 <$
b

□

Le proprietà appena viste valgono anche, eventualmente con leggerissime variazioni, usando l'operatore $\bmod^\star$ invece di mod:

Proprietà 2.8. *$\forall a, k \in \mathbb{N}$, $\forall n \in \mathbb{N}^\star$: $a \bmod^\star n = (a + kn) \bmod^\star n$.*

Dimostrazione. Dimostriamo la proprietà nei due casi possibili:

1. Se $a \bmod n > 0$:

   (a) $(a + kn) \bmod^\star n =$ [da (b)]
   $(a + kn) \bmod n =$ [da (c)]
   $a \bmod n =$ [da 1.]
   $a \bmod^\star n$

   (b) $(a + kn) \bmod n > 0$ [da $a \bmod n > 0$ e dalla (c)]

   (c) $a \bmod n = (a + kn) \bmod n$ [proprietà 2.1]

2. Se $a \bmod n = 0$:

   (a) $(a + kn) \bmod^\star n =$ [da (b)]
   $n =$ [da (c)]
   $a \bmod^\star n$

   (b) $(a + kn) \bmod n =$ [per la proprietà 2.1]
   $a \bmod n =$ [da 2.]
   0

   (c) $a \bmod^\star n = n$ [da 2.]

□

Proprietà 2.9. *$\forall k \in \mathbb{N}$, $\forall b, n \in \mathbb{N}^\star$: $b\,(k \bmod^\star n) = bk \bmod^\star bn$.*

Dimostrazione. Dimostriamo la proprietà nei due casi possibili:

1. Se $k \bmod n > 0$:

(a) $b\,(k \bmod^\star n) =$ [da (b)]
$b\,(k \bmod n) =$ [proprietà 2.3]
$bk \bmod bn =$ [da (c)]
$bk \bmod^\star bn$

(b) $k \bmod^\star n = k \bmod n$ [da 1.]

(c) $bk \bmod bn > 0$ [da i. e ii.]

i. $b\,(k \bmod n) > 0$ [da 1. e perché $b > 0$]

ii. $b\,(k \bmod n) = bk \bmod bn$ [proprietà 2.3]

2. Se $k \bmod n = 0$:

(a) $bk \bmod^\star bn =$ [da (b), per definizione]
$n =$ [da 2.]
$k \bmod^\star n$

(b) $bk \bmod bn =$ [per la proprietà 2.3]
$b\,(k \bmod n) =$ [da 2.]
0

□

Proprietà 2.10. $\forall a, k \in \mathbb{N},\ \forall n \in \mathbb{N}^\star$: $(a + k) \bmod^\star n \leq (a \bmod^\star n) + (k \bmod^\star n)$. *In particolare:*

- $(a \bmod^\star n) + (k \bmod^\star n) \leq n \Rightarrow (a + k) \bmod^\star n = (a \bmod^\star n) + (k \bmod^\star n)$
- $(a \bmod^\star n) + (k \bmod^\star n) > n \Rightarrow (a + k) \bmod^\star n = (a \bmod^\star n) + (k \bmod^\star n) - n$

Dimostrazione. Dimostriamo solo i due punti particolari: ciò è sufficiente, dato che questi implicano l'enunciato principale

1. Se $(a \bmod^\star n) + (k \bmod^\star n) \leq n$:

(a) $(a + k) \bmod^\star n = n = (a \bmod^\star n) + (k \bmod^\star n)$ [da (b)–i., (c)–i. e (d)]

(b) Se $a \bmod n + k \bmod n = n$

i. $(a + k) \bmod^\star n =$ [da ii.]
$n =$ [da (e)]
$(a \bmod^\star n) + (k \bmod^\star n)$

ii. $(a + k) \bmod n =$ [per la proprietà 2.4]
$(a \bmod n) + (k \bmod n) - n =$ [da (b)]
0

(c) Se $a \bmod n + k \bmod n < n$

i. $(a + k) \bmod^\star n =$ [da ii.]
$(a + k) \bmod n =$ [da ii.]
$(a \bmod n) + (k \bmod n) =$ [da (e)]
$(a \bmod^\star n) + (k \bmod^\star n)$

ii. $(a + k) \bmod n =$ [per la proprietà 2.4]
$(a \bmod n) + (k \bmod n) <$ [da (c)]
n

(d) Non può essere $a \bmod n + k \bmod n > n$ [da (e) e 1.]

(e) $a \bmod n = a \bmod^\star n \wedge k \bmod n = k \bmod^\star n$ [da i.]

i. $a \bmod n > 0 \wedge k \bmod n > 0$
[infatti $a \bmod n = 0 \Rightarrow a \bmod^\star n = n \Rightarrow k \bmod^\star n \leq 0$, assurdo; analogamente se $k \bmod n = 0$]

2. Se $(a \bmod^\star n) + (k \bmod^\star n) > n$:

(a) $(a + k) \bmod^\star n = (a \bmod^\star n) + (k \bmod^\star n) - n$ [da (b)–i., (c) e (d)–i.]

(b) Se $a \bmod n = 0$:

i. $(a + k) \bmod^\star n = (a \bmod^\star n) + (k \bmod^\star n) - n$ [da iv. e ii.]

ii. $(a + k) \bmod^\star n =$ [da iii.]
$(nt + k) \bmod^\star n =$ [per la proprietà 2.8]
$k \bmod^\star n$

iii. $\exists t : a = nt$ [da (b)]

iv. $a \bmod^\star n = n$ [da (b)]

(c) Se $a \bmod n > 0 \wedge k \bmod n = 0$: analogo al caso $a \bmod n = 0 \wedge k \bmod n > 0$, incluso nel precedente, basta scambiare a e k

(d) Se $a \bmod n > 0 \wedge k \bmod n > 0$

i. $(a + k) \bmod^\star n = (a \bmod^\star n) + (k \bmod^\star n) - n$ [da ii., iii., viii. e vi.]

ii. $(a + k) \bmod n = (a \bmod n) + (k \bmod n) - n$ [da vi., per la proprietà 2.4]

iii. $(a + k) \bmod n = (a + k) \bmod^\star n$ [da iv.]

iv. $(a + k) \bmod n > 0$ [da v., per la proprietà 2.2]

v. $((a \bmod n) + (k \bmod n)) \bmod n > 0$ [da vi. e da $(a \bmod n)+(k \bmod n) < 2n$]

vi. $(a \bmod n) + (k \bmod n) > n$ [da 2., viii. e vii.]

vii. $k \bmod^\star n = k \bmod n$ [da (d)]

viii. $a \bmod^\star n = a \bmod n$ [da (d)]

□

Proprietà 2.11. $\forall a, k \in \mathbb{N}, \forall n \in \mathbb{N}^\star$: $(a + k) \bmod^\star n = ((a \bmod^\star n) + (k \bmod^\star n)) \bmod^\star n$.

Dimostrazione. La proprietà è una conseguenza della precedente.

□

Proprietà 2.12. $\forall a, k \in \mathbb{N}, \forall n \in \mathbb{N}^\star$: $(a + k) \bmod^\star n = n \wedge a \bmod^\star n < n \Rightarrow a \bmod^\star n + k \bmod^\star n = n$

Dimostrazione.

1. $a \bmod^\star n + k \bmod^\star n = n$
   [da 2. e 3., perché n è l'unico multiplo di n compreso tra 2 e $2n - 1$]

2. $n \mid a \bmod^\star n + k \bmod^\star n$ [da (a), per definizione]

   (a) $n =$ [per ipotesi]
   $(a + k) \bmod^\star n =$ per la proprietà 2.11]
   $(a \bmod^\star n + k \bmod^\star n) \bmod^\star n$

3. $2 \leq a \bmod^\star n + k \bmod^\star n \leq 2n - 1$ [da (a) e (b), per la compatibilità di $\leq$ rispetto alla somma]

   (a) $1 \leq k \bmod^\star n \leq n$

   (b) $1 \leq a \bmod^\star n \leq n - 1$ [per definizione e dall'ipotesi $a \bmod^\star n < n$]

□

Proprietà 2.13. $\forall a, k \in \mathbb{N}, \forall n \in \mathbb{N}^\star$: $ak \bmod^\star n = a\,(k \bmod^\star n) \bmod^\star n$.

Dimostrazione.

1. $ak \bmod^\star n = a\,(k \bmod^\star n) \bmod^\star n$ [da 2.–(c) e 3.–(c)]

2. Se $ak \bmod n = 0$:

   (a) $ak \bmod^\star n =$ [da 2.]
   $n =$ [da (c)–i. e (b)–i.]
   $a\,(k \bmod^\star n) \bmod^\star n$

(b) Se $k \bmod n > 0$:

i. $a\,(k \bmod^\star n) \bmod^\star n =$ [da (b)]
$a\,(k \bmod n) \bmod^\star n =$ [da ii.]
n

ii. $a\,(k \bmod n) \bmod n = 0$ [da 4. e 2.]

(c) Se $k \bmod n = 0$:

i. $a\,(k \bmod^\star n) \bmod^\star n =$ [da (c)]
$an \bmod^\star n =$ [dalla definizione di $\bmod^\star$]
n

3. Se $ak \bmod n > 0$:

(a) $ak \bmod^\star n =$ [da 3.]
$ak \bmod n =$ [da (4)]
$a\,(k \bmod n) \bmod n =$ [da (b)]
$a\,(k \bmod n) \bmod^\star n =$ [da (c)]
$a\,(k \bmod^\star n) \bmod^\star n$

(b) $a\,(k \bmod n) \bmod n > 0$ [da 4. e 3.]

(c) $k \bmod n > 0$ [da 4., perché se fosse $k \bmod n = 0$ sarebbe $a\,(k \bmod n) \bmod n = 0 \bmod n = 0$]

4. $ak \bmod n = a\,(k \bmod n) \bmod n$ [per la proprietà 2.6]

□

Proprietà 2.14. $\forall a, k \in \mathbb{N}, \forall n \in \mathbb{N}^\star$: $kn - a \geq 0 \Rightarrow \begin{cases} (kn-a) \bmod n = n - a \bmod^\star n \\ (kn-a) \bmod^\star n = n - a \bmod n \end{cases}$.

Dimostrazione.

1. $(kn-a) \bmod n =$ [divisione di a per n in $\mathbb{N}$]
$\big(kn - \big(a \bmod n + \big\lfloor \frac{a}{n} \big\rfloor n\big)\big) \bmod n =$
[aggiunta e sottrazione di $\big\lfloor \frac{a}{n} \big\rfloor n$; l'espressione ottenuta contiene la sottrazione $k - \big\lfloor \frac{a}{n} \big\rfloor$ che ha senso per 2.]
$\big(\big\lfloor \frac{a}{n} \big\rfloor n + \big(k - \big\lfloor \frac{a}{n} \big\rfloor\big) n - \big(a \bmod n + \big\lfloor \frac{a}{n} \big\rfloor n\big)\big) \bmod n =$ [semplificazione]
$\big(\big(k - \big\lfloor \frac{a}{n} \big\rfloor\big) n - a \bmod n\big) \bmod n =$ [per la proprietà 2.1]
$(n - a \bmod n) \bmod n =$ [da (a), (a)–i., (b), (b)–i.]
$n - a \bmod^\star n$

(a) Se $a \bmod n > 0$:

i. $(n - a \bmod n) \bmod n =$ [da A.]
$n - a \bmod n =$
$n - a \bmod^\star n$

A. $n - a \bmod n < n$ [da B. e $a \bmod^\star n > 0$]

B. $a \bmod n = a \bmod^\star n$ [da (a)]

(b) Se $a \bmod n = 0$:

i. $(n - a \bmod n) \bmod n =$ [da (b)]
$n \bmod n =$
$0 =$
$n - n =$ [da (b), essendo $a \bmod n = 0 \Rightarrow a \bmod^\star n = n$]
$n - a \bmod^\star n$

2. $k - \left\lfloor \frac{a}{n} \right\rfloor \geq 0$ [da (a), per definizione e con calcoli algebrici]

(a) $\frac{kn - a + a \bmod n}{n} \geq 0$ [da (b)]

(b) $kn - a + a \bmod n \geq 0$ [dall'ipotesi $kn - a \geq 0$, e da $a \bmod n \geq 0$]

Per quanto riguarda la seconda proprietà:

1. $(kn - a) \bmod^\star n = n - a \bmod n$ [da (a)]

(a) $a \bmod n =$
$(kn - (kn - a)) \bmod n =$ [per la prima proprietà, sostituendo a con $kn - a$]
$n - (kn - a) \bmod^\star n$

□

Proprietà 2.15. $\forall a \in \mathbb{N}, \forall b, n \in \mathbb{N}^\star$: $\begin{cases} b \bmod^\star n = 1 + (b - 1) \bmod n \\ a \bmod n = (a + 1) \bmod^\star n - 1 \end{cases}$.

Dimostrazione. Per quanto riguarda la prima proprietà, $b \bmod^\star n = 1 + (b - 1) \bmod n$, distinguiamo due casi:

1. Se $b \bmod n = 0$:

(a) $(b - 1) \bmod n =$ [da 1., per la proprietà 2.1]
$n - 1 \bmod^\star n =$
$n - 1 =$ [da 1.]
$b \bmod^\star n - 1$

2. Se $b \bmod n > 0$:

   (a) $b \bmod^\star n =$ [da 2.]
   $b \bmod n =$ [da (b)]
   $1 + (b-1) \bmod n$

   (b) $b \bmod n - 1 = (b-1) \bmod n$ [da (c) e (d)]

   (c) $b \bmod n - 1 < b - 1$ [da $b \bmod n < b$]

   (d) $b - 1 = n \left\lfloor \frac{b}{n} \right\rfloor + (b \bmod n - 1)$ [da i., sottraendo 1 ad ambo i membri]

      i. $b = n \left\lfloor \frac{b}{n} \right\rfloor + b \bmod n$ [divisione di b per n in $\mathbb{N}$]

La seconda proprietà si ottiene dalla prima sostituendo $b - 1$ con a.

□

Proprietà 2.16. $\forall a \in \mathbb{N}$, $\forall b \in \mathbb{N}^\star$: $\begin{cases} (a \bmod^\star b) \bmod b = a \bmod b \\ (a \bmod b) \bmod^\star b = a \bmod^\star b \end{cases}$.

Dimostrazione. Distinguiamo due casi:

1. Se $a \bmod b = 0$:

   (a) $(a \bmod^\star b) \bmod b =$ [da 1.]
   $b \bmod b =$
   $0 =$ [da 1.]
   $a \bmod b$

   (b) $(a \bmod b) \bmod^\star b =$ [da 1.]
   $0 \bmod^\star b =$
   $b =$ [da 1.]
   $a \bmod^\star b$

2. Se $a \bmod b > 0$:

   (a) $(a \bmod^\star b) \bmod b =$ [da 1.]
   $(a \bmod b) \bmod b =$ [da $a \bmod b < b$]
   $a \bmod b$

   (b) $(a \bmod b) \bmod^\star b =$ [da $0 < a \bmod b < b$]
   $(a \bmod b) \bmod b =$ [da $a \bmod b < b$]
   $a \bmod b =$ [da 2.]
   $a \bmod^\star b$

□

2.2 Proprietà della parte intera

Ora vediamo le proprietà delle funzioni parte intera. Per dimostrarle, ci ricondurremo a quelle del modulo. Volendo, avremmo potuto fare il contrario, cioè dimostrare le proprietà del modulo sulla base di quelle della parte intera: sarebbe stato equivalente.

La proprietà forse più intuitiva è quella di monotonia:

Proprietà 2.17. *[Monotonia della parte intera]*

Sia $b \in \mathbb{N}^\star$. *Le funzioni* $\lambda x. \left\lfloor \frac{x}{b} \right\rfloor : \mathbb{N} \to \mathbb{N}$ *e* $\lambda x. \left\lceil \frac{x}{b} \right\rceil : \mathbb{N} \to \mathbb{N}$ *sono crescenti, ossia per ogni* $x, y \in \mathbb{N}$*:*

- $x < y \Rightarrow \left\lfloor \frac{x}{b} \right\rfloor \leq \left\lfloor \frac{y}{b} \right\rfloor$
- $x < y \Rightarrow \left\lceil \frac{x}{b} \right\rceil \leq \left\lceil \frac{y}{b} \right\rceil$

Dimostrazione.

1. $x < y \Rightarrow$ [sottraendo $x \bmod b$ ad ambo i membri]
   $x - x \bmod b < y - x \bmod b \Rightarrow$ [dividendo ambo i membri per b]
   $\frac{x - x \bmod b}{b} < \frac{y - x \bmod b}{b} \Rightarrow$
   $\left\lfloor \frac{x}{b} \right\rfloor < \frac{y - x \bmod b}{b} \Rightarrow$ [aggiungendo e sottraendo $y \bmod b$]
   $\left\lfloor \frac{x}{b} \right\rfloor < \frac{y - y \bmod b}{b} + \frac{y \bmod b - x \bmod b}{b} \Rightarrow$
   $\left\lfloor \frac{x}{b} \right\rfloor < \left\lfloor \frac{y}{b} \right\rfloor + \frac{y \bmod b - x \bmod b}{b} \Rightarrow$ [da (a)]
   $\left\lfloor \frac{x}{b} \right\rfloor < \left\lfloor \frac{y}{b} \right\rfloor + 1 \Rightarrow$
   $\left\lfloor \frac{x}{b} \right\rfloor \leq \left\lfloor \frac{y}{b} \right\rfloor$

   (a) $\frac{y \bmod b - x \bmod b}{b} < 1$ [da (b), dividendo per b]

   (b) $y \bmod b - x \bmod b \leq$ [da $y \bmod b < b$]
   $b - 1 - x \bmod b \leq$ [da $x \bmod b \geq 0$]
   $b - 1 <$
   b

La dimostrazione della seconda parte della proprietà è del tutto analoga.

□

Osserviamo che da $x < y \Rightarrow \left\lfloor \frac{x}{b} \right\rfloor \leq \left\lfloor \frac{y}{b} \right\rfloor$ e $x < y \Rightarrow \left\lceil \frac{x}{b} \right\rceil \leq \left\lceil \frac{y}{b} \right\rceil$ si ottiene, rispettivamente, $x \leq y \Rightarrow \left\lfloor \frac{x}{b} \right\rfloor \leq \left\lfloor \frac{y}{b} \right\rfloor$ e $x \leq y \Rightarrow \left\lceil \frac{x}{b} \right\rceil \leq \left\lceil \frac{y}{b} \right\rceil$: spesso la proprietà precedene è applicata in quest'ultima forma; abbiamo preferito però dimostrare una forma più forte.

Le parti intere non sono solo monotone, ma anche suriettive. Ciò è facile da provare: dato $b \in \mathbb{N}^\star$, per ogni $a \in \mathbb{N}$ è possibile trovare un x tale che $\left\lfloor \frac{x}{b} \right\rfloor = a$ (basta porre $x \equiv ab$) o tale che $\left\lceil \frac{x}{b} \right\rceil = a$ (basta porre $x \equiv ab + (b > 1)$).

È importante avere ben chiaro il comportamento delle funzioni parte intera. Un esempio può aiutare a fissare le idee. Confrontiamo le funzioni $\left\lfloor \frac{x}{b} \right\rfloor$ e $\left\lceil \frac{x}{b} \right\rceil$, ponendo $b \equiv 3$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\left\lfloor \frac{x}{3} \right\rfloor$	0	0	0	1	1	1	2	2	2	3	3	3	4	4	4	5
$\left\lceil \frac{x}{3} \right\rceil$	0	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5

Si può notare che $\left\lceil \frac{x}{3} \right\rceil = \left\lfloor \frac{x+2}{3} \right\rfloor$; in generale $\left\lceil \frac{x}{b} \right\rceil = \left\lfloor \frac{x+b-1}{b} \right\rfloor$.

Le due funzioni assumono lo stesso valore solo per i multipli di b, come sappiamo dalle definizioni. Inoltre, è facile vedere che, confrontando $\left\lfloor \frac{x}{b} \right\rfloor + 1$ e $\left\lceil \frac{x}{b} \right\rceil$, si ottengono valori diversi solo per i multipli di b:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\left\lfloor \frac{x}{b} \right\rfloor + 1$	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5	6
$\left\lceil \frac{x}{b} \right\rceil$	0	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5

Le osservazioni che abbiamo appena fatto sono abbastanza banali, ma è importante averle ben chiare nel seguito.

Proprietà 2.18. $\forall a \in \mathbb{N}$, $\forall b, c \in \mathbb{N}^\star$: $\begin{cases} \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{ca}{cb} \right\rfloor \\ \left\lceil \frac{a}{b} \right\rceil = \left\lceil \frac{ca}{cb} \right\rceil \end{cases}$

Dimostrazione.

1. $\left\lfloor \frac{ca}{cb} \right\rfloor =$
   $\frac{ca - ca \bmod cb}{cb} =$ [per la proprietà 2.3]
   $\frac{ca - c(a \bmod b)}{cb} =$ [semplificazione]
   $\frac{a - a \bmod b}{b} =$
   $\left\lfloor \frac{a}{b} \right\rfloor$

2. $\left\lceil \frac{ca}{cb} \right\rceil =$
   $\frac{ca - ca \bmod^\star cb}{cb} + 1 =$ [per la proprietà 2.9]
   $\frac{ca - c(a \bmod^\star b)}{cb} + 1 =$ [semplificazione]
   $\frac{a - a \bmod^\star b}{b} + 1 =$
   $\left\lceil \frac{a}{b} \right\rceil$

□

Proprietà 2.19. $\forall a \in \mathbb{N},\ \forall k \in \mathbb{Z}, \forall b \in \mathbb{N}^\star\colon\ a + kb \geq 0 \Rightarrow \begin{cases} \left\lfloor \frac{a+kb}{b} \right\rfloor = \left\lfloor \frac{a}{b} \right\rfloor + k \\ \left\lceil \frac{a+kb}{b} \right\rceil = \left\lceil \frac{a}{b} \right\rceil + k \end{cases}$.

Dimostrazione.

1. $\left\lfloor \frac{kb+a}{b} \right\rfloor =$
   $\frac{kb+a-(kb+a) \bmod b}{b} =$ [per la proprietà 2.1]
   $\frac{kb+a-a \bmod b}{b} =$
   $k + \frac{a-a \bmod b}{b} =$
   $k + \left\lfloor \frac{a}{b} \right\rfloor$

2. $\left\lceil \frac{kb+a}{b} \right\rceil =$
   $\frac{kb+a-(kb+a) \bmod^\star b}{b} + 1 =$ [per la proprietà 2.8]
   $\frac{kb+a-a \bmod^\star b}{b} + 1 =$
   $k + \frac{a-a \bmod^\star b}{b} + 1 =$
   $k + \left\lceil \frac{a}{b} \right\rceil$

□

Proprietà 2.20. $\forall a, k \in \mathbb{N},\ \forall b \in \mathbb{N}^\star\colon\ kb \geq a \Rightarrow \begin{cases} \left\lfloor \frac{kb-a}{b} \right\rfloor = k - \left\lceil \frac{a}{b} \right\rceil \\ \left\lceil \frac{kb-a}{b} \right\rceil = k - \left\lfloor \frac{a}{b} \right\rfloor \end{cases}$.

Dimostrazione.

1. $\left\lfloor \frac{kb-a}{b} \right\rfloor =$
   $\frac{kb-a-(kb-a) \bmod b}{b} =$ [per la proprietà 2.14]
   $\frac{kb-a-b+a \bmod^\star b}{b} =$
   $k - \left(\frac{a-a \bmod^\star b}{b} + 1\right) =$
   $k - \left\lceil \frac{a}{b} \right\rceil$

2. $\left\lceil \frac{kb-a}{b} \right\rceil =$
   $\frac{kb-a-(kb-a) \bmod^\star b}{b} + 1 =$ [per la proprietà 2.14]
   $\frac{kb-a-b+a \bmod b}{b} + 1 =$
   $k - \left(\frac{a-a \bmod b}{b}\right) =$
   $k - \left\lfloor \frac{a}{b} \right\rfloor$

□

Proprietà 2.21. $\forall a, k \in \mathbb{N},\ \forall b \in \mathbb{N}^\star\colon \begin{cases} \left\lfloor \frac{a+k}{b} \right\rfloor = \left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{k+a \bmod b}{b} \right\rfloor \\ \left\lceil \frac{a+k}{b} \right\rceil = \left\lfloor \frac{a}{b} \right\rfloor + \left\lceil \frac{k+a \bmod b}{b} \right\rceil \end{cases}$.

In particolare, se $k = 1$*:* $\begin{cases} \left\lfloor \frac{a+1}{b} \right\rfloor = \left\lfloor \frac{a}{b} \right\rfloor + (a \bmod b = b-1) \\ \left\lceil \frac{a+1}{b} \right\rceil = \left\lfloor \frac{a}{b} \right\rfloor + 1 = \left\lceil \frac{a}{b} \right\rceil + (a \bmod b = 0) \end{cases}$.

Dimostrazione. Dimostriamo prima la parte riguardante la parte intera per eccesso:

1. $\left\lceil \frac{a+k}{b} \right\rceil = \left\lfloor \frac{a}{b} \right\rfloor + \left\lceil \frac{k+a \bmod b}{b} \right\rceil$ [da (a), dividendo tutto per b]
   (a) $\left\lceil \frac{a+k}{b} \right\rceil b = \left\lfloor \frac{a}{b} \right\rfloor b + \left\lceil \frac{k+a \bmod b}{b} \right\rceil b$ [da (b), per definizione]
   (b) $\left\lceil \frac{a+k}{b} \right\rceil b = \left\lfloor \frac{a}{b} \right\rfloor b + \left(\frac{k+a \bmod b - (k+a \bmod b) \bmod^\star b}{b} + 1 \right) b$ [da (c), calcoli algebrici]
   (c) $\left\lceil \frac{a+k}{b} \right\rceil b = \left\lfloor \frac{a}{b} \right\rfloor b + k + a \bmod b - (k + a \bmod b) \bmod^\star b + b$ [da (d), per la proprietà 2.2]
   (d) $\left\lceil \frac{a+k}{b} \right\rceil b = \left\lfloor \frac{a}{b} \right\rfloor b + k + a \bmod b - (a + k) \bmod^\star b + b$ [da (e), riordinando]
   (e) $\left\lfloor \frac{a}{b} \right\rfloor b + a \bmod b + k = \left\lceil \frac{a+k}{b} \right\rceil b - b + (a + k) \bmod^\star b$ [sostituendo i. in ii.]
      i. $a = \left\lfloor \frac{a}{b} \right\rfloor b + a \bmod b$ [divisione di a per b in $\mathbb{N}$]
      ii. $a + k = \left\lceil \frac{a+k}{b} \right\rceil b - b + (a + k) \bmod^\star b$ [da iii.]
      iii. $a + k = \left(\frac{a+k-(a+k) \bmod^\star b}{b} + 1 \right) b - b + (a + k) \bmod^\star b$

2. Se $k = 1$
   (a) $\left\lceil \frac{a+1}{b} \right\rceil =$
   $\left\lfloor \frac{a}{b} \right\rfloor + \left\lceil \frac{1+a \bmod b}{b} \right\rceil =$
   $\left\lfloor \frac{a}{b} \right\rfloor + 1$
      i. $1 =$
      $\left\lceil \frac{1}{b} \right\rceil \leq$ [perché $1 \leq 1 + a \bmod b$ e per monotonia]
      $\left\lceil \frac{1+a \bmod b}{b} \right\rceil \leq$ [perché $a \bmod b \leq b - 1$ e per monotonia]
      $\left\lceil \frac{1+b-1}{b} \right\rceil =$
      $\left\lceil \frac{b}{b} \right\rceil =$
      1
   (b) $\left\lfloor \frac{a}{b} \right\rfloor + 1 = \left\lceil \frac{a}{b} \right\rceil + (a \bmod b = 0)$ [da i., riordinando]
      i. $\left\lceil \frac{a}{b} \right\rceil = \left\lfloor \frac{a}{b} \right\rfloor + 1 - (a \bmod b = 0)$ [da A. e B.]
         A. $\left\lceil \frac{a}{b} \right\rceil = \left\lfloor \frac{a}{b} \right\rfloor + (a \bmod b > 0)$
         B. $(a \bmod b > 0) = 1 - (a \bmod b = 0)$ [essendo $\neg (a \bmod b > 0) \Leftrightarrow (a \bmod b = 0)$]

Vediamo ora le analoghe proprietà della parte intera per difetto:

1. $\left\lfloor \frac{a+k}{b} \right\rfloor =$ [da 2.–(a) della parte precedente]
   $\left\lceil \frac{a+k+1}{b} \right\rceil - 1 =$ [da 1. della parte precedente]
   $\left\lfloor \frac{a}{b} \right\rfloor + \left\lceil \frac{k+1+a \bmod b}{b} \right\rceil - 1 =$ [da 2.–(a) della parte precedente]
   $\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{k+a \bmod b}{b} \right\rfloor$

2. Se $k = 1$

   (a) $\left\lfloor \frac{1+a}{b} \right\rfloor =$ [per la prima proprietà]
   $\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{1+a \bmod b}{b} \right\rfloor =$ [da i.–A. e ii.–A.]
   $\left\lfloor \frac{a}{b} \right\rfloor + (a \bmod b = b - 1)$

      i. Se $a \bmod b < b - 1$

         A. $\left\lfloor \frac{1+a \bmod b}{b} \right\rfloor = 0$ [da B.]

         B. $0 \leq$
         $\left\lfloor \frac{1+a \bmod b}{b} \right\rfloor <$ [da i., per monotonia]
         $\left\lfloor \frac{1+b-1}{b} \right\rfloor =$
         $\left\lfloor \frac{b}{b} \right\rfloor =$
         1

      ii. Se $a \bmod b = b - 1$

         A. $\left\lfloor \frac{1+a \bmod b}{b} \right\rfloor =$ [da ii.]
         $\left\lfloor \frac{1+b-1}{b} \right\rfloor =$
         $\left\lfloor \frac{b}{b} \right\rfloor =$
         1

□

Si noti che la proprietà 2.19, quando $k \geq 0$, è un caso particolare della 2.21. Tuttavia, mentre la prima vale anche per $k < 0$, la seconda vale solo per $k \in \mathbb{N}$.

Proprietà 2.22. $\forall a, c \in \mathbb{N}, \forall b \in \mathbb{N}^\star$*:*
$\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a+c-c \bmod b}{b} \right\rfloor = \left\lfloor \frac{a+c-a \bmod b}{b} \right\rfloor = \left\lfloor \frac{a+c}{b} \right\rfloor - (a \bmod b + c \bmod b \geq b)$
$a \geq c \Rightarrow \left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a-c+c \bmod b}{b} \right\rfloor = \left\lceil \frac{a-c-a \bmod b}{b} \right\rceil = \left\lfloor \frac{a-c}{b} \right\rfloor + (a \bmod b < c \bmod b)$

Dimostrazione.

1. $\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a+c-c \bmod b}{b} \right\rfloor = \left\lfloor \frac{a+c-a \bmod b}{b} \right\rfloor = \left\lfloor \frac{a+c}{b} \right\rfloor - (a \bmod b + c \bmod b \geq b)$ [da (a), (b) e (c)]

   (a) $\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor =$ [per la proprietà 2.19]
   $\left\lfloor \frac{a+b\left\lfloor \frac{c}{b} \right\rfloor}{b} \right\rfloor =$
   $\left\lfloor \frac{a+b\frac{c-c \bmod b}{b}}{b} \right\rfloor =$
   $\left\lfloor \frac{a+c-c \bmod b}{b} \right\rfloor$

   (b) $\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor =$ [per commutatività]
   $\left\lfloor \frac{c}{b} \right\rfloor + \left\lfloor \frac{a}{b} \right\rfloor =$ [per la proprietà 2.19]

$\left\lfloor \frac{c+b\left\lfloor \frac{a}{b} \right\rfloor}{b} \right\rfloor =$
$\left\lfloor \frac{c+b\frac{a-a \bmod b}{b}}{b} \right\rfloor =$
$\left\lfloor \frac{c+a-a \bmod b}{b} \right\rfloor =$ [per commutatività]
$\left\lfloor \frac{a+c-a \bmod b}{b} \right\rfloor$

(c) $\left\lfloor \frac{a+c-a \bmod b}{b} \right\rfloor =$ [per la proprietà 2.21]
$\left\lfloor \frac{a+c}{b} \right\rfloor - \left\lfloor \frac{a \bmod b+(a+c-a \bmod b) \bmod b}{b} \right\rfloor =$ [per la proprietà 2.1, essendo $a - a \bmod b$ multiplo di b]
$\left\lfloor \frac{a+c}{b} \right\rfloor - \left\lfloor \frac{a \bmod b+c \bmod b}{b} \right\rfloor =$ [da i.–A. e ii.–A.]
$\left\lfloor \frac{a+c}{b} \right\rfloor - (a \bmod b + c \bmod b \geq b)$

i. Se $a \bmod b + c \bmod b < b$:

A. $\left\lfloor \frac{a \bmod b+c \bmod b}{b} \right\rfloor = 0$ [da i., per definizione]

ii. Se $a \bmod b + c \bmod b \geq b$:

A. $\left\lfloor \frac{a \bmod b+c \bmod b}{b} \right\rfloor = 1$ [da B. e C.]

B. $\left\lfloor \frac{a \bmod b+c \bmod b}{b} \right\rfloor \geq$ [da ii., per monotonia]
$\left\lfloor \frac{b}{b} \right\rfloor =$
1

C. $\left\lfloor \frac{a \bmod b+c \bmod b}{b} \right\rfloor \leq$ [da D., per monotonia]
$\left\lfloor \frac{2b-1}{b} \right\rfloor =$ [per la proprietà 2.20]
$2 - \left\lceil \frac{1}{b} \right\rceil =$
$2 - 1 =$
1

D. $a \bmod b + c \bmod b < 2b - 1$ [perché $a \bmod b < b$ e $c \bmod b \leq b - 1$]

2. $a \geq c \Rightarrow \left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a-c+c \bmod b}{b} \right\rfloor = \left\lceil \frac{a-c-a \bmod b}{b} \right\rceil = \left\lfloor \frac{a-c}{b} \right\rfloor + (a \bmod b < c \bmod b)$ [da (a), (b) e (c)]

(a) $\left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a-c+c \bmod b}{b} \right\rfloor$ [analogo a 1.–(a)]

(b) $\left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor = \left\lceil \frac{a-c-a \bmod b}{b} \right\rceil$ [analogo a 2.–(a)]

(c) $\left\lfloor \frac{a}{b} \right\rfloor - \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a-c}{b} \right\rfloor + (a \bmod b < c \bmod b)$ [da i., calcoli algebrici]

i. $\left\lfloor \frac{a-c}{b} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a}{b} \right\rfloor - (a \bmod b < c \bmod b)$ [da ii. e iii.]

ii. $\left\lfloor \frac{a-c}{b} \right\rfloor + \left\lfloor \frac{c}{b} \right\rfloor = \left\lfloor \frac{a}{b} \right\rfloor - ((a-c) \bmod b + c \bmod b \geq b)$ [per la 1., sostituendo a con $a - c$]

iii. $((a-c) \bmod b + c \bmod b \geq b) = (a \bmod b < c \bmod b)$ [da iv., iv.–A., v., v.–A.]

iv. Se $a \bmod b \geq c \bmod b$:

A. $((a-c) \bmod b + c \bmod b \geq b) =$ [da iv., per la proprietà 2.7]
$(a \bmod b - c \bmod b + c \bmod b \geq b) =$
$(a \bmod b \geq b) =$
0

v. Se $a \bmod b < c \bmod b$:

A. $((a-c) \bmod b + c \bmod b \geq b) =$ [da v., per la proprietà 2.7]
$(b - (c \bmod b - a \bmod b) + c \bmod b \geq b) =$
$(a \bmod b \geq 0) =$
1

□

Proprietà 2.23. $\forall a, k \in \mathbb{N}, \forall b \in \mathbb{N}^{\star}$: $\begin{cases} \left\lfloor \frac{a}{b} \right\rfloor = k \Leftrightarrow bk \leq a < b(k+1) \\ \left\lceil \frac{a}{b} \right\rceil = k \Leftrightarrow b(k-1) < a \leq bk \end{cases}$.

Dimostrazione.

1. $\left\lfloor \frac{a}{b} \right\rfloor = k \Leftrightarrow bk \leq a < b(k+1)$ [da (a) e (b)]

   (a) $bk \leq a < b(k+1) \Leftrightarrow$
   $bk \leq a \leq b(k+1) - 1 \Rightarrow$ [per monotonia]
   $\left\lfloor \frac{bk}{b} \right\rfloor \leq \left\lfloor \frac{a}{b} \right\rfloor \leq \left\lfloor \frac{b(k+1)-1}{b} \right\rfloor \Leftrightarrow$
   $k \leq \left\lfloor \frac{a}{b} \right\rfloor \leq \left\lfloor \frac{b(k+1)-1}{b} \right\rfloor \Leftrightarrow$ [da i.]
   $k \leq \left\lfloor \frac{a}{b} \right\rfloor \leq k \Leftrightarrow$
   $\left\lfloor \frac{a}{b} \right\rfloor = k$

   i. $\left\lfloor \frac{b(k+1)-1}{b} \right\rfloor =$ [per la proprietà 2.20]
   $k + 1 - \left\lceil \frac{1}{b} \right\rceil =$
   $k + 1 - 1 =$
   k

   (b) $\left\lfloor \frac{a}{b} \right\rfloor = k \Rightarrow bk \leq a < b(k+1)$ [da (c)]

   (c) $\neg(bk \leq a < b(k+1)) \Rightarrow \left\lfloor \frac{a}{b} \right\rfloor \neq k$ [da (d)]

   (d) $a \geq b(k+1) \vee a \leq bk - 1 \Rightarrow \left\lfloor \frac{a}{b} \right\rfloor \neq k$ [da i. e ii.]

   i. $a \geq b(k+1) \Rightarrow$ [per monotonia]
   $\left\lfloor \frac{a}{b} \right\rfloor \geq \left\lfloor \frac{b(k+1)}{b} \right\rfloor \Rightarrow$ [da A.]
   $\left\lfloor \frac{a}{b} \right\rfloor \geq k + 1 \Rightarrow$
   $\left\lfloor \frac{a}{b} \right\rfloor \neq k$

   A. $\left\lfloor \frac{b(k+1)}{b} \right\rfloor = k + 1$

ii. $a \leq bk - 1 \Rightarrow$ [per monotonia]
$\left\lfloor \frac{a}{b} \right\rfloor \leq \left\lfloor \frac{bk-1}{b} \right\rfloor \Rightarrow$ [da A.]
$\left\lfloor \frac{a}{b} \right\rfloor \leq k - 1 \Rightarrow$
$\left\lfloor \frac{a}{b} \right\rfloor \neq k$

A. $\left\lfloor \frac{bk-1}{b} \right\rfloor =$ [per la proprietà 2.20]
$k - \left\lceil \frac{1}{b} \right\rceil =$
$k - 1$

Per quanto riguarda la seconda parte della proprietà:

1. $\left\lceil \frac{a}{b} \right\rceil = k \Leftrightarrow b\,(k-1) < a \leq bk$ [da (a)–i., (b)–i. e (b)–ii.]

   (a) Se $a > 0$

   i. $\left\lceil \frac{a}{b} \right\rceil = k \Leftrightarrow$ [per la proprietà 2.21]
   $\left\lfloor \frac{a-1}{b} \right\rfloor + 1 = k \Leftrightarrow$
   $\left\lfloor \frac{a-1}{b} \right\rfloor = k - 1 \Leftrightarrow$ [per la prima parte della proprietà]
   $b\,(k-1) \leq a - 1 < b\,((k-1)+1) \Leftrightarrow$
   $b\,(k-1) \leq a - 1 < bk \Leftrightarrow$
   $b\,(k-1) + 1 \leq a < bk + 1 \Leftrightarrow$
   $b\,(k-1) < a \leq bk$

   (b) Se $a = 0$

   i. $b\,(k-1) < a \leq bk \Rightarrow$
   $b\,(k-1) < a \Rightarrow$ [da (b)]
   $b\,(k-1) < 0 \Rightarrow$ [perché $b \in \mathbb{N}^\star$]
   $k - 1 < 0 \Rightarrow$
   $k < 1 \Rightarrow$ [perché $k \in \mathbb{N}$]
   $k = 0 \Leftrightarrow$
   $\left\lceil \frac{0}{b} \right\rceil = k \Rightarrow$ [da (b)]
   $\left\lceil \frac{a}{b} \right\rceil = k$

   ii. $\left\lceil \frac{a}{b} \right\rceil = k \Leftrightarrow$ [da (b)]
   $\left\lceil \frac{0}{b} \right\rceil = k \Leftrightarrow$
   $k = 0 \Rightarrow$
   $b\,(k-1) < 0 = bk \Rightarrow$
   $b\,(k-1) < 0 \leq bk \Rightarrow$ [da (b)]
   $b\,(k-1) < a \leq bk$

□

Si noti che la seconda parte della dimostrazione precedente è complicata parecchio dal caso $a = 0$, che è piuttosto banale. Ciò però è necessario, perché la parte intera è definita solo su $\mathbb{N}$ (non su $\mathbb{Z}$), quindi la scrittura $\left\lfloor \frac{a-1}{b} \right\rfloor$ ha senso solo se $a > 0$. I due casi, $a > 0$ e $a = 0$, sarebbero unificati se si ponesse $\left\lfloor \frac{-1}{b} \right\rfloor = -1$, ma le conseguenze di ciò sul resto della teoria devono ancora essere indagate a fondo. Comunque, la complicazione del caso $a = 0$ può essere evitata anche senza cambiamenti così radicali, come vedremo nella dimostrazione della prossima proprietà.

Osservazione 2.1. $\forall k \in \mathbb{N}$, $\forall b \in \mathbb{N}^\star$: $bk = \min\limits_{\left\lfloor \frac{a}{b} \right\rfloor = k} a = \max\limits_{\left\lceil \frac{a}{b} \right\rceil = k} a = 1 + \max\limits_{\left\lfloor \frac{a}{b} \right\rfloor = k-1} a = -1 + \min\limits_{\left\lceil \frac{a}{b} \right\rceil = k+1} a$.

Dimostrazione. Il risultato segue direttamente dalla proprietà 2.23.

□

Proprietà 2.24. $\forall a, k \in \mathbb{N}$, $\forall b \in \mathbb{N}^\star$:

- $\left\lfloor \frac{a}{b} \right\rfloor > k \Leftrightarrow a \geq b\,(k+1)$
- $\left\lfloor \frac{a}{b} \right\rfloor \geq k \Leftrightarrow a \geq bk$
- $\left\lceil \frac{a}{b} \right\rceil > k \Leftrightarrow a \geq bk + 1$
- $\left\lceil \frac{a}{b} \right\rceil \geq k \Leftrightarrow a \geq b\,(k-1) + 1$

Dimostrazione.

1. $\left\lceil \frac{a}{b} \right\rceil > k \Leftrightarrow a \geq bk + 1$ [da (a) e (b)]

   (a) $a \geq bk + 1 \Rightarrow$ [per monotonia]
   $\left\lceil \frac{a}{b} \right\rceil \geq \left\lceil \frac{bk+1}{b} \right\rceil \Rightarrow$ [per la proprietà 2.19]
   $\left\lceil \frac{a}{b} \right\rceil \geq k + \left\lceil \frac{1}{b} \right\rceil \Rightarrow$
   $\left\lceil \frac{a}{b} \right\rceil \geq k + 1 \Rightarrow$
   $\left\lfloor \frac{a}{b} \right\rfloor > k$

   (b) $a \leq bk \Rightarrow$ [da ii.]
   $\left\lceil \frac{a}{b} \right\rceil \leq \left\lceil \frac{bk}{b} \right\rceil \Rightarrow$
   $\left\lceil \frac{a}{b} \right\rceil \leq k$

2. $\left\lfloor \frac{a}{b} \right\rfloor > k \Leftrightarrow$ [per la proprietà 2.21]
   $\left\lceil \frac{a+1}{b} \right\rceil - 1 > k \Leftrightarrow$
   $\left\lceil \frac{a+1}{b} \right\rceil > k + 1 \Leftrightarrow$ [da 1.]
   $a + 1 \geq b\,(k+1) + 1 \Leftrightarrow$
   $a \geq b\,(k+1)$

3. $\left\lfloor \frac{a}{b} \right\rfloor \geq k \Leftrightarrow$
   $\left\lfloor \frac{a}{b} \right\rfloor > k-1 \Leftrightarrow$ [da 1.]
   $a \geq bk$

4. $\left\lceil \frac{a}{b} \right\rceil \geq k \Leftrightarrow$
   $\left\lceil \frac{a}{b} \right\rceil > k-1 \Leftrightarrow$ [da 2.]
   $a \geq b\,(k-1)+1$

□

Come già anticipato, la dimostrazione appena svolta è molto più pulita della precedente, perché si è dimostrata prima la proprietà della parte intera per eccesso e, sulla base di questa, quella della parte intera per difetto.

Osservazione 2.2. $\forall a, k \in \mathbb{N},\ \forall b \in \mathbb{N}^\star$: $\begin{cases} a \geq b\,(k+1) \Leftrightarrow a > bk + a \bmod b \\ a \geq b\,(k+1)+1 \Leftrightarrow a > bk + a \bmod^\star b \end{cases}$

Dimostrazione.

1. $a \geq b\,(k+1) \Leftrightarrow$ [per la proprietà 2.24]
   $\left\lfloor \frac{a}{b} \right\rfloor > k \Leftrightarrow$
   $\frac{a - a \bmod b}{b} > k \Leftrightarrow$
   $a > bk + a \bmod b$

2. $a \geq b\,(k+1)+1 \Leftrightarrow$ [per la proprietà 2.24]
   $\left\lceil \frac{a}{b} \right\rceil > k+1 \Leftrightarrow$
   $\frac{a - a \bmod^\star b}{b} + 1 > k+1 \Leftrightarrow$
   $a > bk + a \bmod^\star b$

□

L'osservazione precedente, pur essendo solamente una forma diversa per esprimere la proprietà 2.24, sembra molto meno intuitiva, in particolare nelle implicazioni verso sinistra: $a > bk + a \bmod b \Rightarrow a \geq b\,(k+1)$ e $a > bk + a \bmod^\star b \Rightarrow a \geq b\,(k+1)+1$. Con poca attenzione si può affermare che $a > bk + a \bmod b \Rightarrow a > bk$, perché $a \bmod b \geq 0$, mentre in realtà $a > bk + a \bmod b \Rightarrow a \geq b\,(k+1)$, ed analogamente si può argomentare per l'altra disuguaglianza. Ovviamente l'"inganno" sta nel fatto che $a \bmod b$ dipende dalle stesse variabili a e b utilizzate nella disuguaglianza, quindi non lo si può togliere tanto facilmente se non si vogliono fare maggiorazioni grossolane. È importante che il lettore familiarizzi con queste proprietà "strane" prima di passare ai capitoli successivi.

Proprietà 2.25. $\forall a, k \in \mathbb{N},\ \forall b \in \mathbb{N}^\star$:

- $\left\lfloor \frac{a}{b} \right\rfloor < k \Leftrightarrow a \leq bk - 1$
- $\left\lfloor \frac{a}{b} \right\rfloor \leq k \Leftrightarrow a \leq b\,(k+1) - 1$
- $\left\lceil \frac{a}{b} \right\rceil < k \Leftrightarrow a \leq b\,(k-1)$
- $\left\lceil \frac{a}{b} \right\rceil \leq k \Leftrightarrow a \leq bk$

Dimostrazione.

1. $\left\lfloor \frac{a}{b} \right\rfloor < k \Leftrightarrow$
   $\neg\left(\left\lfloor \frac{a}{b} \right\rfloor > k \vee \left\lfloor \frac{a}{b} \right\rfloor = k\right) \Leftrightarrow$ [per le proprietà 2.23 e 2.24]
   $\neg\left(a \geq b\,(k+1) \vee bk \leq a < b\,(k+1)\right) \Leftrightarrow$
   $\neg\left(bk \leq a\right) \Leftrightarrow$
   $a \leq bk - 1$

2. $\left\lceil \frac{a}{b} \right\rceil < k \Leftrightarrow$
   $\neg\left(\left\lceil \frac{a}{b} \right\rceil > k \vee \left\lceil \frac{a}{b} \right\rceil = k\right) \Leftrightarrow$ [per le proprietà 2.23 e 2.24]
   $\neg\left(a \geq bk + 1 \vee b\,(k-1) < a \leq bk\right) \Leftrightarrow$
   $\neg\left(b\,(k-1) < a\right) \Leftrightarrow$
   $a \leq b\,(k-1)$

3. $\left\lfloor \frac{a}{b} \right\rfloor \leq k \Leftrightarrow$
   $\left\lfloor \frac{a}{b} \right\rfloor < k + 1 \Leftrightarrow$ [da 1.]
   $a \leq b\,(k+1) - 1$

4. $\left\lceil \frac{a}{b} \right\rceil \leq k \Leftrightarrow$
   $\left\lceil \frac{a}{b} \right\rceil < k + 1 \Leftrightarrow$ [da 2.]
   $a \leq bk$

□

Osservazione 2.3. $\forall a, k \in \mathbb{N},\ \forall b \in \mathbb{N}^{\star}$: $\begin{cases} a \leq bk - 1 \Leftrightarrow a < bk + a \bmod b \\ a \leq bk \Leftrightarrow a < bk + a \bmod^{\star} b \end{cases}$

Dimostrazione.

1. $a \leq bk - 1 \Leftrightarrow$ [per la proprietà 2.24]
   $\left\lfloor \frac{a}{b} \right\rfloor < k \Leftrightarrow$
   $\frac{a - a \bmod b}{b} < k \Leftrightarrow$
   $a < bk + a \bmod b$

2. $a \leq bk \Leftrightarrow$ [per la proprietà 2.24]
   $\left\lceil \frac{a}{b} \right\rceil < k + 1 \Leftrightarrow$
   $\frac{a - a \bmod^{\star} b}{b} + 1 < k + 1 \Leftrightarrow$
   $a < bk + a \bmod^{\star} b$

□

Per l'ultima osservazione è possibile fare considerazioni analoghe a quelle dell'osservazione 2.2. Questa volta le implicazioni poco intuitive sono quelle verso destra.

Proprietà 2.26. $\forall k \in \mathbb{N},\ \forall b, c, n, x \in \mathbb{N}^\star$:

$$\begin{cases} c\,(n-1) \pm k \geq 0 \wedge bx \mp k > 0 \Rightarrow \left(\left\lfloor \frac{c(n-1)\pm k}{b} \right\rfloor < x \leq \left\lfloor \frac{cn \pm k}{b} \right\rfloor \Leftrightarrow n = \left\lceil \frac{bx \mp k}{c} \right\rceil \right) \\ cn \pm k \geq 0 \wedge b\,(x-1) \mp k > 0 \Rightarrow \left(\left\lceil \frac{cn \pm k}{b} \right\rceil < x \leq \left\lceil \frac{c(n+1)\pm k}{b} \right\rceil \Leftrightarrow n = \left\lfloor \frac{b(x-1)\mp k}{c} \right\rfloor \right) \end{cases}$$

Dimostrazione.

1. $\left\lceil \frac{cn\pm k}{b} \right\rceil < x \leq \left\lceil \frac{c(n+1)\pm k}{b} \right\rceil \Leftrightarrow$ [da (a) e (b)]
2. $cn \leq b\,(x-1) \mp k < c\,(n+1) \Leftrightarrow$ [per la proprietà 2.23]
   $n = \left\lfloor \frac{b(x-1)\mp k}{c} \right\rfloor$
   (a) $\left\lceil \frac{cn\pm k}{b} \right\rceil < x \Leftrightarrow$ [per la proprietà 2.25]
   $cn \pm k \leq b\,(x-1) \Leftrightarrow$
   $cn \leq b\,(x-1) \mp k$
   (b) $x \leq \left\lceil \frac{c(n+1)\pm k}{b} \right\rceil \Leftrightarrow$
   $\neg \left(x > \left\lceil \frac{c(n+1)\pm k}{b} \right\rceil \right) \Leftrightarrow$ [per la proprietà 2.25]
   $\neg\,(c\,(n+1) \pm k \leq b\,(x-1)) \Leftrightarrow$
   $b\,(x-1) < c\,(n+1) \pm k \Leftrightarrow$
   $b\,(x-1) \mp k < c\,(n+1)$
3. $\left\lfloor \frac{c(n-1)\pm k}{b} \right\rfloor < x \leq \left\lfloor \frac{cn\pm k}{b} \right\rfloor \Leftrightarrow$ [per la proprietà 2.21]
   $\left\lceil \frac{c(n-1)\pm k+1}{b} \right\rceil - 1 < x \leq \left\lceil \frac{cn\pm k+1}{b} \right\rceil - 1 \Leftrightarrow$
   $\left\lceil \frac{c(n-1)\pm k+1}{b} \right\rceil < x+1 \leq \left\lceil \frac{cn\pm k+1}{b} \right\rceil \Leftrightarrow$ [da 1.]
   $n - 1 = \left\lfloor \frac{bx\mp k-1}{c} \right\rfloor \Leftrightarrow$ [per la proprietà 2.21]
   $n = \left\lceil \frac{bx\mp k}{c} \right\rceil$

□

Proprietà 2.27. $\forall a, k \in \mathbb{N},\ \forall n \in \mathbb{N}^\star$: $\begin{cases} \left\lfloor \frac{ak}{n} \right\rfloor - a \left\lfloor \frac{k}{n} \right\rfloor = \left\lfloor \frac{a(k \bmod n)}{n} \right\rfloor \\ a \left\lceil \frac{k}{n} \right\rceil - \left\lceil \frac{ak}{n} \right\rceil = a - \left\lceil \frac{a(k \bmod^\star n)}{n} \right\rceil \end{cases}$.

Dimostrazione.

1. $\left\lfloor \frac{ak}{n} \right\rfloor - a \left\lfloor \frac{k}{n} \right\rfloor = \left\lfloor \frac{a(k \bmod n)}{n} \right\rfloor$ [da (a), per definizione]
   (a) $\frac{ak - ak \bmod n}{n} - a\frac{k - k \bmod n}{n} = \frac{a(k \bmod n) - a(k \bmod n) \bmod n}{n}$ [da (b), calcoli algebrici]

(b) $ak - ak \bmod n - ak + a\,(k \bmod n) = a\,(k \bmod n) - a\,(k \bmod n) \bmod n$ [da (c), calcoli algebrici]

(c) $-ak \bmod n = -a\,(k \bmod n) \bmod n$ [da (d), calcoli algebrici]

(d) $ak \bmod n = a\,(k \bmod n) \bmod n$ [per la proprietà 2.6]

2. $a\left\lceil \frac{k}{n} \right\rceil - \left\lceil \frac{ak}{n} \right\rceil = a - \left\lceil \frac{a(k \bmod^\star n)}{n} \right\rceil$ [da (a), per definizione]

(a) $a\left(\frac{k - k \bmod^\star n}{n} + 1\right) - \frac{ak - ak \bmod^\star n}{n} - 1 = a - \frac{a(k \bmod^\star n) - a(k \bmod^\star n) \bmod^\star n}{n} - 1$ [da (b), calcoli algebrici]

(b) $ak - a\,(k \bmod^\star n) + an - ak + ak \bmod^\star n - n = an - a\,(k \bmod^\star n) + a\,(k \bmod^\star n) \bmod^\star n - n$ [da (c), calcoli algebrici]

(c) $ak \bmod^\star n = a\,(k \bmod^\star n) \bmod^\star n$ [per la proprietà 2.13]

□

Dalla proprietà appena dimostrata si evince che, per ogni $a, k \in \mathbb{N}$ e per ogni $n \in \mathbb{N}^\star$, $\left\lfloor \frac{ak}{n} \right\rfloor \geq a \left\lfloor \frac{k}{n} \right\rfloor$ e, viceversa, $\left\lceil \frac{ak}{n} \right\rceil \leq a \left\lceil \frac{k}{n} \right\rceil$.

Proprietà 2.28. $\forall a \in \mathbb{N},\ \forall b, c \in \mathbb{N}^\star$: $\begin{cases} \left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor \\ \left\lceil \frac{\lceil \frac{a}{b} \rceil}{c} \right\rceil = \left\lceil \frac{a}{bc} \right\rceil \end{cases}$.

Dimostrazione.

1. $\left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor =$
$\frac{\lfloor \frac{a}{b} \rfloor - \lfloor \frac{a}{b} \rfloor \bmod c}{c} =$ [moltiplicazione e divisione per b]
$\frac{b\lfloor \frac{a}{b} \rfloor - b\left(\lfloor \frac{a}{b} \rfloor \bmod c\right)}{bc} =$ [da (a)]
$\frac{b\lfloor \frac{a}{b} \rfloor - (a - a \bmod b) \bmod bc}{bc} =$
$\frac{b\frac{a - a \bmod b}{b} - (a - a \bmod b) \bmod bc}{bc} =$
$\frac{a - a \bmod b - (a - a \bmod b) \bmod bc}{bc} =$ [perché $a \bmod b < bc$]
$\frac{a - (a \bmod b) \bmod bc - (a - a \bmod b) \bmod bc}{bc} =$ [da (b), per la proprietà 2.4
$\frac{a - (a \bmod b + a - a \bmod b) \bmod bc}{bc} =$
$\frac{a - a \bmod bc}{bc} =$
$\left\lfloor \frac{a}{bc} \right\rfloor$

(a) $b\left(\left\lfloor \frac{a}{b} \right\rfloor \bmod c\right) =$ [per la proprietà 2.3]
$b\left\lfloor \frac{a}{b} \right\rfloor \bmod bc =$
$b\frac{a - a \bmod b}{b} \bmod bc =$
$(a - a \bmod b) \bmod bc$

(b) $(a \bmod b) \bmod bc + (a - a \bmod b) \bmod bc =$ [da (a)]
$a \bmod b + b\left(\left\lfloor \frac{a}{b} \right\rfloor \bmod c\right) \leq$
$a \bmod b + b\,(c-1) <$
$b + b\,(c-1) =$
bc

2. Se $a > 0$

(a) $\left\lceil \frac{\lceil \frac{a}{b} \rceil}{c} \right\rceil =$ [per la proprietà 2.15, applicabile perché $a > 0 \Rightarrow \lceil \frac{a}{b} \rceil > 0$]
$\left\lceil \frac{\lceil \frac{a}{b} \rceil - 1}{c} \right\rceil + 1 =$ [per la proprietà 2.15, applicabile per la 2.]
$\left\lceil \frac{\lfloor \frac{a-1}{b} \rfloor + 1 - 1}{c} \right\rceil + 1 =$
$\left\lceil \frac{\lfloor \frac{a-1}{b} \rfloor}{c} \right\rceil + 1 =$ [da 1.]
$\left\lfloor \frac{a-1}{bc} \right\rfloor + 1 =$ [per la proprietà 2.15]
$\left\lceil \frac{a}{bc} \right\rceil$

3. Se $a = 0$

(a) $\left\lceil \frac{\lceil \frac{a}{b} \rceil}{c} \right\rceil =$ [da 3.]
$\left\lceil \frac{\lceil \frac{0}{b} \rceil}{c} \right\rceil =$
$\lceil \frac{0}{c} \rceil =$
$0 =$
$\lceil \frac{0}{bc} \rceil =$ [da 3.]
$\left\lceil \frac{a}{bc} \right\rceil$

□

Vediamo ora altre proprietà della parte intera, che vanno complessivamente sotto il nome di "cambi di denominatore": essendo queste abbastanza diverse dalle precedenti e meno banali, meritano un paragrafo a parte.

A volte nella teoria dei tratteggi, quando si ha una parte intera come $\left\lfloor \frac{x}{n} \right\rfloor$ o $\left\lceil \frac{x}{n} \right\rceil$, è utile cambiarne il denominatore, passando da n a $n+k$, con $k \in \mathbb{Z}$[1]; in seguito a questo cambiamento di denominatore, come deve cambiare il numeratore, se non si vuole cambiare il valore della parte intera?

Questa domanda generale si può tradurre in due domande più specifiche:

[1]Per generalità consideriamo anche il caso $k = 0$ anche se questo valore di k non fa cambiare affatto il denominatore.

- Dati $x \in \mathbb{N}$, $n \in \mathbb{N}^\star$ e $k \in \mathbb{Z}$, con $k > -n$, per quali $y \in \mathbb{Z}$, $y \geq -x$, si ha che $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x+y}{n+k} \right\rfloor$?
- Dati $x \in \mathbb{N}$, $n \in \mathbb{N}^\star$ e $k \in \mathbb{Z}$, con $k > -n$, per quali $y \in \mathbb{Z}$, $y \geq -x$, si ha che $\left\lceil \frac{x}{n} \right\rceil = \left\lceil \frac{x+y}{n+k} \right\rceil$?

Dove le condizioni $k > -n$ e $y \geq -x$ sono importanti perché le parti intere siano definite.

Rispondiamo alle due domande con la seguente proprietà:

Proprietà 2.29. *$\forall x \in \mathbb{N}$, $\forall n \in \mathbb{N}^\star$ e $\forall k, y \in \mathbb{Z}$, con $k > -n$ e $y \geq -x$:*

$$\begin{cases} \left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x+y}{n+k} \right\rfloor \Leftrightarrow k \left\lfloor \frac{x}{n} \right\rfloor - x \bmod n \leq y < k \left\lfloor \frac{x}{n} \right\rfloor - x \bmod n + k + n \\ \left\lceil \frac{x}{n} \right\rceil = \left\lceil \frac{x+y}{n+k} \right\rceil \Leftrightarrow k \left\lceil \frac{x}{n} \right\rceil - x \bmod^\star n - k < y \leq k \left\lceil \frac{x}{n} \right\rceil - x \bmod^\star n + n \end{cases}$$

Dimostrazione.

1. $\left\lfloor \frac{x+y}{n+k} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor \Leftrightarrow$ [per la proprietà 2.23]
   $(n+k) \left\lfloor \frac{x}{n} \right\rfloor \leq x + y < (n+k) \left(\left\lfloor \frac{x}{n} \right\rfloor + 1 \right) \Leftrightarrow$
   $k \left\lfloor \frac{x}{n} \right\rfloor + n \left\lfloor \frac{x}{n} \right\rfloor \leq x + y < k \left\lfloor \frac{x}{n} \right\rfloor + n \left\lfloor \frac{x}{n} \right\rfloor + k + n \Leftrightarrow$
   $k \left\lfloor \frac{x}{n} \right\rfloor + n \left(\frac{x - x \bmod n}{n} \right) \leq x + y < k \left\lfloor \frac{x}{n} \right\rfloor + n \left(\frac{x - x \bmod n}{n} \right) + k + n \Leftrightarrow$
   $k \left\lfloor \frac{x}{n} \right\rfloor + x - x \bmod n \leq x + y < k \left\lfloor \frac{x}{n} \right\rfloor + x - x \bmod n + k + n \Leftrightarrow$
   $k \left\lfloor \frac{x}{n} \right\rfloor - x \bmod n \leq y < k \left\lfloor \frac{x}{n} \right\rfloor - x \bmod n + k + n$

2. $\left\lceil \frac{x}{n} \right\rceil = \left\lceil \frac{x+y}{n+k} \right\rceil \Leftrightarrow$ [per la proprietà 2.23]
   $(n+k) \left(\left\lceil \frac{x}{n} \right\rceil - 1 \right) < x + y \leq (n+k) \left\lceil \frac{x}{n} \right\rceil \Leftrightarrow$
   $k \left\lceil \frac{x}{n} \right\rceil + n \left(\left\lceil \frac{x}{n} \right\rceil - 1 \right) - k < x + y \leq k \left\lceil \frac{x}{n} \right\rceil + n \left\lceil \frac{x}{n} \right\rceil \Leftrightarrow$
   $k \left\lceil \frac{x}{n} \right\rceil + n \left(\frac{x - x \bmod^\star n}{n} \right) - k < x + y \leq k \left\lceil \frac{x}{n} \right\rceil + n \left(\frac{x - x \bmod^\star n}{n} + 1 \right) \Leftrightarrow$
   $k \left\lceil \frac{x}{n} \right\rceil + x - x \bmod^\star n - k < x + y \leq k \left\lceil \frac{x}{n} \right\rceil + x - x \bmod^\star n + n \Leftrightarrow$
   $k \left\lceil \frac{x}{n} \right\rceil - x \bmod^\star n - k < y \leq k \left\lceil \frac{x}{n} \right\rceil - x \bmod^\star n + n$

□

L'ultima proprietà ha delle conseguenze che possono sembrare poco intuitive, che vale la pena notare.

- Applicando l'osservazione 2.1, otteniamo che $(n+k) \left\lfloor \frac{x}{n} \right\rfloor = \min\limits_{\substack{x+y \in \mathbb{N} \\ \left\lfloor \frac{x+y}{n+k} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor}} x + y$, ma poiché $x + y$ varia solo al variare di y, essendo x fissato, possiamo riscrivere quest'ultima espressione come $x + \min\limits_{\substack{y \in \mathbb{Z}, y \geq -x \\ \left\lfloor \frac{x+y}{n+k} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor}} y$, che per la proprietà appena dimostrata è pari a $k \left\lfloor \frac{x}{n} \right\rfloor + x - x \bmod n$. In definitiva abbiamo che $(n+k) \left\lfloor \frac{x}{n} \right\rfloor = k \left\lfloor \frac{x}{n} \right\rfloor + x - x \bmod n$ e quindi $n + k \mid k \left\lfloor \frac{x}{n} \right\rfloor + x - x \bmod n$. Questa

è la generalizzazione della proprietà, vera per definizione, $n \mid x - x \bmod n$.
Si può fare un discorso analogo usando la parte intera per eccesso, partendo da $(n+k)\left\lfloor \frac{x}{n} \right\rfloor = \max\limits_{\substack{x+y \in \mathbb{N} \\ \left\lceil \frac{x+y}{n+k} \right\rceil = \left\lceil \frac{x}{n} \right\rceil}} x+y$ e ottenendo $n+k \mid k\left\lfloor \frac{x}{n} \right\rfloor + x - x \bmod^{\star} n + n$.

- Per la proprietà appena dimostrata, sappiamo che possiamo scrivere $\left\lfloor \frac{x}{n} \right\rfloor$ come $\left\lfloor \frac{x+a_0+k\left\lfloor \frac{x}{n} \right\rfloor}{n+k} \right\rfloor$, con $-x \bmod n \leq a_0 < -x \bmod n + k + n$. In questa seconda espressione, però, possiamo rifare la stessa sostituzione, ottenendo $\left\lfloor \frac{x+a_0+k\left\lfloor \frac{x+a_1+k\left\lfloor \frac{x}{n} \right\rfloor}{n+k} \right\rfloor}{n+k} \right\rfloor$, con $-x \bmod n \leq a_1 < -x \bmod n + k + n$. Possiamo continuare così all'infinito, enunciando la prima delle due proprietà nel modo seguente:

  $\forall x \in \mathbb{N}, \forall n \in \mathbb{N}^{\star}$ e $\forall k \in \mathbb{Z}$, con $k > -n$: $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x+a_0+k\left\lfloor \frac{x+a_1+k\left\lfloor \frac{x+a_2+k\left\lfloor \frac{\cdots}{n+k} \right\rfloor}{n+k} \right\rfloor}{n+k} \right\rfloor}{n+k} \right\rfloor$

  con $-x \bmod n \leq a_i < -x \bmod n + k + n$ per ogni $i \in \mathbb{N}$.
  In particolare:

  - scegliendo $a_i = 0$ per ogni $i \in \mathbb{N}$ si ottiene $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x+k\left\lfloor \frac{x+k\left\lfloor \frac{\cdots}{n+k} \right\rfloor}{n+k} \right\rfloor}{n+k} \right\rfloor$
  - scegliendo $a_i = 0$ per ogni $i \in \mathbb{N}$ e $k = 1$ si ottiene $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x+\left\lfloor \frac{x+\left\lfloor \frac{\cdots}{n+1} \right\rfloor}{n+1} \right\rfloor}{n+1} \right\rfloor$

  In modo analogo si può ricavare una forma equivalente per la seconda proprietà:

$$\forall x \in \mathbb{N}, \forall n \in \mathbb{N}^\star \text{ e } \forall k \in \mathbb{Z}, \text{ con } k > -n\text{: } \left\lceil \frac{x}{n} \right\rceil = \left\lceil \frac{x+a_0+k \left\lceil \frac{x+a_1+k \left\lceil \frac{x+a_2+k \left\lceil \frac{\cdots}{n+k} \right\rceil}{n+k} \right\rceil}{n+k} \right\rceil}{n+k} \right\rceil$$

con $-x \bmod^\star n - k < a_i \leq -x \bmod^\star n + n$ per ogni $i \in \mathbb{N}$.

Capitolo 3

Una panoramica sui tratteggi

Questo capitolo chiude la prima parte del libro, denominata "Fondamenti di teoria dei tratteggi". Nel primo capitolo abbiamo visto le definizioni essenziali della teoria; nel secondo, alcune proprietà del modulo e della parte intera. Ora abbiamo tutti gli strumenti indispensabili per cominciare a parlare di tratteggi.

In questo capitolo parleremo a grandi linee di tre classi di tratteggi: *lineari*, *lineari con spiazzamento* e *dei quozienti*. I tratteggi lineari con spiazzamento sono molto simili ai tratteggi lineari, ed il loro studio verrà esaurito in questo capitolo; alle altre due classi di tratteggi sono invece dedicate la seconda e la terza parte del testo, dove si entra nel cuore della teoria. Per il momento, ci prefiggiamo i seguenti scopi:

- introdurre le diverse classi di tratteggi;
- trattare alcuni argomenti (come la connessione tra tratteggi lineari e numeri primi) che, non essendo stati studiati a sufficienza, non meritano ancora un capitolo proprio;
- enunciare e dimostrare alcune proprietà basilari dei tratteggi e dei numeri, che serviranno nel resto del libro.

3.1 Proprietà basilari dei tratteggi e dei numeri

Seguono alcune proprietà delle funzioni fondamentali che saranno utili nel resto del libro.

3.1.1 Proprietà delle funzioni fondamentali

Proprietà 3.1. *Per ogni tratteggio T e per ogni $x \in \mathbb{N}^\star$,* $\text{t\_valore}_T(x) = \mathcal{O}_T + \sum_{i=1}^{x} \text{t\_valore\_diff}_T(x)$.

Dimostrazione.

1. $\text{t\_valore}_T(x) = \mathcal{O}_T + \sum_{i=1}^{x} \text{t\_valore\_diff}_T(x)$ [da 2.–(a) e 3.–(a), per induzione]
2. Se $x = 1$
   (a) $\text{t\_valore}_T(x) =$ [da 2., per definizione di t_valore_T]
   $\mathcal{O}_T + \text{t\_valore\_diff}_T(x) =$ [da 2.]
   $\mathcal{O}_T + \sum_{i=1}^{x} \text{t\_valore\_diff}_T(x)$
3. Se $x > 1$
   (a) $\text{t\_valore}_T(x-1) = \mathcal{O}_T + \sum_{i=1}^{x-1} \text{t\_valore\_diff}_T(x) \Rightarrow \text{t\_valore}_T(x) = \mathcal{O}_T + \sum_{i=1}^{x} \text{t\_valore\_diff}_T(x)$ [da i. e ii.]
      i. Sia $\text{t\_valore}_T(x-1) = \mathcal{O}_T + \sum_{i=1}^{x-1} \text{t\_valore\_diff}_T(x)$
      ii. $\text{t\_valore}_T(x) =$
      $\text{t\_valore}_T(x) - \text{t\_valore}_T(x-1) + \text{t\_valore}_T(x-1) =$ [da 3., per definizione]
      $\text{t\_valore\_diff}_T(x) + \text{t\_valore}_T(x-1) =$ [da i.]
      $\text{t\_valore\_diff}_T(x) + \mathcal{O}_T + \sum_{i=1}^{x-1} \text{t\_valore\_diff}_T(x) =$
      $\mathcal{O}_T + \sum_{i=1}^{x} \text{t\_valore\_diff}_T(x)$

□

Per t_classe_diff_T vale una proprietà analoga alla 3.1:

Proprietà 3.2. *Per ogni tratteggio T e per ogni $x \in \mathbb{N}^\star$,* $\text{t\_classe}_T(x) = \mathcal{O}_T + \sum_{i=1}^{x} \text{t\_classe\_diff}_T(x)$.

La dimostrazione è analoga a quella della proprietà 3.1 e la lasciamo al lettore come esercizio.

La funzione t_spazio_T ha la seguente proprietà:

Proprietà 3.3. *Sia T un tratteggio. T ha almeno uno spazio se e solo se* $\exists x \in \mathbb{N}^\star : \text{t\_valore\_diff}_T(x) > 1$.

Dimostrazione.

1. T ha almeno uno spazio $\Leftrightarrow \exists x \in \mathbb{N}^\star : \text{t\_valore\_diff}_T(x) > 1$ [da 2. e 3.]
2. T ha almeno uno spazio $\Leftarrow \exists x \in \mathbb{N}^\star : \text{t\_valore\_diff}_T(x) > 1$
   (a) Sia x tale che $\text{t\_valore\_diff}_T(x) > 1$
   (b) Sia $a = \begin{cases} \text{t\_valore}_T(x-1) & \text{se } x > 0 \\ \mathcal{O}_T & \text{altrimenti} \end{cases}$
   (c) $\text{t\_valore}_T(x) - a =$ [da (b), per definizione di t_valore_diff_T]
   $\text{t\_valore\_diff}_T(x) >$ [da (a)]
   1
   (d) $\text{t\_valore}_T(x)$ è uno spazio di T
3. T ha almeno uno spazio $\Rightarrow \exists x \in \mathbb{N}^\star : \text{t\_valore\_diff}_T(x) > 1$ [da (a), (b), (c), (d), (e)]
   (a) Sia s uno spazio di T
   (b) Sia t il più grande trattino di T di valore minore di s
   (c) Sia $x \equiv \begin{cases} \text{t}_T^{-1}(t) & \text{se } |t| > \mathcal{O}_T \\ 0 & \text{altrimenti} \end{cases}$
   (d) Sia $t' \equiv \text{t\_valore}_T(x+1)$
   (e) $\text{t\_valore\_diff}_T(x+1) =$
   $\text{t\_valore}_T(x+1) - \text{t\_valore}_T(x) =$ [da (b), (c) e (d)]
   $|t'| - |t| \geq$ [da (f)]
   $s + 1 - |t| \geq$ [da (b)]
   $s + 1 - (s-1) =$
   $2 >$
   1
   (f) $|t'| > s$
      i. $|t'| \neq s$ [da (a)]
      ii. $|t'| \geq s$ [da (b) e (d)]

□

Proprietà 3.4. *Per ogni $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, se T ha almeno uno spazio, allora per ogni $a, b \in \mathbb{Z}$, $\mathcal{O}_T \leq a \leq b$:*

$$\left\{\left\{|c|_T \in [a,b] \,|c \text{ è una classe di } T\right\}, \left\{s \in [a,b] \,|s \text{ è uno spazio di } T\right\}\right\}$$

è una partizione di $[a, b]$.

Dimostrazione. L'enunciato segue dal fatto che per ogni tratteggio T, ogni intero maggiore o uguale a $\mathcal{O}_T$ o è il valore di una classe, o uno spazio, ma non entrambe le cose. Lasciamo al lettore i dettagli, abbastanza banali.

L'ipotesi che T ha almeno uno spazio è fondamentale, perché se T non avesse spazi, $\left\{\left\{|c|_T \in [a,b] \,|c \text{ è una classe di } T\right\}, \left\{s \in [a,b] \,|s \text{ è uno spazio di } T\right\}\right\}$ sarebbe uguale a $\left\{[a,b], \emptyset\right\}$, che non è una partizione di $[a, b]$ (perché gli elementi di una partizione devono essere tutti diversi da $\emptyset$).

□

Corollario 3.1. *Per ogni $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, se T ha almeno uno spazio, allora per ogni $a, b \in \mathbb{Z}$, $\mathcal{O}_T \leq a \leq b$:*

$$\left|\left\{|c|_T \in [a,b] \,|c \text{ è una classe di } T\right\}\right| + \left|\left\{s \in [a,b] \,|s \text{ è uno spazio di } T\right\}\right| = b - a + 1$$

Dimostrazione. $\left\{|c|_T \in [a,b] \,|c \text{ è una classe di } T\right\}$ e $\left\{s \in [a,b] \,|s \text{ è uno spazio di } T\right\}$ costituiscono una partizione di $[a, b]$, quindi la somma delle loro cardinalità è $|[a,b]| = b - a + 1$.

□

Corollario 3.2. *Per ogni $T \in \mathcal{T}^{\overline{\mathbb{N}}^\star}$, se T ha infiniti spazi, allora per ogni $x \in \mathbb{N}^\star$:*

$$\text{t\_spazio}_T(x) = \left(\underset{y \in \mathbb{N}^\star | \text{t\_classe}_T(y) < \text{t\_spazio}_T(x)}{\arg\max} y\right) + x + \mathcal{O}_T$$

$$\text{t\_classe}_T(x) = \left(\underset{y \in \mathbb{N}^\star | \text{t\_spazio}_T(y) < \text{t\_classe}_T(x)}{\arg\max} y\right) + x + \mathcal{O}_T$$

Dimostrazione.

Si noti che la scrittura $\text{t\_spazio}_T(x)$ ha senso, per ogni $x \in \mathbb{N}^\star$, perché si è supposto che T ha almeno infiniti spazi. Quindi si può procedere come segue:

1. $\text{t\_spazio}_T(x) = \left(\underset{y \in \mathbb{N}^\star | \text{t\_classe}_T(y) < \text{t\_spazio}_T(x)}{\arg\max} y\right) + x + \mathcal{O}_T \Leftrightarrow$
$\left(\underset{y \in \mathbb{N}^\star | \text{t\_classe}_T(y) < \text{t\_spazio}_T(x)}{\arg\max} y\right) + x = \text{t\_spazio}_T(x) - \mathcal{O}_T \Leftrightarrow$ [per definizione di

t_classe_T e perché $\text{t\_classe}_T(0) = \mathcal{O}_T$]
$|\{|c|_T \in [\mathcal{O}_T + 1, \text{t\_spazio}_T(x)] \mid c \text{ è una classe di } T\}| + x = \text{t\_spazio}_T(x) - \mathcal{O}_T \Leftrightarrow$
[per definizione di t_spazio_T e perché $\text{t\_spazio}_T(1) > \mathcal{O}_T$]
$|\{|c|_T \in [\mathcal{O}_T + 1, \text{t\_spazio}_T(x)] \mid c \text{ è una classe di } T\}| + |\{s \in [\mathcal{O}_T + 1, \text{t\_spazio}_T(x)] \mid s \text{ è uno spazio di } T\}| = \text{t\_spazio}_T(x) - \mathcal{O}_T$
[per il corollario 3.1]

2. $\text{t\_classe}_T(x) = \left(\underset{y \in \mathbb{N}^* | \text{t\_spazio}_T(y) < \text{t\_classe}_T(x)}{\arg\max} y \right) + x + \mathcal{O}_T \Leftrightarrow$
$\left(\underset{y \in \mathbb{N}^* | \text{t\_spazio}_T(y) < \text{t\_classe}_T(x)}{\arg\max} y \right) + x = \text{t\_classe}_T(x) - \mathcal{O}_T \Leftrightarrow$ [per definizione di t_spazio_T e perché $\text{t\_spazio}_T(1) > \mathcal{O}_T$]
$|\{s \in [\mathcal{O}_T + 1, \text{t\_classe}_T(x)] \mid s \text{ è uno spazio di } T\}| + x = \text{t\_classe}_T(x) - \mathcal{O}_T$ [per definizione di $\text{t classe}_T(x)$ e perché $\text{t\_classe}_T(0) = \mathcal{O}_T$]
$|\{s \in [\mathcal{O}_T + 1, \text{t\_classe}_T(x)] \mid s \text{ è uno spazio di } T\}| + |\{|c|_T \in [\mathcal{O}_T + 1, \text{t\_classe}_T(x)] \mid c \text{ è una classe di } T\}| = \text{t\_classe}_T(x) - \mathcal{O}_T$
[per il corollario 3.1]

□

3.1.2 Proprietà dei tratteggi

Proprietà dei tratteggi di primo ordine

Proprietà 3.5. *Sia $T \in \mathcal{T}^1$ strettamente monotono e $A \subset \mathbb{Z}$.*
Allora $|\{x \in A \mid \exists t \in T : T(t) = x\}| = |\{t \in T \mid T(t) \in A\}|$.

Dimostrazione.

1. $|\{x \in A \mid \exists t \in T : T(t) = x\}| = |\{t \in T \mid T(t) \in A\}|$ [da 2., 3. e 4.]
2. Sia $I \equiv \{x \in A \mid \exists t \in T : T(t) = x\}$
3. Sia $J \equiv \{t \in T \mid T(t) \in A\}$
4. $|I| = |J|$ [da 5.]
5. $T_{|J} : J \to \mathbb{Z}$ è una corrispondenza biunivoca tra I e J [da (a) e (b)]
   (a) $T_{|J}$ è suriettiva (rispetto ad I): $\forall x \in I \, \exists t \in J : T_{|J}(t) = x$
      i. Sia $x \in I$
      ii. $\exists t \in J : T_{|J}(t) = x$ [da A., perché $t \in J$]
         A. $\exists t \in J : T(t) = x$ [da B. e 3.]

B. $\exists t \in T : T(t) = x \wedge T(t) \in A$ [da C.]

C. $x \in A \wedge \exists t \in T : T(t) = x$ [da i. e 2.]

(b) $T_{|J}$ è iniettiva: $\forall t, u \in J : t \neq u \Rightarrow T_{|J}(t) \neq T_{|J}(u)$ [da i. e ii.]

i. Siano $t, u \in J$, $t \neq u$

ii. $T_{|J}(t) \neq T_{|J}(u)$ [da iii.]

iii. $T_{|J}(t) < T_{|J}(u) \vee T_{|J}(t) > T_{|J}(u)$ [da iv. e i. (in particolare, $t, u \in J$)]

iv. $T(t) < T(u) \vee T(t) > T(u)$ [da A. e B.]

A. $k < h \vee k > h$ [da D.]

B. $t = \langle 1, k\rangle$, $u = \langle 1, h\rangle$, $h, k \in \mathbb{N}$ [da C., perché $\mathrm{ord}(T) = 1$]

C. $t \in T$, $u \in T$ [da i. (in particolare $t, u \in J$) e 3.]

D. $k \neq h$ [da B. e i. (in particolare $t \neq u$)]

□

Proprietà 3.6. *Sia $T \in \mathcal{T}^1$ strettamente monotono e $A \subset \mathbb{Z}$. $|\{|c|_T \in A \mid c$ è una classe di $T\}| = |\{|t|_T \in A \mid t$ è un trattino di $T\}|$.*

Dimostrazione.

1. $|\{|c|_T \in A \mid c$ è una classe di $T\}| =$ [in un tratteggio di primo ordine strettamente monotono, tutte le classi contengono un solo trattino]
   $|\{|\{t\}|_T \in A \mid t$ è un trattino di $T\}| =$ [per definizione di valore di una classe]
   $|\{|t|_T \in A \mid t$ è un trattino di $T\}|$

□

Proprietà 3.7. *Sia $T \in \mathcal{T}^1$ con insieme delle componenti $\{i\}$, $T(\langle i, 1\rangle) > \mathcal{O}_T$. Allora per ogni $n \in \mathbb{Z}$, $n > \mathcal{O}_T$: $|\{t \in T \mid T(t) \in [\mathcal{O}_T + 1, n]\}| = \underset{k \in \mathbb{N} \mid T(\langle i,k\rangle) \leq n}{\arg\max} T(\langle i, k\rangle)$.*

Dimostrazione.

1. $|\{t \in T \mid T(t) \in [\mathcal{O}_T + 1, n]\}| = \underset{k \in \mathbb{N} \mid T(\langle i,k\rangle) \leq n}{\arg\max} T(\langle i, k\rangle)$ [da 2. e 3.]

2. Sia $h = \underset{k \in \mathbb{N} \mid T(\langle i,k\rangle) \leq n}{\arg\max} T(\langle i, k\rangle)$

3. $|\{t \in T \mid T(t) \in [\mathcal{O}_T + 1, n]\}| =$ [per definizione di trattino, in particolare di $\mathrm{Tratt}_{\{1\}}$]
   $|\{h \in \mathbb{N} \mid T(\langle i, h'\rangle) \in [\mathcal{O}_T + 1, n]\}| =$ [da 4.]
   $|[1, h]| =$
   h

4. $1 \leq h' \leq h \Leftrightarrow T(\langle i, h' \rangle) \in [\mathcal{O}_T + 1, n]$ [da (a) e (b)]

   (a) $1 \leq h' \leq h \Rightarrow T(\langle i, h' \rangle) \in [\mathcal{O}_T + 1, n]$ [da i. e ii.]

      i. $h' \geq 1 \Rightarrow T(\langle i, h' \rangle) \geq \mathcal{O}_T + 1$ [da A. e B.]

         A. $h' > 1 \Rightarrow T(\langle i, h' \rangle) \geq T(\langle i, 1 \rangle)$ [per definizione di tratteggio]

         B. $T(\langle 1, 1 \rangle) > \mathcal{O}_T$ [per ipotesi]

      ii. $h' \leq h \Rightarrow T(\langle i, h' \rangle) \leq n$ [da A. e B.]

         A. $h' < h \Rightarrow T(\langle i, h' \rangle) \leq T(\langle i, h \rangle)$ [per definizione di tratteggio]

         B. $T(\langle i, h \rangle) \leq n$ [da 2.]

   (b) $\neg(1 \leq h' \leq h) \Rightarrow T(\langle i, h' \rangle) \notin [\mathcal{O}_T + 1, n]$ [da i. e ii.]

      i. $h' = 0 \Rightarrow T(\langle i, h' \rangle) = \mathcal{O}_T$ [per definizione di tratteggio]

      ii. $h' > h \Rightarrow T(\langle i, h' \rangle) > n$ [da 2., per definizione di arg max]

□

Proprietà 3.8. *Sia $T \in \mathcal{T}^1$ con insieme delle componenti $\{i\}$. Allora per ogni $P \in [\mathrm{Tratt}_{\{i\}} \to \{\mathrm{V}, \mathrm{F}\}]$: $\underset{t \in T | P(t)}{\arg\max} T(t) = \langle i, x \rangle \Leftrightarrow x = \underset{k \in \mathbb{N} | P(\langle i,k \rangle)}{\arg\max} T(\langle i, k \rangle)$.*

Dimostrazione.

1. $\underset{t \in T | P(t)}{\arg\max} T(t) = \langle 1, x \rangle \Leftrightarrow$ [per definizione di arg max]
   $x \in \mathbb{N} \wedge P(\langle 1, x \rangle) \wedge (u > t \Rightarrow \neg P(u)) \Leftrightarrow$ [ponendo $u \equiv \langle 1, k \rangle$ e per la proprietà 1.1]
   $x \in \mathbb{N} \wedge P(\langle 1, x \rangle) \wedge (k > x \Rightarrow \neg P(\langle 1, k \rangle)) \Leftrightarrow$ [per definizione di arg max]
   $x = \underset{k \in \mathbb{N} | P(\langle 1,k \rangle)}{\arg\max} T(\langle 1, k \rangle)$

□

Si noti che l'ipotesi $n \in [\mathcal{O}_T, +\infty]$ è fondamentale, in quanto se $n < \mathcal{O}_T$, non esisterebbe $\underset{t \in T | T(t) \leq n}{\arg\max} T(t)$ perché nessun trattino $t \in T$ sarebbe tale che $T(t) \leq n < \mathcal{O}_T$.

Proprietà 3.9. *Sia $T \in \mathcal{T}^1$ e siano $t_1 \equiv \langle 1, k_1 \rangle \in T$, $t_3 \equiv \langle 1, k_3 \rangle \in T$, $t_1 \leq t_3$. Allora $|\{t_2 \in T \mid t_1 \leq t_2 \leq t_3\}| = k_3 - k_1 + 1$.*

Dimostrazione.

1. $|\{t_2 \in T \mid t_1 \leq t_2 \leq t_3\}| =$ [per la proprietà 1.1, ponendo $t_2 \equiv \langle 1, k_2 \rangle$]
   $|\{k_2 \in \mathbb{N} \mid k_1 \leq k_2 \leq k_3\}| =$
   $k_3 - k_1 + 1$

□

Corollario 3.3. *Siano $T \in \mathcal{T}^1$, $t \equiv \langle 1, k\rangle \in T$ e $n \in \mathbb{N}$. Allora l'n-esimo trattino successivo a t è $\langle i, k+n\rangle$.*

Proprietà dei tratteggi di d-esimo ordine

Proprietà 3.10. *Sia $T \in \mathcal{T}^d$, $d \in \mathbb{N}^\star$. Sia P un predicato definito sui trattini di T, cioè tale che, per ogni $t \in T$, $P(t)$ può essere vero o falso.*

$$|\{t \in T \mid P(t) \text{ è vero}\}| = \sum_{i=1}^{d} |\{t \in T[i] \mid P(t) \text{ è vero}\}|$$

Dimostrazione. La proprietà deriva dal fatto che $\{\{t \in T[i] \mid P(t) \text{ è vero}\}\}_{i=1,\dots,d}$ è una partizione di $\{t \in T \mid P(t) \text{ è vero}\}$, e ciò si dimostra banalmente a partire dalle definizioni di tratteggio e di sottotratteggio.

□

Proprietà 3.11. *Sia $T \in \mathcal{T}^d$, $d \in \mathbb{N}^\star$. Sia $t_1 \equiv \langle i_1, k_1\rangle \in T$. Allora*

$$\{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2\} = A \setminus B$$

dove:

- $A \equiv \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid |t_1| + (i_2 < i_1) \leq |t_2|\}$
- $B \equiv \{t_2 = \langle i_1, k_2\rangle \in T \mid |t_1| = |t_2| \wedge k_2 < k_1\}$

In particolare, se T è strettamente monotono,$\{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2\} = A$.

Dimostrazione.

1. Sia $D \equiv \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2\}$
2. $D = A \setminus B$ [da (a), (b), (b)–i., (c), (c)–i., (d) e (d)–i.]
   (a) Sia $t_2 \equiv \langle i_2, k_2\rangle \in T$
   (b) Se $i_2 < i_1$
      i. $t_2 \in D \Leftrightarrow$ [da 1.]
      $t_1 \leq t_2 \Leftrightarrow$
      $|t_1| < |t_2| \vee (|t_1| = |t_2| \wedge (i_1 < i_2 \vee (i_1 = i_2 \wedge k_1 \leq k_2))) \Leftrightarrow$ [da (b)]
      $|t_1| < |t_2| \vee (|t_1| = |t_2| \wedge \mathrm{F}) \Leftrightarrow$
      $|t_1| < |t_2| \Leftrightarrow$ [da (b)]
      $t_2 \in A \Leftrightarrow$ [da (b): B contiene solo trattini di $T[i_1]$]
      $t_2 \in A \setminus B$

(c) Se $i_2 = i_1$

i. $t_2 \in D \Leftrightarrow$ [da 1.]
$t_1 \leq t_2 \Leftrightarrow$
$|t_1| < |t_2| \vee (|t_1| = |t_2| \wedge (i_1 < i_2 \vee (i_1 = i_2 \wedge k_1 \leq k_2))) \Leftrightarrow$ [da (c)]
$|t_1| < |t_2| \vee (|t_1| = |t_2| \wedge k_1 \leq k_2) \Leftrightarrow$ [proprietà distributiva di $\vee$ rispetto a $\wedge$]
$|t_1| \leq |t_2| \wedge (|t_1| < |t_2| \vee k_1 \leq k_2) \Leftrightarrow$
$|t_1| \leq |t_2| \wedge \neg (|t_1| \geq |t_2| \wedge k_1 > k_2) \Leftrightarrow$
$t_2 \in A \setminus \{t_2 \equiv \langle i_2, k_2 \rangle \in T \mid |t_1| \geq |t_2| \wedge k_1 > k_2\} \Leftrightarrow$
$t_2 \in A \setminus (B \cup \{t_2 \equiv \langle i_2, k_2 \rangle \in T \mid |t_1| > |t_2| \wedge k_1 > k_2\}) \Leftrightarrow$
$t_2 \in ((A \setminus B) \cap (A \setminus \{t_2 \equiv \langle i_2, k_2 \rangle \in T \mid |t_1| > |t_2| \wedge k_1 > k_2\})) \Leftrightarrow$ [perché in A si ha $|t_1| \leq |t_2|$]
$t_2 \in (A \setminus B) \cap A \Leftrightarrow$
$t_2 \in A \setminus B$

(d) Se $i_2 > i_1$

i. $t_2 \in D \Leftrightarrow$ [da 1.]
$t_1 \leq t_2 \Leftrightarrow$
$|t_1| < |t_2| \vee (|t_1| = |t_2| \wedge (i_1 < i_2 \vee (i_1 = i_2 \wedge k_1 \leq k_2))) \Leftrightarrow$ [da (d)]
$|t_1| < |t_2| \vee (|t_1| = |t_2| \wedge (\mathrm{V} \vee \mathrm{F})) \Leftrightarrow$
$|t_1| < |t_2| \vee (|t_1| = |t_2|) \Leftrightarrow$
$|t_1| \leq |t_2| \Leftrightarrow$ [da (d)]
$t_2 \in A \Leftrightarrow$ [da (d): B contiene solo trattini di $T\,[i_1]$]
$t_2 \in A \setminus B$

3. Se T è strettamente monotono

(a) $D = A$ [da 2. e (b)]

(b) $B = \emptyset$ [da (c)]

(c) $t_2 \equiv \langle i_2, k_2 \rangle \in B \Leftrightarrow$
$i_2 = i_1 \wedge |t_1| = |t_2| \wedge k_2 < k_1 \Leftrightarrow$
$i_2 = i_1 \wedge |\langle i_1, k_1 \rangle| = |\langle i_2, k_2 \rangle| \wedge k_2 < k_1 \Leftrightarrow$
$|\langle i_1, k_1 \rangle| = |\langle i_1, k_2 \rangle| \wedge k_2 < k_1 \Leftrightarrow$
F

□

Proprietà 3.12. *Sia $T \in \mathcal{T}^d$, $d \in \mathbb{N}^\star$. Siano $t_1 \equiv \langle i_1, k_1 \rangle \in T$ e $t_3 \equiv \langle i_3, k_3 \rangle \in T$, $t_1 \leq t_3$. Allora*

$$|\{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2 \leq t_3\}| = |A| - |B| - |C|$$

dove:

- $A \equiv \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid |t_1| + (i_2 < i_1) \leq |t_2| \leq |t_3| - (i_2 > i_3)\}$
- $B \equiv \{t_2 = \langle i_1, k_2\rangle \in T \mid |t_1| = |t_2| \wedge k_2 < k_1\}$
- $C \equiv \{t_2 = \langle i_3, k_2\rangle \in T \mid |t_3| = |t_2| \wedge k_2 > k_3\}$

In particolare, se T è strettamente monotono,$|\{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2 \leq t_3\}| = |A|$.

Dimostrazione.

1. Sia $D \equiv \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2 \leq t_3\}$
2. Sia $A_1 \equiv \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid |t_1| + (i_2 < i_1) \leq |t_2|\}$
3. Sia $A_2 \equiv \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid |t_2| + (i_3 < i_2) \leq |t_3|\}$
4. $|D| =$ [da 5.]
   $|(A \setminus B) \setminus C| =$ [da 6.]
   $|A \setminus B| - |C| =$ [da 7.]
   $|A| - |B| - |C|$
5. $D =$
   $\{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_1 \leq t_2\} \cap \{t_2 \equiv \langle i_2, k_2\rangle \in T \mid t_2 \leq t_3\} =$
   $(A_1 \setminus B) \cap (A_2 \setminus C) =$
   $(A_1 \cap (A_2 \setminus C)) \setminus (B \cap (A_2 \setminus C)) =$
   $((A_1 \cap A_2) \setminus (A_1 \cap C)) \setminus ((B \cap A_2) \setminus (B \cap C)) =$ [da (a)]
   $(A \setminus (A_1 \cap C)) \setminus ((B \cap A_2) \setminus (B \cap C)) =$ [da (c)]
   $(A \setminus (A_1 \cap C)) \setminus (B \setminus (B \cap C)) =$
   $(A \setminus (A_1 \cap C)) \setminus (B \setminus C) =$ [da (b)]
   $(A \setminus C) \setminus (B \setminus C) =$
   $(A \setminus B) \setminus C$

   (a) $A_1 \cap A_2 = A$ [da 1. e 2.]

   (b) $C \subseteq A_1$ [da 7. e i.]

      i. $A \setminus B \subseteq A_1$ [da ii.]

      ii. $A \subseteq A_1$ [da (a)]

(c) $B \subseteq A_2$ [da 6. e i.]

i. $A \subseteq A_2$ [da (a)]

6. $C \subseteq A \setminus B$

(a) Sia $t_2 \equiv \langle i_2, k_2 \rangle \in C$

(b) $t_2 \in A$ [da i.]

i. $|t_1| + (i_2 < i_1) \leq |t_2| \leq |t_3| - (i_2 > i_3)$ [da ii.]

ii. $|t_2| \leq |t_3| - (i_2 > i_3)$ [da iii.]

iii. $i_2 = i_3 \wedge |t_2| \leq |t_3|$ [da iv.]

iv. $i_2 = i_3 \wedge |t_3| = |t_2| \wedge k_2 > k_3$ [da (a)]

(c) $t_2 \notin B$ [da i., i.–A., ii. e ii.–A.]

i. Se $i_2 \neq i_1$

A. $t_2 \notin$ [da i.]
$T[i_1] \supseteq$
B

ii. Se $i_2 = i_1$

A. $t_2 \notin B$ [da B.]

B. $k_2 >$ [da (a)]
$k_3 \geq$ [da C.]
k_1

C. $\langle i_1, k_1 \rangle \leq \langle i_1, k_3 \rangle$ [da D. e E.]

D. $\langle i_1, k_1 \rangle \leq \langle i_3, k_3 \rangle$ [dall'ipotesi $t_1 \leq t_3$]

E. $i_1 = i_3$ [da ii. e F.]

F. $i_2 = i_3$ [da (a)]

7. $B \subseteq A$

(a) Sia $t_2 \equiv \langle i_2, k_2 \rangle \in B$

(b) $t_2 \in A$ [da i.]

i. $|t_1| + (i_2 < i_1) \leq |t_2| \leq |t_3| - (i_2 > i_3)$ [da ii.]

ii. $|t_1| + (i_2 < i_1) \leq |t_2|$ [da iii.]

iii. $i_2 = i_1 \wedge |t_1| \leq |t_2|$ [da iv.]

iv. $i_2 = i_1 \wedge |t_1| = |t_2| \wedge k_2 < k_1$ [da (a)]

□

Proprietà del periodo e dei domini fondamentali

Sia T un tratteggio. Si definisce *periodo* di T il più piccolo $n \in \mathbb{N}^\star$ tale che:

$$\exists m \in \mathbb{N} \, \forall t \in T : \, T(t) = T(t') - m$$

dove t' è l'n-esimo trattino successivo a t nell'ordinamento temporale.

Qualsiasi intervallo del tipo $[a, a+m-1]$, $a \in \mathbb{Z}$, $a \geq \mathcal{O}_T$ si chiama *dominio fondamentale* di T.

Proprietà 3.13. *Se T è un tratteggio periodico, esso ha un unico periodo n e tutti i suoi domini fondamentali hanno la stessa lunghezza m.*

Dimostrazione.

Dimostriamo in modo abbastanza informale questa proprietà, data la sua semplicità.

Per definizione, se T è periodico, esistono degli $n \in \mathbb{N}^\star$ (almeno uno) che soddisfano la (1.3), ed il più piccolo di questi si dice periodo. Allora il periodo è unico, per definizione, essendo stato definito come il più piccolo numero, di un insieme di numeri positivi, con una certa proprietà.

Inoltre, se T è periodico e ha periodo n, allora tutti i suoi domini fondamentali hanno la stessa lunghezza m, ossia la m della (1.3) è unica. Infatti, se esistessero $m, m' \in \mathbb{N}$ che soddisfano la (1.3), si potrebbe fissare un $t \in T$ a caso, trovare il relativo t_n (ossia l'n-esimo trattino successivo) e si avrebbe che $T(t) = T(t_n) - m$ e $T(t) = T(t_n) - m'$, da cui $m = m'$.

□

Proprietà 3.14. *Se T è un tratteggio finito periodico e sia m la lunghezza di un suo dominio fondamentale. Allora per ogni $s \in [\mathcal{O}_T, \infty]$, s è uno spazio di T se e solo se $s+m$ è uno spazio di T.*

Dimostrazione.

1. $\forall s \in [\mathcal{O}_T, \infty]$:s è uno spazio di $T \Leftrightarrow s+m$ è uno spazio di T [da (a), (a)–i., (b) e (b)–i.]

   (a) Sia $s \in [\mathcal{O}_T, \infty]$, s non è uno spazio di T

      i. $s+m$ non è uno spazio di T [da ii.]

      ii. $\exists u \in T : \, T(u) = s+m$ [da iv., ponendo $t_n \equiv u$]

      iii. Sia $t \in T$ tale che $T(t) = s$ [da (a)]

iv. Sia t_n l'n-esimo trattino successivo a t nell'ordinamento temporale [da iii. e (c)]

v. $T(t_n) = s + m$ [da vi.]

vi. $s =$ [da iii.]
$T(t) =$ [da iii., iv. e (c), per le ipotesi che T è periodico e la lunghezza di un suo dominio fondamentale è m]
$T(t_n) - m$

(b) Sia $s \in [\mathcal{O}_T, \infty]$, s spazio di T

i. $s + m$ è uno spazio di T [da ii., ii.–E. e ii.–F., per assurdo]

ii. Se $s + m$ non è uno spazio di T

A. Sia t il più grande trattino di valore minore di s

B. Sia u il trattino successivo a t

C. Sia t_n l'n-esimo trattino successivo a t [da A. e (c)]

D. Sia u_n l'n-esimo trattino successivo a u [da B. e (c)]

E. u_n è il trattino successivo a t_n [da A., B., C. e D.]

F. u_n non è il trattino successivo a t_n [da G. e H.]

G. Sia $v \in T$ tale che $T(v) = s + m$ [da ii.]

H. $T(t_n) <$ [da I. e G.]
$T(v) <$ [da J. e G.]
$T(u_n)$

I. $T(t_n) =$ [da C., (c) e per le ipotesi]
$T(t) + m <$ [da A.]
$s + m$

J. $T(u_n) =$ [da D., (c) e per le ipotesi]
$T(u) + m >$ [da K.]
$s + m$

K. $T(u) > s$ [se fosse $T(u) < s$, u sarebbe, per la B., un trattino maggiore di T di valore minore di s, contraddicendo la A.; per (b) non può essere $T(u) = s$]

(c) Sia n il periodo di T

□

Corollario 3.4. *Se un tratteggio finito periodico ha uno spazio, ha infiniti spazi.*

Dimostrazione. In altri termini: un tratteggio finito periodico T o non ha spazi, o ne ha infiniti. Infatti, se s è uno spazio di T, per la proprietà 3.14, anche $s+m$, $s+2m$, $s+3m$, ... sono spazi di T.

□

Corollario 3.5. *Se T è un tratteggio finito periodico, tutti i suoi domini fondamentali contengono lo stesso numero di spazi.*

Dimostrazione. Attraverso la proposizione 3.14, si può stabilire una corrispondenza biunivoca tra spazi di domini fondamentali diversi, che quindi devono necessariamente avere lo stesso numero di spazi.

□

Corollario 3.6. *Se T è un tratteggio finito periodico, sia m la lunghezza di un suo dominio fondamentale ed s il numero di spazi in un dominio fondamentale di T. Allora per ogni $x \in \mathbb{N}^\star$, $\text{t\_spazio}_T(x) + m = \text{t\_spazio}_T(x+s)$.*

Dimostrazione. Si noti che la definizione di s è ben posta in virtù del corollario 3.5. L'enunciato si ottiene osservando che $[\text{t\_spazio}_T(x), \text{t\_spazio}_T(x)+m-1]$ è un dominio fondamentale di T, e quindi per ipotesi contiene s spazi: essi, per monotonia di t_spazio_T, sono $\text{t\_spazio}_T(x), \ldots, \text{t\_spazio}_T(x+s-1)$, quindi $\text{t\_spazio}_T(x)+m$, che è uno spazio, per la proposizione 3.14, deve essere $\text{t\_spazio}_T(x+s)$.

□

3.1.3 Proprietà dei numeri

Ora enunciamo e dimostriamo il "lemma del conteggio": un risultato abbastanza banale ma molto utile per lo studio delle funzioni fondamentali. Il lemma può essere generalizzato, ma la forma qui presentata è generale quanto basta per l'uso che ne faremo in questo libro.

Lemma 3.1. *[Lemma del conteggio]*

Siano $I \subseteq \mathbb{N}$, $x \in \mathbb{N}^\star$, $n \in I$ e, per ogni $y \in I$, $P(y)$ una condizione che può essere vera o falsa per y. Allora n è l'x-esimo $y \in I$ tale che $P(y)$ è vera se e solo se:

$$\begin{cases} |\{y \in I \mid y \leq n \wedge P(y) \text{ è vera}\}| = x \\ |\{y \in I \mid y < n \wedge P(y) \text{ è vera}\}| = x-1 \end{cases} \tag{3.1}$$

Dimostrazione. Dimostriamo informalmente l'equivalenza tra la proposizione $A \equiv$"n è l'x-esimo $y \in I$ tale che $P(y)$ è vera" e l'equazione 3.2, perché si tratta più di una questione di scelta tra un linguaggio più formale ed uno meno formale. Se n

fosse l'x-esimo $y \in I$ tale che $P(y)$ è vera, allora, al variare di $y \in I$, $y \leq n$, ci sarebbero x numeri y tali che $P(y)$ è vera. Infatti, se ce ne fossero meno di x, l'x-esimo sarebbe maggiore di n; se ce ne fossero di più, sarebbe minore. Quindi $|\{y \in I \mid y \leq n \wedge P(y) \text{ è vera}\}| = x$. Inoltre, sempre se A fosse vera, allora, al variare di $y \in I$, $y < n$, ci sarebbero $x-1$ numeri y tali che $P(y)$ è vera. Infatti, se ce ne fossero meno di $x-1$, n non potrebbe essere l'x-esimo (ma al massimo l'$(x-1)$-esimo); se ce ne fossero di più, cioè se ce ne fossero almeno x, allora l'x-esimo non sarebbe n, ma un numero più piccolo. Così abbiamo dimostrato che $A \Rightarrow$(3.2).
Con ragionamenti analoghi si può dimostrare che $\neg A \Rightarrow \neg$(3.2), cioè che (3.2)$\Rightarrow A$. Se infatti n non fosse l'x-esimo $y \in I$ tale che $P(y)$ è vera, allora l'x-esimo sarebbe un numero o più grande, o più piccolo di n. Se l'x-esimo fosse un numero più grande di n, allora $|\{y \in I \mid y \leq n \wedge P(y) \text{ è vera}\}|$ sarebbe minore di x, in contrasto con la prima riga della (3.2); se l'x-esimo fosse un numero più piccolo di n, cioè se fosse $n-1$ o un numero più piccolo, allora $|\{y \in I \mid y < n \wedge P(y) \text{ è vera}\}|$ sarebbe maggiore o uguale a x, in contrasto con la seconda riga della (3.2).

□

Sarà anche molto utile in seguito la seguente seconda forma del lemma:

Lemma 3.2. *[Lemma del conteggio, seconda forma]*

Siano $I \subseteq \mathbb{N}$, $x \in \mathbb{N}^\star$, $n \in I$ e, per ogni $y \in I$, $P(y)$ una condizione che può essere vera o falsa per y. Allora n è l'x-esimo $y \in I$ tale che $P(y)$ è vera se e solo se:

$$\begin{cases} |\{y \in I \mid y \leq n \wedge P(y) \text{ è vera}\}| = x \\ P(n) \text{ è vera} \end{cases} \tag{3.2}$$

Dimostrazione.

Siano $A \equiv |\{y \in I \mid y \leq n \wedge P(y) \text{ è vera}\}|$ e $B \equiv |\{y \in I \mid y < n \wedge P(y) \text{ è vera}\}|$. Per il lemma 3.1, si ha che $\begin{cases} A = x \\ B = x-1 \end{cases}$. In particolare $A = B+1$. Allora $P(n)$ è vera, altrimenti si avrebbe $A = B$. In definitiva, si ha che $\begin{cases} A = x \\ P(n) \text{ è vera} \end{cases}$, cioè l'equazione 3.2.

□

3.2 Tratteggi lineari

Definizione 3.1. *Sia $T \in \mathcal{T}^{\overline{\mathbb{N}^\star}}$. T si dice* lineare *se $\forall \langle i,k \rangle \in T$:*

$$T(\langle i,k \rangle) = n_i k$$

dove per ogni indice i, $n_i \in \mathbb{N}^\star$ ed n_i dipende solo da i e da T.
Tale tratteggio T si denota più brevemente $\left(n_1, \ldots, n_{\mathrm{ord}(T)}\right)$, se T è finito; $(n_1, n_2, n_3, \ldots)$, se T è infinito. Gli n_i prendono il nome di coefficienti *di T.*

Ad esempio, il tratteggio $T_1 \in \mathcal{T}^2$ tale che per ogni $\langle i, k\rangle \in T$:

$$T_1\left(\langle i, k\rangle\right) = \begin{cases} 2k & \text{se } i = 1 \\ 3k & \text{se } i = 2 \end{cases}$$

è lineare. Infatti, per ogni $i \in \{1, 2\}$ si ha $T_1\left(\langle i, k\rangle\right) = n_i k$, ponendo $n_1 = 2$ e $n_2 = 3$. Quindi si pone $T_1 \equiv (2, 3)$.

Si osservi che i tratteggi lineari sono strettamente monotoni.

Definizione 3.2. *Si definiscono i seguenti simboli:*

- $\mathcal{L}^d$*, con $d \in \overline{\mathbb{N}}^\star$, denota l'insieme di tutti i tratteggi lineari di ordine d*
- $\mathcal{L}^{\mathbb{N}^\star} \equiv \bigcup_{d \in \mathbb{N}^\star} \mathcal{L}^d$ *denota l'insieme di tutti i tratteggi lineari finiti*
- $\mathcal{L}^{\overline{\mathbb{N}}^\star} \equiv \bigcup_{d \in \overline{\mathbb{N}}^\star} \mathcal{L}^d$ *denota l'insieme di tutti i tratteggi lineari (finiti e infiniti)*

Con questa nuova simbologia, si può dire che il tratteggio T_1 poc'anzi definito appartiene a $\mathcal{L}^2$.

Una cosa da notare sui tratteggi lineari finiti riguarda le loro classi per valore, in particolare quelle di cardinalità pari all'ordine del tratteggio.

Sappiamo che in un tratteggio finito qualsiasi $T \in \mathcal{T}^d$ esiste una classe per valore di cardinalità d, quella di valore $\mathcal{O}_T$, ossia $\{\langle 1, 0\rangle, \ldots, \langle d, 0\rangle\}$. In un tratteggio lineare finito, esistono infinite classi di cardinalità d:

Osservazione 3.1. *Sia $S \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$. Esiste una classe di S di valore n e cardinalità d se e solo se* $\mathrm{MCM}(n_1, \ldots, n_d) \mid n$.

Dimostrazione.

1. $\mathrm{MCM}(n_1, \ldots, n_d) \mid n \Leftrightarrow$ [si ricava dalla definizione di MCM]
   $\forall i \in \{1, \ldots, d\} : n_i \mid n \Leftrightarrow$ [per definizione di $\mid$]
   $\forall i \in \{1, \ldots, d\}\, \exists q_i : n_i q_i = n \Leftrightarrow$ [perché S è lineare]
   $\forall i \in \{1, \ldots, d\}\, \exists \langle i, q_i\rangle \in S : S\left(\langle i, q_i\rangle\right) = n \Leftrightarrow$ [per definizione di classe, e perché gli n_i sono tutti distinti]
   $\{\langle 1, q_1\rangle, \ldots, \langle d, q_d\rangle\}$ è una classe di S di valore n e cardinalità d

□

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	...
-		-		-		-		-		-		-		-		-		-	...
-			-			-			-			-			-			-	...

Tabella 3.1: Tratteggio $T_1 \equiv (2, 3)$

L'osservazione precedente è evidente se rappresentiamo un tratteggio come una tabella. Consideriamo, ad esempio, il tratteggio $T_1 \equiv (2, 3)$ definito in precedenza:

Le classi di cardinalità 2 hanno valori 0, 6, 12, eccetera, ossia valori multipli di $6 = \mathrm{MCM}(2, 3)$.

Un'altra conseguenza immediata della definizione di tratteggio lineare è la seguente:

Proprietà 3.15. *Sia $T \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$. $n \in \mathbb{N}$ è uno spazio di T se e solo se $\forall i \in \{1, \ldots, d\} : n \bmod n_i \neq 0$.*

Dimostrazione.

1. n è uno spazio di $T \Leftrightarrow$ [per definizione di spazio]
   $\neg\exists t \equiv \langle i, k\rangle \in T : T(t) = n \Leftrightarrow$ [per definizione di tratteggio lineare]
   $\neg\exists t \equiv \langle i, k\rangle \in T : n_i k = n \Leftrightarrow$ [per definizione di trattino]
   $\neg\exists i \in \{1, \ldots, d\}\, \exists k \in \mathbb{N} : n_i k = n \Leftrightarrow$
   $\forall i \in \{1, \ldots, d\}\, \neg\exists k \in \mathbb{N} : n_i k = n \Leftrightarrow$
   $\forall i \in \{1, \ldots, d\}\, n_i \nmid n \Leftrightarrow$
   $\forall i \in \{1, \ldots, d\}\, n \bmod n_i \neq 0$

□

3.3 Tratteggi lineari con spiazzamento

I tratteggi lineari con spiazzamento sono un esempio di tratteggi impropri, ossia quei tratteggi che non hanno un'origine. Più formalmente:

Definizione 3.3. *Si definisce* trattino improprio *una coppia ordinata $t \equiv \langle i, k\rangle \in \mathbb{N}^\star \times \mathbb{Z}$. i è detto* indice *del trattino, dove la funzione* $\mathrm{ind} : \mathbb{N}^\star \times \mathbb{Z} \to \mathbb{N}^\star$ *è definita come* $\mathrm{ind}(\langle i, k\rangle) = i$.

Sia $C \subseteq \mathbb{N}^\star$. Si pone $\mathrm{ImpTratt}_C \equiv C \times \mathbb{Z}$ *(l'insieme di tutti i possibili trattini impropri con indice in C).*

Definizione 3.4. *Sia* $C \subseteq \mathbb{N}^\star$, $C \neq \emptyset$. *Si definisce* tratteggio improprio *una funzione* $T \in [\mathrm{ImpTratt}_C \to \mathbb{Z}]$ *per cui vale la proprietà di stretta monotonia:*

$$\forall \langle n,k\rangle, \langle n,h\rangle \in \mathrm{ImpTratt}_C : k < h \Rightarrow T(\langle n,k\rangle) < T(\langle n,h\rangle)$$

Come per i tratteggi, C *si dice* insieme delle componenti *del tratteggio,* $|C|$ *è detto ordine del tratteggio, e si indica con* $\mathrm{ord}(T)$. *Se* $\mathrm{ord}(T) = n$, *si dice che* T *è* di n-esimo ordine. *Se* $\mathrm{ord}(T) \in \mathbb{N}$, T *si dice* finito*; altrimenti (cioè se* $\mathrm{ord}(T) = \infty$*) si dice* infinito.

Per i tratteggi impropri andrebbero estese le funzioni fondamentali per gli interi negativi, ma questa parte deve essere ancora studiata.

Un particolare tipo di tratteggi impropri sono i tratteggi lineari con spiazzamento:

Definizione 3.5. *Sia* T *un tratteggio improprio.* T *si dice* lineare con spiazzamento *se* $\forall \langle i,k\rangle \in T$*:*

$$T(\langle i,k\rangle) = n_i k + s_i$$

dove per ogni indice i, $n_i, s_i \in \mathbb{N}$, $n_i > 1$ *ed* n_i *ed* s_i *dipendono solo da* i *e da* T. *Tale tratteggio* T *si denota più brevemente* $\left((n_1,s_1),\ldots,\left(n_{\mathrm{ord}(T)},s_{\mathrm{ord}(T)}\right)\right)$, *se* T *è finito;* $((n_1,s_1),(n_2,s_2),(n_3,s_3),\ldots)$, *se* T *è infinito. Gli* n_i *e gli* s_i *prendono il nome rispettivamente di* coefficienti *e* spiazzamenti *di* T.

Ad esempio, il tratteggio $T_2 \in \mathcal{T}^2$ tale che per ogni $\langle i,k\rangle \in T$:

$$T_2(\langle i,k\rangle) = \begin{cases} 3k & \text{se } i = 1 \\ 4k+2 & \text{se } i = 2 \end{cases}$$

è lineare con spiazzamento. Infatti, per ogni $i \in \{1,2\}$ si ha $T_2(\langle i,k\rangle) = n_i k + s_i$, ponendo $n_1 = 3$, $s_1 = 0$, $n_2 = 4$ ed $s_2 = 2$. Quindi si pone $T_2 \equiv ((3,0),(4,2))$.

È interessante confrontare un tratteggio lineare con spiazzamento col tratteggio lineare avente gli stessi coefficienti. Ad esempio, potremmo confrontare il tratteggio T_2 appena definito:

…	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	…
…			-			-			-			-			-			-	…
…	-				-				-				-				-		…

col tratteggio lineare $(3,4)$:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
-			-			-			-			-			-	...
-				-				-				-				...

Le due tabelle mostrano la stessa disposizione di trattini, ma "traslata" di sei unità (verso destra o verso sinistra, dipende dal punto di vista), oltre che "tagliata a sinistra", per quanto riguarda il tratteggio lineare. Possiamo prendere come punto di riferimento le sovrapposizioni, che hanno valore $0, 12, 18, \ldots$ in $(3, 4)$ e $6, 18, 30, \ldots$ in T_2. A partire da una sovrapposizione, sappiamo che ogni n_i colonne troveremo un trattino sulla i-esima riga, e ciò accade sia in T_2 che in $(3, 4)$: perciò nelle due tabelle la disposizione dei trattini è la stessa. La "traslazione", invece, dipende dalla diversa posizione delle sovrapposizioni.

In generale, gli spiazzamenti determinano la presenza di sovrapposizioni e, se presenti, le loro posizioni (cioè i loro valori), in un tratteggio con spiazzamento. Ricordiamo che una sovrapposizione è una classe per valore di cardinalità pari all'ordine del tratteggio. Dunque, in un tratteggio di ordine d, dobbiamo trovare d trattini con lo stesso valore. In un tratteggio lineare con spiazzamento $T \equiv ((n_1, s_1), \ldots, (n_d, s_d))$, il valore di un trattino $\langle i, k \rangle$ è $n_i k + s_i$. Dunque k generici trattini $\langle 1, k_1 \rangle, \ldots, \langle d, k_d \rangle$ hanno lo stesso valore se e solo se, per qualche n, si ha:

$$n_1 k_1 + s_1 = \ldots = n_d k_d + s_d = n$$

In altri termini:

$$\begin{cases} n \bmod n_1 = s_1 \\ \qquad \ldots \\ n \bmod n_d = s_d \end{cases} \tag{3.3}$$

Gli $n \in \mathbb{Z}$ che risolvono questo sistema sono tutti e soli i valori delle sovrapposizioni del tratteggio T. Se il sistema non avesse soluzioni, vorrebbe dire che T non avrebbe sovrapposizioni.

Abbiamo ottenuto un sistema di congruenza lineari, di solito denotato con la scrittura:

$$\begin{cases} n \equiv s_1 \pmod{n_1} \\ \qquad \ldots \\ n \equiv s_d \pmod{n_d} \end{cases}$$

Tuttavia, per coerenza con le altre notazioni del libro, si preferisce la forma 3.3.

A questo punto la teoria dei tratteggi si intreccia fortemente con l'aritmetica, perché sistemi di questo tipo sono già stati ampiamente studiati. La teoria dei tratteggi è anche in questo caso, come abbiamo visto per i numeri primi nel paragrafo

4.4, un modo alternativo per studiare il problema. Non solo, ma la teoria dei tratteggi approfondisce la questione introducendo nuove problematiche. Basti pensare, ad esempio, che il sistema 3.3 identifica solamente le sovrapposizioni di un tratteggio lineare con spiazzamento, ma si può studiare il tratteggio anche quando il sistema non ha soluzioni: semplicemente, si studierà un tratteggio lineare con spiazzamento senza sovrapposizioni.

I tratteggi lineari con spiazzamento aventi sovrapposizioni sono i più semplici, perché immediatamente riconducibili a tratteggi lineari aventi gli stessi coefficienti, per il discorso della "traslazione", che però non formalizziamo, in attesa di maggiori sviluppi di questa parte della teoria.
Detti tratteggi, inoltre, possono essere utili per studiare da un'altra prospettiva le congruenze lineari. Nel corso della ricerca in teoria dei tratteggi sono stati effettuati studi in tal senso, ma i pochi risultati ottenuti, non rilevantissimi, sono riservati, per il momento, a successive edizioni dell'opera.

Non sono stati per nulla studiati, invece, i tratteggi lineari con spiazzamento non aventi sovrapposizioni e, perciò, non direttamente riconducibili a dei tratteggi lineari.

3.4 Metatratteggi

Il concetto di *metatratteggio* qui introdotto come base per definire una nuova classe di tratteggi, i tratteggi dei quozienti, a partire da una classe di tratteggi già definita, quella dei tratteggi lineari. Più in generale, sarebbe interessante studiare i metatratteggi oltre il caso citato, ma uno studio del genere meriterebbe grande approfondimento.
Cominciamo definendo formalmente gli oggetti di cui stiamo parlando, proseguendo subito dopo con la discussione, attraverso un esempio.

Definizione 3.6. *Siano $A \subset \mathbb{Z}$, avente minimo, e sia $[a, b]$ un intervallo, con $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \cup \{+\infty\}$. Si definisce* funzione di ripartizione *da A in $[a, b]$ una funzione $f \in [A \to [a, b]]$ suriettiva crescente.*

Ad esempio, ponendo $a = 0$ e $b = +\infty$, si ha che $[0, +\infty] = \mathbb{N}$ e la funzione $g \equiv \lambda x.\, \lceil \frac{x}{3} \rceil \in [\mathbb{N} \to \mathbb{N}]$ è una funzione di ripartizione per $\mathbb{N}$. Infatti abbiamo che

$$g(0) = 0,\ g(1) = 1,\ g(2) = 1,\ g(3) = 1,\ g(4) = 2,\ g(5) = 2,\ g(6) = 2,\ g(7) = 3,\ \ldots$$

cioè g è suriettiva crescente.

Se f è una funzione di ripartizione da A in $[a,b]$, è interessante considerare la funzione $f^{-1} \equiv \lambda x.\{n \in A \mid f(n) = x\} \in \left[[a,b] \to 2^A\right]$, che chiameremo *inversa* di f anche se non è propriamente un'inversa. Si può dimostrare facilmente che $\{f^{-1}(x) \mid x \in [a,b]\}$ è una partizione di A, detta *partizione* di A *indotta* da f: da qui il nome *funzione di ripartizione*.
Ad esempio, tornando alla funzione g, possiamo considerare $g^{-1} \in \left[\mathbb{N} \to 2^{\mathbb{N}}\right]$:

$$g^{-1}(0) = \{0\},\ g^{-1}(1) = \{1,2,3\},\ g^{-1}(2) = \{4,5,6\},\ g^{-1}(3) = \{7,8,9\},\ \ldots$$

quindi la partizione di $\mathbb{N}$ indotta da g è:

$$\{\{0\},\{1,2,3\},\{4,5,6\},\{7,8,9\},\ldots\}$$

Definizione 3.7. *Sia $T \in \mathcal{T}$. Siano $l \leq \mathrm{ord}(T)$, $F \equiv (f_i \mid 1 \leq i \leq l)$ una l-upla (sequenza di lunghezza l)*[1] *di funzioni di ripartizione da $[\mathcal{O}_T, \infty]$ in $\mathbb{N}$ ed f una funzione di ripartizione da $[1, \mathrm{ord}(T)]$ in $[1,l]$.*

Si definisce metatratteggio *di T generato da F e da f un tratteggio $T' \in \mathcal{T}^l$, tale che per ogni $\langle i,k\rangle \in \mathrm{Tratt}_{\{1,\ldots,l\}}$:*

$$T'(\langle i,k\rangle) = f_i\left(\mathrm{t\_valore}_{T[f^{-1}(i)]}(k)\right) \tag{3.4}$$

T si definisce tratteggio base *di T'.*

La definizione di metatratteggio può sembrare ostica. In realtà, al di là dei formalismi, si può ottenere un metatratteggio T' da un tratteggio T con delle semplici operazioni. Vediamo un esempio, considerando come tratteggio base il tratteggio lineare $(2,3,4,5)$.
La prima cosa da fare è partizionare gli indici di T, usando la funzione di ripartizione f. Quest'ultima è, per definizione, una funzione suriettiva crescente dall'insieme degli indici di T, $[1, \mathrm{ord}(T)] = \{1,2,3,4\}$, all'insieme $[1,l]$, che sarà l'insieme degli indici del metatratteggio T' che stiamo costruendo. Poniamo, per fissare le idee, $l = 3$ (cosicché $[1,l] = \{1,2,3\}$) e definiamo la seguente funzione di ripartizione f da $\{1,2,3,4\}$ in $\{1,2,3\}$:

$$f(1) = 1,\ f(2) = 1,\ f(3) = 2,\ f(4) = 3$$

Si tratta di una funzione di ripartizione, perché la funzione è suriettiva crescente.

[1] Se $\mathrm{ord}(T) = \infty$, l può essere ∞: in questo caso, la sequenza ha lunghezza infinita.

Si ha che:

$$f^{-1}(1) = \{1,2\},\ f^{-1}(2) = \{3\},\ f^{-1}(3) = \{4\}$$

dunque la partizione di $\{1,2,3,4\}$ indotta da f è $\{\{1,2\},\{3\},\{4\}\}$. La conseguenza di ciò sul metatratteggio è che, pensando alla rappresentazione tabellare, le prime due righe del tratteggio T corrisponderanno alla prima riga del metatratteggio T'; la terza riga e la quarta riga di T corrisponderanno, rispettivamente, alla seconda ed alla terza riga di T'.

Le funzioni di ripartizione $(f_i \mid 1 \leq i \leq l)$, nel nostro caso (f_1, f_2, f_3), indicano come "partizionare" righe o gruppi di righe di T per ottenere ciascuna riga di T'. Precisiamo meglio il significato di questa affermazione. Abbiamo detto che le f_i devono essere funzioni di ripartizione da $[\mathcal{O}_T, \infty]$ in $\mathbb{N}$. Nel nostro esempio, $\mathcal{O}_T = 0$, quindi dobbiamo definire tre funzioni di ripartizione, f_1, f_2 ed f_3, da $\mathbb{N}$ in $\mathbb{N}$. Sia per esempio, per ogni $x \in \mathbb{N}$:

$$f_1(x) = \left\lceil \tfrac{x}{5} \right\rceil$$
$$f_2(x) = \left\lceil \tfrac{x}{3} \right\rceil$$
$$f_3(x) = \left\lceil \tfrac{x}{7} \right\rceil$$

Queste funzioni inducono tre corrispondenti partizioni di $\mathbb{N}$:

$$\{\{0\},\{1,2,3,4,5\},\{6,7,8,9,10\},\ldots\}$$
$$\{\{0\},\{1,2,3\},\{4,5,6\},\ldots\}$$
$$\{\{0\},\{1,2,3,4,5,6,7\},\{8,9,10,11,12,13,14\},\ldots\}$$

tali che il j-esimo elemento (partendo da $j = 0$) della partizione indotta da f_i è $f_i^{-1}(j)$. Ad esempio, $f_2^{-1}(0) = \{0\}$, $f_2^{-1}(1) = \{1,2,3\}$ ed $f_2^{-1}(2) = \{4,5,6\}$.

Ora, per costruire il metatratteggio T', bisogna trovare:

- quali trattini di $T[1,2]$ hanno valori negli insiemi $\{0\}$,$\{1,2,3,4,5\}$,$\{6,7,8,9,10\}$,...
- quali trattini di $T[3]$ hanno valori negli insiemi $\{0\},\{1,2,3\},\{4,5,6\},\ldots$
- quali trattini di $T[4]$ hanno valori negli insiemi $\{0\}$, $\{1,2,3,4,5,6,7\}$, $\{8,9,10,11,12,13,14\}$, ...

cioè bisogna cercare trattini del sottotratteggio di T di indici $f^{-1}(i)$, $i \in \{1,2,3\}$, che abbiano valori negli insiemi della partizione di $\mathbb{N}$ (di $[\mathcal{O}_T, \infty]$, in generale) indotta da f_i. Abbiamo quindi una suddivisione "verticale" del tratteggio, che divide T in $T[1,2]$, $T[3]$ e $T[4]$, ed una suddivisione "orizzontale", che partiziona $\mathbb{N}$, quest'ultima dipendente dal sottotratteggio considerato nella partizione verticale. Ciò è visualizzato nella seguente tabella:

	0	1	2	...
1	**0** **0**	1 **2** 3 **4** 5 1 2 **3** 4 5	**6** 7 **8** 9 **10** **6** 7 8 **9** 10	...
2	**0**	1 2 3	**4** 5 6	...
3	**0**	1 2 3 4 **5** 6 7	8 9 **10** 11 12 13 14	...

Le intestazioni delle righe sono gli interi in $[1, 3]$, che saranno gli indici del metatratteggio; le intestazioni delle colonne sono i numeri naturali. All'incrocio tra riga i e colonna j (chiamiamola "macrocella" di riga i e colonna j) vi sono tutte le celle della tabella di T (chiamiamole "microcelle") che hanno numero di riga nell'insieme $f^{-1}(i)$ e numero di colonna nell'insieme $f_i^{-1}(j)$. Ciascuna cella contiene il numero di colonna che essa aveva nella tabella di T. Sono evidenziati in grassetto i numeri posti nelle celle che contenevano un trattino nella tabella di T.

A questo punto è facile ottenere la tabella del metatratteggio T': basta porre in ciascuna macrocella, tanti trattini quante sono le microcelle in essa contenute che contengono numero in grassetto. In altri termini, la macrocella (che ora diventa semplicemente una cella) di riga i e colonna $j \geq \mathcal{O}_T = \mathcal{O}_{T'}$ contiene tanti trattini, quanti sono i trattini di T aventi indice nell'insieme $f^{-1}(i)$ e valore nell'insieme $f_i^{-1}(j)$.

	0	1	2	...
1	–	- - -	- - - - -	...
2	-		-	...
3	-	-	-	...

Ad esempio, la cella di riga 3 e colonna 2 contiene un trattino perché in T esiste un trattino avente indice in $f^{-1}(3) = \{4\}$ e valore in $f_3^{-1}(2) = \{8, 9, 10, 11, 12, 13, 14\}$. Si tratta precisamente del trattino $\langle 4, 2\rangle$: infatti, $T(\langle 4, 2\rangle) = 5 \cdot 2 = 10 \in \{8, 9, 10, 11, 12, 13, 14\}$. Tutte le celle della prima riga 1 contengono più di un trattino, perché ci sono più trattini di T che hanno valori nei corrispondenti $f_1^{-1}(y)$, $y \in \mathbb{N}^\star$.

Il lettore può verificare che il tratteggio T' ottenuto con questo procedimento è quello che soddisfa la definizione 3.7.

È evidente, a partire dall'esempio, che un metatratteggio di un tratteggio strettamente monotono può non essere strettamente monotono.

Nella definizione 3.7, si definisce un metatratteggio come un particolare tratteggio, dando per scontato che la funzione 3.4 è effettivamente un tratteggio. Lo dimostriamo adesso, assicurandoci così che la definizione 3.7 è ben posta.

Proprietà 3.16. *Sia* $T \in \mathcal{T}$ *e* $T' \in \left[\text{Tratt}_{\{1,\dots,l\}} \to \mathbb{Z}\right]$ *la funzione definita dalla 3.4. Allora* $T' \in \mathcal{T}^l$ *e* $\mathcal{O}_{T'} = 0$.

Dimostrazione.

1. $T' \in \mathcal{T}^l$ [per ipotesi $T' \in \left[\text{Tratt}_{\{1,\dots,l\}} \to \mathbb{Z}\right]$, inoltre per 2. e 2.–(a)]
2. Sia $i \in \{1, \dots, l\}$
   (a) $T'(\langle i, 0\rangle) =$ [per definizione di T']
   $f_i\left(\text{t\_valore}_{T[f^{-1}(i)]}(0)\right) =$ [per definizione di t_valore]
   $f_i\left(\mathcal{O}_{T[f^{-1}(i)]}\right) =$ [l'origine di un tratteggio coincide con quella di un suo sottotratteggio]
   $f_i(\mathcal{O}_T) =$ [perché $f_i : [\mathcal{O}_T, \infty] \to \mathbb{N}$ è suriettiva crescente]
   0
3. $\mathcal{O}_{T'} = 0$ [da 2. e 2.–(a)]

□

3.5 Tratteggi dei quozienti

Vediamo ora un'importante classe di tratteggi, i *tratteggi dei quozienti*, definiti sfruttando la nozione di metatratteggio. Prima, però, dobbiamo introdurre la nozione di *giustapposizione* di tratteggi.

Definizione 3.8. *Siano* $S \in \mathcal{T}^n$, $T \in \mathcal{T}^m$, *con* $n, m \in \mathbb{N}^\star$. *Si definisce* giustapposizione *di* S *e* T, *e si legge: "*S *giustapposto a* T*", il tratteggio* $S\sharp T \in \mathcal{T}^{n+m}$ *tale che* $S\sharp T[1, \dots, n] = S$ *ed* $(S\sharp T[n+1, \dots, m])(\langle i, k\rangle) = T(\langle i - n, k\rangle)$ *per ogni* $\langle i, k\rangle \in \text{Tratt}_{[n+1,\dots,m]}$.

Quindi:

- ogni trattino $\langle i, k\rangle$ appartenente ad S, appartiene anche a $S\sharp T$ e mantiene il suo valore
- ogni trattino $\langle i, k\rangle$ appartenente a T diventa $\langle i + n, k\rangle$ in $S\sharp T$, ma mantiene il valore che aveva in T

Ciò significa che la tabella che rappresenta $S\sharp T$ ha le prime n righe identiche a quelle di S e le successive m identiche a quelle di T.
Ad esempio, se $S \equiv (2, 3)$:

0	1	2	3	4	5	...
-		-		-		...
-			-			...

e $T \equiv (2,4)$:

0	1	2	3	...
-		-		...
-				...

La tabella che rappresenta $S \circ T$ è:

0	1	2	3	4	5	6	7	8	9	10	11	...
-		-		-		-		-		-		...
-			-			-			-			...
-		-		-		-		-		-		...
-				-				-				...

Notazione 3.1. *Si pone, per* $n \in \mathbb{N}^\star$, $\underbrace{T\sharp T\sharp \dots \sharp T}_{T \text{ ripetuto } n \text{ volte}} \equiv T^{\sharp n}$.

Definizione 3.9. *Sia* $T \equiv (n_1, \dots, n_k) \in \mathcal{L}^k$, *con* $k \geq 2$. *Si definisce* tratteggio dei quozienti *di* T *il metatratteggio* Q *di* $(n_k)^{\sharp(k-1)}$ *generato da* $\left(\lambda x. \left\lfloor \frac{x}{n_i} \right\rfloor : \mathbb{N} \to \mathbb{N} \mid i \in \{1, \dots, k-1\}\right)$ *e da* $\lambda x.x : [1, k-1] \to [1, k-1]$. *Si scrive* $Q \equiv q\,(T)$.

Vediamo ora un esempio di tratteggio dei quozienti, rimandando il lettore alla parte III per uno studio approfondito.

Sia T il tratteggio lineare $(2,3,5)$. Vediamo qual è il suo tratteggio dei quozienti, disegnandone la tabella.
Dobbiamo innanzitutto considerare il tratteggio $(5)^{\sharp 2}$, ossia:

0	1	2	3	4	5	6	7	8	9	10	...
-					-					-	...
-					-					-	...

Adattando la definizione all'esempio, si ottiene che il tratteggio dei quozienti di $(2,3,5)$ è il metatratteggio di $(5)^{\sharp 2}$ generato da (f_1, f_2) e da f, dove f_1 ed f_2 sono funzioni di ripartizione da $\mathbb{N}$ in $\mathbb{N}$ tali che $f_1(x) = \left\lfloor \frac{x}{2} \right\rfloor$ e $f_2(x) = \left\lfloor \frac{x}{3} \right\rfloor$; f è la funzione identica definita su $\{1,2\}$.
Il fatto che f sia la funzione identica implica che il tratteggio $q(T)$ che stiamo costruendo ha ordine 2: dalla prima riga di T si ottiene la prima riga di $q(T)$, ed analogamente per la seconda riga.
Dobbiamo usare ora f_1 per partizionare le colonne della prima riga di T ed f_2 per partizionare le colonne della seconda riga. Le partizioni di $\mathbb{N}$ indotte da f_1 ed f_2 sono, rispettivamente:

$$\left\{f_1^{-1}(0), f_1^{-1}(1), f_1^{-1}(2), \ldots\right\} = \{\{0,1\}, \{2,3\}, \{4,5\}, \ldots\}$$

e

$$\left\{f_2^{-1}(0), f_2^{-1}(1), f_2^{-1}(2), \ldots\right\} = \{\{0,1,2\}, \{3,4,5\}, \{6,7,8\}, \ldots\}$$

Partizionando le colonne di T, otteniamo la seguente tabella:

	0	1	2	...
1	**0** 1	2 3	4 **5**	...
2	**0** 1 2	3 4 **5**	6 7 8	...

Dalla quale si ottiene, con lo stesso metodo visto nel paragrafo precedente, la tabella che rappresenta $q(T)$:

	0	1	2	...
1	-			...
2	-	-		...

Oltre alla tabella che lo rappresenta, tuttavia, si potrebbe essere interessati all'espressione del tratteggio $q(T)$, come funzione da $\text{Tratt}_2 \to \mathbb{N}$. Adattando la definizione di metatratteggio al caso particolare, si può scrivere, per ogni $\langle i,k \rangle \in \text{Tratt}_{\{1,2\}}$:

$$q(T)(\langle i,k \rangle) = f_i\left(\text{t\_valore}_{T[f^{-1}(i)]}(k)\right)$$

Ciò definisce senza dubbio il tratteggio $q(T)$, ma probabilmente si è interessati ad una forma più semplice ed esplicita. Preferiamo non introdurre adesso questa forma, ma rimandarla al capitolo 10, in cui la questione sarà vista anche da un'altra prospettiva e con un maggior livello di approfondimento.

Come per i tratteggi lineari, introduciamo i seguenti insiemi di tratteggi del quozienti:

Definizione 3.10. *Si definiscono i seguenti simboli:*

- $\mathcal{Q}^k$, *con* $k \in \overline{\mathbb{N}}^\star$, *denota l'insieme di tutti i tratteggi dei quozienti di ordine* k
- $\mathcal{Q}^{\mathbb{N}^\star} \equiv \bigcup_{k \in \mathbb{N}^\star} \mathcal{Q}^k$ *denota l'insieme di tutti i tratteggi dei quozienti finiti*
- $\mathcal{Q}^{\overline{\mathbb{N}}^\star} \equiv \bigcup_{k \in \overline{\mathbb{N}}^\star} \mathcal{Q}^k$ *denota l'insieme di tutti i tratteggi dei quozienti (finiti e infiniti)*

Parte II

Tratteggi lineari

Questa è la parte del libro in cui si entra maggiormente in dettaglio nella teoria dei tratteggi. Infatti, per la loro semplicità, i tratteggi lineari sono stati i primi ad essere studiati ed approfonditi. Dopo la lettura di questa parte, il termine "semplicità" può sembrare ironico, ma non è così, come si può intuire leggendo la parte III sui tratteggi dei quozienti.

Ho avuto molti ripensamenti su quale fosse la suddivisione in capitoli più opportuna. Infatti, gli argomenti da trattare sono:

- l'upcast di t lineare
- il downcast e la down-conservatività di t lineare
- t_valore lineare
- t_spazio lineare

Ciascuno di questi argomenti dovrebbe essere trattato per i tratteggi lineari di secondo, terzo e, in generale, d-esimo ordine; t_spazio lineare anche per il primo ordine (gli altri problemi nel primo ordine sarebbero banali). Ovviamente basterebbe trattare solamente il caso generale per ciascun argomenti, ma ciò non è nè opporuno, nè attualmente fattibile, per i seguenti motivi:

- I casi generali presentano formule complesse, a cui è meglio arrivare in modo graduali, a beneficio della comprensione
- Esistono molti teoremi per casi particolari (ad es. per il secondo ordine) che non sono stati generalizzati
- Solo il problema dell'upcast di t lineare è stato risolto nel caso generale, per il momento

Dalla necessità di trattare gli stessi argomenti per ordini diversi è nato il dilemma: meglio dedicare un capitolo per ogni ordine di tratteggio (primo, secondo, terzo, d-esimo), trattando tutti gli argomenti in ciascun capitolo, o meglio dedicare un capitolo allo studio di ciascun problema per diversi ordini? La scelta finale è stata la seconda: un capitolo per ciascun problema. Ciò ha il vantaggio di mantenere una buona coerenza all'interno di uno stesso capitolo, ma lo svantaggio che le forme più generali sono distribuite tra i diversi capitoli anziché aggregate, cosa che renderebbe più semplice saltarle in una prima lettura. Anche con la suddivisione per argomenti, però, il lettore può scegliere a quale livello di generalità porsi: ad esempio, leggere di ogni capitolo solo le parti riguardanti il primo (ove applicabile) ed il secondo ordine. La tabella II può essere di aiuto nella scelta di un percorso di lettura.

	$T \in \mathcal{L}^1$	$T \in \mathcal{L}^2$
$\mathrm{Up}^{T' \to T}$ (t)	banale	5.1 nella pagina 137
$\mathrm{DownCons}^{T \to T'}$ (t)	banale	6.3 nella pagina 145
$\mathrm{Down}^{T \to T'}$ (t)	banale	6.4 nella pagina 152
$\mathrm{t\_valore}_T$	banale	6.5 nella pagina 160, nella pagina 225
$\mathrm{t\_spazio}_T$	8.1 nella pagina 200	8.2 nella pagina 206

	$T \in \mathcal{L}^3$	$T \in \mathcal{L}^d$, $d \in \mathbb{N}^\star$
$\mathrm{Up}^{T' \to T}$ (t)	5.2 nella pagina 138	5.3 nella pagina 140
$\mathrm{DownCons}^{T \to T'}$ (t)	6.6 nella pagina 163	mancante
$\mathrm{Down}^{T \to T'}$ (t)	6.7 nella pagina 178	mancante
$\mathrm{t\_valore}_T$	mancante	mancante
$\mathrm{t\_spazio}_T$	mancante	mancante

Tabella 3.2: Guida alla lettura per la parte II

Capitolo 4

Semplici proprietà dei tratteggi lineari

In questo capitolo raccogliamo alcune semplici proprietà sui tratteggi lineari (spesso basate su proprietà generali dei tratteggi, enunciate nel capitolo 3). Esse costituiscono la base per i risultati dei capitoli successivi della parte II.

4.1 Proprietà dei trattini

Proposizione 4.1. *Sia $T \equiv (n) \in \mathcal{L}^1$, con insieme delle componenti $\{i\}$. Per ogni $x \in \mathbb{N}$, il più grande trattino di T di valore minore o uguale a x è $\langle i, \lfloor \frac{x}{n} \rfloor \rangle$.*

Dimostrazione.

1. Sia $t \equiv \langle i, \lfloor \frac{x}{n} \rfloor \rangle$
2. t è il più grande trattino di T di valore minore o uguale a x [da (a) e (b)]
   (a) $|t| =$ [da 1. e perché T è lineare]
   $n \lfloor \frac{x}{n} \rfloor =$
   $n \frac{x - x \bmod n}{n} =$
   $x - x \bmod n \leq$
   x
   (b) $\forall k > \lfloor \frac{x}{n} \rfloor : |\langle i, k \rangle| > x$ [da i. e per la stretta monotonia della funzione valore]
      i. $\left|\langle i, \lfloor \frac{x}{n} \rfloor + 1 \rangle\right| =$ [per ché T è lineare]
      $n \lfloor \frac{x}{n} \rfloor + n =$
      $n \frac{x - x \bmod n}{n} + n =$

$x + (n - x \bmod n) >$ [da $x \bmod n < n$]
x

□

Corollario 4.1. *Sia $T \equiv (n) \in \mathcal{L}^1$, con insieme delle componenti $\{i\}$. Per ogni $x \in \mathbb{N}$, il più piccolo trattino di T di valore maggiore o uguale a x è $\left\langle i, \left\lceil \frac{x}{n} \right\rceil \right\rangle$.*

Dimostrazione.

1. Sia t il più piccolo trattino di T di valore maggiore o uguale a x
2. $t = \left\langle i, \left\lceil \frac{x}{n} \right\rceil \right\rangle$ [da (a), per la proprietà 2.21]
   (a) $t = \left\langle i, \left\lfloor \frac{x-1}{n} \right\rfloor + 1 \right\rangle$ [da (b)]
   (b) Il trattino precedente t è $\left\langle i, \left\lfloor \frac{x-1}{n} \right\rfloor \right\rangle$ [da (c)]
   (c) Il trattino precedente t è il più grande trattino di T di valore minore o uguale di $x - 1$ [da (d)]
   (d) t è il più piccolo trattino di T di valore maggiore di $x - 1$ [da 1.]

□

Un'importante modifica della proposizione 4.1 consiste nel calcolare il più grande trattino minore di un altro trattino: con le parole "più grande" e "minore" si fa riferimento in questo caso all'ordinamento per colonne definito sui trattini, piuttosto che, come nella proposizione 4.1, l'ordinamento sui valori dei trattini (che altro non è che l'usuale ordinamento tra interi).

Proposizione 4.2. *Sia $T \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$, $d \in \mathbb{N}^\star$. Siano inoltre $i, j \in [1, d]$ e $u \in T[i]$. Allora*

$$\max_{t \in T[j] \mid t < u} t = \left\langle j, \left\lfloor \frac{|u| - (i \leq j)}{n_j} \right\rfloor \right\rangle$$

Dimostrazione.

1. $\max_{t \in T[j] \mid t < u} t = \left\langle j, \left\lfloor \frac{|u| - (i \leq j)}{n_j} \right\rfloor \right\rangle$ [da 3.–(a) e 4.–(a)]
2. Sia $u \equiv \langle i, n \rangle$, $n \in \mathbb{N}^\star$
3. Se $i > j$

(a) $\max_{t\in T[j]|t<u} t =$ [ponendo $t \equiv \langle j,m\rangle$]
$\max_{\langle j,m\rangle\in T|\langle j,m\rangle<u} \langle j,m\rangle =$ [da i.]
$\max_{\langle j,m\rangle\in T||\langle j,m\rangle|\leq|u|} \langle j,m\rangle =$ [per la proposizione 4.1]
$\left\langle j, \left\lfloor \frac{|u|}{n_j} \right\rfloor \right\rangle$

i. $\langle j,m\rangle < u \Leftrightarrow$ [da 2., per la proprietà 1.2]
$|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u| \wedge (j < i \vee (j = i \wedge m < n))) \Leftrightarrow$ [da 3.]
$|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u|) \Leftrightarrow$
$|\langle j,m\rangle| \leq |u|$

4. Se $i \leq j$

(a) $\max_{t\in T[j]|t<u} t =$ [ponendo $t \equiv \langle j,m\rangle$]
$\max_{\langle j,m\rangle\in T|\langle j,m\rangle<u} \langle j,m\rangle =$ [da i.]
$\max_{\langle j,m\rangle\in T||\langle j,m\rangle|\leq|u|-1} \langle j,m\rangle =$ [per la proposizione 4.1]
$\left\langle j, \left\lfloor \frac{|u|-1}{n_j} \right\rfloor \right\rangle$

i. $\langle j,m\rangle < u \Leftrightarrow$ [da 2., per la proprietà 1.2]
$|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u| \wedge (j < i \vee (j = i \wedge m < n))) \Leftrightarrow$ [da ii., ii.–A., iii. e iii.–A.]
$|\langle j,m\rangle| < |u| \Leftrightarrow$
$|\langle j,m\rangle| \leq |u| - 1$

ii. Se $i < j$

A. $|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u| \wedge (j < i \vee (j = i \wedge m < n))) \Leftrightarrow$ [da ii.]
$|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u| \wedge \mathrm{F}) \Leftrightarrow$
$|\langle j,m\rangle| < |u|$

iii. Se $i = j$

A. $|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u| \wedge (j < i \vee (j = i \wedge m < n))) \Leftrightarrow$ [da iii.]
$|\langle j,m\rangle| < |u| \vee (|\langle j,m\rangle| = |u| \wedge m < n) \Leftrightarrow$ [da B.]
$|\langle j,m\rangle| < |u| \Leftrightarrow$

B. $|\langle j,m\rangle| = |u| \wedge m < n \Leftrightarrow$ [perché il tratteggio è lineare]
$n_j m = |u| \wedge m < n \Leftrightarrow$ [da 2.]
$n_j m = n_i n \wedge m < n \Leftrightarrow$ [da iii.]
$n_j m = n_j n \wedge m < n \Leftrightarrow$
$m = n \wedge m < n \Leftrightarrow$
F

□

Proposizione 4.3. *Sia $T \equiv (n) \in \mathcal{L}^1$, con insieme delle componenti $\{i\}$. Siano $x \in \mathbb{N}$, $t \equiv \langle i, k\rangle \in T$.*
Allora $|\{t' \in T \mid |t| < |t'| \leq x\}| = \left\lfloor \frac{x-|t|}{n} \right\rfloor$.

Dimostrazione.

1. $|\{t' \in T \mid |t| < |t'| \leq x\}| = \left\lfloor \frac{x-|t|}{n} \right\rfloor$ [da (a), (a)–i., (b), (b)–i.]

   (a) Se $|\langle i, k+1\rangle| > x$

      i. $|\{t' \in T \mid |t| < |t'| \leq x\}| =$ [da ii.]
      $|\emptyset| =$
      $0 =$ [da iii., per definizione]
      $\left\lfloor \frac{x-nk}{n_i} \right\rfloor =$ [per ipotesi e perché il tratteggio è lineare]
      $\left\lfloor \frac{x-|t|}{n} \right\rfloor$

      ii. $|t| < |t'| \Rightarrow$ [da (c)]
      $t' \geq \langle i, k+1\rangle \Rightarrow$ [per monotonia del tratteggio]
      $|t'| \geq |\langle i, k+1\rangle| \Rightarrow$ [da (a)]
      $|t'| > x$

      iii. $x - nk < n$ [da A., calcoli algebrici]

         A. $n\,(k+1) > x$ [da (a), perché il tratteggio è lineare]

   (b) Se $|\langle i, k+1\rangle| \leq x$

      i. $|\{t' \in T \mid |t| < |t'| \leq x\}| =$ [da 2., (c) e per la proposizione 4.1]
      $\left|\left\{\langle i, k+1\rangle, \ldots, \langle i, \left\lfloor \frac{x}{n} \right\rfloor\rangle\right\}\right| =$
      $\left\lfloor \frac{x}{n} \right\rfloor - k =$ [per la proprietà 2.19]
      $\left\lfloor \frac{x-nk}{n} \right\rfloor =$ [per ipotesi]
      $\left\lfloor \frac{x-|t|}{n} \right\rfloor$

   (c) $|t| < |t'| \Rightarrow$
   $|t'| > |t| \Rightarrow$ [per definizione di ordinamento temporale]
   $t' > t \Rightarrow$ [essendo $t = \langle i, k\rangle$]
   $t' \geq \langle i, k+1\rangle$

□

Corollario 4.2. *Sia $T \equiv (n) \in \mathcal{L}^1$, con insieme delle componenti $\{i\}$. Per ogni $x \in \mathbb{N}$, il numero di trattini positivi di T di valore minore o uguale a x è $\left\lfloor \frac{x}{n} \right\rfloor$.*

Dimostrazione. Basta applicare la proposizione precedente con $k = 0$. Questo corollario, comunque, è molto simile alla proprietà 4.1, dalla quale può essere facilmente ricavato applicando la proprietà 3.7.

□

Il lettore può aver notato che le ultime proposizioni hanno in realtà più a che fare coi numeri che coi tratteggi: la proposizione 4.1 dice in sostanza che il più grande multiplo di n_i minore o uguale ad x è $n_i \left\lfloor \frac{x}{n_i} \right\rfloor$; la successiva dice che il numero di multipli di n_i compresi tra $n_i k$ ed x, primo estremo escluso, è $\left\lfloor \frac{x-n_i k}{n_i} \right\rfloor$. Sono cose abbastanza ovvie; ma perché dimostrarle nella teoria dei tratteggi, piuttosto che, in maniera più naturale, nella teoria dei numeri?
La risposta più immediata è che vogliamo studiare la teoria dei tratteggi, e le due proposizioni precedenti sono necessarie come base di altre che seguiranno, le quali a loro volta saranno espresse in termini di teoria dei tratteggi, non di teoria dei numeri; quindi è bene usare da subito i formalismi giusti.
La risposta più profonda è che la teoria dei tratteggi è un'astrazione costruita sopra la teoria dei numeri. Essa permette di vedere problemi e risultati relativi ai numeri da un'altra prospettiva: quella dei tratteggi appunto. Dopo aver letto questo libro, si dovrebbe avere un'idea di quanto questa prospettiva sia interessante e di quanto possa essere utile per risolvere problemi della teoria dei numeri, traducendoli in problemi della teoria dei tratteggi e sfruttando risultati di quest'ultima. Quindi il linguaggio dei numeri può essere preferibile a quello dei tratteggi in questa fase iniziale, ma in seguito la prospettiva sarà invertita.

Non ci si stupisca, inoltre, se molti teoremi sui tratteggi verranno dimostrati passando al formalismo dei numeri: questa commistione è normale, perché la teoria dei numeri è alla base della teoria dei tratteggi. Parleremo nei termini di quest'ultima solo quando serve per sviluppi successivi (come nel caso delle proposizioni 4.1 e 4.3) o per chiarire determinati concetti; altrimenti parleremo semplicemente di numeri.

Alcune proposizioni sui numeri appaiono più chiare, quando sono interpretate nella teoria dei tratteggi. Ad esempio:

Lemma 4.1. *Siano* $a, b, x \in \mathbb{N}^\star$. $\left|\left\{y > x \mid \left\lfloor \frac{ax}{b} \right\rfloor = \left\lfloor \frac{ay}{b} \right\rfloor\right\}\right| = \left\lfloor \frac{b-1-ax \bmod b}{a} \right\rfloor$[1]

Dimostrazione.

1. $\left|\left\{y > x \mid \left\lfloor \frac{ax}{b} \right\rfloor = \left\lfloor \frac{ay}{b} \right\rfloor\right\}\right| = \left\lfloor \frac{b-1-ax \bmod b}{a} \right\rfloor$

[1]Si sarebbe dovuto scrivere $\left|\left\{y \in \mathbb{N}^\star \mid y > x \wedge \left\lfloor \frac{ax}{b} \right\rfloor = \left\lfloor \frac{ay}{b} \right\rfloor\right\}\right|$, ma si intende che l'insieme di appartenenza di y è lo stesso di x. Molte volte si procederà in questo modo, per semplificare la notazione.

(a) $A \equiv$
$\left\{y > x \mid \left\lfloor \frac{ax}{b} \right\rfloor = \left\lfloor \frac{ay}{b} \right\rfloor\right\} =$ [per la proprietà 2.23]
$\left\{y > x \mid b\left\lfloor \frac{ax}{b} \right\rfloor \leq ay \leq b\left\lfloor \frac{ax}{b} \right\rfloor + b - 1\right\} =$ [per definizione, calcoli algebrici]
$\left\{y > x \mid ax - ax \bmod b \leq ay \leq b\left\lfloor \frac{ax}{b} \right\rfloor + b - 1\right\} =$ [da $y > x \Leftrightarrow ax < ay$]
$\left\{y \mid ax < ay \leq b\left\lfloor \frac{ax}{b} \right\rfloor + b - 1\right\}$

(b) $|A| =$ [banale; si può provare che $f \in [A \to aA]$ tale che $f(x) = ax$ per ogni $x \in A$ è una biezione tra A ed aA]
$|aA| =$ [da i., per la proposizione 4.3, considerando $T \equiv (a) \in \mathcal{L}^1$]
$\left\lfloor \frac{b\left\lfloor \frac{ax}{b} \right\rfloor + b - 1 - ax}{a} \right\rfloor =$
$\left\lfloor \frac{b\frac{ax - ax \bmod b}{b} + b - 1 - ax}{a} \right\rfloor =$
$\left\lfloor \frac{b - 1 - ax \bmod b}{a} \right\rfloor$

i. $aA = \left\{ay \mid ax < ay \leq b\left\lfloor \frac{ax}{b} \right\rfloor + b - 1\right\}$ [da (a)]

□

Questa proposizione può sembrare un inutile tecnicismo, ma a livello di tratteggi la si può enunciare in modo molto più interessante:

Proposizione 4.4. *Siano $(a, b) \in \mathcal{L}^2$ e $s \equiv \langle 1, x\rangle \in (a)$ e sia u il più piccolo trattino di (b) maggiore di s.* $|\{t \in (a) \mid |s| < |t| < |u|\}| = \left\lfloor \frac{b - 1 - ax \bmod b}{a} \right\rfloor$.

Dimostrazione.

1. $|\{t \in (a) \mid |s| < |t| < |u|\}| = \left\lfloor \frac{b - 1 - ax \bmod b}{a} \right\rfloor$ [da 2. e 3.]
2. Siano $A \equiv \left\{y > x \mid \left\lfloor \frac{ax}{b} \right\rfloor = \left\lfloor \frac{ay}{b} \right\rfloor\right\}$ e $B \equiv \{t \in (a) \mid |s| < |t| < |u|\}$
3. $|B| =$ [da 4., 5. e 6.]
$|A| =$ [per il lemma 4.1]
$\left\lfloor \frac{b - 1 - ax \bmod b}{a} \right\rfloor$
4. Sia $f \in [A \to B]$ tale che $f(z) = \langle 1, z\rangle$ per ogni $z \in A$
5. f è iniettiva [da (a) e (a)–i.]

(a) Siano $z, w \in A$

i. $z \neq w \Rightarrow$
$\langle 1, z\rangle \neq \langle 1, w\rangle \Rightarrow$ [da 4.]
$f(z) \neq f(w)$

6. f è suriettiva [da (a) e (b)]

   (a) Sia $t \equiv \langle 1, y\rangle \in B$

   (b) $f(y) = \langle 1, y\rangle = t$ [da (a), (c) e 4.]

   (c) $y \in A$ [da (d) ed (e)]

   (d) $y > x$ [da i.]

      i. $ay > ax$ [da ii.]

      ii. $|\langle 1, y\rangle| > |\langle 1, x\rangle|$ [da 2., per definizione di B e di s]

   (e) $\left\lfloor \frac{ax}{b} \right\rfloor = \left\lfloor \frac{ay}{b} \right\rfloor$ [da i., i.–A. e (a) (assurdo perché $|\langle 1, y\rangle| < |u| \Rightarrow \langle 1, y\rangle \notin B$), da ii., ii.–B. e (d) (altro assurdo)]

      i. Se $\left\lfloor \frac{ax}{b} \right\rfloor < \left\lfloor \frac{ay}{b} \right\rfloor$

         A. $|\langle a, y\rangle| =$
         $ay \geq$ [da i. per la proprietà 2.24]
         $b\left(\left\lfloor \frac{ax}{b} \right\rfloor + 1\right) \geq$
         $b\left\lceil \frac{ax}{b} \right\rceil =$ [per la proposizione 4.1]
         $|u|$

      ii. Se $\left\lfloor \frac{ax}{b} \right\rfloor > \left\lfloor \frac{ay}{b} \right\rfloor$

         A. $y < x$ [da B.]

         B. $ay <$ [per la proprietà 2.25]
         $b\left\lfloor \frac{ax}{b} \right\rfloor =$ [per definizione, calcoli algebrici]
         $ax - ax \bmod b \leq$ [da $ax \bmod b \geq 0$]
         ax

□

Il passaggio dai numeri ai tratteggi è molto semplice a livello intuitivo: basta definire la giusta biezione tra un insieme numerico ed un insieme di trattini, come nella dimostrazione della proposizione 4.4. D'altra parte, però, la dimostrazione di biettività è spesso lunga e noiosa.
Si potrebbe allora lavorare direttamente nei tratteggi, quando è possibile. Ad esempio, si potrebbe dimostrare la proposizione 4.4 nel modo seguente:

Dimostrazione.

1. $|\{t \in (a) \mid |s| < |t| < |u|\}| =$
   $|\{t \in (a) \mid |s| < |t| \leq |u| - 1\}| =$ [da (a)]
   $|\{t \in (a) \mid |s| < |t| \leq ax - ax \bmod b + b - 1\}| =$ [per la proposizione 4.4]

$$\left\lfloor \frac{ax - ax \bmod b + b - 1 - |s|}{a} \right\rfloor = [\text{da } s = \langle 1, x \rangle]$$
$$\left\lfloor \frac{ax - ax \bmod b + b - 1 - ax}{a} \right\rfloor =$$
$$\left\lfloor \frac{b - 1 - ax \bmod b}{a} \right\rfloor$$

(a) $|u| =$ [perché il tratteggio è lineare]
$b \left\lceil \frac{|s|+1}{b} \right\rceil =$ [da $s = \langle a, x \rangle$]
$b \left\lceil \frac{ax+1}{b} \right\rceil =$ [per la proprietà 2.21]
$b \left(\left\lfloor \frac{ax}{b} \right\rfloor + 1 \right) =$ [per definizione, calcoli algebrici]
$ax - ax \bmod b + b$

(b) $u = \left\langle 2, \left\lceil \frac{|s|+1}{b} \right\rceil \right\rangle$ [da (c), per la proposizione 4.1, ricordando che $(b) = T\,[2]$]

(c) u è il più piccolo trattino di (b) di valore maggiore o uguale a $|s|+1$ [dalle ipotesi]

□

Alcuni lettori potranno considerare questa dimostrazione più elegante della precedente, perché si basa su proposizioni precedenti della teoria dei tratteggi. Così però non è evidente la connessione tra tratteggi e numeri, un aspetto fondamentale che non può essere trascurato.
Potremmo passare dai tratteggi ai numeri, dimostrando il lemma 4.2 partendo dalla proposizione 4.4 dimostrata nel secondo modo. La biezione è sempre la stessa; guardarla in un senso piuttosto che in un altro è questione di gusti, l'importante è non perderla di vista.
Nel resto del libro avremo troppe cose da dimostrare per poterci permettere di discutere su quale sia l'approccio migliore per farlo; faremo di volta in volta come sarà più comodo. Cercheremo di favorire la percezione della teoria dei tratteggi come un modo particolare di studiare i numeri.

Ora per completezza enunciamo un risultato molto simile al 4.1, che utilizza la parte intera per eccesso anziché per difetto, interpretandolo poi nei tratteggi.

Lemma 4.2. *Siano* $a, b, x \in \mathbb{N}^\star$. $\left|\left\{y > x \mid \left\lceil \frac{ax}{b} \right\rceil = \left\lceil \frac{ay}{b} \right\rceil\right\}\right| = \left\lfloor \frac{b - ax \bmod b}{a} \right\rfloor$.

Lasciamo al lettore la dimostrazione, che può essere simile a quella del lemma 4.1, o basata sulla seguente proposizione:

Proposizione 4.5. *Siano* $(a, b) \in \mathcal{L}^2$ *e* $s \equiv \langle 1, x \rangle \in (a)$ *e sia* u *il più piccolo trattino di* (b) *maggiore di* s. $|\{t \in (a) \mid |s| < |t| \leq |u|\}| = \left\lfloor \frac{b - ax \bmod b}{a} \right\rfloor$.

Il lettore può verificare che la biezione tra $\left\{y > x \mid \left\lceil \frac{ax}{b} \right\rceil = \left\lceil \frac{ay}{b} \right\rceil\right\}$ e $\{t \in (a) \mid |s| < |t| \leq |u|\}$ è la stessa di quella definita nella dimostrazione della proposizione 4.4, cambiano solo il dominio e l'insieme di arrivo. Dimostrando che esiste tale biezione, si può dimostrare la proposizione 4.5 ricorrendo al lemma 4.2, se questo è stato già dimostrato; oppure si può dimostrare la proposizione direttamente, in modo del tutto analogo a come si è fatto per la 4.4. Non facciamo nessuna delle due cose, per evitare di annoiare, essendo le dimostrazioni perfettamente analoghe alle precedenti.

4.2 Proprietà di classi e spazi

Un'importante conseguenza dell'osservazione 3.1 riguarda il calcolo del numero di classi con valore in un certo intervallo. Esso si basa fortemente sul principio di inclusione-esclusione. Ad esempio, in un tratteggio di secondo ordine T, le classi possono contenere o un trattino di $T[1]$, o un trattino di $T[2]$, o entrambi: dunque il loro numero è dato dal numero di classi che contengono almeno un trattino di $T[1]$, più il numero delle classi che contengono almeno un trattino di $T[2]$, meno il numero delle classi che contengono un trattino di $T[1]$ ed un trattino di $T[2]$. Infatti, se non si effettuasse l'ultima sottrazione, le classi che contengono sia un trattino di $T[1]$ che un trattino di $T[2]$ verrebbero conteggiate due volte: una volta perché contengono un trattino di $T[1]$ ed una volta perché contengono un trattino di $T[2]$. Ciò, nel caso dei tratteggi lineari, è formalizzato nella seguente proposizione:

Proposizione 4.6. *Siano* $T \equiv (n_1, n_2) \in \mathcal{L}^2$ *ed* $n \in \mathbb{N}$. *Allora* $|\{c \text{ classe di } T \mid 0 < |c| \leq n\}| = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{\mathrm{MCM}(n_1,n_2)} \right\rfloor$.

Dimostrazione.

1. Sia $C_i \equiv \{c \text{ classe di } T[i] \mid 0 < |c| \leq n\}$, per $i \in \{1, 2\}$

2. $|\{c \text{ classe di } T \mid 0 < |c| \leq n\}| =$ [perché $T \in \mathcal{L}^2$ e per definizione di classe]
   $|C_1 \cup C_2| =$ [per il principio di inclusione-esclusione]
   $|C_1| + |C_2| - |C_1 \cap C_2| =$ [da (a), per il corollario 4.2]
   $\left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - |C_1 \cap C_2| =$ [da (b), per il corollario 4.2]
   $\left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{\mathrm{MCM}(n_1,n_2)} \right\rfloor$

   (a) $C_i =$ [da 1., perché $T[i] \in \mathcal{T}^1$, quindi le classi sono insiemi costituiti da un solo trattino]
   $\{\{t\} \text{ classe di } T[i] \mid 0 < |\{t\}| \leq n\} =$ [per definizione di valore di una classe]

$\{\{t\}$ classe di $T[i] \mid 0 < |t| \leq n\} =$ [per definizione di classe]
$\{\{t\} \mid t \in T[i] \wedge 0 < |t| \leq n\} =$
$\{t \mid t \in T[i] \wedge 0 < |t| \leq n\}$

(b) $C_1 \cap C_2 =$
$\{c$ classe di $T[1]$ e di $T[2] \mid 0 < |c| \leq n\} =$
$\{c$ classe di T di cardinalità $2 \mid 0 < |c| \leq n\} =$
$\{c$ classe di T di cardinalità 2 di valore $m \mid 0 < m \leq n\}$ = [per l'osservazione 3.1]
$\{m \mid (\mathrm{MCM}(n_1, n_2) \mid m \wedge 0 < m \leq n)\}$ = [un multiplo di $\mathrm{MCM}(n_1, n_2)$ è il valore di un trattino di $(\mathrm{MCM}(n_1, n_2)) \in \mathcal{L}^1$]
$\{t \in (\mathrm{MCM}(n_1, n_2)) \mid 0 < |t| \leq n\}$

□

Se n è multiplo di $\mathrm{MCM}(n_1, n_2)$, la formula trovata nella proposizione 4.6 assume una forma particolarmente semplice:

Corollario 4.3. *Siano $T \equiv (n_1, n_2) \in \mathcal{L}^2$ ed $m \in \mathbb{N}$. Allora*

$$|\{c \text{ classe di } T \mid 0 < |c| \leq m\mathrm{MCM}(n_1, n_2)\}| = m\left(\frac{n_1 + n_2}{\mathrm{MCD}(n_1, n_2)} - 1\right)$$

Dimostrazione.

1. $|\{c$ classe di $T \mid 0 < |c| \leq m\mathrm{MCM}(n_1, n_2)\}|$ = [per la proposizione 4.6]
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_2} \right\rfloor - \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{\mathrm{MCM}(n_1,n_2)} \right\rfloor =$
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_2} \right\rfloor - m =$ [perché $n_1 \mid \mathrm{MCM}(n_1, n_2)$ e $n_2 \mid \mathrm{MCM}(n_1, n_2)$]
$\frac{m\mathrm{MCM}(n_1,n_2)}{n_1} + \frac{m\mathrm{MCM}(n_1,n_2)}{n_2} - m =$
$m\left(\frac{\mathrm{MCM}(n_1,n_2)}{n_1} + \frac{\mathrm{MCM}(n_1,n_2)}{n_2} - 1\right) =$
$m\left(\frac{n_2\mathrm{MCM}(n_1,n_2)+n_1\mathrm{MCM}(n_1,n_2)}{n_1 n_2} - 1\right) =$
$m\left(\frac{(n_1+n_2)\mathrm{MCM}(n_1,n_2)}{n_1 n_2} - 1\right) =$ [perché $n_1 n_2 = \mathrm{MCM}(n_1, n_2)\,\mathrm{MCD}(n_1, n_2)$]
$m\left(\frac{n_1+n_2}{\mathrm{MCD}(n_1,n_2)} - 1\right)$

□

Per la complementarietà di classi e spazi, dal corollario 4.3 si può ricavare facilmente la formula per calcolare il numero di spazi minori di $m\mathrm{MCM}(n_1, n_2)$:

Proposizione 4.7. *Siano $T \equiv (n_1, n_2) \in \mathcal{L}^2$ ed $m \in \mathbb{N}$. Allora*

$$|\{s \text{ spazio di } T \mid 0 < s \leq m\mathrm{MCM}(n_1, n_2)\}| = m\left(\frac{(n_1 - 1)(n_2 - 1) - 1}{\mathrm{MCD}(n_1, n_2)} + 1\right)$$

Dimostrazione.

1. $|\{s \text{ spazio di } T \mid 0 < s \leq m\text{MCM}(n_1, n_2)\}| =$
   $|\{s \in [1, m\text{MCM}(n_1, n_2)] \mid s \text{ è uno spazio di } T\}| =$ [per la proprietà 3.4]
   $|[1, m\text{MCM}(n_1, n_2)]| - |\{s \in [1, m\text{MCM}(n_1, n_2)] \mid s \text{ è una classe di } T\}| =$
   $m\text{MCM}(n_1, n_2) - |\{s \in [1, m\text{MCM}(n_1, n_2)] \mid s \text{ è una classe di } T\}| =$ [per il corollario 4.3]
   $m\text{MCM}(n_1, n_2) - m\left(\frac{n_1+n_2}{\text{MCD}(n_1,n_2)} - 1\right) =$
   $m\left(\text{MCM}(n_1, n_2) - \frac{n_1+n_2}{\text{MCD}(n_1,n_2)} + 1\right) =$
   $m\left(\frac{\text{MCD}(n_1,n_2)\text{MCM}(n_1,n_2)-n_1-n_2}{\text{MCD}(n_1,n_2)} + 1\right) =$
   $m\left(\frac{n_1 n_2-n_1-n_2}{\text{MCD}(n_1,n_2)} + 1\right) =$
   $m\left(\frac{(n_1-1)(n_2-1)-1}{\text{MCD}(n_1,n_2)} + 1\right)$

□

Non è difficile immaginare che, sempre col principio di inclusione-esclusione, è possibile generalizzare la proposizione 4.6 a tratteggi lineari di ordine $d \in \mathbb{N}^\star$.

4.3 Periodicità

Chiudiamo con l'osservare che i tratteggi lineari finiti sono periodici. Ad esempio, il tratteggio $T_1 \equiv (2, 3)$ ha periodo pari a 5 e lunghezza di un dominio fondamentale pari a 6, come si vede in tabella 3.1. In generale:

Proposizione 4.8. *Sia $T \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$, $d \in \mathbb{N}^\star$. S è periodico, con periodo $\sum_{i=1}^{d} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_i}$ e lunghezza di un dominio fondamentale pari a $\text{MCM}(n_1, \ldots, n_d)$.*

Dimostrazione.

1. S è periodico, con periodo $\sum_{i=1}^{d} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_i}$ e lunghezza di un dominio fondamentale pari a $\text{MCM}(n_1, \ldots, n_d)$ [da 2., 3. e 4., per la definizione 1.15]

2. Siano $n \equiv \sum_{i=1}^{d} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_i}$ e $m \equiv \text{MCM}(n_1, \ldots, n_d)$; sia, per ogni $t \in T$, t_n l'n-esimo trattino successivo a T

3. $\forall t \in T : T(t) = T(t_n) - m \wedge \text{ind}(t) = \text{ind}(t_n)$ [da 2., (a), (b), (c) e (d)]

   (a) Sia $t \equiv \langle i, k \rangle \in T$

   (b) Sia $v \equiv \left\langle i, k + \frac{\text{MCM}(n_1,\ldots,n_d)}{n_i} \right\rangle$ [k e i definiti in (a)]

(c) $v = t_n$ [da (e) e per la definizione di t_n data in 2.]

(d) $T(t) =$ [da (a), per definizione di T]
$n_i k =$
$n_i \left(k + \frac{\mathrm{MCM}(n_1,\ldots,n_d)}{n_i}\right) - \mathrm{MCM}(n_1,\ldots,n_d) =$ [da (b), per definizione di T]
$T(v) - \mathrm{MCM}(n_1,\ldots,n_d) =$ [da 2.]
$T(v) - m$

(e) $|\{u \in T \mid t \leq u < v\}| =$
[da (f), perché $|\{u \in T \mid t \leq u < v\}| = |\{u \in T \mid t \leq u \leq v\}| - 1$]
$\sum_{i=1}^{d} \frac{\mathrm{MCM}(n_1,\ldots,n_d)}{n_i} =$ [da 2.]
n

(f) $|\{u \in T \mid t \leq u \leq v\}| =$ [per la proprietà 3.12, da (a) e (b) e perché T, essendo lineare, è strettamente monotono]
$|\{u \equiv \langle j,l\rangle \in T \mid T(t) + (j < i) \leq T(u) \leq T(v) - (j > i)\}| =$ [per la proprietà 3.10]
$\sum_{j=1}^{i-1} |\{u \equiv \langle j,l\rangle \in T \mid T(t) + (j < i) \leq T(u) \leq T(v) - (j > i)\}| +$
$|\{u \equiv \langle i,l\rangle \mid T(t) + (i < i) \leq T(u) \leq T(v) - (i > i)\}| +$
$\sum_{j=i+1}^{d} |\{u \equiv \langle j,l\rangle \in T \mid T(t) + (j < i) \leq T(u) \leq T(v) - (j > i)\}| =$ [da i., ii. e iii.]
$\sum_{j=1}^{i-1} \left\lfloor \frac{T(v)-T(t)}{n_j} \right\rfloor + \left(\left\lfloor \frac{T(v)-T(t)}{n_i} \right\rfloor + 1\right) + \sum_{j=i+1}^{d} \left\lceil \frac{T(v)-T(t)}{n_j} \right\rceil =$ [da d. e 2.]
$\sum_{j=1}^{i-1} \frac{\mathrm{MCM}(n_1,\ldots,n_d)}{n_j} + \left(\frac{\mathrm{MCM}(n_1,\ldots,n_d)}{n_i} + 1\right) + \sum_{j=i+1}^{d} \frac{\mathrm{MCM}(n_1,\ldots,n_d)}{n_j} =$
$\sum_{i=1}^{d} \frac{\mathrm{MCM}(n_1,\ldots,n_d)}{n_i} + 1$

i. $\sum_{j=1}^{i-1} |\{u \equiv \langle j,l\rangle \in T \mid T(t) + (j < i) \leq T(u) \leq T(v) - (j > i)\}| =$ [perché $j < i$ per tutta la sommatoria]
$\sum_{j=1}^{i-1} |\{u \equiv \langle j,l\rangle \in T \mid T(t) + 1 \leq T(u) \leq T(v)\}| =$ [per la proposizione 4.3]
$\sum_{j=1}^{i-1} \left\lfloor \frac{T(v)-T(t)}{n_j} \right\rfloor$

ii. $|\{u \equiv \langle i,l\rangle \mid T(t) + (i < i) \leq T(u) \leq T(v) - (i > i)\}| =$
$|\{u \equiv \langle i,l\rangle \mid T(t) \leq T(u) \leq T(v)\}| =$ [per la stretta monotonia di T]
$|\{u \equiv \langle i,l\rangle \mid T(t) < T(u) \leq T(v)\}| + 1 =$ [per la proposizione 4.3]
$\left\lfloor \frac{T(v)-T(t)}{n_i} \right\rfloor + 1$

iii. $\sum_{j=i+1}^{d} |\{u \equiv \langle j, l\rangle \in T \mid T(t) + (j < i) \leq T(u) \leq T(v) - (j > i)\}| =$ [perché $j > i$ per tutta la sommatoria]
$\sum_{j=i+1}^{d} |\{u \equiv \langle j, l\rangle \in T \mid T(t) \leq T(u) \leq T(v) - 1\}| =$ [per la stretta monotonia di T]
$\sum_{j=i+1}^{d} (|\{u \equiv \langle j, l\rangle \in T \mid T(t) < T(u) \leq T(v) - 1\}| + 1) =$ [per la proposizione 4.3]
$\sum_{j=i+1}^{d} \left(\left\lfloor \frac{T(v)-1-T(t)}{n_j} \right\rfloor + 1 \right) =$ [per la proprietà 2.21]
$\sum_{j=i+1}^{d} \left\lceil \frac{T(v)-T(t)}{n_j} \right\rceil$

4. $\exists n' \exists m \forall t \in T : T(t) = T(t_{n'}) - m \wedge \text{ind}(t) = \text{ind}(t_{n'}) \Rightarrow n' \geq \sum_{i=1}^{d} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_i}$ [da (a) e (c)]

   (a) Siano $n' \in \mathbb{N}^\star$, $m \in \mathbb{N}^\star$ tali che $\forall t \in T : T(t) = T(t_{n'}) - m \wedge \text{ind}(t) = \text{ind}(t_{n'})$

   (b) Sia $t \equiv \langle n_i, k\rangle \in T$

   (c) $n' =$ [da (a) e (b), per definizione di $t_{n'}$. Inoltre, per 4., n' non dipende dalla scelta di t]
   $|\{u \in T \mid t \leq u \leq t_{n'}\}| - 1 =$ [da 3.–(f) e 4. (in particolare, $\text{ind}(t) = \text{ind}(t_{n'})$), ponendo $v \equiv t_{n'}$]
   $\sum_{j=1}^{i-1} \left\lfloor \frac{T(t_{n'})-T(t)}{n_j} \right\rfloor + \left(\left\lfloor \frac{T(t_{n'})-T(t)}{n_i} \right\rfloor + 1 \right) + \sum_{j=i+1}^{d} \left\lceil \frac{T(t_{n'})-T(t)}{n_j} \right\rceil - 1 =$ [per la proprietà 3.10]
   $\sum_{j=1}^{i-1} \left\lfloor \frac{m}{n_j} \right\rfloor + \left(\left\lfloor \frac{m}{n_i} \right\rfloor + 1 \right) + \sum_{j=i+1}^{d} \left\lceil \frac{m}{n_j} \right\rceil - 1 \geq$ [da (d)]
   $\sum_{j=1}^{i-1} \left\lfloor \frac{\text{MCM}(n_1,\ldots,n_d)}{n_j} \right\rfloor + \left(\left\lfloor \frac{\text{MCM}(n_1,\ldots,n_d)}{n_i} \right\rfloor + 1 \right) + \sum_{j=i+1}^{d} \left\lceil \frac{\text{MCM}(n_1,\ldots,n_d)}{n_j} \right\rceil - 1 =$
   $\sum_{j=1}^{i-1} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_j} + \left(\frac{\text{MCM}(n_1,\ldots,n_d)}{n_i} + 1 \right) + \sum_{j=i+1}^{d} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_j} - 1 =$
   $\sum_{j=i}^{d} \frac{\text{MCM}(n_1,\ldots,n_d)}{n_j} =$ [da 2.]
   n

   (d) $m \geq \text{MCM}(n_1, \ldots, n_d)$ [da (e) e perché $m \in \mathbb{N}^\star$]

   (e) $\text{MCM}(n_1, \ldots, n_d) \mid m$ [da (f)]

   (f) $\forall n_i \in \{n_1, \ldots, n_d\} : n_i \mid m$ [da i. e ii.]

      i. Sia $t \equiv \langle n_i, k\rangle \in T$

ii. $n_i \mid m$ [da iii.]

iii. $m =$ [da 4.]
$T(t_{n'}) - T(t) =$ [da iv. e v.]
$n_i h - n_i k =$
$n_i (h - k)$

iv. $T(t) = n_i k$ [perché T è lineare]

v. $T(t_{n'}) = n_i h$ [da vi., perché T è lineare]

vi. $t_{n'} = \langle n_i, h \rangle$, $h \in \mathbb{N}$ [da i. e 4. (in particolare, $\text{ind}(t) = \text{ind}(t_{n'})$)]

□

Si noti che nel caso di $d = 1$, $\text{MCM}(n_1, \ldots, n_d) = \text{MCM}(n_1)$ che si pone pari ad n_1 stesso. Dunque un tratteggio di primo ordine (n_i) ha periodo 1 e lunghezza di un dominio fondamentale pari a n_i.

4.4 Tratteggi lineari e numeri primi

Un'interessante applicazione dei tratteggi lineari, che è stata anche ciò che ha fatto nascere la teoria dei tratteggi, è lo studio dei numeri primi. In particolare, uno degli obiettivi principali è trovare un metodo per calcolare l'n-esimo numero primo, utilizzando la teoria dei tratteggi.
Questo problema è stato già risolto da alcuni algoritmi, come il famoso crivello di Eratostene. Tuttavia, il metodo che vogliamo è molto diverso dal crivello di Eratostene: l'intento è esprimere l'n-esimo numero primo mediante una formula matematica, piuttosto che con un algoritmo iterativo. In realtà l'intento non è trovare una singola formula che permetta di calcolare i primi, ma si vorrebbe definire una famiglia di formule, che risolvano il problema, in un certo senso, a livelli di precisione crescenti. Vediamo più in dettaglio cosa significa.

Consideriamo il tratteggio lineare $(2, 3)$; in particolare, analizziamo i suoi spazi. Si ha che:

$$
\begin{gathered}
x \text{ è uno spazio di } (2,3) \Leftrightarrow \\
\neg \exists t \in (2,3) : |t| = x \Leftrightarrow \\
\neg \exists \langle i, k \rangle \in \text{Tratt}_2 : \begin{cases} 2k & \text{se } i = 1 \\ 3k & \text{se } i = 2 \end{cases} = x \Leftrightarrow \\
\neg \left(\exists k \in \mathbb{N} \, \exists c \in \{2,3\} : ck = x \right) \Leftrightarrow \\
\neg \exists c \in \{2,3\} : c \mid x \Leftrightarrow \\
2 \nmid x \wedge 3 \nmid x
\end{gathered}
$$

Cioè gli spazi di $(2,3)$ sono tutti i numeri non divisibili né per 2, né per 3: formalmente:

$$\text{t\_spazio}_{(2,3)}(\mathbb{N}^\star) = \{x \in \mathbb{N} \mid (2 \nmid x \wedge 3 \nmid x)\} = \{1,5,7,11,13,17,19,23,25,29,31,\ldots\}$$

Come è facile osservare, tutti gli spazi di $(2,3)$ fino a 23 sono numeri primi (eccetto 1 che si può considerare un caso particolare). Ciò è naturale, perché se un numero composto non è divisibile né per 2 e né per 3, significa che il suo più piccolo divisore è 5: esso sarà quindi maggiore o uguale a $5 \cdot 5$, cioè 25.
Viceversa, non tutti i numeri primi minori o uguali a 23 sono spazi di $(2,3)$; tuttavia, gli unici mancanti sono proprio 2 e 3. Anche questo è evidente, perché se un numero primo *è* divisibile per 2 o per 3 (cioè che *non* è uno spazio di $(2,3)$), esso non può che coincidere con 2 o con 3, altrimenti sarebbe composto.

Quindi la successione $\left\{\text{t\_spazio}_{(2,3)}(x)\right\}_{x\in\mathbb{N}^\star}$ contiene, nell'ordine, la sequenza dei numeri primi compresi tra 5 e 23. Più esplicitamente, indicando con p_n l'n-esimo numero primo, abbiamo che $\text{t\_spazio}_{(2,3)}(2) = p_3 = 5$, $\text{t\_spazio}_{(2,3)}(3) = p_4 = 7$, …, $\text{t\_spazio}_{(2,3)}(8) = p_7 = 23$, ossia $\forall p_i : 5 \leq \text{t\_spazio}_T(i) \leq 23 \Rightarrow \text{t\_spazio}_{(2,3)}(i) = p_{i+1}$. Abbiamo trovato un modo per calcolare esattamente i numeri primi compresi tra 5 e 23. Non è granché come risultato, ma è un primo passo. Tutto può essere generalizzato partendo dal tratteggio lineare $(2,\ldots,n)$, con n fissato:

Proposizione 4.9. *Siano $n \geq 2$, $T = (2,\ldots,n) \in \mathcal{L}^{n-1}$ e $k = |\{x \in \mathbb{N} \mid 2 \leq x \leq n \wedge x \text{ è primo}\}|$. Allora*

$$\forall i : n+1 \leq \text{t\_spazio}_T(i) < (n+1)^2 \Rightarrow \text{t\_spazio}_T(i) = p_{i+k-1}$$

La proposizione è dimostrabile più facilmente partendo dai seguenti lemmi:

Lemma 4.3. *Siano $\{a_i\}_{i\in\mathbb{N}^\star}$ e $\{b_j\}_{j\in\mathbb{N}^\star}$ due successioni strettamente crescenti di numeri naturali, e sia p tale che $a_p = b_q$, per qualche q. Allora:*
$q = p + |\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus \{a_1,\ldots,a_p\}| - |\{a_1,\ldots,a_p\} \setminus \{b_j \mid j \in \mathbb{N}^\star\}|$.

Dimostrazione.

1. $q = p + |\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus \{a_1,\ldots,a_p\}| - |\{a_1,\ldots,a_p\} \setminus \{b_j \mid j \in \mathbb{N}^\star\}|$ [da 3.)]

2. Siano $A \equiv \{0,\ldots,a_p\} \cap \{a_i \mid i \in \mathbb{N}^\star\}$ e $B \equiv \{0,\ldots,a_p\} \cap \{b_j \mid j \in \mathbb{N}^\star\}$

3. $q - p =$ [da 4. e 5.]
   $|B \setminus A| - |A \setminus B| =$ [da 2.]
   $|(\{0,\ldots,a_p\} \cap \{b_j \mid j \in \mathbb{N}^\star\}) \setminus A| - |A \setminus (\{0,\ldots,a_p\} \cap \{b_j \mid j \in \mathbb{N}^\star\})| =$ [per

ipotesi $\{b_j \mid j \in \mathbb{N}^\star\} \subseteq \mathbb{N}$]
$|\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus A| - |A \setminus (\{0, \ldots, a_p\} \cap \{b_j \mid j \in \mathbb{N}^\star\})| =$ [da 4.–(a)]
$|\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus \{a_1, \ldots, a_p\}| +$
$- |\{a_1, \ldots, a_p\} \setminus (\{0, \ldots, a_p\} \cap \{b_j \mid j \in \mathbb{N}^\star\})| =$
[per ogni terna di insiemi I_1, I_2 e I_3, $I_1 \setminus (I_2 \cap I_3) = (I_1 \setminus I_2) \cup (I_1 \setminus I_3)$]
$|\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus \{a_1, \ldots, a_p\}| +$
$- |(\{a_1, \ldots, a_p\} \setminus \{0, \ldots, a_p\}) \cup (\{a_1, \ldots, a_p\} \setminus \{b_j \mid j \in \mathbb{N}^\star\})| =$
[per ipotesi $\{a_i \mid i \in \mathbb{N}^\star\} \subseteq \mathbb{N}$ e $\{a_i\}_{i \in \mathbb{N}^\star}$ è strettamente crescente]
$|\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus \{a_1, \ldots, a_p\}| - |\emptyset \cup (\{a_1, \ldots, a_p\} \setminus \{b_j \mid j \in \mathbb{N}^\star\})| =$
$|\{b_j \mid j \in \mathbb{N}^\star \wedge b_j \leq a_p\} \setminus \{a_1, \ldots, a_p\}| - |\{a_1, \ldots, a_p\} \setminus \{b_j \mid j \in \mathbb{N}^\star\}|$

4. $p =$ [da 3.]
   $|A| =$ [perché per ogni coppia di insiemi I_1 e I_2, $I_2 \neq \emptyset$, $\{\{I_1 \cap I_2\}, \{I_1 \setminus I_2\}\}$ è una partizione di I_1]
   $|A \cap B| + |A \setminus B|$

   (a) $A = \{a_1, \ldots, a_p\}$ [da 1., perché $\{a_i\}_{i \in \mathbb{N}^\star}$ è strettamente crescente]

5. $q =$ [da 3.]
   $|B| =$ [come la seconda uguaglianza della 4.]
   $|A \cap B| + |B \setminus A|$

   (a) $B = \{b_1, \ldots, b_q\}$ [da 2., perché $\{b_j\}_{j \in \mathbb{N}^\star}$ è strettamente crescente e $a_p = b_q$]

□

Lemma 4.4. $\forall n \in \mathbb{N} : n \geq 1 \wedge (\forall m \in \{2, \ldots, \lfloor \sqrt{n} \rfloor\} : m \nmid n) \Rightarrow n$ *è primo.*

Non dimostriamo questo lemma, perché è un risultato noto in teoria dei numeri.

Lemma 4.5. *Siano* $n \in \mathbb{N}$, $n \geq 2$, $T \equiv (2, \ldots, n)$ *e* $n + 1 \leq p_j$. *Allora* p_j *è uno spazio di* T.

Dimostrazione.

1. p_j è uno spazio di T [da 2.]

2. $\forall m \in \{2, \ldots, n\} : m \nmid p_j$ [da 3., perché p_j è primo]

3. $p_j > n$ [per ipotesi]

□

Lemma 4.6. *Siano* $n \in \mathbb{N}$, $n \geq 2$, $T \equiv (2, \ldots, n)$. $\forall i \in \mathbb{N}^\star : n+1 \leq \text{t\_spazio}_T(i) < (n+1)^2 \Rightarrow \text{t\_spazio}_T(i)$ *è primo.*

Dimostrazione.

1. Sia i tale che $n+1 \leq \text{t\_spazio}_T(i) < (n+1)^2$

   (a) $\text{t\_spazio}_T(i)$ è primo [da (b), per il lemma 4.4]

   (b) $\forall m \in \left\{2, \ldots, \left\lfloor \sqrt{\text{t\_spazio}_T(i)} \right\rfloor \right\} : m \nmid \text{t\_spazio}_T(i)$ [da (c) e (d)]

   (c) $\forall m \in \{2, \ldots, n\} : m \nmid \text{t\_spazio}_T(i)$ [dalla definizione di t_spazio]

   (d) $n \geq \left\lfloor \sqrt{\text{t\_spazio}_T(i)} \right\rfloor$ [da i., perché n è intero]

      i. $n \geq \sqrt{\text{t\_spazio}_T(i)}$ [da ii.]

      ii. $\sqrt{\text{t\_spazio}_T(i)} < n+1$ [da 1., in particolare da $\text{t\_spazio}_T(i) < (n+1)^2$]

□

Dimostriamo ora la proposizione 4.9:

Dimostrazione.

1. Sia i tale che $n+1 \leq \text{t\_spazio}_T(i) < (n+1)^2$

   (a) $\text{t\_spazio}_T(i) =$ [da 2., per i lemmi 4.6 e 4.3]

   $p_{i+|\{p_j | j \in \mathbb{N}^\star \wedge p_j \leq \text{t\_spazio}_T(i)\} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})| - |\text{t\_spazio}_T(\{1,\ldots,i\}) \setminus \{p_j | j \in \mathbb{N}^\star\}|}$ = [da ii. e iii.]

   p_{i+k-1}

      i. Sia $P_{a,b} \equiv \{p_j \mid j \in \mathbb{N}^\star \wedge a \leq p_j \leq b\}$

      ii. $|\{p_j \mid j \in \mathbb{N}^\star \wedge p_j \leq \text{t\_spazio}_T(i)\} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})| =$ [da i.]
      $\left|P_{2,\text{t\_spazio}_T(i)} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})\right| =$
      $\left|\left(P_{2,n} \cup P_{n+1,\text{t\_spazio}_T(i)}\right) \setminus \text{t\_spazio}_T(\{1,\ldots,i\})\right| =$
      [perché $P_{2,n} \cap P_{n+1,\text{t\_spazio}_T(i)} = \emptyset$]
      $|P_{2,n} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})| + \left|P_{n+1,\text{t\_spazio}_T(i)} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})\right| =$
      [da (b)]
      $|P_{2,n}| + \left|P_{n+1,\text{t\_spazio}_T(i)} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})\right| =$ [per ipotesi]
      $k + \left|P_{n+1,\text{t\_spazio}_T(i)} \setminus \text{t\_spazio}_T(\{1,\ldots,i\})\right| =$ [per il lemma 4.5]
      $k + 0 =$
      k

iii. $|\text{t\_spazio}_T(\{1,\dots,i\}) \setminus \{p_j \mid j \in \mathbb{N}^\star\}| =$
$|(\{\text{t\_spazio}_T(1)\} \cup \text{t\_spazio}_T(\{2,\dots,i\})) \setminus \{p_j \mid j \in \mathbb{N}^\star\}| =$
[$\{\text{t\_spazio}_T(1)\}$ e $\text{t\_spazio}_T(\{2,\dots,i\})$ sono disgiunti]
$|\{\text{t\_spazio}_T(1)\} \setminus \{p_j \mid j \in \mathbb{N}^\star\}| + |\text{t\_spazio}_T(\{2,\dots,i\}) \setminus \{p_j \mid j \in \mathbb{N}^\star\}| =$
[1 non è primo]
$1 + |\text{t\_spazio}_T(\{2,\dots,i\}) \setminus \{p_j \mid j \in \mathbb{N}^\star\}| =$ [da A.]
$1 + 0 =$
1

A. $\forall m \in \{2,\dots,i\} : \text{t\_spazio}_T(m)$ è primo [da B. e C., per il lemma 4.6 e perché t_spazio è strettamente crescente]

B. $\text{t\_spazio}_T(2) \geq n+1$ [perché $\text{t\_spazio}_T(2) > \text{t\_spazio}_T(1) = 1$ e da (b)]

C. $\text{t\_spazio}_T(i) < (n+1)^2$ [da 1.]

(b) $2,\dots,n$ non sono spazi di T [perché sono indici di T]

□

Abbiamo così dimostrato che tutti gli spazi di $T \equiv (2,\dots,n)$, compresi tra $n+1$ e $(n+1)^2$ escluso, sono primi (in particolare, vale la relazione $\text{t\_spazio}_T(i) = p_{i+k-1}$). Vale però anche il viceversa: tutti i primi compresi tra gli stessi valori sono spazi T:

Proposizione 4.10. *Siano $n \in \mathbb{N}$, $n \geq 2$, $T \equiv (2,\dots,n)$ e $k = |\{x \in \mathbb{N} \mid 2 \leq x \leq n \wedge x \text{ è primo}\}|$. Allora*

$$\forall p_i : n+1 \leq p_i < (n+1)^2 \Rightarrow p_i = \text{t\_spazio}_T(i-k+1)$$

Dimostrazione.

1. Sia p_i tale che $n+1 \leq p_i < (n+1)^2$

   (a) $p_i = \text{t\_spazio}_T(i-k+1)$ [da (b), (c) e (c)–i.]

   (b) p_i è uno spazio di T [da i.]

      i. p_i non è divisibile per 2, …, n [perché p_i è primo e $2 \leq n < p$]

   (c) Sia $p_i = \text{t\_spazio}_T(j)$

      i. $n+1 \leq \text{t\_spazio}_T(j) < (n+1)^2 \Rightarrow$ [per la proposizione 4.9]
      $\text{t\_spazio}_T(j) = p_{j+k-1} \Rightarrow$ [da (c)]
      $p_i = p_{j+k-1} \Rightarrow$ [perché la successione $\{p_i\}$ è strettamente crescente]
      $i = j+k-1 \Rightarrow$
      $j = i-k+1$

□

Osserviamo che:

- Nel caso $n = 2$ la proposizione dice che $\forall p_i : 3 \leq p_i < 9 \Rightarrow p_i = \text{t\_spazio}_{(2)}(i)$. Gli spazi di (2) sono i numeri dispari, quindi stiamo dicendo che, se l'i-esimo numero primo è compreso tra 3 e 9 (quest'ultimo escluso, ma includendolo non cambia niente), esso è pari all'i-esimo numero dispari. In effetti, i numeri primi compresi tra 3 e 9 sono $p_2 = 3$, $p_3 = 5$ e $p_4 = 7$, ed essi coincidono rispettivamente col secondo, il terzo ed il quarto numero dispari.

- Se $n > 2$, si può anche dimostrare che $\forall p_i : n + 1 \leq p_i < (n + 2)^2 \Rightarrow p_i = \text{t\_spazio}_T(i + n - 2)$, ma l'espressione a destra del $<$ è sempre quadratica in n.

- Si può dimostrare lo stesso risultato, $\forall p_i : n + 1 \leq p_i < (n + 1)^2 \Rightarrow p_i = \text{t\_spazio}_T(i + n - 2)$, considerando $T \equiv (x \in \mathbb{N} \mid 2 \leq x \leq n \wedge x \text{ è primo})$ anziché $T \equiv (x \in \mathbb{N} \mid 2 \leq x \leq n)$. Infatti, come è facile dimostrare, i due tratteggi sono indistinguibili dal punto di vista degli spazi: un numero è spazio di uno se e solo se è spazio dell'altro. Questa proprietà ha delle implicazioni pratiche che vedremo tra un attimo.

Supponiamo ora di aver fissato i e di voler calcolare p_i. Possiamo applicare il corollario 4.10, o direttamente la proposizione 4.9:

- Se vogliamo applicare il corollario 4.10, dobbiamo trovare un n tale che $n+1 \leq p_i < (n + 1)^2$, ovviamente senza conoscere p_i. Inoltre, più piccolo è n, meglio è, perché il calcolo di t_spazio diventa sempre più oneroso al crescere dell'ordine del tratteggio (ma su questo torneremo più avanti). Ciò non è semplice; tuttavia, avendo a disposizione una stima di p_i, sia $\tilde{p_i}$, si può porre per esempio $n = \lfloor \sqrt{\tilde{p_i}} \rfloor$ o $n = \lceil \sqrt{\tilde{p_i}} \rceil$, calcolando $\text{t\_spazio}_T(i + n - 2)$, con $T \equiv (2, \ldots, n)$. Se poi il valore ottenuto dovesse essere minore di $n + 1$ o maggiore o uguale a $(n + 1)^2$, si può ritoccare la scelta di n e ricalcolare $\text{t\_spazio}_T(i + n - 2)$, con T opportunamente variato.

- Se vogliamo applicare la proposizione 4.9, notiamo innanzitutto che la formula $\forall i : n+1 \leq \text{t\_spazio}_T(i) < (n + 1)^2 \Rightarrow \text{t\_spazio}_T(i) = p_{i-n+2}$ si può esprimere in modo equivalente come $\forall i : n + 1 \leq \text{t\_spazio}_T(i + n - 2) < (n + 1)^2 \Rightarrow \text{t\_spazio}_T(i + n - 2) = p_i$. Dobbiamo quindi trovare un n tale che $n + 1 \leq \text{t\_spazio}_T(i + n - 2) < (n + 1)^2$, con $T \equiv (2, \ldots, n)$. Questo problema è più semplice del precedente, ma deve essere ancora studiato.

In entrambi i casi, ci riconduciamo al calcolo di t_spazio_T, dove $T \equiv (2, \ldots, n)$ per qualche n. Questo calcolo si può effettuare direttamente, oppure si può velocizzare considerando il tratteggio $T' \equiv (x \in \mathbb{N} \mid 2 \leq x \leq n \wedge x \text{ è primo})$. Infatti, come abbiamo osservato poc'anzi, esso ha gli stessi spazi di T, ma, avendo meno indici, permette di calcolare t_spazio più velocemente. Gli indici di T' sono i numeri primi minori o uguali ad n, con n fissato: è possibile trovarli applicando t_spazio stesso. Vediamo brevemente come.

Si comincia considerando $T_1 \equiv (2)$ e calcolando $h = \text{t\_spazio}_{T_1}(x)$ per $x = 1, 2, 3, \ldots$, fintanto che h è certamente primo (cioè $h < (2+1)^2 = 9$, applicando il lemma 4.6). Si ottiene così l'insieme $C_2 \equiv \left\{h \in \text{t\_spazio}_{T_1}(\mathbb{N}^\star) \mid h < 9\right\}$ che, per la proposizione 4.9, coincide con l'insieme $\{x \in \mathbb{N}^\star \mid x < 9 \wedge x \text{ primo}\}$. Se $\max C_2 \geq n$, possiamo porre $T' = (x \in C_2 \mid x \leq n)$ e fermarci: è facile dimostrare che questo coincide col tratteggio che volevamo, $(x \in \mathbb{N} \mid 2 \leq x \leq n \wedge x \text{ è primo})$, applicando le proposizioni 4.9 e 4.10. Altrimenti, si considera il tratteggio $T_2 \equiv (C_2)$ e si ripete lo stesso procedimento: si calcola $h = \text{t\_spazio}_{T_2}(x)$ per $x = 2, 3, \ldots$ (d'ora in poi partiamo sempre da $x = 2$), fintanto che $h < (\max C_2 + 1)^2$, ottenendo l'insieme $C_3 \equiv \left\{h \in \text{t\_spazio}_{T_2}(\mathbb{N}^\star) \mid \text{t\_spazio}_{T_2}(2) \leq h < (\max C_2 + 1)^2\right\}$; ma $\text{t\_spazio}_{T_2}(2) \geq \max C_2 + 1$ (perché, se non lo fosse, sarebbe o composto, o coincidente con uno dei coefficienti di T_2; invitiamo il lettore a riflettere su questo), quindi $C_3 = \left\{x \in \mathbb{N}^\star \mid \max C_2 + 1 \leq x < (\max C_2 + 1)^2 \wedge x \text{ primo}\right\}$. Ora, se $\max C_3 \geq n$, possiamo porre $T' = (x \in C_2 \cup C_3 \mid x \leq n)$ (otteniamo così quello che volevamo, invitiamo il lettore a dimostrarlo); altrimenti, si considera il tratteggio $(C_2 \cup C_3)$ e si ripete il procedimento. In questo modo, si ottengono successivamente gli insiemi $C_2, C_3, C_4, C_5, \ldots$, che contengono "pezzi" sempre più grossi della successione dei numeri primi, cominciando da $1 \in C_2$ e senza saltare nessun primo[2]. A un certo punto si raggiungerà o si supererà n: a quel punto si saranno trovati sicuramente tutti i primi minori o uguali ad n.

Abbiamo solo accennato a come si potrebbe risolvere il problema del calcolo dell'i-esimo numero primo – arrivando a considerare anche il problema del calcolo dei numeri primi minori o uguali ad n – applicando le proposizioni 4.10 e 4.9. Chiudiamo qui questo discorso, perché una trattazione approfondita ci allontanerebbe dalla teoria dei tratteggi. Continuiamo con altre considerazioni, rimanendo su un livello intuitivo.

Le proposizioni 4.10 e 4.9considerano il tratteggio *finito* $T \equiv (2, \ldots, n)$. Cosa succede se si considera il tratteggio infinito $T' \equiv (2, 3, \ldots)$? Innanzitutto, l'unico spazio di T' è 1: qualsiasi altro numero non è uno spazio, perché è un coefficiente

[2]Più formalmente, $\{C_i \mid i \geq 2\}$ è una partizione dell'insieme dei numeri primi.

del tratteggio. E i numeri primi? Essi corrispondono questa volta col valore delle classi di cardinalità 1. Non lo dimostriamo, pur essendo semplice, ma proponiamo la rappresentazione tabellare di T':

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
-		-		-		-		-		-		-		-		-		...
-			-			-			-			-			-			...
-				-				-				-				-		...
-					-					-					-			...
-						-						-						...
-							-							-				...
-								-								-		...
-									-									...
-										-								...
-											-							...
-												-						...
-													-					...
-														-				...
-															-			...
-																-		...
-																	-	...
-																		...

Considerando le prime $n-1$ righe della tabella, si ottiene il tratteggio finito $(2, \ldots, n)$. Anche in quest'ultimo i numeri primi coincidono coi valori delle classi di un solo elemento, ma questo accade solo tra 2 ed n. Ad esempio, per $n = 7$:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
-		-		-		-		-		-		-		-		-		...
-			-			-			-			-			-			...
-				-				-				-				-		...
-					-					-					-			...
-						-						-						...
-							-							-				...

Abbiamo che, tra 2 ed $n = 7$, i numeri primi sono i valori delle classi di cardinalità 1, mentre da $n + 1 = 8$ ad (almeno) $(n + 1)^2 - 1 = 63$, essi sono spazi (stando alla

proposizione 4.10). Al crescere di n, però, il numero di numeri primi minori o uguali ad n aumenta linearmente, mentre il numero di numeri primi compresi tra $n+1$ ed $(n+1)^2-1$ aumenta quadraticamente: perciò conviene considerare gli spazi piuttosto che le classi di cardinalità 1 (oltre al fatto che il problema di trovare l'i-esima classe di cardinalità 1 in un tratteggio non è ancora stato studiato).

Il fatto che in un tratteggio lineare finito del tipo $(2,\dots,n)$ si debba partire da $n+1$ per trovare numeri primi può risultare fastidioso: per conoscere i numeri primi minori di $n+1$ bisogna necessariamente considerare un tratteggio di ordine inferiore (a meno di considerare le classi di cardinalità 1, come abbiamo detto). La questione si può risolvere considerando una classe di tratteggi molto simile a quella lineare, a cui non diamo un nome:

$$\left\{ T \in \mathcal{T}^{\overline{\mathbb{N}^\star}} \mid \forall \langle i,k\rangle \in T : T\left(\langle n,k\rangle\right) = \begin{cases} 0 & \text{se } k=0 \\ n_i\,(k+1) & \text{altrimenti} \end{cases} \right\}$$

con coefficienti n_i fissati e dipendenti solo da i e da T.

Rappresentiamo il tratteggio di questa classe con n_i pari rispettivamente, per $i=1,\dots,6$, a $2,3,4,5,6,7$:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
-				-		-		-		-		-		-		-		...
-						-			-			-			-			...
-								-				-				-		...
-										-					-			...
-												-						...
-														-				...

Ora tutti gli spazi a partire da 2 (non più da $n+1=7+1=8$) a $(7+1)^2-1=63$ sono numeri primi: la connessione tra spazi e numeri primi si è semplificata. Inoltre, questa proprietà è conservata dal tratteggio infinito, della stessa classe di tratteggi, con coefficienti $\{n \in \mathbb{N} \mid n \geq 2\}$, in quanto tutti (e soli) gli spazi maggiori di 2 sono numeri primi:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
-				-		-		-		-		-		-		-		...
-						-			-			-			-			...
-								-				-				-		...
-										-					-			...
-												-						...
-														-				...
-																-		...
-																		...
-																		...
-																		...
-																		...
-																		...
-																		...
-																		...
-																		...
-																		...
-																		...

Abbiamo trovato un modo molto semplice di caratterizzare i numeri primi nei termini della teoria dei tratteggi. Purtroppo la funzione valore della classe di tratteggi che stiamo considerando non è facile da trattare. Per questo motivo si è preferito studiare i numeri primi attraverso i tratteggi lineari, nonostante la connessione tra questi e gli spazi sia un po' più complicata.

Capitolo 5

Upcast di t lineare

In questo breve capitolo trattiamo il problema dell'upcast di t lineare. Esso costituisce la base per la risoluzione dei problemi di downcast della stessa funzione. Trattiamo il problema dapprima, in due contesti particolari; poi tratteremo il caso più generale possibile.

5.1 Upcast di t lineare dal primo al secondo ordine

Teorema 5.1. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1, 2\}$, $i \neq j$:*

$$\mathrm{Up}^{T[i] \to T}(\mathrm{t}) = \left\{ \lambda n.n + \left\lfloor \frac{n_i n - (i < j)}{n_j} \right\rfloor \right\}$$

Dimostrazione.

1. $\mathrm{Up}^{T[i] \to T}(\mathrm{t}) = \left\{ \lambda n.n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor \right\}$ [da 2., perché t lineare è upcast-sicura]
2. $\lambda n.n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor \in \mathrm{Up}^{T[i] \to T}(\mathrm{t})$ [da 3. e 4., per definizione di upcast]
3. Sia $\mathrm{t}_T(x) = \mathrm{t}_{T[i]}(n) = \langle i, n \rangle$
4. $n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor = x$ [da (b), (c) e (d)]

   (a) Sia, per $y \in \{1, 2\}$:
   $$A_y \equiv \begin{cases} \{t \in T[y] \mid |t| \leq n_i n\} & \text{se } y \leq i \\ \{t \in T[y] \mid |t| < n_i n\} & \text{altrimenti} \end{cases} = \{t \in T[y] \mid |t| \leq n_i n - (i < y)\}$$

   (b) $|A_i| =$ [da (a)]
   $|\{t \in T[i] \mid |t| \leq n_i n\}| =$ [per il corollario 4.2]

$\left\lfloor \frac{n_i n}{n_i} \right\rfloor =$
n

(c) $|A_j| =$ [da (a)]
$|\{t \in T\,[j] \mid |t| \leq n_i n - (i < j)\}| =$[per il corollario 4.2]
$\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor$

(d) $|A_i| + |A_j| = x$ [da i., ii. e iii.]

i. Sia $B \equiv \{t \in T \mid t \leq \langle i, n \rangle\}$

ii. $|B| = x$ [da i. e 3., per definizione di t_T]

iii. $|B| =$ [per definizione di ordinamento per colonne]
$|\{t \in T \mid |t| < n_i n \vee (|t| = n_i n \wedge \mathrm{ind}\,(t) \leq i)\}| =$ [per definizione di unione]
$|\{t \in T \mid |t| < n_i n\} \cup \{t \in T \mid |t| = n_i n \wedge \mathrm{ind}\,(t) \leq i\}| =$ [per la proprietà 3.10]

$$\left|\{t \in T\,[1] \mid |t| < n_i n\} \cup \begin{cases} \{t \in T\,[1] \mid |t| = n_i n\} & \text{se } 1 \leq i \\ \emptyset & \text{altrimenti} \end{cases}\right| +$$

$$+ \left|\{t \in T\,[2] \mid |t| < n_i n\} \cup \begin{cases} \{t \in T\,[2] \mid |t| = n_i n\} & \text{se } 2 \leq i \\ \emptyset & \text{altrimenti} \end{cases}\right| =$$

$$\left|\begin{cases} \{t \in T\,[1] \mid |t| < n_i n\} \cup \{t \in T\,[1] \mid |t| = n_i n\} & \text{se } 1 \leq i \\ \{t \in T\,[1] \mid |t| < n_i n\} \cup \emptyset & \text{altrimenti} \end{cases}\right| +$$

$$+ \left|\begin{cases} \{t \in T\,[2] \mid |t| < n_i n\} \cup \{t \in T\,[2] \mid |t| = n_i n\} & \text{se } 2 \leq i \\ \{t \in T\,[2] \mid |t| < n_i n\} \cup \emptyset & \text{altrimenti} \end{cases}\right| =$$

$$\left|\begin{cases} \{t \in T\,[1] \mid |t| \leq n_i n\} & \text{se } 1 \leq i \\ \{t \in T\,[1] \mid |t| < n_i n\} & \text{altrimenti} \end{cases}\right| + \left|\begin{cases} \{t \in T\,[2] \mid |t| \leq n_i n\} & \text{se } 2 \leq i \\ \{t \in T\,[2] \mid |t| < n_i n\} & \text{altrimenti} \end{cases}\right| =$$

[per (a)]
$|A_1| + |A_2| =$ [perché $i, j \in \{1, 2\}$, $i \neq j$]
$|A_i| + |A_j|$

□

5.2 Upcast di t lineare dal primo al d-esimo ordine

La dimostrazione del teorema 5.1, riguardante l'upcast dal primo ordine al secondo, contiene gran parte del ragionamento che verrà sfruttato per dimostrare teoremi più generali. Il primo passo di generalizzazione consiste nel lasciare arbitrario l'ordine del sovratratteggio, considerando cioè l'upcast dal primo al d-esimo ordine.

Nel trattare il generico ordine d-esimo, occorrerebbero d simboli per indicare i diversi generici indici del tratteggio (gli i e j di prima, con $\{i,j\}=\{1,2\}$). Per ovviare a questa difficoltà notazionale, astraendo un po' la materia, possiamo introdurre una permutazione $\sigma \in S_d$, in modo che i generici indici da 1 a d sono $\sigma(1),\ldots,\sigma(d)$. Il fatto che σ è una permutazione di S_d garantisce che $\{\sigma(1),\ldots,\sigma(d)\}=\{1,\ldots,d\}$: $\sigma(1),\ldots,\sigma(d)$ sono tutti diversi tra loro e ricoprono, complessivamente, l'insieme dei possibili indici. Se σ è generica, anche $\sigma(1),\ldots,\sigma(d)$ sono indici generici diversi tra loro, quindi la i di $\mathrm{Up}^{T[i]\to T}$ può diventare uno qualsiasi tra $\sigma(1),\ldots,\sigma(d)$, ad esempio, per semplicità, $\sigma(1)$.

Prima di proseguire, occorre fare un'altra precisazione di natura notazionale. Si scriverà $T\equiv(n_1,\ldots,n_d)\in\mathcal{L}^d$ per indicare un generico tratteggio lineare di d-esimo ordine. Si sottointende, in questo caso, che $d\in\mathbb{N}^\star$. Se $d=1$, la notazione $(n_1,\ldots,n_d)$ va intesa come (n_1), non come (n_1,n_1), che non ha senso.

Teorema 5.2. *Sia $T\equiv(n_1,\ldots,n_d)\in\mathcal{L}^d$. Per ogni $\sigma\in S_d$:*

$$\mathrm{Up}^{T[\sigma(1)]\to T}(\mathrm{t})=\left\{\lambda n.n+\sum_{i=2}^{d}\left\lfloor\frac{n_{\sigma(1)}n-(\sigma(1)<\sigma(i))}{n_{\sigma(i)}}\right\rfloor\right\}$$

Dimostrazione.

1. $\mathrm{Up}^{T[\sigma(1)]\to T}(\mathrm{t})=\left\{\lambda n.n+\sum_{i=2}^{d}\left\lfloor\frac{n_{\sigma(1)}n-(\sigma(1)<\sigma(i))}{n_{\sigma(i)}}\right\rfloor\right\}$ [da 2., perché t lineare è upcast-sicura]

2. $\lambda n.n+\sum_{i=2}^{d}\left\lfloor\frac{n_{\sigma(1)}n-(\sigma(1)<\sigma(i))}{n_{\sigma(i)}}\right\rfloor\in\mathrm{Up}^{T[\sigma(1)]\to T}(\mathrm{t})$ [da 3. e 4., per definizione di upcast]

3. Sia $\mathrm{t}_T(x)=\mathrm{t}_{T[\sigma(1)]}(n)=\langle\sigma(1),n\rangle$

4. $n+\sum_{i=2}^{d}\left\lfloor\frac{n_{\sigma(1)}n-(\sigma(1)<\sigma(i))}{n_{\sigma(i)}}\right\rfloor=x$ [da (b), (c), (c)–i., (d) ed (e)]

   (a) Sia, per $y\in\{1,\ldots,d\}$, $A_y\equiv\begin{cases}\{t\in T[y]\mid|t|\le n_{\sigma(1)}n\} & \text{se } y\le\sigma(1)\\ \{t\in T[y]\mid|t|<n_{\sigma(1)}n\} & \text{altrimenti}\end{cases}=$
   $\{t\in T[y]\mid|t|\le n_{\sigma(1)}n-(\sigma(1)<y)\}$

   (b) $|A_{\sigma(1)}|=$ [da (a)]
   $|\{t\in T[\sigma(1)]\mid|t|\le n_{\sigma(1)}n\}|=$ [per il corollario 4.2]
   $\left\lfloor\frac{n_{\sigma(1)}n}{n_{\sigma(1)}}\right\rfloor=$
   n

   (c) Per $2\le i\le d$:

i. $\left|A_{\sigma(i)}\right| =$ [da (a)]
$\left|\left\{t \in T\left[\sigma\left(i\right)\right] \mid |t| \leq n_{\sigma(1)}n - \left(\sigma\left(1\right) < \sigma\left(i\right)\right)\right\}\right| =$[per il corollario 4.2]
$\left\lfloor \frac{n_{\sigma(1)}n - (\sigma(1) < \sigma(i))}{n_{\sigma(i)}} \right\rfloor$

(d) $\left|A_{\sigma(1)}\right| + \sum_{i=2}^{d} \left|A_{\sigma(i)}\right| = x$ [da i., ii. e iii.]

i. Sia $B \equiv \left\{t \in T \mid t \leq \left\langle \sigma\left(1\right), n\right\rangle\right\}$

ii. $|B| = x$ [da i. e 3., per definizione di t_T]

iii. $|B| =$ [per definizione di ordinamento per colonne]
$\left|\left\{t \in T \mid |t| < n_{\sigma(1)}n \vee \left(|t| = n_{\sigma(1)}n \wedge \mathrm{ind}\left(t\right) \leq \sigma\left(1\right)\right)\right\}\right| =$ [per definizione di unione]
$\left|\left\{t \in T \mid |t| < n_{\sigma(1)}n\right\} \cup \left\{t \in T \mid |t| = n_{\sigma(1)}n \wedge \mathrm{ind}\left(t\right) \leq \sigma\left(1\right)\right\}\right| =$ [per la proprietà 3.10]
$\sum_{y=1}^{d} \left|\left\{t \in T\left[y\right] \mid |t| < n_{\sigma(1)}n\right\} \cup \left\{t \in T\left[y\right] \mid |t| = n_{\sigma(1)}n \wedge y \leq \sigma\left(1\right)\right\}\right| =$
$\sum_{y=1}^{d} \left| \begin{cases} \left\{t \in T\left[y\right] \mid |t| < n_{\sigma(1)}n\right\} \cup \left\{t \in T\left[y\right] \mid |t| = n_{\sigma(1)}n\right\} & \text{se } y \leq \sigma\left(1\right) \\ \left\{t \in T\left[y\right] \mid |t| < n_{\sigma(1)}n\right\} \cup \emptyset & \text{altrimenti} \end{cases} \right| =$
$\sum_{y=1}^{d} \left| \begin{cases} \left\{t \in T\left[y\right] \mid |t| \leq n_{\sigma(1)}n\right\} & \text{se } y \leq \sigma\left(1\right) \\ \left\{t \in T\left[y\right] \mid |t| < n_{\sigma(1)}n\right\} & \text{altrimenti} \end{cases} \right| =$ [per (a)]
$\sum_{y=1}^{d} |A_y| =$ [perché $\left\{\sigma\left(1\right), \ldots, \sigma\left(d\right)\right\} = \left\{1, \ldots, d\right\}$]
$\sum_{y=1}^{d} \left|A_{\sigma(y)}\right|$

□

5.3 Teorema fondamentale dell'upcast di t lineare

Nel paragrafo precedente abbiamo generalizzato sull'ordine del sovratratteggio: per completare la generalizzazione, occorre farlo sul sottotratteggio, ossia il tratteggio $T\left[\sigma\left(1\right)\right]$ in $\mathrm{Up}^{T[\sigma(1)] \to T}$, eliminando il vincolo che sia di primo ordine. La generalizzazione che si ottiene presuppone che si possa calcolare la funzione t nel sottotratteggio, argomento trattato in dettaglio nel capitolo 6.

Il seguente teorema è chiamato, per la sua generalità, *teorema fondamentale dell'upcast di* t *lineare*. La formula che esprime la funzione di upcast è analoga a quella del teorema 5.2: $n_{\sigma(i)}n$ è generalizzato come $\mathrm{t\_valore}_{T'}\left(n\right)$, dove T' è il sottotratteggio, e $\sigma\left(1\right)$ è generalizzato come $\mathrm{ind}\left(\mathrm{t}_{T'}\left(n\right)\right)$. Dalla dimostrazione risulta più chiaro, tuttavia, che il termine n iniziale rappresenta il numero di trattini già

presenti nel sottotratteggio, che ovviamente non vengono tolti quando si considera il sovratratteggio.

Teorema 5.3. *Sia* $T \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$. *Per ogni* $\sigma \in S_d$ *e per ogni* $h \in \mathbb{N}^\star$, $h \leq d$, *ponendo* $T' \equiv T[\sigma(1), \ldots, \sigma(h)]$:

$$\mathrm{Up}^{T' \to T}(\mathrm{t}) = \left\{ \lambda n.n + \sum_{i=h+1}^{d} \left\lfloor \frac{\mathrm{t\_valore}_{T'}(n) - (\mathrm{ind}(\mathrm{t}_{T'}(n)) < \sigma(i))}{n_{\sigma(i)}} \right\rfloor \right\}$$

Dimostrazione.

1. $\mathrm{Up}^{T' \to T}(\mathrm{t}) = \left\{ \lambda n.n + \sum_{i=h+1}^{d} \left\lfloor \frac{\mathrm{t\_valore}_{T'}(n) - (\mathrm{ind}(\mathrm{t}_{T'}(n)) < \sigma(i))}{n_{\sigma(i)}} \right\rfloor \right\}$ [da 2., perché t lineare è upcast-sicura]

2. $\lambda n.n + \sum_{i=h+1}^{d} \left\lfloor \frac{\mathrm{t\_valore}_{T'}(n) - (\mathrm{ind}(\mathrm{t}_{T'}(n)) < \sigma(i))}{n_{\sigma(i)}} \right\rfloor \in \mathrm{Up}^{T' \to T}(\mathrm{t})$ [da 3. e 4., per definizione di upcast]

3. Sia $\mathrm{t}_T(x) = \mathrm{t}_{T'}(n)$ e $k = \mathrm{ind}(\mathrm{t}_{T'}(n))$ $(k \in \{\sigma(1), \ldots, \sigma(h)\})$

4. $n + \sum_{i=h+1}^{d} \left\lfloor \frac{\mathrm{t\_valore}_{T'}(n) - (\mathrm{ind}(\mathrm{t}_{T'}(n)) < \sigma(i))}{n_{\sigma(i)}} \right\rfloor = x$ [da (b)–i., (c), (c)–i., (d) ed (e)]

   (a) Sia, per $y \in \{\sigma(h+1), \ldots, \sigma(d)\}$:
   $$A_y \equiv \begin{cases} \{t \in T[y] \mid |t| \leq \mathrm{t\_valore}_{T'}(n)\} & \text{se } y \leq k \\ \{t \in T[y] \mid |t| < \mathrm{t\_valore}_{T'}(n)\} & \text{altrimenti} \end{cases} =$$
   $$= \{t \in T[y] \mid |t| \leq \mathrm{t\_valore}_{T'}(n) - (k < y)\}$$

   (b) Sia $A \equiv \{t \in T' \mid t \leq \mathrm{t}_{T'}(n)\}$

      i. $|A| = n$ [da (b), per definizione di t]

   (c) Per $h + 1 \leq i \leq d$:

      i. $\left|A_{\sigma(i)}\right| =$ [da (a)]
      $|\{t \in T[\sigma(i)] \mid |t| \leq \mathrm{t\_valore}_{T'}(n) - (k < \sigma(i))\}| =$[per il corollario 4.2]
      $\left\lfloor \frac{\mathrm{t\_valore}_{T'}(n) - (k < \sigma(i))}{n_{\sigma(i)}} \right\rfloor =$ [da 3.]
      $\left\lfloor \frac{\mathrm{t\_valore}_{T'}(n) - (\mathrm{ind}(\mathrm{t}_{T'}(n)) < \sigma(i))}{n_{\sigma(i)}} \right\rfloor$

   (d) $|A| + \sum_{i=h+1}^{d} \left|A_{\sigma(i)}\right| = x$ [da i., ii. e iii.]

      i. Sia $B \equiv \{t \in T \mid t \leq \mathrm{t}_{T'}(n)\}$

      ii. $|B| = x$ [da i. e 3., per definizione di t_T]

iii. $|B| = |A| + \sum_{i=h+1}^{d} \left|A_{\sigma(i)}\right|$ [da B.]

A. Sia $T'' \equiv T\left[\sigma\left(h+1\right), \ldots, \sigma\left(d\right)\right]$

B. $|B| =$ [da (b), ricordando che $T' = T\left[\sigma\left(1\right), \ldots, \sigma\left(h\right)\right]$]
$|A| + |\{t \in T'' \mid t \leq \mathrm{t}_{T'}\left(n\right)\}| =$ [per definizione di ordinamento per colonne e per 3.]
$|A| + |\{t \in T'' \mid |t| < \mathrm{t\_valore}_{T'}\left(n\right) \vee (|t| = \mathrm{t\_valore}_{T'}\left(n\right) \wedge \mathrm{ind}\left(t\right) \leq k)\}| =$ [per definizione di unione]
$|A| + \left| \begin{array}{l} \{t \in T'' \mid |t| < \mathrm{t\_valore}_{T'}\left(n\right)\} \cup \\ \cup \{t \in T'' \mid |t| = \mathrm{t\_valore}_{T'}\left(n\right) \wedge \mathrm{ind}\left(t\right) \leq k\} \end{array} \right| =$ [da A., per la proprietà 3.10]
$|A| + \sum_{y=h+1}^{d} \left| \begin{array}{l} \{t \in T\left[y\right] \mid |t| < \mathrm{t\_valore}_{T'}\left(n\right)\} \cup \\ \cup \{t \in T\left[y\right] \mid |t| = \mathrm{t\_valore}_{T'}\left(n\right) \wedge y \leq k\} \end{array} \right| =$
$|A| + \sum_{y=h+1}^{d} \left| \begin{cases} \{t \in T\left[y\right] \mid |t| < \mathrm{t\_valore}_{T'}\left(n\right)\} \cup & \\ \cup \{t \in T\left[y\right] \mid |t| = \mathrm{t\_valore}_{T'}\left(n\right)\} & \text{se } y \leq k \\ \{t \in T\left[y\right] \mid |t| < \mathrm{t\_valore}_{T'}\left(n\right)\} \cup \emptyset & \text{altrimenti} \end{cases} \right| =$
$|A| + \sum_{y=h+1}^{d} \left| \begin{cases} \{t \in T\left[y\right] \mid |t| \leq \mathrm{t\_valore}_{T'}\left(n\right)\} & \text{se } y \leq k \\ \{t \in T\left[y\right] \mid |t| < \mathrm{t\_valore}_{T'}\left(n\right)\} & \text{altrimenti} \end{cases} \right| =$ [per (a)]
$|A| + \sum_{y=h+1}^{d} |A_y| =$ [perché $\{\sigma\left(h+1\right), \ldots, \sigma\left(d\right)\} = \{h+1, \ldots, d\}$]
$|A| + \sum_{y=h+1}^{d} \left|A_{\sigma(y)}\right|$

□

Si noti che, essendo σ una generica permutazione, il sottotratteggio $T\left[\sigma\left(1\right), \ldots, \sigma\left(h\right)\right]$ può anche non avere le righe, per così dire, "tutte attaccate". In altri termini, può esistere un indice compreso tra $\min\{\sigma\left(1\right), \ldots, \sigma\left(h\right)\}$ e $\max\{\sigma\left(1\right), \ldots, \sigma\left(h\right)\}$ che non appartiene a $\{\sigma\left(1\right), \ldots, \sigma\left(h\right)\}$. Ad esempio, si può avere $T = (n_1, n_2, n_3, n_4)$, $h = 2$ e $T\left[\sigma\left(1\right), \ldots, \sigma\left(h\right)\right] = T\left[1, 3\right] = (n_1, n_3)$, ottenendo $\mathrm{Up}^{T[\sigma(1),\ldots,\sigma(h)] \to T}\left(\mathrm{t}\right) = \mathrm{Up}^{(n_1,n_3) \to (n_1,n_2,n_3,n_4)}\left(\mathrm{t}\right)$. Nel caso le righe del sottotratteggio siano "tutte attaccate", ad esempio (n_1, n_2) o (n_2, n_3), si può semplificare l'enunciato, eliminando $\mathrm{ind}\left(\mathrm{t}_{T[\sigma(1),\ldots,\sigma(h)]}\left(n\right)\right)$. Comunque, questo caso particolare è attualmente di scarso interesse, perciò non lo trattiamo; può costituire, invece, un utile esercizio per il lettore.

Capitolo 6

Downcast e down-conservatività di t lineare

La matematica è un'arte.

Sappiamo che la funzione t lineare è upcast-sicura, ma non downcast-sicura (e nemmeno down-conservativa), perciò è più complesso risolvere il problema del downcast rispetto a quello dell'upcast. Questo capitolo esplora in dettaglio le problematiche connesse al downcast e alla down-conservatività di t lineare ed è attualmente il più ricco di risultati.

6.1 Downcast e down-conservatività per il calcolo di t lineare in tratteggi di ordine superiore al primo

Prima di entrare nel dettaglio, vediamo, in un'ottica più generale, per cosa vogliamo usare queste funzioni. Questo discorso in realtà si è iniziato nel capitolo 1, in cui abbiamo visto alcuni problemi pratici risolvibili grazie a queste funzioni. Questa però è solo una parte della questione; l'altra parte è di carattere più teorico. Può risultare strano, infatti, che affrontiamo lo studio del downcast di t lineare senza sapere come calcolarlo (a parte in $\mathcal{L}^1$, dove il problema è banale). Può risultare ancora più strano che non ci sia in questo libro un capitolo dedicato al calcolo di t lineare, nonostante l'importanza pratica del problema (si veda il paragrafo 1.6, prima domanda). Ci si aspetterebbe un capitolo in cui si trova una formula per il calcolo di t lineare in $\mathcal{L}^d$, $d \in \mathbb{N}^\star$, dimostrata senza fare appello al concetto di downcast, prima di questo capitolo, che discute altre formule, per il downcast di t da $\mathcal{L}^d$ a

$\mathcal{L}^h$, $h \leq d$. Le cose, però, non stanno così. Mi è parso incredibilmente complesso calcolare t lineare in tratteggi di ordine superiore al primo, senza fare appello ai concetti di downcast e down-conservatività. È invece molto facile, sebbene forse controintuitivo, trattare prima in dettaglio i problemi del downcast e della down-conservatività, e poi, sfruttando questi concetti, calcolare t in $\mathcal{L}^d$, $d \in \mathbb{N}^\star$. Vediamo come.

Sia $T \in \mathcal{L}^d$, $d \in \mathbb{N}^\star$ e consideriamo il problema del calcolo di $\mathrm{t}_T(x)$, $x \in \mathbb{N}^\star$. L'idea fondamentale è osservare che $\mathrm{t}_T(x)$ deve appartenere ad uno solo dei d sottotratteggi di primo ordine. Sia per esempio $\mathrm{t}_T(x) = \langle i, k\rangle$. Allora $\mathrm{t}_T(x) \in T[i]$ e $\mathrm{t}_T(x) \notin T[j]$, per ogni $j \in \{1, \ldots, d\}$, $j \neq i$. Possiamo sapere, quindi, a quale sottotratteggio di primo ordine appartiene $\mathrm{t}_T(x)$, calcolando la funzione di down-conservatività $\mathrm{DownCons}^{T \to T[j]}(\mathrm{t})(x)$ per i diversi $j \in \{1, \ldots, d\}$: si otterrà 1 solo per $j = i$ e 0 negli altri casi. Una volta stabilito che $\mathrm{t}_T(x) \in T[i]$, si può calcolare $\mathrm{t}_T(x)$ attraverso il downcast. Infatti $\mathrm{t}_T(x) = \langle i, k\rangle = \mathrm{t}_{T[i]}(k)$, quindi $k = f(x)$, con $f \in \mathrm{Down}^{T \to T[i]}(\mathrm{t})$ (o $f \in \mathrm{Spec\ Down}^{T \to T[i]}(\mathrm{t})$).

Il raggionamento appena concluso mostra che è possibile calcolare t in qualsiasi tratteggio lineare finito, se si sanno calcolare le funzioni di down-conservatività e di downcast. In realtà questo non è l'unico modo per calcolare t lineare che verrà presentato, ma solo il più generalizzato, solido teoricamente ed economico a livello di calcolo. Vedremo infatti un altro metodo nel capitolo 7 (corollario 7.2): esso, in sostanza, calcola una $f \in \mathrm{Spec\ Down}^{T \to T[j]}(\mathrm{t})$ per ogni $j \in \{1, \ldots, d\}$, ma non calcola $\mathrm{DownCons}^{T \to T[j]}(\mathrm{t})$ (cosa che, se vogliamo, è il contrario del metodo visto prima, che calcolava $\mathrm{DownCons}^{T \to T[j]}(\mathrm{t})$ per ogni j). Infine, è degna di nota, in questo contesto, l'esistenza di un metodo per approssimare t_valore lineare, senza usare né $\mathrm{Down}^{T \to T[i]}(\mathrm{t})$, né $\mathrm{DownCons}^{T \to T[j]}(\mathrm{t})$, che tratteremo nei paragrafi 6.5 e 6.8.

6.2 La funzione modulo a tre argomenti

Definiamo una funzione che sarà utile per tutto il capitolo: la funzione modulo a tre argomenti.

Definizione 6.1. *Si definisce la funzione* $\mathrm{mod} : \mathbb{N} \times \mathbb{N}^\star \times \{\mathrm{V}, \mathrm{F}\} \to \mathbb{N}$ *tale che per ogni* $a \in \mathbb{N}$, $b \in \mathbb{N}^\star$, $v \in \{\mathrm{V}, \mathrm{F}\}$*:*

$$\mathrm{mod}(a, b, v) \equiv \begin{cases} a \bmod b & \textit{se } v \\ a \bmod^\star b & \textit{altrimenti} \end{cases}$$

Si verifica facilmente, alla luce della proprietà 2.15, che:

Proprietà 6.1. *Per ogni* $a, c \in \mathbb{N}$, $b, d \in \mathbb{N}^\star$, $v \in \{\mathrm{V}, \mathrm{F}\}$*:*

- $\mathrm{mod}\,(a, b, v) = \neg v + (a - \neg v) \bmod b$
- $(a - \neg v) \bmod b = (c - \neg v) \bmod d \Leftrightarrow \mathrm{mod}\,(a, b, v) = \mathrm{mod}\,(c, d, v)$

Un'applicazione immediata della funzione è la seguente proposizione:

Proposizione 6.1. *Sia* $T \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$, $d \in \mathbb{N}^\star$. *Siano inoltre* $j \in [1, d]$ *ed* $x \in \mathbb{N}^\star$.

$$\mathrm{t\_valore}_T\,(x) - \left| \max_{t \in T[j] | t < \mathrm{t}_T(x)} t \right| = \mathrm{mod}\,(\mathrm{t\_valore}_T\,(x)\,, n_j, (\mathrm{ind}\,(\mathrm{t}_T\,(x)) > j))$$

Dimostrazione.

1. Siano $\mathrm{t}_T\,(x) = \langle i, n \rangle$ (con $i \in [1, d]$, $n \in \mathbb{N}$) e $\mathrm{t\_valore}_T\,(x) \equiv v$
2. $\mathrm{t\_valore}_T\,(x) - \left| \max_{t \in T[j] | t < \mathrm{t}_T(x)} t \right| =$ [da 1., per la proposizione 4.2]
   $v - \left| \left\langle j, \left\lfloor \frac{v - (i \leq j)}{n_j} \right\rfloor \right\rangle \right| =$ [perché il tratteggio è lineare]
   $v - n_j \left\lfloor \frac{v - (i \leq j)}{n_j} \right\rfloor =$
   $v - (v - (i \leq j) - (v - (i \leq j)) \bmod n_j) =$
   $(i \leq j) + (v - (i \leq j)) \bmod n_j =$ [per la proprietà 6.1]
   $\mathrm{mod}\,(v, n_j, (i > j)) =$ [da 1.]
   $\mathrm{mod}\,(\mathrm{t\_valore}_T\,(x)\,, n_j, (\mathrm{ind}\,(\mathrm{t}_T\,(x)) > j))$

□

Ovviamente la proposizione 6.1 vale anche per tratteggi infiniti: è stata enunciata nel caso di tratteggi finiti solo per comodità notazionale.

6.3 Down-conservatività di t lineare di secondo ordine

La chiave per studiare la down-conservatività – ed, in seguito, anche il downcast – di t lineare da $T \equiv (n_1, n_2)$ a $T\,[n_1]$ o $T\,[n_2]$, è osservare quali sono i resti dei valori dei trattini modulo n_1, modulo n_2 e modulo $n_1 + n_2$. La seguente proposizione presenta l'osservazione principale:

Proposizione 6.2. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$. *Per ogni* $i, j \in \{1, 2\}$, $i \neq j$ *e per ogni* $x \in \mathbb{N}^\star$*:*

$$\mathrm{t}_T(x) = \langle n_i, n \rangle \Rightarrow (n_i x - (i < j)) \bmod (n_i + n_j) = (n_i n - (i < j)) \bmod n_j$$

Dimostrazione.

1. Sia $\mathrm{t}_T(x) = \langle n_i, n \rangle$
2. $n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor = x$ [da 1., per il teorema 5.1]
3. $(n_i x - (i < j)) \bmod (n_i + n_j) =$ [da 2.]
   $\left(n_i \left(n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor\right) - (i < j)\right) \bmod (n_i + n_j) =$ [per definizione, calcoli algebrici]
   $\left(n_i \left(\frac{n_j n + n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_j}\right) - (i < j)\right) \bmod (n_i + n_j) =$
   $\left(\frac{n_i n_j n + n_i^2 n - n_i (i<j) - n_i ((n_i n - (i<j)) \bmod n_j)}{n_j} - (i < j)\right) \bmod (n_i + n_j) =$
   [aggiunta e sottrazione di $n_j (i < j) + n_j ((n_i n - (i < j)) \bmod n_j)$]
   $\left(\left(\begin{array}{c} \frac{n_i n_j n + n_i^2 n - n_i (i<j) - n_i ((n_i n - (i<j)) \bmod n_j)}{n_j} + \\ \frac{-n_j (i<j) - n_j ((n_i n - (i<j)) \bmod n_j) + n_j (i<j) + n_j ((n_i n - (i<j)) \bmod n_j)}{n_j} \end{array}\right) - (i < j)\right) \bmod (n_i + n_j) =$
   $\left(\frac{(n_i + n_j)(n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j) + n_j (i<j) + n_j ((n_i n - (i<j)) \bmod n_j)}{n_j} - (i < j)\right) \bmod (n_i + n_j) =$
   $\left(\begin{array}{l} (n_i + n_j) \frac{n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_j} + \\ + (i < j) + (n_i n - (i < j)) \bmod n_j - (i < j) \end{array}\right) \bmod (n_i + n_j) =$
   $\left((n_i + n_j) \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + (n_i n - (i < j)) \bmod n_j\right) \bmod (n_i + n_j) =$ [per definizione di modulo e perché $(n_i n - (i < j)) \bmod n_j < n_i + n_j$]
   $(n_i n - (i < j)) \bmod n_j$

□

Verifichiamo il lemma su un semplice esempio, come il tratteggio $T_1 \equiv (3, 4)$, considerando cioè $n_1 = 3$ e $n_2 = 4$. Lo rappresentiamo come tabella, scrivendo però, al posto dei trattini, il loro numero progressivo nell'ordinamento per colonne (ossia la x di $\mathrm{t}_{T_1}(x)$), in tabella 6.1.

0	1	2	3	4	5	6	7	8	9	10	11	12
-			1			3			5			6
-				2				4				7

Tabella 6.1: Rappresentazione del tratteggio $(3, 4)$ con l'indicazione del numero progressivo dei trattini nell'ordinamento per colonne

0	1	2	3	4	5	6	7	8	9	10	11	12
-			4			5			6			3
-				1				2				0

Tabella 6.2: Rappresentazione del tratteggio $(3, 4)$ con l'indicazione di $4x \bmod (3 + 4) = 4x \bmod 7$ nella posizione dell'x-esimo trattino

Vediamo cosa succede quando $i = 2$ e $j = 1$ (quindi $(i < j) = 0$). Ripetiamo la tabella 6.1 scrivendo $(n_i x - (i < j)) \bmod (n_i + n_j) = n_i x \bmod (n_i + n_j) = 4x \bmod 7$ al posto della semplice x, ottenendo la tabella 6.2.

Osserviamo che i numeri sulla seconda riga coincidono con i resti del valore del corrispondente trattino, modulo $n_j = 3$. Ad esempio, il trattino $\langle 2, 1\rangle = \langle n_i, n\rangle$, pari a $\mathrm{t}_{T_1}(x)$ per $n = 1$ e $x = 2$, è tale che $(n_i n - (i < j)) \bmod n_j = n_i n \bmod n_j = 4n \bmod 3 = 1$, che coincide col numero che leggiamo nella tabella nella cella corrispondente al trattino, ossia con $(n_i x - (i < j)) \bmod (n_i + n_j)$.

Dalla tabella precedente si vede che vale anche l'implicazione inversa rispetto a quella della proposizione 6.2, cioè solo quando $(n_i x - (i < j)) \bmod (n_i + n_j) = (n_i n - (i < j)) \bmod n_j$ si ha che $\mathrm{t}_T(x) = \langle n_i, n\rangle$. Infatti, se vale la prima uguaglianza, allora $(n_i x - (i < j)) \bmod (n_i + n_j)$ deve essere minore di n_j (perché è esprimibile come modulo rispetto a n_j), cioè può essere 0, 1 o 2 nell'esempio; più in dettaglio:

$$(n_i x - (i < j)) \bmod (n_i + n_j) = 4x \bmod 7 = \begin{cases} 0 & \text{per } x = 7 \\ 1 & \text{per } x = 2 \\ 2 & \text{per } x = 4 \end{cases}$$

D'altra parte:

$$\mathrm{t}_T(x) = \begin{cases} \langle 2, 3\rangle & \text{per } x = 7 \\ \langle 2, 1\rangle & \text{per } x = 2 \\ \langle 2, 2\rangle & \text{per } x = 4 \end{cases}$$

I quali sono tutti trattini di $T[i]$, cioè sono tutti nella forma $\langle n_i, n\rangle$ per qualche n. Il seguente lemma e la successiva proposizione dimostrano formalmente questa proprietà.

Lemma 6.1. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1, 2\}$, $i \neq j$ e per ogni $x \in \mathbb{N}^\star$:*

$$(n_i x - (i < j)) \bmod (n_i + n_j) < n_j \Leftrightarrow (n_j x - (j < i)) \bmod (n_i + n_j) \geq n_i$$

Dimostrazione.

1. $(n_i x - (i < j)) \bmod (n_i + n_j) < n_j \Leftrightarrow$ [aggiunta di $(n_j x - (j < i)) \bmod (n_i + n_j)$ ad ambo i membri]
   $(n_i x - (i < j)) \bmod (n_i + n_j) + (n_j x - (j < i)) \bmod (n_i + n_j) <$
   $< n_j + (n_j x - (j < i)) \bmod (n_i + n_j) \Leftrightarrow$ [da i.]
   $n_i + n_j - 1 < n_j + (n_j x - (j < i)) \bmod (n_i + n_j) \Leftrightarrow$ [sottrazione di n_j da ambo i membri]]
   $n_i - 1 < (n_j x - (j < i)) \bmod (n_i + n_j) \Leftrightarrow$
   $(n_j x - (j < i)) \bmod (n_i + n_j) \geq n_i$

   (a) $(n_i x - (i < j)) \bmod (n_i + n_j) + (n_j x - (j < i)) \bmod (n_i + n_j) = n_i + n_j - 1$ [da ii. e iii.]

      i. $(n_i x - (i < j)) \bmod (n_i + n_j) + (n_j x - (j < i)) \bmod (n_i + n_j) \in$ [per la proposizione 2.4]
      $\left\{ \begin{array}{l} (n_i x - (i < j) + n_j x - (j < i)) \bmod (n_i + n_j), \\ (n_i x - (i < j) + n_j x - (j < i)) \bmod (n_i + n_j) + n_i + n_j \end{array} \right\} =$ [da A.]
      $\{n_i + n_j - 1, 2(n_i + n_j) - 1\}$

         A. $(n_i x - (i < j)) \bmod (n_i + n_j) + (n_j x - (j < i)) \bmod (n_i + n_j) \geq$ [per la proposizione 2.4]
         $(n_i x - (i < j) + n_j x - (j < i)) \bmod (n_i + n_j) =$ [perché, essendo $i \neq j$, una e una sola delle due condizioni è vera]
         $(n_i x + n_j x - 1) \bmod (n_i + n_j) =$
         $((n_i + n_j)(x - 1) + n_i + n_j - 1) \bmod (n_i + n_j) =$ [calcolo del modulo]
         $n_i + n_j - 1$

      ii. $(n_i x - (i < j)) \bmod (n_i + n_j) + (n_j x - (j < i)) \bmod (n_i + n_j) \leq$ [perché entrambi gli addendi sono minori o uguali a $n_i + n_j - 1$]
      $(n_i + n_j - 1) + (n_i + n_j - 1) =$
      $2(n_i + n_j) - 2$

□

Proposizione 6.3. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1, 2\}$, $i \neq j$ e per ogni $x \in \mathbb{N}^\star$:*

$$\mathrm{t}_T(x)[i] \Leftarrow (n_i x - (i < j)) \bmod (n_i + n_j) = (\mathrm{t\_valore}_T(x) - (i < j)) \bmod n_j$$

Dimostrazione.

1. $\mathrm{t}_T(x) \in T[i] \Leftarrow (n_i x - (i<j)) \bmod (n_i+n_j) = (\mathrm{t\_valore}_T(x) - (i<j)) \bmod n_j$ [da 2.]

2. $\mathrm{t}_T(x) \notin T[i] \Rightarrow$ [perché $i,j \in \{1,2\}$, $i \neq j$]
   $\mathrm{t}_T(x) \in T[j] \Rightarrow$ [per la proposizione 6.2]
   $(n_j x - (j<i)) \bmod (n_i+n_j) = (n_j n - (j<i)) \bmod n_i \Rightarrow$
   $(n_j x - (j<i)) \bmod (n_i+n_j) < n_i \Rightarrow$ [per il lemma 6.1]
   $(n_i x - (i<j)) \bmod (n_i+n_j) \geq n_j \Rightarrow$
   $\neg((n_i x - (i<j)) \bmod (n_i+n_j) = (\mathrm{t\_valore}_T(x) - (i<j)) \bmod n_j)$

□

Riassumendo le proposizioni 6.2 e 6.3, possiamo dire che:

$$\mathrm{t}_T(x) = \langle n_i, n\rangle \Leftrightarrow (n_i x - (i<j)) \bmod (n_i+n_j) = (n_i n - (i<j)) \bmod n_j$$

o, equivalentemente:

$$\begin{aligned} &\mathrm{t}_T(x) \in T[i] \Leftrightarrow \\ &(n_i x - (i<j)) \bmod (n_i+n_j) = (\mathrm{t\_valore}_T(x) - (i<j)) \bmod n_j \end{aligned} \tag{6.1}$$

Dunque la condizione $(n_i x - (i<j)) \bmod (n_i+n_j) = (\mathrm{t\_valore}_T(x) - (i<j)) \bmod n_j$ caratterizza l'appartenenza dell'x-esimo trattino a $T[i]$. Questa condizione non è immediatamente verificabile, perché dipende dalla conoscenza di $\mathrm{t\_valore}_T(x)$, ma questo problema è facilmente superabile riscrivendo la 6.1 come:

$$\mathrm{t}_T(x) \in T[i] \Leftrightarrow (n_i x - (i<j)) \bmod (n_i+n_j) < n_j$$

L'equivalenza tra le due forme è la base della dimostrazione del seguente teorema:

Teorema 6.1. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i,j \in \{1,2\}$, $i \neq j$ e per ogni $x \in \mathbb{N}^\star$:*

$$\begin{aligned} \mathrm{DownCons}^{T\to T[i]}(\mathrm{t})(x) &= ((n_i x - (i<j)) \bmod (n_i+n_j) < n_j) \\ &= ((n_j x - (j<i)) \bmod (n_i+n_j) \geq n_i) \end{aligned}$$

In particolare, se $\mathrm{t}_T(x) \in T[i]$, $n_j \mid \mathrm{t\_valore}_T(x) \Leftrightarrow n_i x \bmod (n_i+n_j) = n_j$ $(i<j)$.

Dimostrazione.

1. $\text{DownCons}^{T \to T[i]}(\mathrm{t})(x) =$
   $(\mathrm{t}_T(x) \in T[i]) =$ [per le proposizioni 6.2 e 6.3]
   $((n_i x - (i < j)) \bmod (n_i + n_j) = (\text{t\_valore}_T(x) - (i < j)) \bmod n_j) =$ [da (a) e (b)]
   $((n_i x - (i < j)) \bmod (n_i + n_j) < n_j) =$ [per il lemma 6.1]
   $((n_j x - (j < i)) \bmod (n_i + n_j) \geq n_i)$

   (a) $(n_i x - (i < j)) \bmod (n_i + n_j) = (\text{t\_valore}_T(x) - (i < j)) \bmod n_j \Rightarrow$
   $(n_i x - (i < j)) \bmod (n_i + n_j) < n_j$

   (b) $(n_i x - (i < j)) \bmod (n_i + n_j) < n_j \Rightarrow$ [per la proposizione 6.3]
   $\mathrm{t}_T(x) \in T[i] \Rightarrow$ [per la proposizione 6.2]
   $(n_i x - (i < j)) \bmod (n_i + n_j) = (\text{t\_valore}_T(x) - (i < j)) \bmod n_j$

□

Un importante corollario della proposizione 6.2 è il seguente:

Corollario 6.1. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$. *Per ogni* $i, j \in \{1, 2\}$, $i \neq j$ *e per ogni* $x \in \mathbb{N}^\star$, *se* $\mathrm{t}_T(x) \in T[i]$, *allora la differenza tra il valore di* $\mathrm{t}_T(x)$ *ed il valore del precedente trattino di* T *di componente* n_j *è* $\bmod(n_i x, n_i + n_j, (i > j))$.

Dimostrazione.

1. Sia d la differenza tra il valore di $\mathrm{t}_T(x)$ ed il valore del precedente trattino di T di componente n_j

2. Sia $\mathrm{t}_T(x) = \langle n_i, n \rangle$, $n \in \mathbb{N}$ [perché $\mathrm{t}_T(x) \in T[i]$]

3. $d =$
   $\bmod(\text{t\_valore}_T(x), n_j, (i > j)) =$ [da 2., per la proposizione 6.1]
   $\bmod(n_i n, n_j, (i > j)) =$ [da (a), per la proprietà 6.1]
   $\bmod(n_i x, n_i + n_j, (i > j))$

   (a) $(n_i x - (i \leq j)) \bmod (n_i + n_j) = (n_i n - (i \leq j)) \bmod n_j$ [da (b) e $i \neq j$]

   (b) $(n_i x - (i < j)) \bmod (n_i + n_j) = (n_i n - (i < j)) \bmod n_j$ [da $\mathrm{t}_T(x) \in T[i]$, per la proposizione 6.2]

□

Alla luce del corollario 6.1, possiamo guardare la tabella 6.2 da un'altra prospettiva. Infatti il valore indicato nella tabella nella cella contente $\mathrm{t}_{(3,4)}(x)$ è $4x \bmod 7 = n_2 x \bmod (n_1 + n_2) = \bmod(n_2 x, n_1 + n_2, 2 > 1)$ (essendo $(3, 4) \equiv (n_1, n_2)$); quindi,

0	1	2	3	4	5	6	7	8	9	10	11	12
-			3			2			1			4
-				6				5				7

Tabella 6.3: Rappresentazione del tratteggio $(3,4)$ con l'indicazione di $3x \bmod^\star (3+4) = 3x \bmod^\star 7$ nella posizione dell'x-esimo trattino

applicando il corollario 6.1 con $i = 2$ e $j = 1$, si ha che, se $\mathrm{t}_{(3,4)}(x) \in (3,4)[2] = (4)$, allora la differenza tra il valore di $\mathrm{t}_{(3,4)}(x)$ ed il valore del precedente trattino di $(3,4)$ di componente n_1 è proprio il valore riportato nella tabella nella cella contenente $\mathrm{t}_{(3,4)}(x)$. Ad esempio, per $x = 4$, $\mathrm{t}_{(3,4)}(x) = \langle 2,2\rangle$ e la cella corrispondente contiene il numero $4x \bmod 7 = 16 \bmod 7 = 2$, che è appunto la differenza tra $\left|\mathrm{t}_{(3,4)}(x)\right| = |\langle 2,2\rangle| = 8$ e $|\langle 1,2\rangle| = 6$, essendo $\langle 1,2\rangle$ il più grande trattino di $(3,4)[1] = (3)$ minore di $\langle 2,2\rangle$. Notiamo anche che, per $x = 7$, $\mathrm{t}_{(3,4)}(x) = \langle 2,3\rangle$ e $4x \bmod 7 = 0$: ciò indica che esiste un trattino di (3) che precede $\langle 2,3\rangle$ ma avente lo stesso valore: infatti $\{\langle 1,4\rangle, \langle 2,3\rangle\}$ è una classe di $(3,4)$, di valore 12, e $\langle 1,4\rangle < \langle 2,3\rangle$ (perché i due trattini hanno lo stesso valore, ma $1 < 2$).

Possiamo analizzare, infine, la tabella 6.3, nella quale il valore indicato nella tabella nella cella contente $\mathrm{t}_{(3,4)}(x)$ è $3x \bmod^\star 7 = n_1 x \bmod^\star (n_1 + n_2) = \mathrm{mod}(n_1 x, n_1 + n_2, 1 > 2)$: esso è quindi, in base al corollario 6.1, la differenza tra il valore di $\mathrm{t}_{(3,4)}(x)$ ed il valore del precedente trattino di $(3,4)$ di componente n_2. È particolarmente interessante verificare questo per $x = 6$, per cui si ottiene $3x \bmod^\star 7 = 18 \bmod^\star 7 = 4$, che è la differenza tra $\mathrm{t}_{(3,4)}(6) = \langle 1,4\rangle$ ed il precedente trattino di $(3,4)[2]$, che è $\langle 2,2\rangle$; infatti, pur esistendo il trattino $\langle 2,3\rangle$ dello stesso valore di $\langle 1,4\rangle$ ma di componente 2, esso è maggiore di $\langle 1,4\rangle$.

Un'altra cosa che si può notare è che nella tabella 6.2 i numeri sulla seconda riga costituiscono l'insieme $\{0,1,2\} = \{x \bmod 3 \mid x \in \mathbb{N}\}$, mentre nella tabella 6.3 i numeri sulla prima riga costituiscono l'insieme $\{1,2,3,4\} = \{x \bmod^\star 4 \mid x \in \mathbb{N}\}$. Questa è una diretta conseguenza del teorema 6.1, la cui prima parte può essere scritta infatti nel seguente modo alternativo:

Corollario 6.2. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1,2\}$, $i \neq j$ e per ogni $x \in \mathbb{N}^\star$:*

$$\mathrm{DownCons}^{T \to T[i]}(\mathrm{t})(x) = (\mathrm{mod}(n_i x, n_i + n_j, (i > j)) \in \{\mathrm{mod}(x, n_j, (i > j)) \mid x \in \mathbb{N}\})$$

Dimostrazione.

1. Se $i > j$

(a) $\mathrm{DownCons}^{T\to T[i]}(\mathrm{t})(x) =$ [per il teorema 6.1]
$((n_i x - (i<j)) \bmod (n_i+n_j) < n_j) =$ [da 1.]
$(n_i x \bmod (n_i+n_j) < n_j) =$
$(n_i x \bmod (n_i+n_j) \in \{0,\ldots,n_j-1\}) =$
$(n_i x \bmod (n_i+n_j) \in \{x \bmod n_j \mid x \in \mathbb{N}\}) =$ [da 1.]
$(n_i x \bmod (n_i+n_j) \in \{\mathrm{mod}\,(x, n_j, (i>j)) \mid x \in \mathbb{N}\})$

2. Se $i < j$

(a) $\mathrm{DownCons}^{T\to T[i]}(\mathrm{t})(x) =$ [per il teorema 6.1]
$((n_i x - (i<j)) \bmod (n_i+n_j) < n_j) =$ [da 2.]
$((n_i x - 1) \bmod (n_i+n_j) < n_j) =$
$(n_i x \bmod^\star (n_i+n_j) - 1 \in \{0,\ldots,n_j-1\}) =$
$(n_i x \bmod^\star (n_i+n_j) \in \{1,\ldots,n_j\}) =$
$(n_i x \bmod (n_i+n_j) \in \{x \bmod^\star n_j \mid x \in \mathbb{N}\}) =$ [da 2.]
$(n_i x \bmod (n_i+n_j) \in \{\mathrm{mod}\,(x, n_j, (i>j)) \mid x \in \mathbb{N}\})$

□

Questa formulazione del teorema 6.1 sembra inutilmente artificiosa, tuttavia in essa è riconoscibile un caso degenere della forma più generale dello stesso teorema che presenteremo nel caso dei tratteggi lineari di terzo ordine, la proposizione 6.7.

6.4 Downcast di t lineare di secondo ordine

In questo paragrafo otteniamo una formula che esprime il downcast di t lineare di secondo ordine, e lo facciamo in due modi diversi. Cominciamo col modo più semplice, basato sull'intuizione che la formula per il downcast si può ottenere da quella per l'upcast che abbiamo già trovato:

Teorema 6.2. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1,2\}$, $i \neq j$:*

$$\lambda x. \left\lceil \frac{n_j x + (i<j)}{n_i + n_j} \right\rceil \in \mathrm{Spec}\,\mathrm{Down}^{T\to T[i]}(\mathrm{t})$$

Dimostrazione.

1. $\lambda x. \left\lceil \frac{n_j x + (i<j)}{n_i+n_j} \right\rceil \in \mathrm{Spec}\,\mathrm{Down}^{T\to T[i]}(\mathrm{t})$ [da 2. e 4., per definizione]
2. Sia $x \in \mathbb{N}^\star$ e $\mathrm{t}_T(x) = \langle n_i, n\rangle$
3. $x = n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor$ [da 2., per il teorema 5.1]

4. $n = \left\lceil \frac{n_j x + (i<j)}{n_i + n_j} \right\rceil$ [da 3. e 5.]

5. $x = n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor \Leftrightarrow$ [per la proprietà 2.19]
$x = \left\lfloor \frac{(n_i + n_j) n - (i<j)}{n_j} \right\rfloor \Leftrightarrow$ [per la proprietà 2.23]
$n_j x \leq (n_i + n_j)\, n - (i<j) < n_j\,(x+1) \Leftrightarrow$ [somma di $(i<j)$ a tutti i membri]
$n_j x + (i<j) \leq (n_i + n_j)\, n < n_j\,(x+1) + (i<j) \Leftrightarrow$
$\begin{cases} n_j x + (i<j) \leq (n_i + n_j)\, n \\ (n_i + n_j)\, n < n_j\,(x+1) + (i<j) \end{cases} \Leftrightarrow$ [sottrazione di n_j]
$\begin{cases} n_j x + (i<j) \leq (n_i + n_j)\, n \\ (n_i + n_j)\, n - n_j < n_j x + (i<j) \end{cases} \Rightarrow$ [perché $(n_i + n_j)\,(n-1) < (n_i + n_j)\, n - n_j$]
$\begin{cases} n_j x + (i<j) \leq (n_i + n_j)\, n \\ (n_i + n_j)\,(n-1) < n_j x + (i<j) \end{cases} \Leftrightarrow$
$(n_i + n_j)\,(n-1) < n_j x + (i<j) \leq (n_i + n_j)\, n \Leftrightarrow$ [per la proprietà 2.23]
$n = \left\lceil \frac{n_j x + (i<j)}{n_i + n_j} \right\rceil$

□

La dimostrazione alternativa richiede il seguente lemma (strettamente legato alla proposizione 6.2:

Lemma 6.2. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1,2\}$, $i \neq j$ e per ogni $x \in \mathbb{N}^\star$:*

$$\mathrm{t}_T(x) = \langle n_i, n \rangle \Rightarrow \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor = \left\lfloor \frac{n_i x - (i<j)}{n_i + n_j} \right\rfloor$$

Dimostrazione.

1. $\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor = \left\lfloor \frac{n_i x - (i<j)}{n_i + n_j} \right\rfloor$ [da 2., per definizione]

2. $\frac{n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_j} = \frac{n_i x - (i<j) - (n_i x - (i<j)) \bmod (n_i + n_j)}{n_i + n_j}$ [da 3., per il teorema 5.1]

3. $\frac{n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_j} = \frac{n_i \left(n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor \right) - (i<j) - (n_i x - (i<j)) \bmod (n_i + n_j)}{n_i + n_j}$ [da 4., per la proposizione 6.2]

4. $\frac{n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_j} = \frac{n_i \left(n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor \right) - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_i + n_j}$ [da 5., dividendo per $(n_i + n_j)\, n_j$]

5. $(n_i + n_j)\,(n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j) = n_i n_j \left(n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor \right) - n_j\,(i<j) - n_j\,((n_i n - (i<j)) \bmod n_j)$ [da 6., calcoli algebrici]

6. $n_i^2 n - n_i\,(i<j) - n_i\,((n_i n - (i<j)) \bmod n_j) + n_i n_j n - n_j\,(i<j) - n_j\,((n_i n - (i<j)) \bmod n_j) = n_i n_j n + n_i n_j \left\lfloor \frac{n_i n-(i<j)}{n_j} \right\rfloor - n_j\,(i<j) - n_j\,((n_i n - (i<j)) \bmod n_j)$ [da 7., calcoli algebrici]

7. $n_i^2 n - n_i\,(i<j) - n_i\,((n_i n - (i<j)) \bmod n_j) = n_i n_j \left\lfloor \frac{n_i n-(i<j)}{n_j} \right\rfloor$ [da 8., moltiplicazione per n_i]

8. $n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j = n_j \left\lfloor \frac{n_i n-(i<j)}{n_j} \right\rfloor$ [da 9., per definizione]

9. $n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j = n_j \frac{n_i n-(i<j)-(n_i n-(i<j)) \bmod n_j}{n_j}$ [da 10., calcoli algebrici]

10. $n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j = n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j$

□

Ora dimostriamo nuovamente il teorema 6.2, con l'ausilio del lemma precedente:

Dimostrazione.

1. $\lambda x. \left\lfloor \frac{n_j x+(i<j)}{n_i+n_j} \right\rfloor \in \mathrm{Spec\,Down}^{T\to T[i]}\,(\mathrm{t})$ [da 2. e 3., per definizione di $\mathrm{Spec\,Down}^{T\to T[i]}\,(\mathrm{t})$]

2. Sia $x \in \mathbb{N}^\star$ e $\mathrm{t}_T\,(x) = \langle n_i, n\rangle$

3. $n =$ [da 1., per il teorema 5.1]
   $x - \left\lfloor \frac{n_i n-(i<j)}{n_j} \right\rfloor =$ [da 2., per la proposizione 6.2]
   $x - \left\lfloor \frac{n_i x-(i<j)}{n_i+n_j} \right\rfloor =$ [per la proprietà 2.20]
   $\left\lceil \frac{x(n_i+n_j)-(n_i x-(i<j))}{n_i+n_j} \right\rceil =$
   $\left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil$

□

Poiché la funzione $\lambda x. \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil$ ricorrerà spesso in seguito, conviene darle un nome:

Definizione 6.2. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$ e siano $i, j \in \{1, 2\}$, $i \neq j$. Si definisce la seguente funzione da $\mathbb{N}$ in $\mathbb{N}$:*

$$d_T^{i,j}\,(x) \equiv \lambda x. \left\lceil \frac{n_j x + (i<j)}{n_i + n_j} \right\rceil$$

6.4.1 Esempio di calcolo dell'x-esimo trattino

Riprendiamo l'esempio del tratteggio $T_1 \equiv (n_1, n_2) \equiv (3, 4)$ (si veda al esempio la tabella 6.1, in cui è riportato il numero progressivo dei trattini) e vediamo un semplice esempio dell'utilizzo dei teoremi 6.1 e 6.2 per calcolare $\mathrm{t}_{T_1}(x)$. Prendiamo ad esempio $x = 4$. Per prima cosa dobbiamo sapere se $\mathrm{t}_{T_1}(4)$ appartiene a $T_1[1]$ o a $T_1[2]$; allora cominciamo a domandarci: $\mathrm{t}_{T_1}(4) \in T_1[1]$? Applicando il teorema 6.1 con $i = 1$, si ha che:

$\mathrm{t}_{T_1}(4) \in T_1[1] \Leftrightarrow$
$(n_1 \cdot 4 - (1 < 2)) \bmod (n_1 + n_2) < n_2 \Leftrightarrow$
$n_1 \cdot 4 \bmod (n_1 + n_2) < n_2 \Leftrightarrow$
$3 \cdot 4 \bmod 7 < 4 \Leftrightarrow$
$5 < 4 \Leftrightarrow$
F

Quindi $\mathrm{t}_{T_1}(4) \notin T_1[1]$. Allora sicuramente $\mathrm{t}_{T_1}(4) \in T_1[2]$ (o, in altri termini, $\mathrm{DownCons}^{T_1 \to T_1[2]}(\mathrm{t})(4) = 1$), perché T_1 è di secondo ordine (volendo, possiamo riapplicare il teorema 6.1 con $i = 2$ ed avremmo questa volta un risultato vero). Applicando il teorema 6.2 per $i = 2$ abbiamo che $\lambda x. \left\lceil \frac{n_1 x}{n_1+n_2} \right\rceil \in \mathrm{Spec}\,\mathrm{Down}^{T_1 \to T_1[2]}(\mathrm{t})$; ma abbiamo appena dimostrato che $\mathrm{DownCons}^{T_1 \to T_1[2]}(\mathrm{t})(4) = 1$, quindi, per la proprietà 1.5, $\left\lceil \frac{n_1 4}{n_1+n_2} \right\rceil \in \mathrm{Down}_4^{T_1 \to T_1[2]}(\mathrm{t})$, cioè (definizione 1.32) $\mathrm{t}_{T_1}(4) = \mathrm{t}_{T_1[2]}\left(\left\lceil \frac{n_1 4}{n_1+n_2} \right\rceil\right)$. Svolgendo, si ha $\mathrm{t}_{T_1}(4) = \mathrm{t}_{T_1[2]}\left(\left\lceil \frac{n_1 4}{n_1+n_2} \right\rceil\right) = \mathrm{t}_{T_1[2]}\left(\left\lceil \frac{12}{7} \right\rceil\right) = \mathrm{t}_{T_1[2]}(2) = \langle 2, 2 \rangle$, come è possibile verificare nella tabella 6.1.

6.4.2 Interpretazione

Il lemma 6.2 merita maggiore attenzione, ad un livello più intuitivo. Ricordando la proposizione 4.2, possiamo dire che $\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor$ è il numero di trattini positivi di indice j minori di $\langle i, n \rangle$ nel tratteggio T (sono sottintese le notazioni $T \equiv (n_1, n_2) \in \mathcal{L}^2$, $i, j \in \{1, 2\}$, $i \neq j$), e $\left\lfloor \frac{n_i x - (i<j)}{n_i+n_j} \right\rfloor$ è il numero di trattini positivi di indice j minori o uguali a $\langle i, x \rangle$ nel tratteggio $S \equiv \begin{cases} (n_i, n_i + n_j) & \text{se } j = 2 \\ (n_i + n_j, n_i) & \text{se } j = 1 \end{cases}$. Dunque possiamo interpretare il lemma dicendo:

Osservazione 6.1. *Siano $T \equiv (n_1, n_2) \in \mathcal{L}^2$, $i, j \in \{1, 2\}$, $i \neq j$ e $x \in \mathbb{N}^\star$.*

Se $\mathrm{t}_T(x) \in T[i]$, il numero di trattini positivi di indice j minori di $\mathrm{t}_T(x)$ nel tratteggio T è pari al numero di trattini positivi di indice j minori di $\langle i, x \rangle$ nel tratteggio $S \equiv \begin{cases} (n_i, n_i + n_j) & \text{se } j = 2 \\ (n_i + n_j, n_i) & \text{se } j = 1 \end{cases}$.

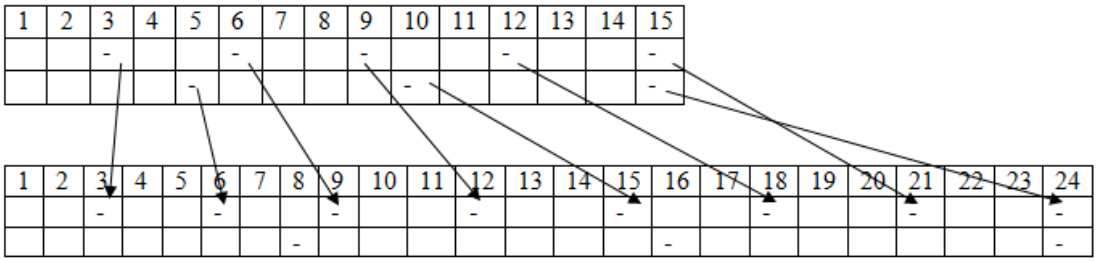

Figura 6.1: Interpretazione del lemma 6.2

Possiamo definire allora una corrispondenza biunivoca f tra Tratt_T e $\mathrm{Tratt}_{S[i]}$, definita da:

$$f\left(\mathrm{t}_T\left(x\right)\right) = \langle i, x\rangle$$

Essa, per l'osservazione 6.1, è tale che, se $t \equiv \mathrm{t}_T\left(x\right) \in T\left[i\right]$, allora il numero di trattini di componente j minori di t in T coincide col numero di trattini di componente j minori di $f\left(t\right)$ in S.

Per chiarire questo concetto, si osservi la figura 6.1, dove è esemplificato il caso di $(n_1, n_2) = (3, 5)$. Consideriamo un qualsiasi trattino di $(3, 5)$ di indice $i = 1$, ad esempio $\langle 1, 4\rangle$. Si può osservare che esistono due trattini di indice $j = 2$ minori di $\langle 1, 4\rangle$ ($\langle 2, 1\rangle$ e $\langle 2, 2\rangle$) nel tratteggio $(3, 5)$, ed altrettanti minori di $f\left(\langle 1, 4\rangle\right) = \langle 1, 6\rangle$ nel tratteggio $S = (3, 3 + 5) = (3, 8)$ ($\langle 2, 1\rangle$ e $\langle 2, 2\rangle$). Per come abbiamo definito f e per l'osservazione 6.1, ciò accade qualsiasi trattino di $T\left[1\right]$ scegliessimo inizialmente, al posto di $\langle 1, 4\rangle$.

Questa proprietà è molto importante, se si considera il seguente aspetto. f mappa trattini di un tratteggio di secondo ordine in trattini di un sottotratteggio *di primo ordine* di un tratteggio di secondo ordine, ossia mappa trattini di T in trattini di $S\left[i\right] = (n_i)$: ecco perché questa funzione è utile nel downcast di t lineare dal secondo ordine al primo.

Possiamo fare, inoltre, una seconda osservazione:

Osservazione 6.2. *Siano* $T \equiv (n_1, n_2) \in \mathcal{L}^2$, $i, j \in \{1, 2\}$, $i \neq j$ *e* $x \in \mathbb{N}^\star$.

Se $\mathrm{t}_T\left(x\right) = \langle j, n\rangle$, $f\left(\mathrm{t}_T\left(x\right)\right)$ *è il più grande trattino di indice* i *minore di* $\mathrm{t}_{S[j]}\left(n\right)$ *nel tratteggio* $S \equiv \begin{cases} (n_i, n_i + n_j) & \text{se } j = 2 \\ (n_i + n_j, n_i) & \text{se } j = 1 \end{cases}$.

Per fare un esempio, riferiamoci come prima alla figura 6.1 e consideriamo il trattino $\mathrm{t}_{(3,5)}\left(5\right) = \langle 2, 2\rangle \equiv \langle j, n\rangle$. Secondo l'osservazione 6.2, $f\left(\mathrm{t}_{(3,5)}\left(5\right)\right)$ è il più grande trattino di indice $i = 1$ minore di $\mathrm{t}_{S[2]}\left(2\right)$ nel tratteggio $S = (3, 8)$. Infatti $f\left(\mathrm{t}_{(3,5)}\left(5\right)\right) = \langle 1, 5\rangle$ e $\mathrm{t}_{S[2]}\left(2\right) = \langle 2, 2\rangle$ e, come si può vedere, il primo precede immediatamente l'altro nell'ordinamento per colonne indotto da S sui suoi trattini.

6.4.3 Tratteggi superiori: un mezzo per risolvere il problema del downcast di t

Le osservazioni 6.1 e 6.2 sono state ottenute a partire dal lemma 6.2. È importante sottolineare che si può, viceversa, dimostrare il lemma 6.2, e quindi il teorema 6.2, a condizione che si trovi un tratteggio T' che soddisfa la seguente definizione di *tratteggio superiore*, generalizzazione delle due osservazioni citate:

Definizione 6.3. *Siano T un tratteggio di ordine $d > 1$, $j \in [1, d]$ e $T' \equiv T[1, \dots, j-1, j+1, \dots d]$. Un tratteggio $S \in \mathcal{T}^d$ è detto* tratteggio superiore *di T rispetto a j se, posto $S' \equiv S[1, \dots, j-1, j+1, \dots d]$, per ogni $x \in \mathbb{N}^\star$ valgono le seguenti proprietà:*

- *Se $\mathrm{t}_T(x) \in T'$, $|\{t \in T[j] \mid \langle j, 0\rangle < t < \mathrm{t}_T(x)\}| = |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\}|$* [1]
- *Per ogni $n \in \mathbb{N}^\star$, $\mathrm{t}_{S'}(x)$ è il più grande trattino di S' minore di $\mathrm{t}_{S[j]}(n)$ nel tratteggio S se e solo se $\mathrm{t}_T(x) = \langle j, n\rangle$*

Dato un tratteggio $T \in \mathcal{T}^d$, se si conosce un suo tratteggio superiore S rispetto a j, è possibile risolvere il problema del downcast da T a $T[1, \dots, j-1, j+1, \dots d]$, grazie alla seguente proposizione.

Proposizione 6.4. *Siano T un tratteggio di ordine $d > 1$, $j \in [1, d]$ e $T' \equiv T[1, \dots, j-1, j+1, \dots d]$. Siano S un tratteggio superiore di T rispetto a j ed $S' \equiv S[1, \dots, j-1, j+1, \dots d]$. Allora*

$$\lambda x.\,(x - |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\}|) \in \mathrm{Spec}\,\mathrm{Down}^{T \to T'}(\mathrm{t})$$

dove il segno di $<$ si riferisce all'ordinamento dei trattini di S.

Dimostrazione.

1. $\lambda x.\,(x - |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\}|) \in \mathrm{Spec}\,\mathrm{Down}^{T \to T'}(\mathrm{t})$ [da 2. e 3.]
2. Sia $\mathrm{t}_T(x) = \mathrm{t}_{T'}(n)$, $n \in \mathbb{N}^\star$
3. $n =$ [per definizione di t]
   $|\{t \in T' \mid \langle j, 0\rangle < t \leq \mathrm{t}_{T'}(n)\}| =$ [da 2.]
   $|\{t \in T' \mid \langle j, 0\rangle < t \leq \mathrm{t}_T(x)\}| =$ [dall'ipotesi $T' \equiv T[1, \dots, j-1, j+1, \dots d]$]
   $|\{t \in T \mid \langle j, 0\rangle < t \leq \mathrm{t}_T(x)\}| - |\{t \in T[j] \mid \langle j, 0\rangle < t \leq \mathrm{t}_T(x)\}| =$
   $x - |\{t \in T[j] \mid \langle j, 0\rangle < t \leq \mathrm{t}_T(x)\}| =$ [perché, da 2., $\mathrm{t}_T(x) \in T'$, quindi

[1] Il segno di minore nell'insieme di sinistra è l'ordinamento dei trattini di T; quello nell'insieme di destra è l'ordinamento dei trattini di S'.

$\mathrm{t}_T(x) \notin T[j]]$
$x - |\{t \in T[j] \mid \langle j, 0\rangle < t < \mathrm{t}_T(x)\}| =$ [perché S è tratteggio superiore di T]
$x - |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\}|$

□

Si noti che la proposizione 6.4 sfrutta solo la prima delle due proprietà del tratteggio superiore. Sfruttando anche la seconda, si ottiene il seguente risultato:

Proposizione 6.5. *Siano T un tratteggio di ordine $d > 1$, $j \in [1, d]$ e $T' \equiv T[1, \ldots, j-1, j+1, \ldots d]$. Siano S un tratteggio superiore di T rispetto a j ed $S' \equiv S[1, \ldots, j-1, j+1, \ldots d]$. Allora*

$$\lambda x.\,(x - |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x+1)\}|) \in \mathrm{Spec\,Down}^{T \to T'}(\mathrm{t})$$

$$\lambda x.\,|\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x+1)\}| \in \mathrm{Spec\,Down}^{T \to T[j]}(\mathrm{t})$$

dove il segno di $<$ si riferisce all'ordinamento dei trattini di S.

Dimostrazione.

1. $\lambda x.\,(x - |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x+1)\}|) \in \mathrm{Spec\,Down}^{T \to T'}(\mathrm{t})$ [da (a), (b) e (c)]

   (a) Sia $\mathrm{t}_T(x) \in T'$

   (b) $\lambda x.\,(x - |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\}|) \in \mathrm{Spec\,Down}^{T \to T'}(\mathrm{t})$ [per la proposizione 6.4]

   (c) $\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x+1)\} =$
   $\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\} + \{t \in S[j] \mid \mathrm{t}_{S'}(x) \leq t < \mathrm{t}_{S'}(x+1)\} =$ [per l'ipotesi $S' \equiv S[1, \ldots, j-1, j+1, \ldots d]$]
   $\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\} + \{t \in S[j] \mid \mathrm{t}_{S'}(x) < t < \mathrm{t}_{S'}(x+1)\} =$ [da i. e ii.]
   $\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x)\}$

      i. Sia $A \equiv \{t \in S[j] \mid \mathrm{t}_{S'}(x) < t < \mathrm{t}_{S'}(x+1)\}$

      ii. $A = \emptyset$ [da (a), iii. e iii.–C. per assurdo: infatti $\mathrm{t}_T(x) \in T' \Rightarrow \mathrm{t}_T(x) \notin T[j]]$

      iii. Se $A \neq \emptyset$

         A. Sia $t \equiv \langle j, h\rangle \in A$, $h \in \mathbb{N}^\star$

         B. $\mathrm{t}_{S'}(x)$ è il più grande trattino di S' minore di t in S [da A. e i.]

C. $\mathrm{t}_T(x) =$ [perché S è tratteggio superiore di T]
$t \in$ [da A.]
$T[j]$

2. $\lambda x.\,|\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x+1)\}| \in \mathrm{Spec}\,\mathrm{Down}^{T \to T[j]}(\mathrm{t})$ [da (a) e (b)]

   (a) Sia $\mathrm{t}_T(x) = \langle j, n\rangle$

   (b) $n = |\{t \in S[j] \mid \langle j, 0\rangle < t < \mathrm{t}_{S'}(x+1)\}|$ [da (c)]

   (c) $\mathrm{t}_{S[j]}(n)$ è il più grande trattino di $S[j]$ minore di $\mathrm{t}_{S'}(x+1)$ [da (d) ed (e)]

   (d) $\mathrm{t}_{S[j]}(n) < \mathrm{t}_{S'}(x+1)$ [da i.]

      i. $\mathrm{t}_{S'}(x+1)$ è il più piccolo trattino di S' maggiore di $\mathrm{t}_{S[j]}(n)$ nel tratteggio S [da ii.]

      ii. $\mathrm{t}_{S'}(x)$ è il più grande trattino di S' minore di $\mathrm{t}_{S[j]}(n)$ nel tratteggio S [da (a), perché S è tratteggio superiore di T]

   (e) $\mathrm{t}_{S[j]}(n+1) \geq \mathrm{t}_{S'}(x+1)$ [da (f), (f)–ii. e (a), per assurdo]

   (f) Se $\mathrm{t}_{S[j]}(n+1) < \mathrm{t}_{S'}(x+1)$

      i. $\mathrm{t}_{S'}(x)$ è il più grande trattino di S' minore di $\mathrm{t}_{S[j]}(n+1)$ nel tratteggio S [da (f) e (d)–ii.]

      ii. $\mathrm{t}_T(x) = \langle j, n+1\rangle$ [da i., perché S è tratteggio superiore di T]

□

Per quanto riguarda $\mathcal{L}^2$, dalle osservazioni 6.1 e 6.2 si ottiene che, dato un tratteggio $T \equiv (n_1, n_2)$, un suo tratteggio superiore rispetto a j è il tratteggio:

$$S \equiv \begin{cases} (n_i, n_i + n_j) & \text{se } j = 2 \\ (n_i + n_j, n_i) & \text{se } j = 1 \end{cases} \tag{6.2}$$

Inoltre, si può anche dimostrare che esso è anche l'unico tratteggio superiore primitivo del tratteggio T (tuttavia si è scelto di non dimostrarlo in questa edizione, così come non sono state formalmente dimostrate le osservazioni 6.1 e 6.2). Si noti che questo tratteggio S è esattamente il tratteggio usato "inconsapevolmente" nella soluzione che abbiamo dato al problema del downcast, che può essere riassunta nei teoremi 6.1 e 6.2. Si potrebbe, tuttavia, risolvere il problema del downcast anche senza che ciò corrisponda a conoscere un tratteggio superiore, come osserveremo a proposito di $\mathcal{L}^3$ (si veda il paragrafo 6.7.3).

6.5 Stima di t_valore lineare di secondo ordine

Sembra superfluo dedicare un paragrafo alla funzione t_valore lineare in un capitolo che tratta in dettaglio la funzione t: infatti, $\text{t\_valore}_T(x)$ è per definizione $T(\text{t}_T(x))$, per x positivi: è facile immaginare che le proprietà di t_valore discendano da quelle di t. Tuttavia, potrebbe essere utile avere solo una stima di $\text{t\_valore}_T(x)$, anziché il valore esatto: come vedremo di seguito, questa stima può essere calcolata anche senza passare per $\text{t}_T(x)$, ed in modo più semplice.

Teorema 6.3. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$. *Per ogni* $x \in \mathbb{N}^\star$,

$$\begin{cases} \text{t\_valore}_T(x) = \left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor & \textit{se } \text{MCM}(n_1,n_2) \mid \text{t\_valore}_T(x) \wedge \text{t}_T(x) \in (n_2) \\ \left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor < \text{t\_valore}_T(x) \leq \left\lfloor \frac{n_1 n_2 (x+1)}{n_1+n_2} \right\rfloor & \textit{altrimenti} \end{cases}$$

Dimostrazione.

1. $\text{SeMCM}(n_1, n_2) \mid \text{t\_valore}_T(x) \wedge \text{t}_T(x) \in (n_2)$

   (a) $\text{t_valore}_T(x) = $ [da (b)]
   $n_2 \left\lceil \frac{n_1 x}{n_1+n_2} \right\rceil =$
   $n_2 \frac{n_1 x - n_1 x \bmod (n_1+n_2)}{n_1+n_2} =$ [da (c)]
   $n_2 \frac{n_1 x}{n_1+n_2} =$
   $\frac{n_1 n_2 x}{n_1+n_2} =$ [da (d)]
   $\frac{n_1 n_2 x - n_1 n_2 x \bmod (n_1+n_2)}{n_1+n_2} =$
   $\left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor$

   (b) $\text{t}_T(x) = \left\langle n_2, \left\lceil \frac{n_1 x}{n_1+n_2} \right\rceil \right\rangle$ [da 1. (in particolare $\text{t}_T(x) \in (n_2)$), per il teorema 6.2]

   (c) $n_1 x \bmod (n_1+n_2) =$
   $((n_1+n_2)\, x - n_2 x) \bmod (n_1+n_2) =$ [per la proprietà 2.14]
   $n_1 + n_2 - n_2 x \bmod^\star (n_1+n_2) =$ [da (e)]
   $n_1 + n_2 - (n_1+n_2) =$
   0

   (d) $n_1 n_2 x \bmod (n_1+n_2) =$ [per la proprietà 2.6]
   $n_1 (n_2 x \bmod (n_1+n_2)) \bmod (n_1+n_2) =$ [da (e)]
   $0 \bmod (n_1+n_2) =$
   0

   (e) $n_2 x \bmod (n_1+n_2) =$ [da 1. (in particolare $\text{t}_T(x) \in (n_2)$) per la proposizione 6.2]

$\text{t\_valore}_T(x) \bmod n_1 =$ [da 1., in particolare da $\text{MCM}(n_1, n_2) \mid \text{t\_valore}_T(x)$]
0

2. Altrimenti:

   (a) $\left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor < \text{t\_valore}_T(x) \leq \left\lfloor \frac{n_1 n_2 (x+1)}{n_1+n_2} \right\rfloor$ [da (b), per la proprietà 2.26]

   (b) $x+1 = \left\lceil \frac{(n_1+n_2)\text{t\_valore}_T(x)}{n_1 n_2} \right\rceil$ [da (c), (d) ed (e)]

   (c) Sia $\text{t\_valore}_T(x) \in (n_i)$, $i \in \{1,2\}$

   (d) $\text{t\_valore}_T(x) = n_i \left\lceil \frac{n_j x + (i<j)}{n_i+n_j} \right\rceil$, $i \neq j$ [da (c), per il teorema 6.2]

   (e) $x+1 = \left\lceil \frac{(n_1+n_2) n_i \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil}{n_1 n_2} \right\rceil$ [da (f), per qualsiasi scelta di $i, j \in \{1,2\}$, $i \neq j$]

   (f) $x+1 = \left\lceil \frac{(n_i+n_j) n_i \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil}{n_i n_j} \right\rceil$ [da (g), calcoli algebrici]

   (g) $x+1 = \left\lceil \frac{(n_i+n_j) \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil}{n_j} \right\rceil$ [da (h), per definizione]

   (h) $x+1 = \left\lceil \frac{(n_i+n_j)\left(\frac{n_j x+(i<j)-\left(n_j x+(i<j)\right) \bmod^\star \left(n_i+n_j\right)}{n_i+n_j}+1 \right)}{n_j} \right\rceil$ [da (i), calcoli algebrici]

   (i) $x+1 = \left\lceil \frac{n_j x+(i<j)-(n_j x+(i<j)) \bmod^\star (n_i+n_j)+n_i+n_j}{n_j} \right\rceil$ [da (j), per la proprietà 2.19]

   (j) $x+1 = x + \left\lceil \frac{(i<j)-(n_j x+(i<j)) \bmod^\star (n_i+n_j)+n_i+n_j}{n_j} \right\rceil$ [da (k), calcoli algebrici]

   (k) $1 = \left\lceil \frac{(i<j)-(n_j x+(i<j)) \bmod^\star (n_i+n_j)+n_i+n_j}{n_j} \right\rceil$ [da (l), per la proprietà 2.23]

   (l) $0 < (i<j) - (n_j x + (i<j)) \bmod^\star (n_i+n_j) + n_i + n_j \leq n_j$ [da (m) ed (n)]

   (m) $0 < (i<j) - (n_j x + (i<j)) \bmod^\star (n_i+n_j) + n_i + n_j$ [da i., per le proprietà delle disuguaglianze]

      i. $(n_j x + (i<j)) \bmod^\star (n_i+n_j) < (i<j) + n_i + n_j$ [da ii., ii.–A., iii., iii.-A.]

      ii. Se $i < j$

         A. $(n_j x + 1) \bmod^\star (n_i+n_j) < 1 + n_i + n_j$

      iii. Se $j < i$

A. $n_j x \bmod^\star (n_i + n_j) < n_i + n_j$ [da B., perché $n_j x \bmod^\star (n_i + n_j) \leq n_i + n_j$]

B. $n_j x \bmod^\star (n_i + n_j) \neq n_i + n_j$ [da C., per definizione]

C. $n_j x \bmod (n_i + n_j) \neq 0$ [da D. ed E.]

D. $n_j x \bmod (n_i + n_j) = 0 \Rightarrow n_i x \bmod (n_i + n_j) = 0$
[infatti, sostituendo nella proprietà 2.4 $n_i x$ al posto di a, $n_j x$ al posto di k e $(n_i + n_j)$ al posto di n, si ottiene che, se $n_i x \bmod (n_i + n_j) + n_j x \bmod (n_i + n_j) < n_i + n_j$, allora $(n_i x + n_j x) \bmod (n_i + n_j) = n_i x \bmod (n_i + n_j) + n_j x \bmod (n_i + n_j)$. La condizione richiesta è verificata, perché per ipotesi $n_j x \bmod (n_i + n_j) = 0$ e l'altro addendo è minore di $n_i + n_j$. Dunque $(n_i x + n_j x) \bmod (n_i + n_j) = n_i x \bmod (n_i + n_j) + n_j x \bmod (n_i + n_j)$, dove il membro di sinistra ed il secondo addendo di destra sono nulli, implicando che $n_i x \bmod (n_i + n_j) = 0$.]

E. $n_i x \bmod (n_i + n_j) \neq 0$ [da F., per il teorema 6.1 (in particolare l'ultima parte: "se $\mathrm{t}_T(x) \in T[i], n_j \mid \mathrm{t\_valore}_T(x) \Leftrightarrow n_i x \bmod (n_i + n_j) = n_j \; (i < j)$")]

F. $n_j \nmid \mathrm{t\_valore}_T(x)$ [da G., perché $n_j \mid \mathrm{MCM}(n_1, n_2)$]

G. $\mathrm{MCM}(n_1, n_2) \nmid \mathrm{t\_valore}_T(x)$ [da H. e (o)]

H. $\mathrm{t}_T(x) \in (n_2)$ [da (c) e I.]

I. $i = 2$ [da iii., essendo $i, j \in \{1, 2\}$]

(n) $(i < j) - (n_j x + (i < j)) \bmod^\star (n_i + n_j) + n_i + n_j \leq n_j$

i. $(i < j) - (n_j x + (i < j)) \bmod^\star (n_i + n_j) + n_i \leq 0$

ii. $(n_j x + (i < j)) \bmod^\star (n_i + n_j) \geq (i < j) + n_i$

(o) $\neg \mathrm{t}_T(x) \in (n_1) \Rightarrow \mathrm{MCM}(n_1, n_2) \nmid \mathrm{t\_valore}_T(x)$ [da i.]

i. $\mathrm{MCM}(n_1, n_2) \mid \mathrm{t\_valore}_T(x) \Rightarrow \mathrm{t}_T(x) \in (n_1)$ [da ii.]

ii. $\mathrm{MCM}(n_1, n_2) \nmid \mathrm{t\_valore}_T(x) \vee \mathrm{t}_T(x) \in (n_1)$ [2. scritto in formule, ottenuto negando la 1.]

□

A titolo di esempio, applichiamo il teorema appena dimostrato al tratteggio $(3, 11)$. In figura 6.2 vediamo la tabella che rappresenta il tratteggio, dove per ogni $x > 0$ sono stati marcati i passaggi tra la colonna $\left\lfloor \frac{n_1 n_2 x}{n_1 + n_2} \right\rfloor = \left\lfloor \frac{33x}{14} \right\rfloor$ (il cui numero è evidenziato in grassetto) e la colonna $\left\lfloor \frac{33(x+1)}{14} \right\rfloor$. Le colonne della tabella sono così ripartite in gruppi o di due o di tre colonne, nell'x-esimo dei quali vi è

0	1	**2**	3	**4**	5	6	**7**	8	**9**	10	**11**	12	13	**14**	15	**16**
-			-			-			-			-			-	
-											-					

17	**18**	19	20	**21**	22	**23**	24	**25**	26	27	**28**	29	**30**	31	32	**33**
	-			-			-			-			-			-
					-											-

Figura 6.2: Stime di t_valore nel tratteggio $(3, 11)$

l'x-esimo trattino. L'unica eccezione, contemplata dal teorema, è l'ultimo gruppo di colonne, 31, 32 e 33, che contiene due trattini. Infatti per $\mathrm{t}_{(3,11)}(14)$, essendo $\mathrm{MCM}(n_1, n_2) \mid \mathrm{t\_valore}_{(3,11)}(14) \wedge \mathrm{t}_{(3,11)}(14) \in (11)$, per il teorema 6.3 si ha che $\mathrm{t\_valore}_{(3,11)}(14) = \left\lfloor \frac{33 \cdot 14}{14} \right\rfloor = 33$, mentre per $\mathrm{t}_{(3,11)}(13)$ si ha che $30 = \left\lfloor \frac{33 \cdot 13}{14} \right\rfloor < \mathrm{t\_valore}_{(3,11)}(14) \leq \left\lfloor \frac{33 \cdot 14}{14} \right\rfloor = 33$.

L'ampiezza dell'x-esimo gruppo di colonne (quello che contiene $\mathrm{t}_{(3,11)}(x)$) è $\left\lfloor \frac{n_1 n_2 (x+1)}{n_1+n_2} \right\rfloor - \left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor$: troveremo quest'espressione nel capitolo 9. La posizione di $\mathrm{t}_{(3,11)}(x)$ all'interno del suo gruppo di colonne, ottenibile con $p(x) \equiv \mathrm{t\_valore}_{(3,11)}(x) - \left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor$, sembra non seguire un andamento regolare: le posizioni $p(x)$ da $x = 1$ in poi sono $0, 1, 1, 1, 0, 0, 1, 2, 0, 0, 1, 1, 2$. Si potrebbe studiare $p(x)$ calcolando $\mathrm{t\_valore}_{(3,11)}(x)$ a partire da $\mathrm{t}_{(3,11)}(x)$ e quindi sfruttando i teoremi 6.1 e 6.2: probabilmente si arriverebbe ad una espressione semplice. In alternatica, è possibile studiare $p(x)$ di per sè, dimenticandosi dei teoremi già noti sui tratteggi: in questo modo si può calcolare $\mathrm{t\_valore}_{(3,11)}(x)$ direttamente come $\left\lfloor \frac{n_1 n_2 x}{n_1+n_2} \right\rfloor + p(x)$, ossia come stima più correzione. Ciò è stato svolto effettivamente, pervenendo ad una espressione estremamente complessa, che vedremo nell'appendice 8.2.

6.6 Down-conservatività di t lineare di terzo ordine

In questo paragrafo generalizziamo al terzo ordine i risultato visti nel paragrafo 6.3 per il secondo ordine. La seguente proposizione è la generalizzazione della proposizione 6.2.

Proposizione 6.6. *Sia $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. Per ogni i, j, k tali che $\{i, j, k\} = \{1, 2, 3\}$ e per ogni $x \in \mathbb{N}^\star$, ponendo $y \equiv \mathrm{t\_valore}_T(x)$:*

$$\mathrm{t}_T(x) \in (n_i) \Rightarrow \begin{array}{l} (n_j + n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k) = \\ n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) \end{array}$$

Dimostrazione.

1. Sia $\mathrm{t}_T(x) = \langle n_i, n \rangle$

2. Sia $m \equiv n_i n_j + n_i n_k + n_j n_k$

3. $(n_j + n_k)\, n_i x \bmod m =$ [da 2. e 1., per il teorema 5.2]
$(n_j + n_k)\, n_i \left(n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) \bmod m =$
$\left((n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + (n_j + n_k)\, n_i n\right) \bmod m =$
[aggiunta e sottrazione di $n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right)$]
$$\left(\begin{array}{c}(n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) \\ + (n_j + n_k)\, n_i n - n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) - n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right)\end{array}\right) \bmod m =$$
$$\left(\begin{array}{c}(n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) \\ + n_i n_k n - n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) + n_i n_j n - n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right)\end{array}\right) \bmod m =$$
[moltiplicazione e divisione per $n_j n_k$]
$$\left(\begin{array}{c}(n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) \\ + n_j n_k \left(\frac{n_i n_k n - n_k (\mathrm{mod}(n_i n, n_j, j<i)) + n_i n_j n - n_j (\mathrm{mod}(n_i n, n_k, k<i))}{n_j n_k}\right)\end{array}\right) \bmod m =$$
$$\left(\begin{array}{c}(n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) + \\ + n_j n_k \left(\frac{n_i n - \mathrm{mod}(n_i n, n_j, j<i)}{n_j} + \frac{n_i n - \mathrm{mod}(n_i n, n_k, k<i)}{n_k}\right)\end{array}\right) \bmod m =$$
$$\left(\begin{array}{c}(n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) + \\ + n_j n_k \left(\frac{n_i n - (i<j) - (n_i n - (i<j)) \bmod n_j}{n_j} + \frac{n_i n - (i<k) - (n_i n - (i<k)) \bmod n_k}{n_k}\right)\end{array}\right) \bmod m =$$
$$\left(\begin{array}{c}(n_j + n_k)\, n_i \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) + \\ + n_j n_k \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right)\end{array}\right) \bmod m =$$
$$\left(\begin{array}{c}(n_i n_j + n_i n_k + n_j n_k) \left(\left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor\right) + \\ + n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right)\end{array}\right) \bmod m =$$
[da 2., per definizione di modulo e perché $n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right) < m$]
$n_j \left(\mathrm{mod}\left(n_i n, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i n, n_j, j < i\right)\right)$

□

Si può dimostrare che una forma equivalente dell'enunciato, che non fa uso della funzione modulo a tre argomenti, è la seguente:

$$\mathrm{t}_T(x) \in (n_i) \Rightarrow \begin{array}{c} ((n_j+n_k)\, n_i x - n_k\,(j<i) - n_j\,(k<i)) \bmod (n_i n_j + n_i n_k + n_j n_k) = \\ n_j\,((y-(k<i)) \bmod n_k) + n_k\,((y-(j<i)) \bmod n_j) \end{array}$$

Questa forma è più simile a quella della proposizione 6.2, ma come generalizzazione preferiamo quella con la funzione modulo a tre argomenti, perché più sintetica.

Ora ci chiediamo: vale l'inverso della proposizione 6.6? La domanda è lecita, in quanto la proposizione 6.6 è la generalizzazione della proposizione 6.2, l'inverso della quale vale in $\mathcal{L}^2$. Purtroppo le cose non sono così semplici, in quanto nel terzo ordine bisogna trattare alcuni casi particolari.

Proposizione 6.7. *Sia* $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. *Siano* i, j, k *tali che* $\{i,j,k\} = \{1,2,3\}$. *Sia* $x \in \mathbb{N}^\star$ *tale che, posto* $y \equiv \mathrm{t\_valore}_T(x)$, *valga la seguente uguaglianza:*

$$(n_j+n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k) = n_j\,(\mathrm{mod}\,(y, n_k, k<i)) + n_k\,(\mathrm{mod}\,(y, n_j, j<i))$$

Si ha che:

- *Se* $i=1$, $n_2 \mid y$, $n_2 n_3 = (n_2+n_3)\,(n_1 - y \bmod n_1)$, *allora* $\mathrm{t}_T(x) \in (n_1, n_3)$. *In particolare, se i due membri dell'uguaglianza valgono* $2n_2n_3$, *allora* $\mathrm{t}_T(x) \in (n_3)$; *altrimenti,* $\mathrm{t}_T(x) \in (n_1)$.
- *Se* $i=3$, $n_2 \mid y$, $n_1 n_2 = (n_1+n_2)\,(y \bmod^\star n_3)$, *allora* $\mathrm{t}_T(x) \in (n_1, n_3)$. *In particolare, se i due membri dell'uguaglianza valgono* 0, *allora* $\mathrm{t}_T(x) \in (n_1)$; *altrimenti,* $\mathrm{t}_T(x) \in (n_3)$.
- *In tutti gli altri casi,* $\mathrm{t}_T(x) \in (n_i)$.

Dimostrazione.

L'enunciato segue da 2., 6., 6.–(a), 6.–(b), 6.–(c), 7., 7.–(a), 7.–(b), 7.–(c), 8., 8.–(a).

1. Sia $m \equiv n_1 n_2 + n_1 n_3 + n_2 n_3$
2. Sia $(n_j+n_k)\, n_i x \bmod m = n_j\,(\mathrm{mod}\,(y, n_k, k<i)) + n_k\,(\mathrm{mod}\,(y, n_j, j<i))$ [per ipotesi]
3. $A \equiv m \mid \left(\begin{array}{c} (n_j+n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i<\mathrm{comp}\,(t))) + \\ +n_j\,(\mathrm{mod}\,(y, n_k, k<\mathrm{comp}\,(t))) + n_k\,(\mathrm{mod}\,(y, n_j, j<\mathrm{comp}\,(t))) + \\ -n_j\,(\mathrm{mod}\,(y, n_k, k<i)) - n_k\,(\mathrm{mod}\,(y, n_j, j<i)) \end{array} \right)$

4. $B \equiv n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) < n_1 n_2 + n_1 n_3 + n_2 n_3$

5. $\left(n_j + n_k\right) n_i x \bmod m = n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) \Leftrightarrow A \wedge B$

6. Se $i = 1$, $n_2 \mid y$, $n_2 n_3 = \left(n_2 + n_3\right)\left(n_1 - y \bmod n_1\right)$

   (a) $\mathrm{comp}\left(t\right) \neq 2$

      i. Se $\mathrm{comp}\left(t\right) = 2$

         A. L'ipotesi 2. è falsa [da 45 e B.]

         B. $A =$ [da 3. e C.]
         $m \mid \left(\begin{array}{c} n_2 n_3 + n_j \left(\mathrm{mod}\left(y, n_k, k < \mathrm{comp}\left(t\right)\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < \mathrm{comp}\left(t\right)\right)\right) + \\ -n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) - n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) \end{array} \right)$
         [da i.]
         $m \mid \left(\begin{array}{c} n_2 n_3 + n_j \left(\mathrm{mod}\left(y, n_k, k < 2\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < 2\right)\right) + \\ -n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) - n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) \end{array} \right) =$
         [da 6.]
         $m \mid \left(\begin{array}{c} n_2 n_3 + n_j \left(\mathrm{mod}\left(y, n_k, k < 2\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < 2\right)\right) + \\ -n_j \left(\mathrm{mod}\left(y, n_k, k < 1\right)\right) - n_k \left(\mathrm{mod}\left(y, n_j, j < 1\right)\right) \end{array} \right) =$
         [per simmetria rispetto a n_j e n_k]
         $m \mid \left(\begin{array}{c} n_2 n_3 + n_2 \left(\mathrm{mod}\left(y, n_3, 3 < 2\right)\right) + n_3 \left(\mathrm{mod}\left(y, n_2, 2 < 2\right)\right) + \\ -n_2 \left(\mathrm{mod}\left(y, n_3, 3 < 1\right)\right) - n_3 \left(\mathrm{mod}\left(y, n_2, 2 < 1\right)\right) \end{array} \right) =$
         [perché $\left(3 < 2\right) = \left(3 < 1\right)$ e $\left(2 < 2\right) = \left(2 < 1\right)$]
         $m \mid n_2 n_3 =$ [perché $0 < n_2 n_3 < m$]
         F

         C. $\left(n_j + n_k\right)\left(n_i - \mathrm{mod}\left(y, n_i, i < \mathrm{comp}\left(t\right)\right)\right) =$ [da i.]
         $\left(n_j + n_k\right)\left(n_i - \mathrm{mod}\left(y, n_i, i < 2\right)\right) =$ [da 5.]
         $\left(n_j + n_k\right)\left(n_1 - \mathrm{mod}\left(y, n_1, 1 < 2\right)\right) =$
         $\left(n_j + n_k\right)\left(n_1 - y \bmod n_1\right) =$ [per simmetria rispetto a n_j e n_k]
         $\left(n_2 + n_3\right)\left(n_1 - y \bmod n_1\right) =$ [da 5.]
         $n_2 n_3$

   (b) $n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) < 2 n_2 n_3 \Rightarrow \mathrm{comp}\left(t\right) = 1$
   [da i., i.–A. e ii.]

      i. Se $\mathrm{comp}\left(t\right) = 1$

         A. $n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) < 2 n_2 n_3$ [da B. e C.]

         B. $n_j \left(\mathrm{mod}\left(y, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(y, n_j, j < i\right)\right) < m$ [da 2., 4. e 5.]

         C. $n_2 n_3 = \left(n_2 + n_3\right) n_1$ [da 5. e D.]

D. $y \bmod n_1 = 0$ [da i.]

ii. Non ci sono valori di $\mathrm{comp}(t)$ diversi da 1 per cui vale i.–A. [da (a), (c)–i. e (c)–i.–A.]

(c) $n_j(\mathrm{mod}(y, n_k, k < i)) + n_k(\mathrm{mod}(y, n_j, j < i)) = 2n_2n_3 \Rightarrow \mathrm{comp}(t) = 3$ [da i., i.–A. e ii.]

i. Se $\mathrm{comp}(t) = 3$

A. $n_j(\mathrm{mod}(y, n_k, k < i)) + n_k(\mathrm{mod}(y, n_j, j < i)) =$ [per simmetria rispetto a n_j e n_k]
$n_2(\mathrm{mod}(y, n_3, 3 < i)) + n_3(\mathrm{mod}(y, n_2, 2 < i)) =$ [da 6.]
$n_2(\mathrm{mod}(y, n_3, 3 < 1)) + n_3(\mathrm{mod}(y, n_2, 2 < 1)) =$ [per definizione, essendo false le condizioni]
$n_2(y \bmod^\star n_3) + n_3(y \bmod^\star n_2) =$ [da 6.]
$n_2(y \bmod^\star n_3) + n_2n_3 =$ [da i.]
$n_2n_3 + n_2n_3 =$
$2n_2n_3$

ii. Non ci sono valori di $\mathrm{comp}(t)$ diversi da 3 per cui vale i.–A. [da (a), (b)–i. e (b)–i.–A.]

7. Se $i = 3$, $n_2 \mid y$, $n_1n_2 = (n_1 + n_2)(y \bmod^\star n_3)$

(a) $\mathrm{comp}(t) \neq 2$

i. Se $\mathrm{comp}(t) = 2$

A. L'ipotesi 1. è falsa [da 5. e B.]

B. $A =$ [da 3. e C.]

$$m \mid \left(\begin{array}{c} (n_1 + n_2)\, n_3 - n_1n_2 + \\ +n_j(\mathrm{mod}(y, n_k, k < \mathrm{comp}(t))) + n_k(\mathrm{mod}(y, n_j, j < \mathrm{comp}(t))) + \\ -n_j(\mathrm{mod}(y, n_k, k < i)) - n_k(\mathrm{mod}(y, n_j, j < i)) \end{array} \right) =$$

[da i.]

$$m \mid \left(\begin{array}{c} (n_1 + n_2)\, n_3 - n_1n_2 + n_j(\mathrm{mod}(y, n_k, k < 2)) + n_k(\mathrm{mod}(y, n_j, j < 2)) \\ -n_j(\mathrm{mod}(y, n_k, k < i)) - n_k(\mathrm{mod}(y, n_j, j < i)) \end{array} \right) =$$

[da 7.]

$$m \mid \left(\begin{array}{c} (n_1 + n_2)\, n_3 - n_1n_2 + n_j(\mathrm{mod}(y, n_k, k < 2)) + n_k(\mathrm{mod}(y, n_j, j < 2)) \\ -n_j(\mathrm{mod}(y, n_k, k < 3)) - n_k(\mathrm{mod}(y, n_j, j < 3)) \end{array} \right) =$$

[per simmetria rispetto a n_j e n_k]

$$m \mid \left(\begin{array}{c} (n_1 + n_2)\, n_3 - n_1n_2 + n_1(\mathrm{mod}(y, n_2, 2 < 2)) + n_2(\mathrm{mod}(y, n_1, 1 < 2)) \\ -n_1(\mathrm{mod}(y, n_2, 2 < 3)) - n_2(\mathrm{mod}(y, n_1, 1 < 3)) \end{array} \right) =$$

[perché $(1 < 2) = (1 < 3)$]

$m \mid ((n_1 + n_2)\, n_3 - n_1 n_2 + n_1 \,(\mathrm{mod}\,(y, n_2, 2 < 2)) - n_1 \,(\mathrm{mod}\,(y, n_2, 2 < 3))) =$
[per definizione, essendo $2 < 2$ falso e $2 < 3$ vero]
$m \mid ((n_1 + n_2)\, n_3 - n_1 n_2 + n_1 \,(y \,\mathrm{mod}^\star\, n_2) - n_1 \,(y \,\mathrm{mod}\, n_2)) =$ [da 7.]
$m \mid ((n_1 + n_2)\, n_3 - n_1 n_2 + n_1 n_2 - n_1 \cdot 0) =$
$m \mid (n_1 + n_2)\, n_3 =$ [perché $0 < (n_1 + n_2)\, n_3 < m$]
F

C. $(n_j + n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i < \mathrm{comp}\,(t))) =$ [da i.]
$(n_j + n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i < 2)) =$ [da 6.]
$(n_j + n_k)\,(n_3 - \mathrm{mod}\,(y, n_3, 3 < 2)) =$
$(n_j + n_k)\,(n_3 - y \,\mathrm{mod}^\star\, n_3) =$ [per simmetria rispetto a n_j e n_k]
$(n_1 + n_2)\,(n_3 - y \,\mathrm{mod}^\star\, n_3) =$
$(n_1 + n_2)\, n_3 - (n_1 + n_2)\,(y \,\mathrm{mod}^\star\, n_3) =$ [da 7.]
$(n_1 + n_2)\, n_3 - n_1 n_2$

(b) $n_j \,(\mathrm{mod}\,(y, n_k, k < i)) + n_k \,(\mathrm{mod}\,(y, n_j, j < i)) > 0 \Rightarrow \mathrm{comp}\,(t) = 3$ [da i., i.–A. e ii.]

i. $n_j \,(\mathrm{mod}\,(y, n_k, k < i)) + n_k \,(\mathrm{mod}\,(y, n_j, j < i)) > 0 \Rightarrow$ [per simmetria rispetto a n_j e n_k]
$n_1 \,(\mathrm{mod}\,(y, n_2, 2 < i)) + n_2 \,(\mathrm{mod}\,(y, n_1, 1 < i)) > 0 \Rightarrow$ [da 7.]
$n_1 \,(\mathrm{mod}\,(y, n_2, 2 < 3)) + n_2 \,(\mathrm{mod}\,(y, n_1, 1 < 3)) > 0 \Rightarrow$ [per definizione, essendo vere le condizioni]
$n_1 \,(y \,\mathrm{mod}\, n_2) + n_2 \,(y \,\mathrm{mod}\, n_1) > 0 \Rightarrow$ [da 7.]
$n_2 \,(y \,\mathrm{mod}\, n_1) > 0 \Rightarrow$ [da B.]
$y \,\mathrm{mod}\, n_1 > 0 \Rightarrow$ [perché $y = |t|$]
$\mathrm{comp}\,(t) \neq 1 \Rightarrow$ [da A.]
$\mathrm{comp}\,(t) = 3$

(c) $n_j \,(\mathrm{mod}\,(y, n_k, k < i)) + n_k \,(\mathrm{mod}\,(y, n_j, j < i)) = 0 \Rightarrow \mathrm{comp}\,(t) = 1$ [da i., i.–A. e ii.]

i. Se $\mathrm{comp}\,(t) = 1$

A. $n_j \,(\mathrm{mod}\,(y, n_k, k < i)) + n_k \,(\mathrm{mod}\,(y, n_j, j < i)) =$ [per simmetria rispetto a n_j e n_k]
$n_1 \,(\mathrm{mod}\,(y, n_2, 2 < i)) + n_2 \,(\mathrm{mod}\,(y, n_1, 1 < i)) =$ [da 7.]
$n_1 \,(\mathrm{mod}\,(y, n_2, 2 < 3)) + n_2 \,(\mathrm{mod}\,(y, n_1, 1 < 3)) =$ [per definizione, essendo vere le condizioni]
$n_1 \,(y \,\mathrm{mod}\, n_2) + n_2 \,(y \,\mathrm{mod}\, n_1) =$ [da 7.]

$n_2 (y \bmod n_1) =$ [da i.]
0

ii. Non ci sono valori di $\mathrm{comp}(t)$ diversi da 1 per cui vale i.–A. [da (a), (b)–i. e (b)–i.–A.]

8. Se non valgono 6. e 7.

(a) $\mathrm{comp}_T(t) = i$ [da (b) e (c)]

(b) $\mathrm{comp}_T(t)$ può essere i [basta fare un esempio. Lasciamo al lettore questa parte.]

(c) $\mathrm{comp}_T(t)$ non può essere diverso da i [da (d)–i.–A. e (d)–ii.–A.]

(d) Se $\mathrm{comp}_T(t) = j$, $j \neq i$

i. Se $j < i$:

A. $A \Leftrightarrow$ [da B. e (e)]
$(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) +$
$n_k(\mathrm{mod}(y, n_j, j < i)) = 0 \Leftrightarrow$ [da C.]
$(n_j + n_k)(y \bmod^\star n_i) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) =$
$0 \Leftrightarrow$
$(n_j + n_k)(y \bmod^\star n_i) = n_j(\mathrm{mod}(y, n_k, k < j) - \mathrm{mod}(y, n_k, k < i)) \Rightarrow$
$(n_j + n_k)(y \bmod^\star n_i) \leq n_j(\mathrm{mod}(y, n_k, k < j) - \mathrm{mod}(y, n_k, k < i)) \Leftrightarrow$
[da iii.]
$(n_j + n_k)(y \bmod^\star n_i) \leq 0 \Leftrightarrow$ [perché $y \bmod^\star n_i > 0$]
F

B. $(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) +$
$n_k(\mathrm{mod}(y, n_j, j < i)) < m$ [da C. e D.]

C. $(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) +$
$n_k(\mathrm{mod}(y, n_j, j < i)) =$ [da i. e (d)]
$(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) =$
[da i.]
$(n_j + n_k)(y \bmod^\star n_i) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) =$
[da iii.]
$(n_j + n_k)(y \bmod^\star n_i)$

D. $(n_j + n_k)(y \bmod^\star n_i) \leq$
$(n_j + n_k) n_i <$ [perché $n_j n_k > 0$]
$n_i n_j + n_i n_k + n_j n_k =$ [da 1., per simmetria del polinomio]
m

ii. Se $i < j$:

A. $A \Leftrightarrow$ [da B. e (e)]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) = m \Leftrightarrow$ [da 1., per simmetria del polinomio]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) = n_i n_j + n_i n_k + n_j n_k \Leftrightarrow$ [da C.]
$(n_j + n_k)\,(y \bmod n_i) + n_k n_j = n_i n_j + n_i n_k + n_j n_k \Leftrightarrow$
$(n_j + n_k)\,(y \bmod n_i) = n_i n_j + n_i n_k \Leftrightarrow$
$(n_j + n_k)\,(y \bmod n_i) = (n_j + n_k)\,n_i \Leftrightarrow$ [calcoli algebrici, $n_j + n_k > 0$]
$y \bmod n_i = n_i \Leftrightarrow$
F

B. $(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) > 0$ [da C. e D.]

C. $(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) =$ [da ii. e (d)]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k n_j =$ [da ii.]
$(n_j + n_k)\,(y \bmod n_i) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k n_j =$ [da iii.]
$(n_j + n_k)\,(y \bmod n_i) + n_k n_j$

D. $(n_j + n_k)\,(y \bmod n_i) + n_k n_j <$
$(n_j + n_k)\,n_i + n_k n_j =$
$n_i n_j + n_i n_k + n_j n_k$

iii. $\mathrm{mod}\,(y, n_k, k < j) - \mathrm{mod}\,(y, n_k, k < i) = 0$ [da A. e B.]

A. $\mathrm{mod}\,(y, n_k, k < j) - \mathrm{mod}\,(y, n_k, k < i) > 0 \Leftrightarrow$
$\mathrm{mod}\,(y, n_k, k < j) > \mathrm{mod}\,(y, n_k, k < i) \Leftrightarrow$ [omettiamo la derivazione, abbastanza facile]
$\mathrm{mod}\,(y, n_k, k < j) = y \bmod^{\star} n_k \wedge \mathrm{mod}\,(y, n_k, k < i) = y \bmod n_k \Leftrightarrow$
[per definizione; omettiamo la derivazione]
$n_k \mid y \wedge j < k < i \Leftrightarrow$ [essendo $j < k < i$]
$n_2 \mid y \wedge i = 3 \Leftrightarrow$ [da 8., in particolare perché non vale la 7.]
F

B. $\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j) > 0 \Leftrightarrow$
$\mathrm{mod}\,(y, n_k, k < i) > \mathrm{mod}\,(y, n_k, k < j) \Leftrightarrow$
$\mathrm{mod}\,(y, n_k, k < i) = y \bmod^{\star} n_k \wedge \mathrm{mod}\,(y, n_k, k < j) = y \bmod n_k \Leftrightarrow$

$n_k \mid y \wedge i < k < j \Leftrightarrow$
$n_2 \mid y \wedge i = 1 \Leftrightarrow$ [da 8., in particolare perché non vale la 6.]
F

(e) $A \equiv$ [da 3.]

$$m \mid \left(\begin{array}{c} (n_j + n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i < \mathrm{comp}\,(t))) + \\ +n_j\,(\mathrm{mod}\,(y, n_k, k < \mathrm{comp}\,(t))) + n_k\,(\mathrm{mod}\,(y, n_j, j < \mathrm{comp}\,(t))) + \\ -n_j\,(\mathrm{mod}\,(y, n_k, k < i)) - n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \end{array} \right) \Leftrightarrow$$

[da (d)]

$$m \mid \left(\begin{array}{c} (n_j + n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i < j)) + \\ +n_j\,(\mathrm{mod}\,(y, n_k, k < j)) + n_k\,(\mathrm{mod}\,(y, n_j, j < j)) + \\ -n_j\,(\mathrm{mod}\,(y, n_k, k < i)) - n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \end{array} \right) \Leftrightarrow$$ [perché $j < j$ è falso]

$m \mid (n_j + n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < j)) + n_k\,(y \,\mathrm{mod}^\star\, n_j) -$
$n_j\,(\mathrm{mod}\,(y, n_k, k < i)) - n_k\,(\mathrm{mod}\,(y, n_j, j < i))$
[da (d)]
$m \mid (n_j + n_k)\,(n_i - \mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < j)) + n_k n_j -$
$n_j\,(\mathrm{mod}\,(y, n_k, k < i)) - n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \Leftrightarrow$
[sottrazione di $(n_i n_j + n_i n_k + n_j n_k) = (n_1 n_2 + n_1 n_3 + n_2 n_3)$ dal secondo membro]
$m \mid (n_j + n_k)\,(-\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < j)) - n_j\,(\mathrm{mod}\,(y, n_k, k < i)) -$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i))$
[cambio di segno al secondo membro]
$m \mid (n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) - n_j\,(\mathrm{mod}\,(y, n_k, k < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i))$

$m \mid (n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \Leftrightarrow$ [da i. e ii.]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \in \{0, (n_1 n_2 + n_1 n_3 + n_2 n_3)\}$

i. $(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(\mathrm{mod}\,(y, n_k, k < i) - \mathrm{mod}\,(y, n_k, k < j)) +$
$n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \leq$ [perché $\mathrm{mod}\,(y, n_k, k < i) \leq n_k$]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(n_k - \mathrm{mod}\,(y, n_k, k < j)) + n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \leq$
[perché $-\mathrm{mod}\,(y, n_k, k < j) \leq 0$]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j\,(n_k + 0) + n_k\,(\mathrm{mod}\,(y, n_j, j < i)) =$
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j n_k + n_k\,(\mathrm{mod}\,(y, n_j, j < i)) \leq$ [perché $\mathrm{mod}\,(y, n_j, j < i) \leq n_j$]
$(n_j + n_k)\,(\mathrm{mod}\,(y, n_i, i < j)) + n_j n_k + n_k n_j \leq$ [perché $\mathrm{mod}\,(y, n_i, i < j) \leq$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
-					-					-					-			
-			-			-			-			-			-			-
-						-						-						-

Tabella 6.4: Tratteggio $(5,3,6) \in \mathcal{L}^3$

$n_i]$
$(n_j + n_k)(n_i) + n_j n_k + n_k n_j <$ [essendo $(n_i n_k + n_j n_k) > 0$]
$(n_j + n_k)(n_i) + n_j n_k + n_k n_j + (n_i n_k + n_j n_k) =$
$2(n_i n_j + n_i n_k + n_j n_k) =$ [da 1., per simmetria del polinomio]
$2m$

ii. $(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(\mathrm{mod}(y, n_k, k < i) - \mathrm{mod}(y, n_k, k < j)) +$
$n_k(\mathrm{mod}(y, n_j, j < i)) \geq$ [perché $\mathrm{mod}(y, n_k, k < i) \geq 0$]
$(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(0 - \mathrm{mod}(y, n_k, k < j)) + n_k(\mathrm{mod}(y, n_j, j < i)) \geq$
[perché $-\mathrm{mod}(y, n_k, k < j) \geq n_k$]
$(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) + n_j(0 - n_k) + n_k(\mathrm{mod}(y, n_j, j < i)) \geq$
$(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) - n_j n_k + n_k(\mathrm{mod}(y, n_j, j < i)) \geq$ [perché $(n_j + n_k)(\mathrm{mod}(y, n_i, i < j)) \geq 0$]
$-n_j n_k + n_k(\mathrm{mod}(y, n_j, j < i)) \geq$ [essendo $n_k(\mathrm{mod}(y, n_j, j < i)) \geq 0$]
$-n_j n_k >$ [essendo $n_i n_j + n_i n_k > 0$]
$-(n_i n_j + n_i n_k + n_j n_k) =$[da 1., per simmetria del polinomio]
$-m$

□

Vediamo degli esempi di applicazione della proposizione.

Sia $T \equiv (5,3,6)$ e $(i,j,k) \equiv (1,3,2)$, cosicché $(5,3,6) = (n_i, n_k, n_j)$. Sia inoltre $x \equiv 12$. Come si può verificare nella tabella 6.4, $\mathrm{t}_T(x) = \mathrm{t}_T(12) = \langle 3,3 \rangle$ e $\mathrm{t\_valore}_T(x) = 18 \equiv y$. Verifichiamo innanzitutto l'ipotesi principale della proposizione:

$$(n_j + n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k) = \begin{pmatrix} n_j(\mathrm{mod}(y, n_k, k < i)) + \\ +n_k(\mathrm{mod}(y, n_j, j < i)) \end{pmatrix} \Leftrightarrow \tag{6.3}$$

$$\begin{aligned}
(6+3)\,5x \bmod (5 \cdot 6 + 5 \cdot 3 + 6 \cdot 3) &= 6(\mathrm{mod}(18, 3, 2 < 1)) + 3(\mathrm{mod}(18, 6, 3 < 1)) \Leftrightarrow \\
45x \bmod 63 &= 6(18 \bmod^\star 3) + 3(18 \bmod^\star 6) \Leftrightarrow \\
45x \bmod 63 &= 18 + 18 \Leftrightarrow \\
45 \cdot 12 \bmod 63 &= 36 \Leftrightarrow \\
36 &= 36
\end{aligned}$$

0	1	2	3	4	5	6	7	8	9	10	11	12
-			-			-			-			-
-						-						
-					-					-		

Tabella 6.5: Tratteggio $(3, 6, 5) \in \mathcal{L}^3$

Inoltre con le stesse assunzioni si applica il primo punto della proposizione 6.7, infatti abbiamo che $i = 1$, $n_2 \mid y \Leftrightarrow 3 \mid 18$ e $n_2 n_3 = 18 = 9 \cdot (5 - 18 \bmod 5) = (n_2 + n_3)(n_1 - y \bmod n_1)$. Con queste informazioni possiamo concludere, grazie alla proposizione, che $\mathrm{t}_T(x) \in (n_1, n_3)$. In particolare, si può dire che $\mathrm{t}_T(x) \in (n_3)$, in quanto i due membri dell'ugualianza 6.3 valgono $2n_2n_3 = 36$.
Questo esempio ci mostra che il semplice fatto che valga l'uguaglianza 6.3 non garantisce che $\mathrm{t}_T(x) \in (n_i)$ (n_1 nell'esempio), diversamente da quanto accade in $\mathcal{L}^2$ (6.3). Tuttavia, è importante osservate che esiste un altro valore di x per cui vale la 6.3, ma $\mathrm{t}_T(x) \in (n_1)$: 19. Infatti, se si prolungasse la tabella 6.4 fino al valore 30 (che poi è MCM $(5, 3, 6)$), si osservarebbe che $\mathrm{t}_T(19) = \langle 1, 6 \rangle$, $\mathrm{t\_valore}_T(19) = 30 \equiv y$ e

$$\begin{aligned}
(n_j + n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k) &= \left(\begin{array}{l} n_j \,(\mathrm{mod}\,(y, n_k, k < i)) + \\ +n_k \,(\mathrm{mod}\,(y, n_j, j < i)) \end{array} \right) \Leftrightarrow \\
45x \bmod 63 &= 6\,(30 \bmod^\star 3) + 3\,(30 \bmod^\star 6) \Leftrightarrow \\
45 \cdot 19 \bmod 63 &= 36 \Leftrightarrow \\
36 &= 36
\end{aligned}$$

Ora il primo caso della proposizione non si può più applicare, perché $n_2 n_3 = 18 \neq 45 = 9 \cdot (5 - 30 \bmod 5) = (n_2 + n_3)(n_1 - y \bmod n_1)$, dunque si applica il terzo caso, secondo il quale $\mathrm{t}_T(x) \in (n_i)$. Si noti che in entrambi i casi l'uguaglianza si riduce a $36 = 36$, sebbene (x, y) sia $(12, 18)$ nel primo caso e $(7, 12)$ nel secondo.

Vediamo ora un esempio del secondo caso.
Sia $T \equiv (3, 6, 5)$ e $(i, j, k) \equiv (3, 1, 2)$, cosicché $(3, 6, 5) = (n_j, n_k, n_i)$. Sia inoltre $x \equiv 7$. Come si può verificare nella tabella 6.5, $\mathrm{t}_T(x) = \mathrm{t}_T(7) = \langle 1, 4 \rangle$ e $\mathrm{t\_valore}_T(x) =$

$12 \equiv y$. Anche in questo caso vale l'uguaglianza:

$$\begin{aligned}
(n_j + n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k) &= \left(\begin{array}{l} n_j \,(\mathrm{mod}\,(y, n_k, k < i)) + \\ +n_k \,(\mathrm{mod}\,(y, n_j, j < i)) \end{array} \right) \Leftrightarrow \qquad (6.4)\\
(3+6)\, 5x \bmod (5 \cdot 3 + 5 \cdot 6 + 3 \cdot 6) &= 3\,(\mathrm{mod}\,(12, 6, 2 < 3)) + 6\,(\mathrm{mod}\,(12, 3, 1 < 3)) \Leftrightarrow \\
45x \bmod 63 &= 3\,(12 \bmod 6) + 6\,(12 \bmod 3) \Leftrightarrow \\
45x \bmod 63 &= 0 + 0 \Leftrightarrow \\
45 \cdot 7 \bmod 63 &= 0 \Leftrightarrow \\
0 &= 0
\end{aligned}$$

Ora si applica il secondo punto della proposizione 6.7, in quanto $i = 3$, $n_2 \mid y \Leftrightarrow 6 \mid 12$ e $n_1 n_2 = 18 = 9 \cdot (12 \bmod^\star 5) = (n_1 + n_2)\,(y \bmod^\star n_3)$. Con queste informazioni possiamo concludere, grazie alla proposizione, che $\mathrm{t}_T\,(x) \in (n_1, n_3)$. In particolare, si può dire che $\mathrm{t}_T\,(x) \in (n_1)$, in quanto i due membri dell'uguaglianza 6.4 valgono 0.
Anche in questo caso si può trovare un altro valore di x per cui vale la 6.4 ma $\mathrm{t}_T\,(x) \in (n_i) = (n_3)$: 21. Invitiamo il lettore a verificarlo, e a notare che anche in questo caso si ha $\mathrm{t\_valore}_T\,(x) = \mathrm{MCM}\,(n_1, n_2, n_3)$ e l'uguaglianza 6.4 si riduce a $0 = 0$.

Riassumendo, abbiamo visto che, sebbene l'uguaglianza

$$(n_j + n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k) = n_j\,(\mathrm{mod}\,(y, n_k, k < i)) + n_k\,(\mathrm{mod}\,(y, n_j, j < i))$$

non garantisca che $\mathrm{t}_T\,(x) \in (n_i)$, è possibile trovare $z \in \mathbb{N}^\star$ tale che $\mathrm{t}_T\,(z) \in (n_i)$ e

$$\begin{aligned}
(n_j + n_k)\, n_i z \bmod (n_i n_j + n_i n_k + n_j n_k) &= \\
n_j\,(\mathrm{mod}\,(\mathrm{t_valore}_T\,(z), n_k, k < i)) + n_k\,(\mathrm{mod}\,(\mathrm{t_valore}_T\,(z), n_j, j < i)) &= \\
n_j\,(\mathrm{mod}\,(y, n_k, k < i)) + n_k\,(\mathrm{mod}\,(y, n_j, j < i))
\end{aligned}$$

dove tuttavia $\mathrm{t\_valore}_T\,(z) \neq y$. Il fatto che sia sempre possibile trovare tale z deriva da una proprietà più generale:
per qualsiasi $b \in \{n_j\,(\mathrm{mod}\,(n_i m, n_k, k < i)) + n_k\,(\mathrm{mod}\,(n_i m, n_j, j < i)) \mid m \in \mathbb{N}\}$ è possibile trovare un $z \in \mathbb{N}^\star$ tale che $\mathrm{t}_T\,(z) \in (n_i)$, è sempre possibile trovare tale che

$$\begin{aligned}
(n_j + n_k)\, n_i z \bmod (n_i n_j + n_i n_k + n_j n_k) &= \\
b &= \\
n_j\,(\mathrm{mod}\,(\mathrm{t_valore}_T\,(z), n_k, k < i)) + n_k\,(\mathrm{mod}\,(\mathrm{t_valore}_T\,(z), n_j, j < i))
\end{aligned}$$

La cosa "strana" dunque è che lo stesso b si possa ottenere come $(n_j + n_k)\, n_i x \bmod (n_i n_j + n_i n_k + n_j n_k)$, con $\mathrm{t}_T(x) \notin (n_i)$, ma questo accade solo nei casi citati dalla proposizione 6.7 e comunque non rappresenta l'aspetto essenziale della questione, che è formalizzato invece nella seguente proposizione.

Definizione 6.4. *Siano $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$ e $i \in \{1,2,3\}$. Si definisce l'insieme:*

$$R_T(i) \equiv \{n_j \,(\mathrm{mod}\,(n_i m, n_k, k < i)) + n_k \,(\mathrm{mod}\,(n_i m, n_j, j < i)) \mid m \in \mathbb{N}\}$$

dove j e k sono tali che $\{i,j,k\} = \{1,2,3\}$.

Si noti che la definizione di $R_T(i)$ è ben posta, in quanto l'espressione dell'insieme resta invariata scambiando j e k.

Proposizione 6.8. *Sia $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. Siano i, j, k tali che $\{i,j,k\} = \{1,2,3\}$. Allora:*

$$\{(n_j + n_k)\, n_i z \bmod (n_i n_j + n_i n_k + n_j n_k) \mid \mathrm{t}_T(z) \in (n_i),\ z \in \mathbb{N}^\star\} = R_T(i)$$

Dimostrazione.

1. Sia $B \equiv \{n_j \,(\mathrm{mod}\,(n_i m, n_k, k < i)) + n_k \,(\mathrm{mod}\,(n_i m, n_j, j < i)) \mid m \in \mathbb{N}\}$
2. $R_T(i) \subseteq B$ [da (a) e (b)]
   (a) Sia $a \in R_T(i)$, $a \equiv (n_j + n_k)\, n_i z \bmod (n_i n_j + n_i n_k + n_j n_k)$, con $\mathrm{t}_T(z) \in (n_i)$ e $z \in \mathbb{N}^\star$
   (b) $a =$ [da (a), per la proposizione 6.6]
   $n_j \,(\mathrm{mod}\,(\mathrm{t\_valore}_T(z), n_k, k < i)) + n_k \,(\mathrm{mod}\,(\mathrm{t\_valore}_T(z), n_j, j < i)) \in$
   [perché, per (a), $n_i \mid \mathrm{t\_valore}_T(z)$]
   B
3. $B \subseteq R_T(i)$ [da (a) e (b)]
   (a) Sia $b \in B$, $b = n_j \,(\mathrm{mod}\,(n_i m, n_k, k < i)) + n_k \,(\mathrm{mod}\,(n_i m, n_j, j < i))$, con $m \in \mathbb{N}$
   (b) $b \in A$
      i. Sia $z \in \mathbb{N}^\star$ tale che $\mathrm{t}_T(z) = \langle n_i, m \rangle$
      ii. $(n_j + n_k)\, n_i z \bmod (n_i n_j + n_i n_k + n_j n_k) =$ [da (b), per la proposizione 6.6]
      $n_j \,(\mathrm{mod}\,(\mathrm{t\_valore}_T(z), n_k, k < i)) + n_k \,(\mathrm{mod}\,(\mathrm{t\_valore}_T(z), n_j, j < i)) =$

[da (b)]
$n_j \left(\mathrm{mod}\left(n_i m, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i m, n_j, j < i\right)\right) =$ [da (a)]
b

iii. $\left(n_j + n_k\right) n_i z \bmod \left(n_i n_j + n_i n_k + n_j n_k\right) \in R_T\left(i\right)$ [da (b)]

□

Posto $r \equiv \left(n_j + n_k\right) n_i x \bmod \left(n_i n_j + n_i n_k + n_j n_k\right)$ La proposizione 6.8 suggerisce che si può calcolare $\mathrm{DownCons}^{T \to T[i]}\left(\mathrm{t}\right)\left(x\right)$ controllando se r appartiene all'insieme $R_T\left(i\right)$. Secondo la proposizione 6.8, questo metodo non dà mai falsi negativi: se $r \notin R_T\left(i\right)$, allora certamente $\mathrm{t}_T\left(x\right) \notin \left(n_i\right)$. Resta da chiedersi, allora, perché il metodo sia corretto, se $r \in R_T\left(i\right)$ implica che $\mathrm{t}_T\left(x\right) \in \left(n_i\right)$. La risposta purtroppo è negativa: solo in alcuni casi il metodo è corretto, non sempre. Concludiamo il paragrafo discutendo di questo punto attraverso esempi, lasciando una trattazione formale a successive edizioni.

Vediamo un caso in cui l'implicazione $r \in R_T\left(i\right) \Rightarrow \mathrm{t}_T\left(x\right) \in \left(n_i\right)$ vale ed un caso in cui non vale, entrambi per il tratteggio $T \equiv \left(3, 4, 4\right)$. Se scegliamo $\left(i, j, k\right) \equiv \left(3, 2, 1\right)$, abbiamo

$$r = \left(3 + 4\right) 4x \bmod 40 = 28x \bmod 40$$

e

$$\begin{aligned} R_T\left(i\right) &= \\ \left\{n_j \left(\mathrm{mod}\left(n_i m, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i m, n_j, j < i\right)\right) \mid m \in \mathbb{N}\right\} &= \\ \left\{4 \left(4m \bmod 3\right) + 3 \left(4m \bmod 4\right) \mid m \in \mathbb{N}\right\} &= \\ \left\{0, 4, 8\right\} & \end{aligned}$$

Come si vede in tabella 6.6, $28x \bmod 40$ assume valori in $R_T\left(i\right)$ solo quando $\mathrm{t}_T\left(x\right) \in \left(n_i\right) = \left(n_3\right)$, quindi l'implicazione è verificata.

Se invece scegliamo $\left(i, j, k\right) \equiv \left(1, 2, 3\right)$, abbiamo

$$r = \left(4 + 4\right) 3x \bmod 40 = 24x \bmod 40$$

e

$$\begin{aligned} R_T\left(i\right) &= \\ \left\{n_j \left(\mathrm{mod}\left(n_i m, n_k, k < i\right)\right) + n_k \left(\mathrm{mod}\left(n_i m, n_j, j < i\right)\right) \mid m \in \mathbb{N}\right\} &= \\ \left\{4 \left(3m \bmod^\star 4\right) + 4 \left(3m \bmod^\star 4\right) \mid m \in \mathbb{N}\right\} &= \\ \left\{8, 16, 24, 32\right\} & \end{aligned}$$

0	1	2	3	4	5	6	7	8	9	10	11	12
-			28			32			36			24
-				16				20				12
-				**4**				**8**				**0**

Tabella 6.6: Tratteggio $T \equiv (3,4,4) \in \mathcal{L}^3$, calcolo di $(3+4)\,4x \bmod 40 = 28x \bmod 40$, $R_T(3) = \{0,4,8\}$

0	1	2	3	4	5	6	7	8	9	10	11	12
-			**24**			**16**			**8**			**32**
-				8				0				16
-				32				24				0

Tabella 6.7: Tratteggio $T \equiv (3,4,4) \in \mathcal{L}^3$, calcolo di $(4+4)\,3x \bmod 40 = 24x \bmod 40$, $R_T(1) = \{8,16,24,32\}$

Come si vede in tabella 6.7, $24x \bmod 40$ assume valori in $R_T(i)$ anche quando $\mathrm{t}_T(x) \notin (n_i) = (n_1)$, quindi l'implicazione non è verificata.

Confrontando i due casi, è evidente che il problema è che nel secondo caso i valori di $24x \bmod 40$ si ripetono con un periodo inferiore a quello del tratteggio (i valori di $24x \bmod 40$ si ripetono con periodo $\frac{40}{\mathrm{MCD}(40,24)} = \frac{40}{8} = 5$, mentre il tratteggio ha periodo $\frac{\mathrm{MCM}(3,4,4)}{3} + \frac{\mathrm{MCM}(3,4,4)}{4} + \frac{\mathrm{MCM}(3,4,4)}{4} = 10$).

Gli esempi visti mostrano che non è facile, per generici tratteggi lineari di terzo ordine, calcolare la down-conservatività di t semplicemente esaminando se il valore di un modulo appartiene ad un certo insieme, diversamente da quanto accade per il secondo ordine (corollario 6.2). Come e perché la questione si complichi passando da $\mathcal{L}^2$ a $\mathcal{L}^3$ è ancora da chiarire. In ogni caso, il problema della down-conservatività di t potrebbe essere risolto anche in $\mathcal{L}^3$ con approcci diversi, come vedremo nel capitolo 7.

Infine, è bene notare che abbiamo solo parlato della down-conservatività di t lineare da un tratteggio di terzo ordine ad un suo sottotratteggio di primo ordine. Sarebbe altrettanto interessante estendere la trattazione nel caso in cui il sottotratteggio è di secondo ordine, ad esempio studiare $\mathrm{DownCons}^{T \to T[i,j]}(\mathrm{t})$. Sebbene ovviamente sia:

$$\mathrm{DownCons}^{T \to T[i,j]}(\mathrm{t}) = \mathrm{DownCons}^{T \to T[i]}(\mathrm{t}) + \mathrm{DownCons}^{T \to T[j]}(\mathrm{t})$$

potrebbe essere più facile calcolare $\mathrm{DownCons}^{T \to T[i,j]}(\mathrm{t})$ rispetto a $\mathrm{DownCons}^{T \to T[i]}(\mathrm{t})$ e $\mathrm{DownCons}^{T \to T[j]}(\mathrm{t})$. Inoltre, sapendo calcolare la down-conservatività verso un sottotratteggio di secondo ordine, è possibile anche calcolare la down-conservatività

verso un sottotratteggio di primo ordine; infatti:

$$\text{DownCons}^{T\to T[i]}(\mathrm{t}) = 1 - \text{DownCons}^{T\to T[j,k]}(\mathrm{t})$$

6.7 Downcast di t lineare di terzo ordine

6.7.1 Downcast di t lineare dal terzo ordine al secondo

Vediamo come è possibile calcolare il downcast di t lineare dal terzo ordine al secondo.

Lemma 6.3. *Sia $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. Siano i, j, k tali che $\{i, j, k\} = \{1, 2, 3\}$. Sia $x \in \mathbb{N}^\star$ tale che $\mathrm{t}_T(x) \in T[i]$. Allora:*

$$x - \left\lfloor \frac{n_i n_j (x+1) - (i<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rfloor \in \text{Down}_x^{T\to T[i,j]}(\mathrm{t})$$

o, equivalentemente:

$$\left\lceil \frac{(n_i+n_j) n_k x - n_i n_j + (i<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil \in \text{Down}_x^{T\to T[i,j]}(\mathrm{t})$$

Dimostrazione.

1. $x - \left\lfloor \frac{n_i n_j (x+1) - (i<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rfloor =$ [per la proprietà 2.20] $\left\lceil \frac{(n_i n_j + n_i n_k + n_j n_k)x - (n_i n_j (x+1) - (i<k)(n_i+n_j))}{n_i n_j + n_i n_k + n_j n_k} \right\rceil = \left\lceil \frac{(n_i+n_j) n_k x - n_i n_j + (i<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$
2. Sia $n \in \text{Down}_x^{T\to T[i,j]}(\mathrm{t})$
3. $\left\lceil \frac{(n_i+n_j) n_k x - n_i n_j + (n_i+n_j)(i<k)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil = n$ [da (a), per la proprietà 2.26]
   (a) $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)(n-1) + n_i n_j - (n_i+n_j)(i<k)}{(n_i+n_j) n_k} \right\rfloor < x \leq \left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k) n + n_i n_j - (n_i+n_j)(i<k)}{(n_i+n_j) n_k} \right\rfloor$ [da (b)]
   (b) $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)(n-1) + n_i n_j - (n_i+n_j)(i<k)}{(n_i+n_j) n_k} \right\rfloor + 1 \leq x \leq \left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k) n + n_i n_j - (n_i+n_j)(i<k)}{(n_i+n_j) n_k} \right\rfloor$ [da (c)]
   (c) $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k) n - (n_i+n_j)(i<k)}{(n_i+n_j) n_k} \right\rfloor \leq$ [da i. e (d), per monotonia] $x \leq$ [da ii. e (d), per monotonia] $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k) n + n_i n_j - (n_i+n_j)(i<k)}{(n_i+n_j) n_k} \right\rfloor$
      i. $n_i ((i<j) + (n_i n - (i<j)) \bmod (n_i+n_j)) \geq 0$

ii. $(i<j)+(n_i n-(i<j)) \bmod (n_i+n_j) \leq$
$1+(n_i n-(i<j)) \bmod (n_i+n_j) \leq$ [dall'ipotesi $\mathrm{t}_T(x) \in T[i]$ e da 2., per il teorema 6.1]
n_j

(d) $x =$ [da 2., per il teorema 5.3]
$n+\left\lfloor \frac{\text{t\_valore}_{T[i,j]}(n)-(i<k)}{n_k} \right\rfloor =$ [da i.]
$n+\left\lfloor \frac{n_i\left\lceil \frac{n_j n+(i<j)}{n_i+n_j} \right\rceil-(i<k)}{n_k} \right\rfloor =$ [per la proprietà 2.19]
$\left\lfloor \frac{n_k n+n_i\left\lceil \frac{n_j n+(i<j)}{n_i+n_j} \right\rceil-(i<k)}{n_k} \right\rfloor =$ [per la proprietà 2.18]
$\left\lfloor \frac{(n_i+n_j)n_k n+n_i(n_i+n_j)\left\lceil \frac{n_j n+(i<j)}{n_i+n_j} \right\rceil-(n_i+n_j)(i<k)}{(n_i+n_j)n_k} \right\rfloor =$
$\left\lfloor \frac{(n_i+n_j)n_k n+n_i(n_i+n_j)\left(\frac{n_j n+(i<j)-\left(n_j n+(i<j)\right) \bmod^\star \left(n_i+n_j\right)}{n_i+n_j}+1\right)-(n_i+n_j)(i<k)}{(n_i+n_j)n_k} \right\rfloor =$
$\left\lfloor \frac{(n_i+n_j)n_k n+n_i(n_j n+(n_i+n_j)+(i<j)-(n_j n+(i<j))(b) \bmod^\star (n_i+n_j))-(n_i+n_j)(i<k)}{(n_i+n_j)n_k} \right\rfloor =$
$\left\lfloor \frac{(n_i n_j+n_i n_k+n_j n_k)n+n_i((n_i+n_j)+(i<j)-(n_j n+(i<j)) \bmod^\star (n_i+n_j))-(n_i+n_j)(i<k)}{(n_i+n_j)n_k} \right\rfloor =$ [per la proprietà 2.14]
$\left\lfloor \frac{(n_i n_j+n_i n_k+n_j n_k)n+n_i((i<j)+(n_i n-(i<j)) \bmod (n_i+n_j))-(n_i+n_j)(i<k)}{n_k(n_i+n_j)} \right\rfloor$

i. $\text{t\_valore}_{T[i,j]}(n) = n_i\left\lceil \frac{n_j n+(i<j)}{n_i+n_j} \right\rceil$ [da ii.]

ii. $\mathrm{t}_{T[i,j]}(n) = \left\langle n_i, \left\lceil \frac{n_j n+(i<j)}{n_i+n_j} \right\rceil \right\rangle$ [da 2., per il teorema 6.2]

□

Teorema 6.4. *Sia $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. Per ogni i, j, k tali che $\{i, j, k\} = \{1, 2, 3\}$:*

$$\lambda x.x - \left\lfloor \frac{n_i n_j (x+1) - (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rfloor \in \operatorname{Spec} \operatorname{Down}^{T \to T[i,j]}(\mathrm{t})$$

o, equivalentemente:

$$\lambda x. \left\lceil \frac{(n_i+n_j) n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil \in \operatorname{Spec} \operatorname{Down}^{T \to T[i,j]}(\mathrm{t})$$

Dimostrazione.

1. $x - \left\lfloor \frac{n_i n_j (x+1) - (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rfloor =$ [per la proprietà 2.20]
$\left\lceil \frac{(n_i n_j + n_i n_k + n_j n_k)x - (n_i n_j (x+1) - (i<k)(j<k)(n_i+n_j))}{n_i n_j + n_i n_k + n_j n_k} \right\rceil =$
$\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$

2. $\lambda x. \left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil \in \operatorname{Spec} \operatorname{Down}^{T \to T[i,j]}(\mathrm{t})$ [da 3. e 4.]

3. Sia $n \in \operatorname{Down}_x^{T \to T[i,j]}(\mathrm{t})$

4. $n = \left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$ [da (a)–i.–A., (a)–ii.–A., (b)–i.]

   (a) Se $(i < k) = (j < k)$

      i. Se $\operatorname{ind}\left(\mathrm{t}_{T[i,j]}(n)\right) = i$:

         A. $n =$ [da i., per il lemma 6.3]
         $\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil =$ [da iii.]
         $\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$

      ii. Se $\operatorname{ind}\left(\mathrm{t}_{T[i,j]}(n)\right) = j$:

         A. $n =$ [da i., per il lemma 6.3]
         $\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil =$ [da iii.]
         $\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$

      iii. $(i < k) = (j < k) = (i < k)\,(j < k)$ [da (a)]

   (b) Se $(i < k) \neq (j < k)$

      i. $n =$ [da ii., per la proprietà 2.26]
      $\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j}{n_i n_j + n_i n_k + n_j n_k} \right\rceil =$ [da vii.]
      $\left\lceil \frac{(n_i+n_j)n_k x - n_i n_j + (i<k)(j<k)(n_i+n_j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$

      ii. $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)(n-1) + n_i n_j}{(n_i+n_j)n_k} \right\rfloor < x \leq \left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)n + n_i n_j}{(n_i+n_j)n_k} \right\rfloor$ [da iii.]

      iii. $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)(n-1) + n_i n_j}{(n_i+n_j)n_k} \right\rfloor + 1 \leq x \leq \left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)n + n_i n_j}{(n_i+n_j)n_k} \right\rfloor$ [da iv.]

      iv. $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)n}{(n_i+n_j)n_k} \right\rfloor \leq x \leq \left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)n + n_i n_j}{(n_i+n_j)n_k} \right\rfloor$ [da v.]

      v. $\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)n}{(n_i+n_j)n_k} \right\rfloor =$ [per la proprietà 2.18]
      $\left\lfloor \frac{\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k)n}{n_i+n_j} \right\rfloor}{n_k} \right\rfloor =$ [per la proprietà 2.19]
      $\left\lfloor \frac{n_k n + \left\lfloor \frac{n_i n_j n}{n_i+n_j} \right\rfloor}{n_k} \right\rfloor \leq$ [da A. e B.]
      $x \leq$ [da vi.]

$\left\lfloor \frac{n_k n + \text{t\_valore}_{T[i,j]}(n)}{n_k} \right\rfloor \leq$ [per il teorema 6.3 e per monotonia della parte intera]
$\left\lfloor \frac{n_k n + \left\lfloor \frac{n_i n_j (n+1)}{n_i + n_j} \right\rfloor}{n_k} \right\rfloor =$
$\left\lfloor \frac{(n_i+n_j) n_k n + (n_i+n_j) \left\lfloor \frac{n_i n_j (n+1)}{n_i+n_j} \right\rfloor}{(n_i+n_j) n_k} \right\rfloor =$
$\left\lfloor \frac{(n_i+n_j) n_k n + n_i n_j (n+1) - n_i n_j (n+1) \bmod (n_i+n_j)}{(n_i+n_j) n_k} \right\rfloor =$
$\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k) n + n_i n_j - n_i n_j (n+1) \bmod (n_i+n_j)}{(n_i+n_j) n_k} \right\rfloor \leq$ [per monotonia della parte intera]
$\left\lfloor \frac{(n_i n_j + n_i n_k + n_j n_k) n + n_i n_j}{(n_i+n_j) n_k} \right\rfloor$

A. Se $\text{ind}\left(\text{t}_{T[i,j]}(n)\right) = \min\{i,j\}$:
$\left\lfloor \frac{n_k n + \left\lfloor \frac{n_i n_j n}{n_i+n_j} \right\rfloor}{n_k} \right\rfloor \leq$ [da A., per il teorema 6.3]
$\left\lfloor \frac{n_k n + \text{t\_valore}_{T[i,j]}(n) - 1}{n_k} \right\rfloor =$ [da (b)]
$\left\lfloor \frac{n_k n + \text{t\_valore}_{T[i,j]}(n) - (\min\{i,j\} < k)}{n_k} \right\rfloor =$
x

B. Se $\text{ind}\left(\text{t}_{T[i,j]}(n)\right) = \max\{i,j\}$:
$\left\lfloor \frac{n_k n + \left\lfloor \frac{n_i n_j n}{n_i+n_j} \right\rfloor}{n_k} \right\rfloor \leq$ [da B., per il teorema 6.3]
$\left\lfloor \frac{n_k n + \text{t\_valore}_{T[i,j]}(n)}{n_k} \right\rfloor =$ [da (b)]
$\left\lfloor \frac{n_k n + \text{t\_valore}_{T[i,j]}(n) - (\max\{i,j\} < k)}{n_k} \right\rfloor =$
x

vi. $x =$ [da 2., per il teorema 5.3]
$n + \left\lfloor \frac{\text{t\_valore}_{T[i,j]}(n) - \left(\text{ind}\left(\text{t}_{T[i,j]}(n)\right) < k\right)}{n_k} \right\rfloor =$ [per la proprietà 2.19]
$\left\lfloor \frac{n_k n + \text{t\_valore}_{T[i,j]}(n) - \left(\text{ind}\left(\text{t}_{T[i,j]}(n)\right) < k\right)}{n_k} \right\rfloor$

vii. $(i < k)(j < k) = 0$ [da (b)]

□

Il lemma 6.3 ed il teorema 6.4 offrono uno spunto per riflettere sull'importanza della simmetria nella teoria dei tratteggi. Infatti, la formula del teorema 6.4 per il downcast da T a $T[i,j]$ è simmetrica rispetto allo scambio di i e j: deve essere così, perché non c'è nessuna proprietà che distingue i da j nel sottotratteggio $T[i,j]$. Questo discorso apparentemente non vale per il lemma 6.3, che fornisce una formula molto simile per il downcast, ma non simmetrica; bisogna notare, però, che nel

lemma i e j non sono indistinguibili, per via dell'ipotesi aggiuntiva $\mathrm{t}_T(x) \in T[i]$, assente nel teorema 6.4.

6.7.2 Downcast di t lineare dal terzo ordine al primo

Siano $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$ e i, j, k tali che $\{i, j, k\} = \{1, 2, 3\}$. Supponiamo che per un certo $x \in \mathbb{N}^\star$ sia $\mathrm{t}_T(x) \in T[i]$. Volendo calcolare $\mathrm{Down}_x^{T \to T[i]}(\mathrm{t})$, possiamo prima calcolare $m \in \mathrm{Down}_x^{T \to T[i,j]}(\mathrm{t})$ e poi $n \in \mathrm{Down}_n^{T[i,j] \to T[i]}(\mathrm{t})$ (m e n esistono perché $\mathrm{t}_T(x) \in T[i]$); infatti:

$$m \in \mathrm{Down}_x^{T \to T[i,j]}(\mathrm{t}) \Leftrightarrow \mathrm{t}_T(x) = \mathrm{t}_{T[i,j]}(m)$$

$$n \in \mathrm{Down}_m^{T[i,j] \to T[i]}(\mathrm{t}) \Leftrightarrow \mathrm{t}_{T[i,j]}(m) = \mathrm{t}_{T[i]}(n)$$

da cui

$$\mathrm{t}_T(x) = \mathrm{t}_{T[i]}(n)$$

cioè $n \in \mathrm{Down}_x^{T \to T[i]}(\mathrm{t})$. In questo modo ci si calcolerebbe n da x grazie al teorema 6.3 ed n da m grazie al teorema 6.2. Tuttavia, ci si può chiedere: esiste un metodo per calcolare direttamente n da x? Il seguente teorema fornisce una parziale risposta positiva.

Teorema 6.5. *Sia $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. Siano $x, n \in \mathbb{N}^\star$ tali che $\mathrm{t}_T(x) = \langle n_i, n \rangle$. Sia inoltre $n_i(n_j + n_k) \geq n_j((n_i n - (i < k)) \bmod n_k)$. Allora per ogni i, j, k tali che $\{i, j, k\} = \{1, 2, 3\}$:*

$$n = \left\lceil \frac{n_j n_k x + n_j (i < k) + n_k (i < j)}{n_i n_j + n_i n_k + n_j n_k} \right\rceil \in \mathrm{Down}_x^{T \to T[i]}(\mathrm{t})$$

Dimostrazione.

1. $n \in \mathrm{Down}_x^{T \to T[i]}(\mathrm{t})$ [dall'ipotesi $\mathrm{t}_T(x) = \langle n_i, n \rangle$]
2. $n = \left\lceil \frac{n_j n_k x}{n_i n_j + n_i n_k + n_j n_k} \right\rceil$ [da (a) e (b)]
   (a) $x = n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor$ [dall'ipotesi $\mathrm{t}_T(x) = \langle n_i, n \rangle$, per il teorema 5.2]
   (b) $x = n + \left\lfloor \frac{n_i n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor \Leftrightarrow$
   $x = \left\lfloor \frac{(n_i + n_j) n - (i<j)}{n_j} \right\rfloor + \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor \Leftrightarrow$
   $x - \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor = \left\lfloor \frac{(n_i + n_j) n - (i<j)}{n_j} \right\rfloor \Leftrightarrow$
   $n_j \left(x - \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor \right) \leq (n_i + n_j) n - (i < j) < n_j \left(x - \left\lfloor \frac{n_i n - (i<k)}{n_k} \right\rfloor + 1 \right) \Leftrightarrow$

$$
\begin{cases}
n_j\left(x-\left\lfloor\frac{n_in-(i<k)}{n_k}\right\rfloor\right)\leq(n_i+n_j)\,n-(i<j)\\
(n_i+n_j)\,n-(i<j)<n_j\left(x-\left\lfloor\frac{n_in-(i<k)}{n_k}\right\rfloor+1\right)
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
n_jx-n_j\left\lfloor\frac{n_in-(i<k)}{n_k}\right\rfloor\leq(n_i+n_j)\,n-(i<j)\\
(n_i+n_j)\,n-(i<j)<n_jx-n_j\left\lfloor\frac{n_in-(i<k)}{n_k}\right\rfloor+n_j
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
n_jx-(n_i+n_j)\,n+(i<j)\leq n_j\left\lfloor\frac{n_in-(i<k)}{n_k}\right\rfloor\\
n_j\left\lfloor\frac{n_in-(i<k)}{n_k}\right\rfloor<n_jx-(n_i+n_j)\,n+(i<j)+n_j
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
n_jx-(n_i+n_j)\,n+(i<j)\leq n_j\frac{n_in-(i<k)-(n_in-(i<k))\bmod n_k}{n_k}\\
n_j\frac{n_in-(i<k)-(n_in-(i<k))\bmod n_k}{n_k}<n_jx-(n_i+n_j)\,n+(i<j)+n_j
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
n_jx-(n_i+n_j)\,n+(i<j)\leq\frac{n_in_jn-n_j(i<k)-n_j((n_in-(i<k))\bmod n_k)}{n_k}\\
\frac{n_in_jn-n_j(i<k)-n_j((n_in-(i<k))\bmod n_k)}{n_k}<n_jx-(n_i+n_j)\,n+(i<j)+n_j
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
n_jn_kx-n_k\,(n_i+n_j)\,n+n_k\,(i<j)\leq\\
\leq n_in_jn-n_j\,(i<k)-n_j\,((n_in-(i<k))\bmod n_k)\\
n_in_jn-n_j\,(i<k)-n_j\,((n_in-(i<k))\bmod n_k)<\\
<n_jn_kx-n_k\,(n_i+n_j)\,n+n_k\,(i<j)+n_jn_k
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
(n_in_j+n_in_k+n_jn_k)\,n-n_j\,((n_in-(i<k))\bmod n_k)\geq\\
\geq n_jn_kx+n_j\,(i<k)+n_k\,(i<j)\\
(n_in_j+n_in_k+n_jn_k)\,n-n_j\,((n_in-(i<k))\bmod n_k)-n_jn_k<\\
<n_jn_kx+n_j\,(i<k)+n_k\,(i<j)
\end{cases}\Leftrightarrow
$$

$$
\begin{cases}
(n_in_j+n_in_k+n_jn_k)\,n-n_j\,((n_in-(i<k))\bmod n_k)\geq\\
\geq n_jn_kx+n_j\,(i<k)+n_k\,(i<j)\\
(n_in_j+n_in_k+n_jn_k)\,(n-1)-n_j\,((n_in-(i<k))\bmod n_k)+n_i\,(n_j+n_k)<\\
<n_jn_kx+n_j\,(i<k)+n_k\,(i<j)
\end{cases}\Rightarrow
$$

[dall'ipotesi $n_i\,(n_j+n_k)\geq n_j\,((n_in-(i<k))\bmod n_k)$]

$$
\begin{cases}
(n_in_j+n_in_k+n_jn_k)\,n\geq n_jn_kx+n_j\,(i<k)+n_k\,(i<j)\\
(n_in_j+n_in_k+n_jn_k)\,(n-1)<n_jn_kx+n_j\,(i<k)+n_k\,(i<j)
\end{cases}\Leftrightarrow
$$

$$
(n_in_j+n_in_k+n_jn_k)\,(n-1)<n_jn_kx+n_j\,(i<k)+n_k\,(i<j)\leq(n_in_j+n_in_k+n_jn_k)\,n\Leftrightarrow
$$

$$
n=\left\lceil\frac{n_jn_kx+n_j(i<k)+n_k(i<j)}{n_in_j+n_in_k+n_jn_k}\right\rceil
$$

□

L'ipotesi $n_i\,(n_j+n_k)\geq n_j\,((n_in-(i<k))\bmod n_k)$, oltre a essere non utilizzabile in pratica (in quanto richiede la conoscenza di n, che è ciò che si vuole calcolare col teorema), è anche abbastanza poco elegante da lasciare il dubbio che il problema del downcast di t lineare dal terzo ordine al primo si possa risolvere senza ipotesi del genere: questo problema è ancora aperto.

6.7.3 Esistono tratteggi superiori in $\mathcal{L}^3$?

In $\mathcal{L}^2$ abbiamo visto che il modo in cui abbiamo calcolato il downcast al primo ordine è equivalente ad aver trovato un tratteggio lineare superiore del tratteggio di partenza (paragrafo 6.4.3). In $\mathcal{L}^3$ non è stato così. Infatti, se si trovasse un tratteggio superiore S di un tratteggio $T \in \mathcal{L}^3$, il downcast si dovrebbe scrivere nella forma prevista dalla proposizione 6.4, ossia $\lambda x.\,(x - |\{t \in S\,[d] \mid t < \mathrm{t}_{S'}\,(x)\}|)$, dove S' è dello stesso ordine del tratteggio verso il quale si fa downcast, di secondo ordine in questo caso. Se osserviamo la formula del downcast al secondo ordine (teorema 6.4), non è certo evidente come questa formula possa ricondursi alla forma citata: dunque il modo con cui abbiamo calcolato il downcast è concettualmente diverso dal trovare un tratteggio superiore. Tuttavia, come sappiamo dalla proposizione 6.4, il downcast si può calcolare anche quando è noto un tratteggio superiore: si otterrebbe quindi un secondo metodo.

Ciò porta a domandarsi se esistono tratteggi superiori in $\mathcal{L}^3$. Questo studio è ancora ad uno stadio iniziale, ma esiste una buona congettura a riguardo:

Congettura 6.1. *Sia $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. Tutti e soli i tratteggi superiori primitivi di T rispetto ad n_3 sono del tipo:*

$$\left(d\frac{n_1}{\mathrm{MCD}\,(n_1, n_3)}, e\frac{n_2}{\mathrm{MCD}\,(n_2, n_3)}, kde\right)$$

dove d, e e k sono soluzioni dell'equazione:

$$k\left(d\frac{n_1}{\mathrm{MCD}\,(n_1, n_3)} + e\frac{n_2}{\mathrm{MCD}\,(n_2, n_3)}\right) = \frac{n_1n_2 + n_1n_3 + n_2n_3}{\mathrm{MCD}\,(n_1, n_3)\,\mathrm{MCD}\,(n_2, n_3)}$$

Per esempio, se $T \equiv (3, 4, 5)$, per trovare i suoi tratteggi superiori primitivi dobbiamo risolvere l'equazione:

$$k\,(3d + 4e) = 47$$

una soluzione della quale è $k = 1$, $e = 2$, $d = 13$, da cui il tratteggio superiore $S \equiv \left(d\frac{n_1}{\mathrm{MCD}(n_1,n_3)}, e\frac{n_2}{\mathrm{MCD}(n_2,n_3)}, kde\right) = (39, 8, 26)$. Ora, applicando la proposizione 6.4, si ottiene che:

$$\lambda x.\,\left(x - \left|\left\{t \in (26) \mid t < \mathrm{t}_{(39,8)}\,(x)\right\}\right|\right) \in \mathrm{Spec}\,\mathrm{Down}^{T\to(3,4)}\,(\mathrm{t}) \tag{6.5}$$

Dalla rappresentazione delle prime colonne della tabella del tratteggio T (figura 6.3), si può vedere che $\mathrm{DownCons}^{T\to(3,4)}\,(\mathrm{t})\,(10) = 1$, quindi dall'equazione 6.5 si

0	1	2	3	4	5	6	7	8	9	10	11	12	...
-			-			-			-			-	
-				-				-				-	
-					-					-			

Figura 6.3: Prime colonne della tabella che rappresenta il tratteggio $(3, 4, 5)$

ottiene che $\text{Down}_{10}^{T\to(3,4)}(\text{t}) = \left\{10 - \left|\left\{t \in (26) \mid t < \text{t}_{(39,8)}(10)\right\}\right|\right\}$: verifichiamolo. Applicando i teoremi 6.1 e 6.2 si ottiene che $\text{t}_{(39,8)}(10) = \langle 2, 9\rangle$. I trattini di (26) (cioè $S[3]$) minori di $\langle 2, 9\rangle$ in S sono due: $\langle 3, 1\rangle$ e $\langle 3, 2\rangle$, di valori rispettivamente 26 e 52 (il trattino $\langle 3, 3\rangle$ ha valore 78, che è maggiore del valore di $\langle 2, 9\rangle$). Quindi $10 - \left|\left\{t \in (26) \mid t < \text{t}_{(39,8)}(10)\right\}\right| = 10 - 2 = 8$ ed effettivamente, come si può vedere in figura 6.3, $\text{Down}_{10}^{T\to(3,4)}(\text{t}) = \{8\}$.

6.8 Stima di t_valore lineare di terzo ordine

Anche per il terzo ordine si può voler trovare una stima di t_valore, senza dover calcolare t, come si è fatto per il secondo ordine, nel paragrafo 6.5. Riportiamo a questo proposito una congettura, la cui dimostrazione è in fase di studio:

Congettura 6.2. *Sia* $T \equiv (n_1, n_2, n_3) \in \mathcal{L}^3$. *Per ogni* $x \in \mathbb{N}^\star$:

$$\begin{cases} \text{t\_valore}_T(x) = \left\lfloor \frac{n_1 n_2 n_3 x}{n_1 n_2 + n_2 n_3 + n_1 n_3} \right\rfloor & \text{se } \begin{cases} \text{MCM}(n_1, n_2, n_3) \mid \text{t\_valore}_T(x) \\ \text{t}_T(x) \in (n_3) \end{cases} \\ \left\lfloor \frac{n_1 n_2 n_3 x}{n_1 n_2 + n_2 n_3 + n_1 n_3} \right\rfloor < \text{t\_valore}_T(x) \leq \left\lfloor \frac{n_1 n_2 n_3 (x+2)}{n_1 n_2 + n_2 n_3 + n_1 n_3} \right\rfloor & \textit{altrimenti} \end{cases}$$

Capitolo 7

Approfondimenti su t lineare in $\mathcal{L}^2$

7.1 Altre proprietà di $\mathcal{L}^2$

Proposizione 7.1. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$. *Per ogni* $i, j \in \{1, 2\}$, $i \neq j$ *e per ogni* $x \in \mathbb{N}^\star$, *se* $\mathrm{t}_T(x) \in T[i]$, *allora*

$$n_j \mid \mathrm{t\_valore}_T(x) \Leftrightarrow n_i x \bmod (n_i + n_j) = n_j \, (i < j)$$

Dimostrazione.

1. $n_j \mid \mathrm{t\_valore}_T(x) \Leftrightarrow n_i x \bmod (n_i + n_j) = n_j \, (i < j)$ [da 3., 3.–(a), 4. e 4.–(a)]
2. Sia $\mathrm{t}_T(x) = \langle n_i, n \rangle$
3. Se $i > j$
   (a) $n_j \mid \mathrm{t\_valore}_T(x) \Leftrightarrow$ [da 2.]
   $n_j \mid n_i n \Leftrightarrow$
   $n_i n \bmod n_j = 0 \Leftrightarrow$ [da 3.]
   $(n_i n - (i < j)) \bmod n_j = 0 \Leftrightarrow$ [da 2., per la proposizione 6.2]
   $(n_i x - (i < j)) \bmod (n_i + n_j) = 0 \Leftrightarrow$ [da 3.]
   $n_i x \bmod (n_i + n_j) = 0$
4. Se $i < j$
   (a) $n_j \mid \mathrm{t\_valore}_T(x) \Leftrightarrow$ [da 2.]
   $n_j \mid n_i n \Leftrightarrow$
   $n_i n \bmod n_j = 0 \Leftrightarrow$
   $(n_i n - 1) \bmod n_j = n_j - 1 \Leftrightarrow$ [da 4.]
   $(n_i n - (i < j)) \bmod n_j = n_j - 1 \Leftrightarrow$ [da 2., per la proposizione 6.2]

$(n_i x - (i < j)) \bmod (n_i + n_j) = n_j - 1 \Leftrightarrow$ [da 4.]
$(n_i x - 1) \bmod (n_i + n_j) = n_j - 1 \Leftrightarrow$ [per la proprietà 2.15]
$n_i x \bmod^\star (n_i + n_j) - 1 = n_j - 1 \Leftrightarrow$
$n_i x \bmod^\star (n_i + n_j) = n_j \Leftrightarrow$ [perché $n_j < n_i + n_j - 1$]
$n_i x \bmod (n_i + n_j) = n_j$

□

Proposizione 7.2. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1, 2\}$, $i \neq j$ e per ogni $x \in \mathbb{N}^\star$:*

$$\mathrm{t}_T(x) \in T[i] \wedge n_i x \bmod (n_i + n_j) = 0 \Rightarrow i > j$$

Dimostrazione.

1. $i > j$ [per assurdo, da 2., 2.–(a) e dalla premessa $\mathrm{t}_T(x) \in T[i]$]
2. Se $i < j$
   (a) $\mathrm{t}_T(x) \notin T[i]$ [da (b), per definizione]
   (b) $\mathrm{DownCons}^{T \to T[i]}(\mathrm{t})(x) =$ [da 2., per il teorema 6.1]
   $((n_i x - 1) \bmod (n_i + n_j) < n_i) =$ [calcoli algebrici; si noti che la scrittura $\frac{n_i x}{n_i + n_j}$ ha senso perché $n_i x \bmod (n_i + n_j) = 0$]
   $\left(\left(\left((n_i + n_j)\left(\frac{n_i x}{n_i + n_j} - 1\right)\right) + n_i + n_j - 1\right) \bmod (n_i + n_j) < n_i\right) =$ [per la proprietà 2.1]
   $((n_i + n_j - 1) \bmod (n_i + n_j) < n_i) =$ [perché $n_i + n_j - 1 < n_i + n_j$]
   $(n_i + n_j - 1 < n_i) =$
   $(n_j < 1) =$
   0

□

Lemma 7.1. $\forall n_1, n_2, x \in \mathbb{N}^\star \, \forall i, j \in \{1, 2\}, i \neq j$:

$$n_i d^{i,j}_{(n_i,n_j)}(x) + n_j - n_j d^{j,i}_{(n_i,n_j)}(x) = \bmod (n_i x, n_i + n_j, (i > j))$$

Dimostrazione.

1. $n_i d^{i,j}_{(n_i,n_j)}(x) + n_j - n_j d^{j,i}_{(n_i,n_j)}(x) = \bmod (n_i x, n_i + n_j, (i > j))$ [da 2., per definizione]
2. $n_i \left\lceil \frac{n_j x + (i<j)}{n_i + n_j} \right\rceil + n_j - n_j \left\lceil \frac{n_i x + (j<i)}{n_i + n_j} \right\rceil = \bmod (n_i x, n_i + n_j, (i > j))$ [da 3., 3.–(a), 3.–(b), 4. e 4.–(a)]

3. Se $i < j$

   (a) $n_j \left\lceil \frac{n_i x+(j<i)}{n_i+n_j} \right\rceil - n_i \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil =$ [da 3.]
   $n_j \left\lceil \frac{n_i x}{n_i+n_j} \right\rceil - n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil =$
   $n_j \left(\frac{n_i x - n_i x \bmod^\star (n_i+n_j)}{n_i+n_j} + 1 \right) - n_i \left(\frac{n_j x+1-(n_j x+1) \bmod^\star (n_i+n_j)}{n_i+n_j} + 1 \right) =$
   $\frac{n_j(n_i x+n_i+n_j-n_i x \bmod^\star (n_i+n_j))-n_i(n_j x+1+n_i+n_j-(n_j x+1) \bmod^\star (n_i+n_j))}{n_i+n_j} =$
   $\frac{n_j(n_i+n_j-n_i x \bmod^\star (n_i+n_j))-n_i(1+n_i+n_j-(n_j x+1) \bmod^\star (n_i+n_j))}{n_i+n_j}$ = [per la proprietà 2.14, con $k = x$]
   $\frac{n_j(n_j x \bmod (n_i+n_j))-n_i(1+n_i+n_j-(n_j x+1) \bmod^\star (n_i+n_j))}{n_i+n_j}$ = [per la proprietà 2.15]
   $\frac{n_j(n_j x \bmod (n_i+n_j))-n_i(1+n_i+n_j-(1+n_j x \bmod (n_i+n_j)))}{n_i+n_j} =$
   $\frac{n_j(n_j x \bmod (n_i+n_j))-n_i(n_i+n_j-n_j x \bmod (n_i+n_j))}{n_i+n_j} =$
   $\frac{(n_i+n_j)(n_j x \bmod (n_i+n_j))-n_i(n_i+n_j)}{n_i+n_j} =$
   $\frac{(n_i+n_j)(n_j x \bmod (n_i+n_j)-n_i)}{n_i+n_j} =$
   $n_j x \bmod (n_i+n_j) - n_i$

   (b) $n_j x \bmod (n_i+n_j) - n_i = n_j - n_i x \bmod^\star (n_i+n_j)$ [da i., per la proprietà 2.14]

      i. $((n_i+n_j)\, x - n_i x) \bmod (n_i+n_j) = n_i + n_j - n_i x \bmod^\star (n_i+n_j)$

4. Se $i > j$ [da 3.–(a), scambiando i e j]

   (a) $n_i \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil - n_j \left\lceil \frac{n_i x+(j<i)}{n_i+n_j} \right\rceil =$
   $n_i x \bmod (n_i+n_j) - n_j$

□

A partire dal lemma 7.1 si può dimostrare il seguente importante teorema:

Teorema 7.1. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1, 2\}$, $i \neq j$, se $t \equiv \mathrm{t}_T(x) \in (n_i)$, il più piccolo trattino di indice j maggiore di t è $\left\langle j, d_T^{j,i}(x) \right\rangle$.*

Dimostrazione.

1. Il più piccolo trattino di indice j maggiore di t è $\left\langle j, d_T^{j,i}(x) \right\rangle$ [da 2.]
2. Il più piccolo trattino di indice j maggiore di t è $\left\langle j, \left\lceil \frac{n_i x+(j<i)}{n_i+n_j} \right\rceil \right\rangle$ [da 4. e 4.–(a), 5. e 5.–(a)]
3. $t = \left\langle i, \left\lceil \frac{n_j x+(i<j)}{n_i+n_j} \right\rceil \right\rangle$ [dall'ipotesi $t \equiv \mathrm{t}_T(x) \in (n_i)$, per il teorema 6.2]
4. Se $i < j$

(a) Il più piccolo trattino di indice n_j maggiore di t è $\left\langle j, \left\lceil \frac{n_i x}{n_i+n_j} \right\rceil \right\rangle$ [da (b) e (c)]

(b) Il più piccolo trattino di indice n_j maggiore di t è il più piccolo trattino di indice n_j di valore maggiore o uguale a $|t|$
[dalla definizione di ordinamento per colonne]

(c) Il più piccolo trattino di indice n_j di valore maggiore o uguale a $|t|$ è $\left\langle j, \left\lceil \frac{n_i x}{n_i+n_j} \right\rceil \right\rangle$ [da (d) ed (e)]

(d) $|t| = n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil$ [da 3. e 4.]

(e) Il più piccolo trattino di indice n_j di valore maggiore o uguale a $n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil$ è $\left\langle j, \left\lceil \frac{n_i x}{n_i+n_j} \right\rceil \right\rangle$ [da (f) e (g)]

(f) Il più piccolo trattino di indice n_j di valore maggiore o uguale a $n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil$ è $\left\langle j, \left\lceil \frac{n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil}{n_j} \right\rceil \right\rangle$ [per il teorema 4.1]

(g) $\left\lceil \frac{n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil}{n_j} \right\rceil =$
$\frac{n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil - n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil \bmod^\star n_j}{n_j} + 1 =$ [da (h)]
$\frac{n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil - n_i x \bmod^\star (n_i+n_j)}{n_j} + 1 =$ [da 4., per il lemma 7.1]
$\frac{n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil - \left(n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil + n_j - n_j \left\lceil \frac{n_i x}{n_i+n_j} \right\rceil \right)}{n_j} + 1 =$
$\frac{n_j \left\lceil \frac{n_i x}{n_i+n_j} \right\rceil - n_j}{n_j} + 1 =$
$\frac{n_j \left(\left\lceil \frac{n_i x}{n_i+n_j} \right\rceil - 1 \right)}{n_j} + 1 =$
$\left\lceil \frac{n_i x}{n_i+n_j} \right\rceil$

(h) $n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil \bmod^\star n_j =$ [per la proprietà 2.15]
$1 + \left(n_i \left\lceil \frac{n_j x+1}{n_i+n_j} \right\rceil - 1 \right) \bmod n_j =$[da 4. e 3., per la proposizione 6.2]
$1 + (n_i x - 1) \bmod (n_i + n_j) =$ [per la proprietà 2.15]
$n_i x \bmod^\star (n_i + n_j)$

5. Se $i > j$

(a) Il più piccolo trattino di indice n_j maggiore di t è $\left\langle j, \left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil \right\rangle$ [da (b) e (c)]

(b) Il più piccolo trattino di indice n_j maggiore di t è il più piccolo trattino di indice n_j di valore maggiore di $|t|$
[dalla definizione di ordinamento per colonne]

(c) Il più piccolo trattino di indice n_j di valore maggiore di $|t|$ è $\left\langle j, \left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil \right\rangle$
[da (d) ed (e)]

(d) $|t| = n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil$ [da 3. e 5.]

(e) Il più piccolo trattino di indice n_j di valore maggiore di $n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil$ è $\left\langle j, \left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil \right\rangle$ [da (f)]

(f) Il più piccolo trattino di indice n_j di valore maggiore o uguale a $n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1$ è $\left\langle j, \left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil \right\rangle$ [da (g) ed (h)]

(g) Il più piccolo trattino di indice n_j di valore maggiore o uguale a $n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1$ è $\left\langle j, \left\lceil \frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1}{n_j} \right\rceil \right\rangle$ [per il teorema 4.1]

(h) $\left\lceil \frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1}{n_j} \right\rceil =$

$$\frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1 - \left(n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1 \right) \bmod^{\star} n_j}{n_j} + 1 = \text{[per la proprietà 2.15]}$$

$$\frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + 1 - \left(n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil \bmod n_j + 1 \right)}{n_j} + 1 =$$

$$\frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil - n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil \bmod n_j}{n_j} + 1 = \text{[da (i)]}$$

$$\frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil - n_i x \bmod (n_i+n_j)}{n_j} + 1 = \text{[per il lemma 7.1]}$$

$$\frac{n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil - \left(n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil + n_j - n_j \left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil \right)}{n_j} + 1 =$$

$$\frac{n_j \left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil - n_j}{n_j} + 1 =$$

$$\frac{n_j \left(\left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil - 1 \right)}{n_j} + 1 =$$

$$\left\lceil \frac{n_i x+1}{n_i+n_j} \right\rceil$$

(i) $n_i x \bmod (n_i + n_j) = n_i \left\lceil \frac{n_j x}{n_i+n_j} \right\rceil \bmod n_j$ [da 5. e 3., per la proposizione 6.2]

□

Si noti che il teorema 7.1 non è molto diverso dal corollario 6.1, che stabilisce, nelle stesse ipotesi di detto teorema, che la differenza tra il valore di $\mathrm{t}_T(x)$ ed il

valore del precedente trattino di T di componente n_j è $\mathrm{mod}\,(n_i x, n_i + n_j, (i > j))$. A partire da questo risultato, infatti, si potrebbe non solo dimostrare il teorema 7.1, ma anche il lemma 7.1.

Un altro aspetto importante da sottolineare è la connessione, alla luce del corollario 6.1, tra il teorema 7.1 ed il lemma 7.1. Quest'ultimo afferma, posto $T \equiv (n_i, n_j)$ e nelle stesse ipotesi del teorema, che

$$n_i d_T^{i,j}(x) + n_j - n_j d_T^{j,i}(x) = \mathrm{mod}\,(n_i x, n_i + n_j, (i > j))$$

che si può riscrivere come

$$\left|\left\langle i, d_T^{i,j}(x)\right\rangle\right| - \left|\left\langle j, d_T^{j,i}(x) - 1\right\rangle\right| = \mathrm{mod}\,(n_i x, n_i + n_j, (i > j))$$

dove $\left\langle i, d_T^{i,j}(x)\right\rangle = \mathrm{t}_T(x)$ per il teorema 6.2 e $\left\langle j, d_T^{j,i}(x) - 1\right\rangle$ è il trattino precedente a $\left\langle j, d_T^{j,i}(x)\right\rangle$, che per il teorema 7.1 è il più piccolo trattino di (n_j) maggiore di $\mathrm{t}_T(x)$. Dunque $\left\langle j, d_T^{j,i}(x) - 1\right\rangle$ è il più grande trattino di (n_j) minore o uguale a $\mathrm{t}_T(x)$, e la differenza di valore tra questo e $\mathrm{t}_T(x)$ è proprio $\mathrm{mod}\,(n_i x, n_i + n_j, (i > j))$, come affermato dal corollario 6.1. Questo è un altro esempio di come un risultato puramente algebrico, come quello del lemma 7.1, può trovare una sua naturale spiegazione nella teoria dei tratteggi.

Seguono due dimostrazioni alternative del teorema 7.1, interessanti per le diverse tecniche utilizzate, precedute entrambe, rispettivamente, da un lemma.

Lemma 7.2. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1, 2\}$, $i \neq j$, e per ogni $x \in \mathbb{N}$:* $|\{t \in (n_i) \mid \langle j, x\rangle < t < \langle j, x+1\rangle\}| \leq \left\lceil \frac{n_j}{n_i} \right\rceil$

Dimostrazione.

1. $|\{t \in (n_i) \mid \langle j, x\rangle < t < \langle j, x+1\rangle\}| =$
   $|\{t \in (n_i) \mid t < \langle j, x+1\rangle \wedge \neg(t \leq \langle j, x\rangle)\}| =$
   $|\{t \in (n_i) \mid t < \langle j, x+1\rangle\} \setminus \{t \in (n_i) \mid t \leq \langle j, x\rangle\}| =$ [perché $\langle n_i, 0\rangle$ appartiene a entrambi gli insiemi]
   $|\{t \in (n_i) \mid \langle i, 0\rangle < t < \langle j, x+1\rangle\} \setminus \{t \in (n_i) \mid \langle i, 0\rangle < t \leq \langle j, x\rangle\}| =$ [perché l'insieme di destra è incluso nell'altro]
   $|\{t \in (n_i) \mid \langle i, 0\rangle < t < \langle j, x+1\rangle\}| - |\{t \in (n_i) \mid \langle i, 0\rangle < t \leq \langle j, x\rangle\}| =$ [da (a) e (b)]
   $\left\lfloor \frac{n_j(x+1) - (j \leq i)}{n_i} \right\rfloor - \left\lfloor \frac{n_j x - (j \leq i)}{n_i} \right\rfloor =$ [per la proprietà 2.22]
   $\left\lceil \frac{n_j - (n_j(x+1) - (j \leq i)) \bmod n_i}{n_i} \right\rceil \leq$ [per monotonia]
   $\left\lceil \frac{n_j}{n_i} \right\rceil$

(a) $|\{t \in (n_i) \mid \langle i, 0\rangle < t < \langle j, x+1\rangle\}| =$ [per la proposizione 4.2]
$\left|\left\{t \in (n_i) \mid \langle i, 0\rangle < t \leq \left\langle n_i, \left\lfloor \frac{|\langle j,x+1\rangle|-(j\leq i)}{n_i} \right\rfloor \right\rangle\right\}\right| =$
$\left|\left\{t \in (n_i) \mid \langle i, 1\rangle \leq t \leq \left\langle n_i, \left\lfloor \frac{|\langle j,x+1\rangle|-(j\leq i)}{n_i} \right\rfloor \right\rangle\right\}\right| =$ [per la proprietà 1.1]
$\left|\left\{k \in \mathbb{N} \mid 1 \leq k \leq \left\lfloor \frac{|\langle j,x+1\rangle|-(j\leq i)}{n_i} \right\rfloor\right\}\right| =$
$\left\lfloor \frac{|\langle j,x+1\rangle|-(j\leq i)}{n_i} \right\rfloor =$ [perché T è lineare]
$\left\lfloor \frac{n_j(x+1)-(j\leq i)}{n_i} \right\rfloor$

(b) $|\{t \in (n_i) \mid \langle i, 0\rangle < t \leq \langle j, x\rangle\}| =$ [perché $\langle j, x\rangle \in (n_j)$ ma $t \in (n_i)$]
$|\{t \in (n_i) \mid \langle i, 0\rangle < t < \langle j, x\rangle\}| =$ [da (a), con x al posto di $x+1$]
$\left\lfloor \frac{n_j x-(j\leq i)}{n_i} \right\rfloor$

□

Segue la prima dimostrazione alternativa del teorema 7.1.

Dimostrazione.

1. Il più piccolo trattino di indice n_j maggiore di t è $\left\langle j, d_T^{j,i}(x)\right\rangle$ [da 2. e 3.]

2. Sia $\mathrm{t}_T(y)$ il più grande trattino di indice j minore di t

   (a) $\mathrm{t}_T(y) = \left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil \right\rangle$ [da 2., per il teorema 6.2]

   (b) $y < x$ [da i., per la definizione di t_T]

      i. $\mathrm{t}_T(y) < \mathrm{t}_T(x)$ [da 2., perché si è posto $\mathrm{t}_T(x) \equiv t$]

   (c) $\mathrm{DownCons}^{T\to T[j]}(\mathrm{t})(y) = 1$ [da 2.]

3. $t <$ [da (a)]
   $\mathrm{t}_T(y+1) =$ [da 2.–(a)]
   $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle =$ [da (b), per la proprietà 2.23]
   $\left\langle j, \left\lceil \frac{n_i x+(j<i)}{n_i+n_j} \right\rceil \right\rangle =$
   $\left\langle j, d_T^{j,i}(x)\right\rangle$

   (a) $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle$ è il più piccolo trattino di indice j maggiore di t [da i.]

      i. $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil \right\rangle <$ [da 2. e 2.–(a)]
      $t <$ [da ii. e 2., per contrapposizione]
      $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle$

ii. $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle \leq t \Rightarrow$ [perché $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle \neq t$, perché $t \in (n_i)$ e $n_j \neq n_i$]
$\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle < t \Rightarrow$ [perché $\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil \right\rangle < \left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right\rangle$]
$\left\langle j, \left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil \right\rangle$ non è il più grande trattino di indice j minore di $t \Rightarrow$ [da 2.–(a)]
$\mathrm{t}_T(y)$ non è il più grande trattino di indice j minore di t

(b) $(n_i+n_j)\left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil < n_i x + (j<i) \leq (n_i+n_j)\left(\left\lceil \frac{n_i y+(j<i)}{n_i+n_j} \right\rceil + 1 \right)$ [da i., per definizione]

i. $(n_i+n_j)\left(\frac{n_i y+(j<i)-(n_i y+(j<i)) \bmod^\star (n_i+n_j)}{n_i+n_j} + 1 \right) < n_i x + (j<i) \leq$
$< (n_i+n_j)\left(\frac{n_i y+(j<i)-(n_i y+(j<i)) \bmod^\star (n_i+n_j)}{n_i+n_j} + 2 \right)$ [da ii., calcoli algebrici]

ii. $n_i y + (j<i) - (n_i y + (j<i)) \bmod^\star (n_i+n_j) + n_i + n_j < n_i x + (j<i) \leq$
$\leq n_i y + (j<i) - (n_i y + (j<i)) \bmod^\star (n_i+n_j) + 2(n_i+n_j)$ [da iii., calcoli algebrici]

iii. $n_i + n_j - (n_i y + (j<i)) \bmod^\star (n_i+n_j) < n_i(x-y) \leq 2(n_i+n_j) - (n_i y + (j<i)) \bmod^\star (n_i+n_j)$ [da iv. e v.]

iv. $n_i + n_j - (n_i y + (j<i)) \bmod^\star (n_i+n_j) =$ [per la proprietà 2.14]
$((n_i+n_j)y - (n_i y + (j<i))) \bmod (n_i+n_j) =$
$(n_j y - (j<i)) \bmod (n_i+n_j) <$ [da 2.–(c), per il teorema 6.1]
$n_i \leq$ [da 2.–(b)]
$n_i(x-y)$

v. $n_i(x-y) \leq$
$n_i \left\lceil \frac{n_j}{n_i} \right\rceil =$
$n_i \left(\frac{n_j - n_j \bmod^\star n_i}{n_i} + 1 \right) =$
$n_i + n_j - n_j \bmod^\star n_i \leq$ [perché $n_j \bmod^\star n_i \geq 0$]
$n_i + n_j \leq$ [perché $(n_i y + (j<i)) \bmod^\star (n_i+n_j) \leq n_i + n_j$]
$n_i + n_j + (n_i + n_j - (n_i y + (j<i)) \bmod^\star (n_i+n_j)) =$
$2(n_i+n_j) - (n_i y + (j<i)) \bmod^\star (n_i+n_j)$

□

Ora la terza ed ultima dimostrazione, anch'essa preceduta da un lemma.

Lemma 7.3. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$. Per ogni $i, j \in \{1,2\}$, $i \neq j$, se $t \in (n_i)$, il più piccolo trattino di indice j maggiore di t è l'unico trattino di indice j di valore compreso tra $|t| + 1 - (i<j)$ e $|t| + n_j - (i<j)$.*

Dimostrazione.

1. Esiste uno e un solo trattino di (n_j) con valore in $[|t|+1-(i<j), |t|+n_j-(i<j)]$ [da (a), per l'osservazione 1.1]

   (a) $[|t|+1-(i<j), |t|+n_j-(i<j)]$ è un dominio fondamentale di (n_j) [perché ha lunghezza n_j che è pari alla lunghezza dei domini fondamentali di (n_j), per la proposizione 4.8]

2. Sia $u \equiv \langle j, k\rangle$ il trattino di indice j con valore in $[|t|+1-(i<j), |t|+n_j-(i<j)]$ [da 1.]

3. u è il più piccolo trattino di indice j maggiore di t [da (a), (b) e (b)–i.]

   (a) $u > t$ [da i., ii., ii.–A., iii., iii.–A.]

      i. $u > t \Leftrightarrow$
      $t < u \Leftrightarrow$ [da $i \neq j$, per la proprietà 1.2]
      $|t| < |u| \vee (|t| = |u| \wedge i < j)$

      ii. Se $i > j$

         A. $|u| \geq$
         $|t|+1-(i<j) =$
         $|t|+1 >$
         $|t|$

      iii. Se $i < j$

         A. $|u| \geq$
         $|t|+1-(i<j) =$
         $|t|+1-1 =$
         $|t|$

   (b) Sia $v \in (n_j)$, $v < u$

      i. $v < t$ [da ii., iii., iii.–A., iv., iv.–A.]

      ii. $v < t \Leftrightarrow$ [da $i \neq j$, per la proprietà 1.2]
      $|v| < |t| \vee (|v| = |t| \wedge j < i)$

      iii. Se $i < j$

         A. $|v| < |t|$ [da iii. e v.]

      iv. Se $i > j$

         A. $|v| < |t|+1$ [da iv. e v.]

      v. $|v| < |t|+1-(i<j)$ [da 1., 2. e (b)]

□

Segue la seconda dimostrazione alternativa del teorema 7.1.

Dimostrazione. 1. Il più piccolo trattino di indice j maggiore di t è $\left\langle j, d_T^{j,i}(x)\right\rangle$ [da 2., per il lemma 7.3]

2. $\left\langle j, d_T^{j,i}(x)\right\rangle$ ha valore compreso tra $|t|+1-(i<j)$ e $|t|+n_j-(i<j)$ [da 3., scrivendo a parole]

3. $|t|+1-(i<j) \leq \left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| \leq |t|+n_j-(i<j)$ [da 4., sommando $|t|$ a tutti i membri]

4. $1-(i<j) \leq \left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - |t| \leq n_j-(i<j)$ [da 5., 5.–(a) e 6.–(a)]

5. Se $i<j$

   (a) $0 \leq \left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - |t| \leq n_j - 1$ [da (b) e (c)]

   (b) $\left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - |t| =$ [da $t = \mathrm{t}_T(x) \in (n_i)$, per il teorema 6.2]
   $\left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - \left|\left\langle i, d_T^{i,j}(x)\right\rangle\right| =$ [perché T è lineare]
   $n_j d_T^{j,i}(x) - n_i d_T^{i,j}(x) =$ [da 5., per il lemma 7.1]
   $n_j x \bmod (n_i+n_j) - n_i$

   (c) $0 \leq n_j x \bmod (n_i+n_j) - n_i \leq n_j - 1$ [da i. ed ii.]

      i. $n_j x \bmod (n_i+n_j) \geq n_i$ [da 5., per il teorema 6.1]

      ii. $n_j x \bmod (n_i+n_j) \leq n_i + n_j - 1$

6. Se $j<i$

   (a) $1 \leq \left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - |t| \leq n_j$ [da (b) e (c)]

   (b) $\left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - |t| =$ [da $t = \mathrm{t}_T(x) \in (n_i)$, per il teorema 6.2]
   $\left|\left\langle j, d_T^{j,i}(x)\right\rangle\right| - \left|\left\langle i, d_T^{i,j}(x)\right\rangle\right| =$ [perché T è lineare]
   $n_j d_T^{j,i}(x) - n_i d_T^{i,j}(x) =$ [da 6., per il lemma 7.1]
   $n_j - n_i x \bmod (n_i+n_j)$

   (c) $1 \leq n_j - n_i x \bmod (n_i+n_j) \leq n_j$ [da i. ed ii.]

      i. $n_i x \bmod (n_i+n_j) \leq n_j - 1$ [da A.]

         A. $n_i x \bmod (n_i+n_j) < n_j$ [da 6., per il teorema 6.1]

      ii. $n_i x \bmod (n_i+n_j) \geq 0$

□

Sostituendo nel teorema 7.1 l'affermazione "il più piccolo trattino di indice j maggiore di t" con la più debole "un trattino di indice j maggiore di t" e riformulando il tutto, si ottiene il seguente corollario:

Corollario 7.1. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$. *Per ogni* $i, j \in \{1, 2\}$, $i \neq j$, *se* $t \equiv \mathrm{t}_T(x) \in (n_i)$, $t < \langle j, d_T^{j,i}(x) \rangle$.

7.2 Calcolo di t senza verifica della down-conservatività

Dal teorema 7.1 si ricava il seguente modo di calcolare t_T senza preoccuparsi della down-conservatività:

Corollario 7.2. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$. $\mathrm{t}_T(x) = \min\left\{\langle 1, d_T^{1,2}(x)\rangle, \langle 2, d_T^{2,1}(x)\rangle\right\}$.

Dimostrazione.

1. $\mathrm{t}_T(x) = \min\left\{\langle 1, d_T^{1,2}(x)\rangle, \langle 2, d_T^{2,1}(x)\rangle\right\}$ [da 2. e 2.–(a), perché i è generico]

2. Sia $\mathrm{t}_T(x) \in T[i]$, $i \in \{1, 2\}$. Sia $j = \begin{cases} 1 & \text{se } i = 2 \\ 2 & \text{se } i = 1 \end{cases}$

   (a) $\mathrm{t}_T(x) = \min\left\{\langle 1, d_T^{1,2}(x)\rangle, \langle 2, d_T^{2,1}(x)\rangle\right\}$ [da (b) e (c)]

   (b) $\left\{\langle i, d_T^{i,j}(x)\rangle, \langle j, d_T^{j,i}(x)\rangle\right\} = \left\{\langle 1, d_T^{1,2}(x)\rangle, \langle 2, d_T^{2,1}(x)\rangle\right\}$ [da 2.]

   (c) $\mathrm{t}_T(x) = \min\left\{\langle i, d_T^{i,j}(x)\rangle, \langle j, d_T^{j,i}(x)\rangle\right\}$ [da (d) ed (e)]

   (d) $\langle i, d_T^{i,j}(x)\rangle = \min\left\{\langle i, d_T^{i,j}(x)\rangle, \langle j, d_T^{j,i}(x)\rangle\right\}$ [da (f)]

   (e) $\mathrm{t}_T(x) = \langle i, d_T^{i,j}(x)\rangle$ [da 2., per il teorema 6.2]

   (f) $\langle i, d_T^{i,j}(x)\rangle < \langle j, d_T^{j,i}(x)\rangle$ [da (e), per il corollario 7.1]

□

La differenza tra il calcolo di $\mathrm{t}_T(x)$ col corollario 7.2, rispetto al calcolo dello stesso con i teoremi 6.1 e 6.2, è notevole, in quanto nel secondo caso si deve prima calcolare se $\mathrm{t}_T(x)$ appartiene a $T[1]$ o $T[2]$ e solo in seguito si può trovare effettivamente $\mathrm{t}_T(x)$; col corollario 7.2 invece in un unico passaggio si ottiene sia $\mathrm{t}_T(x)$ che, ovviamente, il sottotratteggio di primo ordine a cui esso appartiene (ovviamente, perché lo si ottiene immediatamente dall'indice del trattino).

7.2.1 Esempio di calcolo dell'x-esimo trattino

Nel paragrafo 6.4.1 abbiamo calcolato $\mathrm{t}_{T_1}(4)$, con $T_1 \equiv (n_1, n_2) \equiv (3, 4)$, applicando i teoremi 6.1 e 6.2. Ora ripetiamo lo stesso esempio, ma applicando il corollario 7.2:

$$\begin{aligned}
\mathrm{t}_T(x) &= \min\left\{\left\langle 1, d_{T_1}^{1,2}(x)\right\rangle, \left\langle 2, d_{T_1}^{2,1}(x)\right\rangle\right\} \\
&= \min\left\{\left\langle 1, \left\lceil \frac{n_2 x + (1<2)}{n_1+n_2} \right\rceil \right\rangle, \left\langle 2, \left\lceil \frac{n_1 x + (2<1)}{n_1+n_2} \right\rceil \right\rangle\right\} \\
&= \min\left\{\left\langle 1, \left\lceil \frac{n_2 x + 1}{n_1+n_2} \right\rceil \right\rangle, \left\langle 2, \left\lceil \frac{n_1 x}{n_1+n_2} \right\rceil \right\rangle\right\} \\
&= \min\left\{\left\langle 1, \left\lceil \frac{4x+1}{7} \right\rceil \right\rangle, \left\langle 2, \left\lceil \frac{3x}{7} \right\rceil \right\rangle\right\} \\
&= \min\left\{\left\langle 1, \left\lceil \frac{17}{7} \right\rceil \right\rangle, \left\langle 2, \left\lceil \frac{12}{7} \right\rceil \right\rangle\right\} \\
&= \min\left\{\langle 1, 3\rangle, \langle 2, 2\rangle\right\} \\
&= \langle 2, 2\rangle
\end{aligned}$$

dove $\min\left\{\langle 1, 3\rangle, \langle 2, 2\rangle\right\} = \langle 2, 2\rangle$ perché $|\langle 2, 2\rangle| = 4 \cdot 2 = 8 < 9 = 3 \cdot 3 = |\langle 1, 3\rangle|$ e per la proprietà 1.2.

Capitolo 8

t_spazio **lineare**

In questo capitolo affrontiamo il calcolo della funzione t_spazio in $\mathcal{L}^1$ ed $\mathcal{L}^2$. Premessa fondamentale è stabilire qual è la condizione per la quale un tratteggio lineare ha spazi:

Proprietà 8.1. *Sia $T \equiv (n_1, \ldots, n_d) \in \mathcal{L}^d$. Se $\forall i \in \{1, \ldots, d\} : n_i > 1$, allora T ha infiniti spazi; altrimenti, T non ha spazi.*

Dimostrazione.

1. Se $\forall i \in \{1, \ldots, d\} : n_i > 1$
   (a) T ha infiniti spazi [da (b) e (c), per la proprietà 3.14]
   (b) 1 è uno spazio di T [da i., per la proprietà 3.15]
      i. $\forall i \in \{1, \ldots, d\} : 1 \bmod n_i = 1$
   (c) T è priodico [per la proposizione 4.8]
2. Se $\exists i \in \{1, \ldots, d\} : n_i = 1$
   (a) T non ha spazi [da (b) e (c)]
   (b) Sia $n \in \mathbb{N}$
   (c) n non è uno spazio
      i. $T(\langle i, n \rangle) =$
      $n_i n =$ [da 2.]
      n

□

0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
-	-	-	-	-	-	-	-	-	-	-	-	-	-	...

Figura 8.1: I tratteggi lineari privi di spazi hanno (1) come sottotratteggio

Se un tratteggio lineare non ha spazi, dunque, è necessario che almeno una delle due componenti sia 1, generando un sottotratteggio di primo ordine come quello nella Figura 8.1, che chiaramente impedisce all'intero tratteggio di avere spazi. Se invece nessuna delle componenti è 1, allora, come chiarito nella dimostrazione, almeno il numero 1 è uno spazio del tratteggio, che quindi, essendo periodico, ha infiniti spazi.

8.1 t_spazio lineare di primo ordine

Proposizione 8.1. *Sia $T \equiv (n_1) \in \mathcal{L}^1$ avente spazi. Allora per ogni $x \in \mathbb{N}^\star$:*

$$n = \text{t\_spazio}_T(x) \Leftrightarrow \begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n - x = \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases} \Leftrightarrow \begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n \bmod n_1 \neq 0 \end{cases}$$

Dimostrazione.

1. $n = \text{t\_spazio}_T(x) \Leftrightarrow$ [per il lemma del conteggio (lemma 3.1)]
$$\begin{cases} |\{y \in \{1,\dots,n\} \mid y \text{ è uno spazio di } T\}| = x \\ |\{y \in \{1,\dots,n-1\} \mid y \text{ è uno spazio di } T\}| = x - 1 \end{cases} \Leftrightarrow$$
$$\begin{cases} |\{y \in \{1,\dots,n\} \mid y \text{ è uno spazio di } T\}| + \\ +|\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } T\}| = \\ x + |\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } T\}| \\ |\{y \in \{1,\dots,n-1\} \mid y \text{ è uno spazio di } T\}| + \\ +|\{y \in \{1,\dots,n-1\} \mid y \text{ non è uno spazio di } T\}| = \\ x - 1 + |\{y \in \{1,\dots,n-1\} \mid y \text{ non è uno spazio di } T\}| \end{cases} \Leftrightarrow$$
$$\begin{cases} n = x + |\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } T\}| \\ n - 1 = x - 1 + |\{y \in \{1,\dots,n-1\} \mid y \text{ non è uno spazio di } T\}| \end{cases} \Leftrightarrow$$ [per il corollario 4.2]
$$\begin{cases} n = x + \left\lfloor \frac{n}{n_1} \right\rfloor \\ n - 1 = x - 1 + \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases} \Leftrightarrow$$
$$\begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n - x = \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases}$$

2. $\begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n - x = \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases} \Leftrightarrow$
$\begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ \left\lfloor \frac{n}{n_1} \right\rfloor = \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases} \Leftrightarrow$ [da (a)]
$\begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n \bmod n_1 \neq 0 \end{cases}$

   (a) $\left\lfloor \frac{n}{n_1} \right\rfloor = \left\lfloor \frac{n-1}{n_1} \right\rfloor \Leftrightarrow$ [per la proprietà 2.21]
   $((n-1) \bmod n_1 = n_1 - 1) = 0 \Leftrightarrow$
   $(n-1) \bmod n_1 \neq n_1 - 1 \Leftrightarrow$ [per la proprietà 2.15]
   $n \bmod^\star n_1 - 1 \neq n_1 - 1 \Leftrightarrow$
   $n \bmod^\star n_1 \neq n_1 \Leftrightarrow$ [per definizione di $\bmod^\star$]
   $n \bmod n_1 \neq 0$

□

Si noti che è possibile dimostrare in modo molto diretto la seconda equivalenza della proposizione 8.1, sfruttando la seconda forma del lemma del conteggio:

Dimostrazione.

1. $n = \text{t\_spazio}_T(x) \Leftrightarrow$ [per il lemma del conteggio, seconda forma (lemma 3.2)]
$\begin{cases} |\{y \in \{1, \ldots, n\} \mid y \text{ è uno spazio di } T\}| = x \\ n \text{ è uno spazio di } T \end{cases} \Leftrightarrow$ [per la proposizione 3.15]
$\begin{cases} |\{y \in \{1, \ldots, n\} \mid y \text{ è uno spazio di } T\}| = x \\ n \bmod n_1 \neq 0 \end{cases} \Leftrightarrow$
$\begin{cases} |\{y \in \{1, \ldots, n\} \mid y \text{ è uno spazio di } T\}| + \\ + |\{y \in \{1, \ldots, n\} \mid y \text{ non è uno spazio di } T\}| = \\ x + |\{y \in \{1, \ldots, n\} \mid y \text{ non è uno spazio di } T\}| \\ n \bmod n_1 \neq 0 \end{cases} \Leftrightarrow$
$\begin{cases} n = x + |\{y \in \{1, \ldots, n\} \mid y \text{ non è uno spazio di } T\}| \\ n \bmod n_1 \neq 0 \end{cases} \Leftrightarrow$ [per il corollario 4.2]
$\begin{cases} n = x + \left\lfloor \frac{n}{n_1} \right\rfloor \\ n \bmod n_1 \neq 0 \end{cases}$

□

Nello studio degli ordini superiori al primo, generalizzeremo la forma:

$$\begin{cases} n = x + \left\lfloor \frac{n}{n_1} \right\rfloor \\ n \bmod n_1 \neq 0 \end{cases} \tag{8.1}$$

più concisa dell'equivalente $\begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n - x = \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases}$. Chiameremo il sistema 8.1 *sistema caratteristico* di t_spazio lineare di primo ordine, perché risolvendolo rispetto ad n, per la proposizione 8.1, possiamo calcolare t_spazio in $\mathcal{L}^1$. La formula è data dal seguente teorema:

Teorema 8.1. *Sia $T \equiv (n_1) \in \mathcal{L}^1$ avente spazi. Allora per ogni $x \in \mathbb{N}^\star$:*

$$\text{t\_spazio}_T(x) = \left\lfloor \frac{n_1 x - 1}{n_1 - 1} \right\rfloor$$

Dimostrazione.

1. $\text{t\_spazio}_T(x) = \left\lfloor \frac{n_1 x - 1}{n_1 - 1} \right\rfloor$ [da 2.]
2. $n = \text{t\_spazio}_T(x) \Leftrightarrow$ [per la proposizione 8.1]
   $\begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor \\ n - x = \left\lfloor \frac{n-1}{n_1} \right\rfloor \end{cases} \Leftrightarrow$ [per la proprietà 2.23]
   $\begin{cases} n_1 (n - x) \leq n < n_1 (n - x + 1) \\ n_1 (n - x) \leq n - 1 < n_1 (n - x + 1) \end{cases} \Leftrightarrow$ [aggiunta di $n_1 x$ a tutti i membri)
   $\begin{cases} n_1 n \leq n + n_1 x < n_1 (n + 1) \\ n_1 n \leq n - 1 + n_1 x < n_1 (n + 1) \end{cases} \Leftrightarrow$ [sottrazione di $n + 1$ nella prima equazione e di n nella seconda]
   $\begin{cases} n_1 n - (n + 1) \leq n_1 x - 1 < n_1 (n + 1) - (n + 1) \\ n_1 n - n \leq n_1 x - 1 < n_1 (n + 1) - n \end{cases} \Leftrightarrow$
   $\begin{cases} (n_1 - 1) n + 1 \leq n_1 x - 1 < (n_1 - 1)(n + 1) \\ (n_1 - 1) n \leq n_1 x - 1 < (n_1 - 1)(n + 1) - 1 \end{cases} \Leftrightarrow$
   $\min\{(n_1 - 1) n, (n_1 - 1) n + 1\} \leq n_1 x - 1 < \max\{(n_1 - 1)(n + 1) - 1, (n_1 - 1)(n + 1)\} \Leftrightarrow$
   $(n_1 - 1) n \leq n_1 x - 1 < (n_1 - 1)(n + 1) \Leftrightarrow$ [per la proprietà 2.23]
   $n = \left\lfloor \frac{n_1 x - 1}{n_1 - 1} \right\rfloor$

□

Nonostante i tecnicismi della precedente dimostrazione, la formula ha un elevato grado di interpretabilità. Possiamo innanzitutto riscroverla come nel seguente corollario:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
-				-				-				-		...

Figura 8.2: Tratteggio (4)

Corollario 8.1. *Sia* $T \equiv (n_1) \in \mathcal{L}^1$ *avente spazi. Allora per ogni* $x \in \mathbb{N}^\star$*:*

$$\text{t\_spazio}_T(x) = x + \left\lfloor \frac{x-1}{n_1-1} \right\rfloor$$

Dimostrazione.

1. $\text{t\_spazio}_T(x) =$ [per il teorema 8.1]
   $\left\lfloor \frac{n_1 x - 1}{n_1 - 1} \right\rfloor =$
   $\left\lfloor \frac{(n_1-1)x + x - 1}{n_1 - 1} \right\rfloor =$ [per la proprietà 2.19]
   $x + \left\lfloor \frac{x-1}{n_1-1} \right\rfloor$

□

Esprimere $\text{t\_spazio}_T(x)$ come $x + f(x)$, per qualche f funzione di x, significa che nell'intervallo $[1, \text{t\_spazio}_T(x)]$ ci sono, oltre agli x spazi richiesti, $f(x)$ numeri che non sono spazi. Aiutandosi con una tabella, è possibile comprendere perché $f(x) = \left\lfloor \frac{x-1}{n_1-1} \right\rfloor$. Consideriamo per esempio il tratteggio (4) mostrato in Figura 8.2. Se prendiamo qualsiasi spazio $n \in \mathbb{N}^\star$, vediamo che gli spazi minori o uguali ad n si susseguono raggruppati in intervalli di $3 = 4 - 1 = n_1 - 1$ spazi consecutivi, separati da un non-spazio. Quindi è possibile contare i non-spazi precedenti n, cioè calcolare la $f(x)$ precedente, contando quanti intervalli di 3 spazi precedono n, ponendo che n sia l'x-esimo spazio. Per esempio, se $n = 10 = \text{t\_spazio}_{(4)}(8)$, esistono due intervalli di tre spazi che precedono n, $[1, 3]$ e $[5, 7]$ (va escluso l'intervallo $[9, 11]$, che include n). La formula $\left\lfloor \frac{x-1}{3} \right\rfloor = \left\lfloor \frac{x-1}{n_1-1} \right\rfloor$ calcola proprio quanti intervalli di 3 spazi precedono l'x-esimo spazio. Per $n = 10$, ad esempio, si ha $\left\lfloor \frac{8-1}{3} \right\rfloor = 2$ (8 perché 10 è l'ottavo spazio di (4)). Queste idee potrebbero condurre ad una dimostrazione alternativa del teorema 8.1, ma formalizzarle sarebbe più complicato della dimostrazione fornita; ciononostante, esse costituiscono senz'altro uno dei concetti fondamentali su t_spazio in $\mathcal{L}^1$.

Proposizione 8.2. *Sia* $T \equiv (n_1) \in \mathcal{L}^1$ *avente spazi. Allora per ogni* $x \in \mathbb{N}^\star$*:*

$$\text{t\_spazio}^{-1}{}_T(x) = x - \left\lfloor \frac{x}{n_1} \right\rfloor$$

Dimostrazione.

1. $\text{t\_spazio}^{-1}{}_T(x) =$[per l'osservazione 1.3]
   $|\{s \in [1,x] \mid s \text{ è uno spazio di } T\}| =$ [per il corollario 3.1]
   $x - |\{|c|_T \in [1,x] \mid c \text{ è una classe di } T\}| =$ [per la proprietà 3.6]
   $x - |\{|t|_T \in [1,x] \mid t \text{ è un trattino di } T\}| =$ [per il corollario 4.2]
   $x - \left\lfloor \frac{x}{n_1} \right\rfloor$

□

La proposizione può essere dimostrata anche per via puramente algebrica, partendo dal teorema 8.1 e sfruttando la proprietà 2.26, ma la dimostrazione sarebbe molto più complicata e noiosa di quella fornita, perciò la omettiamo.

Corollario 8.2. *Siano $T \equiv (n_1) \in \mathcal{L}^1$ avente spazi, $x \in \mathbb{N}^\star$ e $n = \text{t\_spazio}_T(x)$. Siano $S \equiv \{s \in [1,n] \mid s \text{ è uno spazio di } T\}$ e $V \equiv \{v \in [1,n] \mid v \text{ non è uno spazio di } T\}$. Siano inoltre $T' \equiv (n_1 - 1) \in \mathcal{L}^1$ e $V' \equiv \{v \in [1, x-1] \mid v \text{ non è uno spazio di } T'\}$. Allora la funzione $\lambda x : x - \left\lfloor \frac{x}{n_1} \right\rfloor$ è una corrispondenza biunivoca tra S e $[1,x]$ e tra V e V'.*

Dimostrazione.

1. $f : S \to \mathbb{Z}$ tale che $\forall x \in S : f(x) = x - \left\lfloor \frac{x}{n_1} \right\rfloor$ è una corrispondenza biunivoca tra S e $[1,x]$ [da (a) e (b)]

   (a) f è iniettiva [da i. e iv.]

   i. Siano $s, s' \in S$, $s < s'$

   ii. Sia $s = \text{t\_spazio}_T(a)$ e $s' = \text{t\_spazio}_T(b)$ [lecito, perché s ed s' sono spazi di T]

   iii. $a < b$ [da $s < s'$ e perché t_spazio_T è strettamente crescente]

   iv. $f(s) =$ [da (c)]
   $\text{t\_spazio}^{-1}{}_T(s) =$ [da ii.]
   $\text{t\_spazio}^{-1}{}_T(\text{t\_spazio}_T(a)) =$ [per l'osservazione 1.3]
   $a <$ [da iii.]
   $b =$ [per l'osservazione 1.3]
   $\text{t\_spazio}^{-1}{}_T(\text{t\_spazio}_T(b)) =$ [da ii.]
   $\text{t\_spazio}^{-1}{}_T(s') =$ [da (c)]
   $f(s')$

   (b) f è suriettiva [da i., iii. e iv.]

   i. Sia $y \in [1,x]$

   ii. Sia $s \equiv \text{t\_spazio}_T(y)$

iii. $s \in S$ [da A., B. e C.]

A. $s \geq 1$ [da C. (ricordando che $\mathcal{O}_T = 0$ non è uno spazio)]

B. $s \leq$ [da i. e ii., perché $y \leq x \Rightarrow \text{t\_spazio}_T(y) \leq \text{t\_spazio}_T(x)$]
$\text{t\_spazio}_T(x) =$ [per ipotesi]
n

C. s è uno spazio di T [da ii.]

iv. $f(s) =$ [da (c)]
$\text{t\_spazio}^{-1}{}_T(s) =$ [da ii.]
$\text{t\_spazio}^{-1}{}_T(\text{t\_spazio}_T(y)) =$ [per l'osservazione 1.3]
y

(c) $\forall x \in S : f(x) = \text{t\_spazio}^{-1}{}_T(x)$ [da 1., per la proposizione 8.2]

2. $g : V \to \mathbb{Z}$ tale che $\forall x \in V : f(x) = x - \left\lfloor \frac{x}{n_1} \right\rfloor$ è una corrispondenza biunivoca tra V e V' [da (a) e (b)]

(a) g è iniettiva [da i. e iii.]

i. Siano $v, v' \in V$, $v < v'$

ii. Sia $v = n_1 a$ e $v' = n_1 b$, con $a, b \in \mathbb{N}^\star$ [da i., per definizione di V]

iii. $f(v) =$ [da ii.]
$f(n_1 a) =$ [da 2.]
$n_1 a - \left\lfloor \frac{n_1 a}{n_1} \right\rfloor =$
$n_1 a - a =$
$(n_1 - 1)\, a <$ [da ii. e i. (in particolare, $v < v'$)]
$(n_1 - 1)\, b =$
$n_1 b - b =$
$n_1 b - \left\lfloor \frac{n_1 a}{n_1} \right\rfloor =$ [da 2.]
$f(n_1 b) =$ [da ii.]
$f(v')$

(b) g è suriettiva

i. Sia $v \in V'$

ii. Sia $v = (n_1 - 1)\, a$, con $a \in \mathbb{N}^\star$ [lecito per i. e per definizione di V']

iii. $n_1 a \in V$ [perché $n_1 a$ non è uno spazio di T e per A.]

A. $n_1 a \leq n$ [da B. e C.]

B. $n_1 a > n \Rightarrow \text{t\_spazio}^{-1}{}_T(n_1 a) \geq \text{t\_spazio}^{-1}{}_T(n)$ [per l'osservazione 1.3]

C. $\text{t\_spazio}^{-1}{}_T(n_1 a) =$ [da (c)]
$g(n_1 a) =$ [da iv.]
$(n_1 - 1)\, a <$ [da ii.]
$x =$ [per l'osservazione 1.3]
$\text{t\_spazio}^{-1}{}_T(\text{t\_spazio}_T(x)) =$ [per ipotesi, $\text{t\_spazio}_T(x) = n$]
$\text{t\_spazio}^{-1}{}_T(n)$

iv. $g(n_1 a) =$ [da 2.]
$n_1 a - \left\lfloor \frac{n_1 a}{n_1} \right\rfloor =$
$n_1 a - a =$
$(n_1 - 1)\, a =$ [da ii.]
v

(c) $\forall x \in S : g(x) = \text{t\_spazio}^{-1}{}_T(x)$

□

L'aspetto interessante di questo corollario è che è stato ricavato in modo semplice a partire dalla proposizione 8.2, la quale a sua volta ha una dimostrazione molto intuitiva, mentre sarebbe complicato dimostrarlo direttamente per via algebrica: provare per credere! Ciò mostra come, nella teoria dei tratteggi, poche semplici intuizioni e pochi concetti possono evitare moltissimi passaggi algebrici.

8.2 t_spazio lineare di secondo ordine

Anche nel secondo ordine possiamo legare im modo piuttosto semplice il calcolo di t_spazio alla soluzione di un sistema, come stabilito dalla seguente proposizione:

Proposizione 8.3. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$ avente spazi. Allora per ogni $x \in \mathbb{N}^\star$:*

$$n = \text{t\_spazio}_T(x) \Leftrightarrow \begin{cases} n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{\text{MCM}(n_1,n_2)} \right\rfloor \\ n \bmod n_1 \neq 0 \\ n \bmod n_2 \neq 0 \end{cases}$$

Dimostrazione.

1. $n = \text{t\_spazio}_T(x) \Leftrightarrow$ [per il lemma del conteggio, seconda forma (lemma 3.2)]
$\begin{cases} |\{y \in \{1, \ldots, n\} \mid y \text{ è uno spazio di } T\}| = x \\ n \text{ è uno spazio di } T \end{cases}$ $\Leftrightarrow$ [per la proposizione 3.15]

$$
\begin{cases}
\quad |\{y \in \{1,\dots,n\} \mid y \text{ è uno spazio di } T\}| + \\
\quad + |\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } T\}| = \\
\quad x + |\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } T\}| \quad \Leftrightarrow \\
n \bmod n_1 \neq 0 \\
n \bmod n_2 \neq 0
\end{cases}
$$

$$
\begin{cases}
n = x + |\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } T\}| \\
n \bmod n_1 \neq 0 \qquad \Leftrightarrow \text{[per definizione di} \\
n \bmod n_2 \neq 0
\end{cases}
$$

spazio e di classe]

$$
\begin{cases}
n = x + |\{y \in \{1,\dots,n\} \mid y \text{ è una classe di } T\}| \\
n \bmod n_1 \neq 0 \qquad \Leftrightarrow \text{[per la proposizione 4.6]} \\
n \bmod n_2 \neq 0
\end{cases}
$$

$$
\begin{cases}
n = x + \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{\text{MCM}(n_1,n_2)} \right\rfloor \\
n \bmod n_1 \neq 0 \qquad \Leftrightarrow \\
n \bmod n_2 \neq 0
\end{cases}
$$

$$
\begin{cases}
n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{\text{MCM}(n_1,n_2)} \right\rfloor \\
n \bmod n_1 \neq 0 \\
n \bmod n_2 \neq 0
\end{cases}
$$

□

La proposizione 8.3 afferma in pratica che per calcolare $\text{t\_spazio}_T(x)$ nel secondo ordine occorre risolvere il seguente *sistema caratteristico*, nell'incognita n:

$$
\begin{cases}
n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{\text{MCM}(n_1,n_2)} \right\rfloor \\
n \bmod n_1 \neq 0 \\
n \bmod n_2 \neq 0
\end{cases} \tag{8.2}
$$

Le pagine seguenti sono dedicate alla soluzione di questo sistema. Il termine $\left\lfloor \frac{n}{\text{MCM}(n_1,n_2)} \right\rfloor$ complica notevolmente il problema; perciò l'approccio che seguiremo sarà quello di risolvere il seguente sistema più semplice:

$$
\begin{cases}
n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor \\
n \bmod n_1 \neq 0 \\
n \bmod n_2 \neq 0
\end{cases} \tag{8.3}
$$

Una volta risolto quest'ultimo, otterremo anche la soluzione del sistema 8.3. Il metodo risolutivo nel complesso è abbastanza articolato e sembra difficilmente generalizzabile per ordini superiori al secondo, in quanto le generalizzazioni del sistema

caratteristico 8.3 conterranno, per via del principio di inclusione-esclusione, molti termini del tipo $\left\lfloor \frac{n}{\mathrm{MCM}(n_{i_1},\ldots,n_{i_k})} \right\rfloor$ (più precisamente, il numero di tali termini è $2^{d-1}-1$, se d è l'ordine del tratteggio T di cui si vuole calcolare $\mathrm{t\_spazio}_T$), per cui è difficile pensare di poterli trascurare così facilmente, come abbiamo fatto nel sistema 8.3. Nonostante ciò, il procedimento solutivo che segue resta un interessante caso di studio.

Osserviamo che le soluzioni del sistema 8.3 vanno cercate sempre tra gli interi positivi; infatti le espressioni $n \bmod n_1$ e $n \bmod n_2$, stando alle nostre convenzioni, non hanno senso se $n \leq 0$.

Lemma 8.1. *Siano $n_1, n_2 \in \mathbb{N}$, $n_1 > 1$, $n_2 > 1$, $(n_1, n_2) \neq (2,2)$ e sia $x \in \mathbb{N}^\star$. Se il sistema 8.3 ha due soluzioni n' ed n'', $n' > n'' > 0$, allora $n' - n'' = 2$ e $\left\lfloor \frac{n'}{n_1} \right\rfloor - \left\lfloor \frac{n''}{n_1} \right\rfloor = \left\lfloor \frac{n'}{n_2} \right\rfloor - \left\lfloor \frac{n''}{n_2} \right\rfloor = 1$.*

Dimostrazione.

1. $n' - n'' = 2$ [da 2., 3., 4. e 5.]
2. Siano $h \equiv \left\lfloor \frac{n'}{n_1} \right\rfloor - \left\lfloor \frac{n''}{n_1} \right\rfloor$ e $k \equiv \left\lfloor \frac{n'}{n_2} \right\rfloor - \left\lfloor \frac{n''}{n_2} \right\rfloor$
3. $n' - n'' =$ [perché n' ed n'' sono soluzioni del sistema 8.3]
   $x + \left\lfloor \frac{n'}{n_1} \right\rfloor + \left\lfloor \frac{n'}{n_2} \right\rfloor - \left(x + \left\lfloor \frac{n''}{n_1} \right\rfloor + \left\lfloor \frac{n''}{n_2} \right\rfloor \right) =$
   $\left(\left\lfloor \frac{n'}{n_1} \right\rfloor - \left\lfloor \frac{n''}{n_1} \right\rfloor \right) + \left(\left\lfloor \frac{n'}{n_2} \right\rfloor - \left\lfloor \frac{n''}{n_2} \right\rfloor \right) =$ [da 2.]
   $h + k$
4. $k = 1$ [da (a), e 6. e per l'ipotesi $n_1 > 1$, $n_2 > 1$, $(n_1, n_2) \neq (2,2)$]
   (a) $(k-1)(n_2-1)(n_1-1) \leq k-1$ [da (b)]
   (b) $(k-1)(n_2-1) \leq \frac{k-1}{n_1-1}$ [da (c)]
   (c) $(k-1)(n_2-1)+1 \leq \frac{k-1}{n_1-1}+1$ [da (d) ed (e)]
   (d) $h \leq \frac{k-1}{n_1-1}+1$ [da i.]
      i. $h(n_1-1) \leq k-1+(n_1-1)$ [da ii.]
      ii. $h(n_1-1) \leq k+n_1-2$ [da iii.]
      iii. $h+k \geq hn_1-n_1+2$ [da iv.]
      iv. $h+k \geq (h-1)n_1+2$ [da v., 3. e 2.]
      v. $n'-n'' \geq \left(\left\lfloor \frac{n'}{n_1} \right\rfloor - \left\lfloor \frac{n''}{n_1} \right\rfloor - 1 \right) n_1 + 2$ [da vi.]
      vi. $n'-n'' \geq n' - n' \bmod n_1 - (n'' - n'' \bmod n_1) - n_1 + 2$ [da vii.]
      vii. $n_1 + n' \bmod n_1 \geq n'' \bmod n_1 + 2$ [da viii. e ix., sommando membro a membro]

viii. $n_1 \geq n'' \bmod n_1 + 1$ [perché $n'' \bmod n_1 < n_1$]

ix. $n' \bmod n_1 \geq 1$ [perché n' è soluzione del sistema 8.3]

(e) $h \geq (k-1)(n_2 - 1) + 1$ [da i.]

i. $h \geq k(n_2 - 1) - (n_2 - 1) + 1$ [da ii.]

ii. $h \geq k(n_2 - 1) - n_2 + 2$ [da iii.]

iii. $h + k \geq kn_2 - n_2 + 2$ [da iv.]

iv. $h + k \geq (k-1)n_2 + 2$ [da v., 3. e 2.]

v. $n' - n'' \geq \left(\left\lfloor \frac{n'}{n_2} \right\rfloor - \left\lfloor \frac{n''}{n_2} \right\rfloor - 1\right) n_2 + 2$ [da vi.]

vi. $n' - n'' \geq n' - n' \bmod n_2 - (n'' - n'' \bmod n_2) - n_2 + 2$ [da vii.]

vii. $n_2 + n' \bmod n_2 \geq n'' \bmod n_2 + 2$ [da viii. e ix., sommando membro a membro]

viii. $n_2 \geq n'' \bmod n_2 + 1$ [perché $n'' \bmod n_2 < n_2$]

ix. $n' \bmod n_2 \geq 1$ [perché n' è soluzione del sistema 8.3]

5. $h = 1$ [come per 6.]

6. $h > 0$ e $k > 0$ [da (a) e perché (b) e (b)–i., (c) e (c)–i. sono delle contraddizioni]

(a) $h \geq 0$ e $k \geq 0$ [da 2. e da $n' > n''$, per monotonia della parte intera]

(b) Se $h > 0$ e $k = 0$

i. $h \leq$ [da ii.]
$\frac{n_1 - 2}{n_1 - 1} <$
1

ii. $h(n_1 - 1) \leq n_1 - 2$ [da iii.]

iii. $h \geq hn_1 - n_1 + 2$ [da iv.]

iv. $h \geq (h-1)n_1 + 2$ [da 4.–(d)–iv. e (b)]

(c) Se $h = 0$ e $k > 0$

i. $k \leq$ [da ii.]
$\frac{n_2 - 2}{n_2 - 1} <$
1

ii. $k(n_2 - 1) \leq n_2 - 2$ [da iii.]

iii. $k \geq kn_2 - n_2 + 2$ [da iv.]

iv. $k \geq (k-1)n_2 + 2$ [da 4.–(e)–iv. e (c)]

□

Osservazione 8.1. *Si noti che, nel caso degenere $n_1 = n_2 = 2$, il sistema 8.3 può avere o infinite soluzioni (se $x = 1$) o messuna soluzione (se $x \neq 1$). Infatti in questo caso possiamo riscrivere il sistema come:*

$$\begin{cases} n - x = 2\left\lfloor \frac{n}{2} \right\rfloor \\ n \bmod 2 = 1 \end{cases} \tag{8.4}$$

da cui $n - x = 2\left\lfloor \frac{n}{2} \right\rfloor = n - n \bmod 2 = n - 1$, che è un'identità se $x = 1$ (nel qual caso ogni n tale che $n \bmod 2 = 1$ è soluzione del sistema 8.4) ed impossibile se $x \neq 1$.

Proposizione 8.4. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$ avente spazi, $T \neq (2, 2)$, sia $x \in \mathbb{N}^\star$ e siano $s \equiv |\{y \text{ spazio di } T \mid 0 < y \leq \mathrm{MCM}(n_1, n_2)\}|$ e $c \equiv |\{z \text{ classe di } T \mid 0 < |z| \leq \mathrm{MCM}(n_1, n_2)\}|$. Allora:*

- *Se $x - 1 = m(s - 1)$, $m \in \mathbb{N}^\star$, allora il sistema 8.3 ha le seguenti due soluzioni:*

$$x + (c + 1)\, m = m\mathrm{MCM}(n_1, n_2) + 1$$

e

$$x + (c + 1)\, m - 2 = m\mathrm{MCM}(n_1, n_2) - 1$$

- *Altrimenti, il sistema ammette una sola soluzione.*

Dimostrazione.

1. L'enunciato segue da 2., 2.–(a-d), 3., 3.–(a-c)]
2. Se $x - 1 = m(s - 1)$, $m \in \mathbb{N}^\star$
   (a) $m\mathrm{MCM}(n_1, n_2) + 1$ è soluzione del sistema 8.3 [da $m \in \mathbb{N}^\star$, i., ii. e iii.]
      i. $m\mathrm{MCM}(n_1, n_2) + 1 - x = \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)+1}{n_1} \right\rfloor + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)+1}{n_2} \right\rfloor$ [da A., per la proprietà 2.21]
         A. $m\mathrm{MCM}(n_1, n_2) + 1 - x = \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor + (m\mathrm{MCM}(n_1, n_2) \bmod n_1 = n_1 - 1) + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)+1}{n_2} \right\rfloor$ [da B. e 4.]
         B. $m\mathrm{MCM}(n_1, n_2) + 1 - x = \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)+1}{n_2} \right\rfloor$ [da C., per la proprietà 2.21]
         C. $m\mathrm{MCM}(n_1, n_2) + 1 - x = \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_2} \right\rfloor + (m\mathrm{MCM}(n_1, n_2) \bmod n_2 = n_2 - 1)$ [da D. e 4.]
         D. $m\mathrm{MCM}(n_1, n_2) + 1 - x = \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor + \left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_2} \right\rfloor$ [da E.]

E. $m\mathrm{MCM}(n_1,n_2)+1-x=\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}+\frac{m\mathrm{MCM}(n_1,n_2)}{n_2}$ [da F.]

F. $x-1=m\mathrm{MCM}(n_1,n_2)-\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}-\frac{m\mathrm{MCM}(n_1,n_2)}{n_2}$ [da G.]

G. $x-1=\frac{n_1n_2m\mathrm{MCM}(n_1,n_2)-n_2m\mathrm{MCM}(n_1,n_2)-n_1m\mathrm{MCM}(n_1,n_2)}{n_1n_2}$ [da H.]

H. $x-1=m\frac{\mathrm{MCM}(n_1,n_2)(n_1n_2-n_2-n_1)}{n_1n_2}$ [da I.]

I. $x-1=m\frac{n_1n_2-n_2-n_1}{\mathrm{MCD}(n_1,n_2)}$ [da J.]

J. $x-1=m\frac{(n_1-1)(n_2-1)-1}{\mathrm{MCD}(n_1,n_2)}$ [da 2., per la definizione di s e per la proposizione 4.7]

ii. $(m\mathrm{MCM}(n_1,n_2)+1)\bmod n_1\neq 0$ [da 4.]

iii. $(m\mathrm{MCM}(n_1,n_2)+1)\bmod n_2\neq 0$ [da 4.]

(b) $m\mathrm{MCM}(n_1,n_2)-1$ è soluzione del sistema 8.3 [da $m\in\mathbb{N}^\star$, i., ii. e iii.]

i. $m\mathrm{MCM}(n_1,n_2)-1-x=\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)-1}{n_1}\right\rfloor+\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)-1}{n_2}\right\rfloor$ [da A., per la proprietà 2.21]

A. $m\mathrm{MCM}(n_1,n_2)-1-x=\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}\right\rfloor-((m\mathrm{MCM}(n_1,n_2)-1)\bmod n_1=n_1-1)+\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)+1}{n_2}\right\rfloor$ [da B. e 4.]

B. $m\mathrm{MCM}(n_1,n_2)-1-x=\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}\right\rfloor-1+\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)+1}{n_2}\right\rfloor$ [da C., per la proprietà 2.21]

C. $m\mathrm{MCM}(n_1,n_2)-1-x=\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}\right\rfloor+\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)}{n_2}\right\rfloor-((m\mathrm{MCM}(n_1,n_2)-1)\bmod n_2=n_2-1)$ [da D. e 4.]

D. $m\mathrm{MCM}(n_1,n_2)-1-x=\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}\right\rfloor-1+\left\lfloor\frac{m\mathrm{MCM}(n_1,n_2)}{n_2}\right\rfloor-1$ [da E.]

E. $m\mathrm{MCM}(n_1,n_2)-1-x=\frac{m\mathrm{MCM}(n_1,n_2)}{n_1}-1+\frac{m\mathrm{MCM}(n_1,n_2)}{n_2}-1$ [da 2.–(a)–i.–E.]

ii. $(m\mathrm{MCM}(n_1,n_2)-1)\bmod n_1\neq 0$ [da 4.]

iii. $(m\mathrm{MCM}(n_1,n_2)-1)\bmod n_2\neq 0$ [da 4.]

(c) $x+(c+1)m=m\mathrm{MCM}(n_1,n_2)+1$ [da (i.)]

i. $x-1+(c+1)m=m\mathrm{MCM}(n_1,n_2)$ [da (ii.)]

ii. $c+\frac{x-1}{m}+1=\mathrm{MCM}(n_1,n_2)$ [da iii. e 2.]

iii. $c+s=\mathrm{MCM}(n_1,n_2)$ [per il corollario 3.1]

(d) $x+(c+1)m-2=m\mathrm{MCM}(n_1,n_2)-1$ [da (c)]

3. Se il sistema ha due soluzioni distinte

(a) Siano n' ed n'', $n'>n''>0$ due soluzioni del sistema.

i. $n' - 1 = m\mathrm{MCM}(n_1, n_2)$, $m \in \mathbb{N}$ [da ii. e iii.]

ii. $(n' - 1) \bmod n_1 = 0$ [da A.]

A. $\left\lceil \frac{n'-1}{n_1} \right\rceil + ((n' - 1) \bmod n_1 = 0) =$ [per la proposizione 2.21]
$\left\lceil \frac{n'}{n_1} \right\rceil =$ [da (a): essendo n' soluzione del sistema, si ha $n' \bmod n_1 > 0$]
$\left\lfloor \frac{n'}{n_1} \right\rfloor + 1 =$ [da (a), per il lemma 8.1]
$\left(\left\lfloor \frac{n''}{n_1} \right\rfloor + 1 \right) + 1 =$ [da (a), per il lemma 8.1]
$\left(\left\lfloor \frac{n'-2}{n_1} \right\rfloor + 1 \right) + 1 =$ [per la proposizione 2.21]
$\left\lceil \frac{n'-1}{n_1} \right\rceil + 1$

iii. $(n' - 1) \bmod n_2 = 0$ [come ii.]

(b) $x - 1 =$
$n' - 1 - (n' - x) =$ [da (a)–i.]
$m\mathrm{MCM}(n_1, n_2) - (n' - x) =$ [da (a)]
$m\mathrm{MCM}(n_1, n_2) - \left\lfloor \frac{n'}{n_1} \right\rfloor - \left\lfloor \frac{n'}{n_2} \right\rfloor =$ [da i. e ii.]
$m\mathrm{MCM}(n_1, n_2) - \frac{mn_2}{\mathrm{MCD}(n_1,n_2)} - \frac{mn_1}{\mathrm{MCD}(n_1,n_2)} =$
$\frac{m\mathrm{MCM}(n_1,n_2)\mathrm{MCD}(n_1,n_2) - mn_2 - mn_1}{\mathrm{MCD}(n_1,n_2)} =$
$\frac{mn_1n_2 - mn_2 - mn_1}{\mathrm{MCD}(n_1,n_2)} =$
$m\frac{n_1n_2 - n_2 - n_1}{\mathrm{MCD}(n_1,n_2)} =$ [per la definizione di s e per la proposizione 4.7]
$m(s - 1)$

i. $\left\lfloor \frac{n'}{n_1} \right\rfloor =$ [da (a)–i.]
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)+1}{n_1} \right\rfloor =$ [per la proprietà 2.21]
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor - (m\mathrm{MCM}(n_1, n_2) \bmod n_1 = n_1 - 1) =$
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor - (0 = n_1 - 1) =$
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor =$ [perché $\mathrm{MCD}(n_1, n_2)\,\mathrm{MCM}(n_1, n_2) = n_1n_2$]
$\left\lfloor \frac{m\mathrm{MCM}(n_1,n_2)}{n_1} \frac{n_1n_2}{\mathrm{MCD}(n_1,n_2)\mathrm{MCM}(n_1,n_2)} \right\rfloor =$
$\left\lfloor \frac{mn_2}{\mathrm{MCD}(n_1,n_2)} \right\rfloor =$
$\frac{mn_2}{\mathrm{MCD}(n_1,n_2)}$

ii. $\left\lfloor \frac{n'}{n_2} \right\rfloor = \frac{mn_1}{\mathrm{MCD}(n_1,n_2)}$ [da (a), scambiando n_2 ed n_1]

(c) $m > 0$ [da i., i.–A. e i.–B., per assurdo]

i. Se $m = 0$

A. Il sistema ha una sola soluzione [da B., perché le soluzioni devono essere positive]

B. $m\mathrm{MCM}(n_1, n_2) - 1 < 0$ [da (a) e (a)–i.]

4. $n_1 > 1$, $n_2 > 1$ [perché il tratteggio ha spazi e per la proprietà 8.1]

□

Proposizione 8.5. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$ *avente spazi,* $T \neq (2,2)$*, sia* $x \in \mathbb{N}^\star$ *e siano* $s \equiv |\{y \text{ spazio di } T \mid 0 < y \leq \mathrm{MCM}(n_1, n_2)\}|$ *e* $c \equiv |\{z \text{ classe di } T \mid 0 < |z| \leq \mathrm{MCM}(n_1, n_2)\}|$*. Sia inoltre* $m \in \mathbb{N}^\star$*. Allora ciascuno dei due interi*

$$x + (c+1)\, m = m\mathrm{MCM}(n_1, n_2) + 1$$

e

$$x + (c+1)\, m - 2 = m\mathrm{MCM}(n_1, n_2) - 1$$

è soluzione del sistema 8.3 se e solo se $x - 1 = m(s-1)$*.*

Dimostrazione.

1. Se $x - 1 = m(s-1)$, allora $m\mathrm{MCM}(n_1, n_2) + 1$ e $m\mathrm{MCM}(n_1, n_2) - 1$ sono soluzioni del sistema 8.3 [per la proposizione 8.4]
2. Se $x - 1 \neq m(s-1)$
   (a) Il sistema 8.3 ha una sola soluzione n [per la proposizione 8.4]
   (b) $n \neq m\mathrm{MCM}(n_1, n_2) - 1$ e $n \neq m\mathrm{MCM}(n_1, n_2) + 1$ [da (c)]
   (c) $(n \bmod n_1 \neq n_1 - 1 \vee n \bmod n_2 \neq n_2 - 1) \wedge (n \bmod n_1 \neq 1 \vee n \bmod n_2 \neq 1)$ [da (d) e (d)–i.]
   (d) Se $\neg\,(n \bmod n_1 \neq n_1 - 1 \vee n \bmod n_2 \neq n_2 - 1) \wedge (n \bmod n_1 \neq 1 \vee n \bmod n_2 \neq 1)$
      i. Il sistema 8.3 ha due soluzioni distinte [da iii., iii.–A., iv. e iv.–A.]
      ii. $(n \bmod n_1 = n_1 - 1 \wedge n \bmod n_2 = n_2 - 1) \vee (n \bmod n_1 = 1 \wedge n \bmod n_2 = 1)$ [da (d)]
      iii. Se $n \bmod n_1 = n_1 - 1 \wedge n \bmod n_2 = n_2 - 1$
         A. Il sistema 8.3 ha due soluzioni distinte [da 1. e B.]
         B. $n + 2$ è soluzione del sistema 8.3 [da C. e iii.]
         C. $n + 2 - x = \left\lfloor \frac{n+2}{n_1} \right\rfloor + \left\lfloor \frac{n+2}{n_2} \right\rfloor$ [da D., per la proprietà 2.21]
         D. $n+2-x = \left\lfloor \frac{n+1}{n_1} \right\rfloor + ((n+1) \bmod n_1 = n_1 - 1) + \left\lfloor \frac{n+1}{n_2} \right\rfloor + ((n+1) \bmod n_2 = n_2 - 1)$ [da E. e iii.]
         E. $n + 2 - x = \frac{n+1}{n_1} + \frac{n+1}{n_2}$ [da F.]
         F. $n - x = \left(\frac{n+1}{n_1} - 1\right) + \left(\frac{n+1}{n_2} - 1\right)$ [da G.]

G. $n - x = \frac{n-(n_1-1)}{n_1} + \frac{n-(n_2-1)}{n_2}$ [da H.]

H. $n - x = \frac{n-n \bmod n_1}{n_1} + \frac{n-n \bmod n_2}{n_2}$ [da I.]

I. $n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor$ [da 1., in particolare dal fatto che n è soluzione]

iv. Se $n \bmod n_1 = 1 \wedge n \bmod n_2 = 1$

A. Il sistema 8.3 ha due soluzioni distinte

B. $n - 2$ è soluzione del sistema 8.3 [da C., I. e iv.]

C. $n - 2 - x = \left\lfloor \frac{n-2}{n_1} \right\rfloor + \left\lfloor \frac{n-2}{n_2} \right\rfloor$ [da D. e I., per la proprietà 2.21]

D. $n - 2 - x = \left\lceil \frac{n-1}{n_1} \right\rceil - 1 + \left\lceil \frac{n-1}{n_2} \right\rceil - 1$ [da E. e iv.]

E. $n - 2 - x = \frac{n-1}{n_1} - 1 + \frac{n-1}{n_2} - 1$ [da F.]

F. $n - x = \frac{n-1}{n_1} + \frac{n-1}{n_2}$ [da G.]

G. $n - x = \frac{n-n \bmod n_1}{n_1} + \frac{n-n \bmod n_2}{n_2}$ [da H.]

H. $n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor$ [da 1., in particolare dal fatto che n è soluzione]

I. $n \geq 2$ [si ottiene da iv., da $n - x = \left\lfloor \frac{n}{n_1} \right\rfloor + \left\lfloor \frac{n}{n_2} \right\rfloor$ e da $T \neq (2, 2)$: tralasciamo i dettagli]

□

Considerando globalmente il lemma 8.1, la proposizione 8.4 e la proposizione 8.5, abbiamo imparato che, se $n_1 > 1$, $n_2 > 1$ e $(n_1, n_2) \neq (2, 2)$:

- Il sistema 8.3 ha due soluzioni distinte se e solo se $x - 1 = m(s - 1) = m\frac{(n_1-1)(n_2-1)-1}{\text{MCD}(n_1,n_2)}$ per qualche m positivo, nel qual caso le soluzioni sono MCM $(n_1, n_2) \pm 1$.

- Nei casi in cui il sistema ammette una sola soluzione, questa non può essere MCM $(n_1, n_2) \pm 1$: ciascuno di questi due valori è soluzione solo quando il sistema ammette due soluzioni.

Ad esempio, siano $n_1 = 3$ ed $n_2 = 5$. Allora $s - 1 = \frac{(n_1-1)(n_2-1)-1}{\text{MCD}(n_1,n_2)} = \frac{2 \cdot 4-1}{1} = 7$. Per $x = 8$ quindi si ha $x - 1 = s - 1$ ed il sistema corrispondente:

$$\begin{cases} n - 8 = \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{5} \right\rfloor \\ n \bmod 3 \neq 0 \\ n \bmod 5 \neq 0 \end{cases}$$

ammette le due soluzioni $n = 14 = \mathrm{MCM}(3,5) - 1$ ed $n = 16 = \mathrm{MCM}(3,5) + 1$. Infatti $14 - 8 = 6 = \left\lfloor \frac{14}{3} \right\rfloor + \left\lfloor \frac{14}{5} \right\rfloor$ e $16 - 8 = 8 = \left\lfloor \frac{16}{3} \right\rfloor + \left\lfloor \frac{16}{5} \right\rfloor$ e nessuno dei due è multiplo di 3 o di 5.

Per $x = 7$, invece, si ha una sola soluzione $n = 13$; infatti $13 - 7 = 6 = \left\lfloor \frac{13}{3} \right\rfloor + \left\lfloor \frac{13}{5} \right\rfloor$ e 13 non è multplo né di 3, né di 5.

Lemma 8.2. *Siano $n_1, n_2 \in \mathbb{N}$, $n_1 > 1$, $n_2 > 1$. Siano $x \in \mathbb{N}^\star$ ed n una soluzione del sistema 8.3. Sia inoltre $n \bmod n_1 \neq n_1 - 1$ oppure $n \bmod n_2 \neq n_2 - 1$. Allora*

$$\left\lfloor \frac{(n_1 - 1)(n_2 x - 1) + x + \left\lfloor \frac{n}{n_2} \right\rfloor}{(n_1 - 1)(n_2 - 1)} \right\rfloor = x + \left\lfloor \frac{n}{n_2} \right\rfloor$$

Dimostrazione.

1. $\left\lfloor \frac{(n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor}{(n_1-1)(n_2-1)} \right\rfloor = x + \left\lfloor \frac{n}{n_2} \right\rfloor$ [da (a), per la proprietà 2.23]

   (a) $\left(x + \left\lfloor \frac{n}{n_2} \right\rfloor\right)(n_1 - 1)(n_2 - 1) \leq (n_1 - 1)(n_2 x - 1) + x + \left\lfloor \frac{n}{n_2} \right\rfloor < \left(x + \left\lfloor \frac{n}{n_2} \right\rfloor\right)((n_1 - 1)(n_2 - 1) + 1)$ [da (b) e (c)]

   (b) $\left(x + \left\lfloor \frac{n}{n_2} \right\rfloor\right)(n_1 - 1)(n_2 - 1) \leq (n_1 - 1)(n_2 x - 1) + x + \left\lfloor \frac{n}{n_2} \right\rfloor$ [da i.]

   i. $\left(x + \left\lfloor \frac{n}{n_2} \right\rfloor\right)((n_1 - 1)(n_2 - 1) - 1) \leq (n_1 - 1)(n_2 x - 1)$ [da ii.]

   ii. $\left(x + \left\lfloor \frac{n}{n_2} \right\rfloor\right)(n_1 n_2 - n_1 - n_2) \leq (n_1 - 1)(n_2 x - 1)$ [da iii.]

   iii. $\left\lfloor \frac{n}{n_2} \right\rfloor (n_1 n_2 - n_1 - n_2) \leq (n_1 - 1)(n_2 x - 1) - (n_1 n_2 - n_1 - n_2)\, x$ [da iv.]

   iv. $\left\lfloor \frac{n}{n_2} \right\rfloor (n_1 n_2 - n_1 - n_2) \leq n_1 n_2 x - n_1 - n_2 x + 1 - n_1 n_2 x + n_1 x + n_2 x$ [da v.]

   v. $\left\lfloor \frac{n}{n_2} \right\rfloor (n_1 n_2 - n_1 - n_2) \leq -n_1 + 1 + n_1 x$ [da vi.]

   vi. $\left\lfloor \frac{n}{n_2} \right\rfloor (n_1 n_2 - n_1 - n_2) \leq 1 + n_1 (x - 1)$ [da vii., perché n è soluzione del sistema 8.3]

   vii. $\left\lfloor \frac{n}{n_2} \right\rfloor (n_1 n_2 - n_1 - n_2) \leq 1 + n_1 \left(n - \left\lfloor \frac{n}{n_2} \right\rfloor - \left\lfloor \frac{n}{n_1} \right\rfloor - 1\right)$ [da viii.]

   viii. $\left\lfloor \frac{n}{n_2} \right\rfloor n_2 (n_1 - 1) \leq 1 + n_1 \left(n - \left\lfloor \frac{n}{n_1} \right\rfloor - 1\right)$ [da ix.]

   ix. $(n - n \bmod n_2)(n_1 - 1) \leq 1 + n_1 n - n + n \bmod n_1 - n_1$ [da x.]

   x. $(-n \bmod n_2)(n_1 - 1) \leq 1 + n \bmod n_1 - n_1$ [da xi.]

   xi. $n \bmod n_2 (n_1 - 1) \geq n_1 - 1 - n \bmod n_1$ [da xi.]

   xii. $n_1 - 1 \geq n_1 - 1 - n \bmod n_1$ [perché $n \bmod n_1 \geq 0$]

(c) $(n_1-1)(n_2x-1)+x+\left\lfloor\frac{n}{n_2}\right\rfloor<\left(x+\left\lfloor\frac{n}{n_2}\right\rfloor+1\right)(n_1-1)(n_2-1)$ [da i.]

i. $(n_1-1)(n_2x-1)+\left(x+\left\lfloor\frac{n}{n_2}\right\rfloor+1\right)-1<\left(x+\left\lfloor\frac{n}{n_2}\right\rfloor+1\right)(n_1n_2-n_1-n_2+1)$ [da ii.]

ii. $(n_1-1)(n_2x-1)-1<\left(x+\left\lfloor\frac{n}{n_2}\right\rfloor+1\right)(n_1n_2-n_1-n_2)$ [da iii.]

iii. $(n_1-1)(n_2x-1)-1-(x+1)(n_1n_2-n_1-n_2)<(n_1n_2-n_1-n_2)\left\lfloor\frac{n}{n_2}\right\rfloor$ [da iv.]

iv. $n_1n_2x-n_1-n_2x-(x+1)(n_1n_2-n_1-n_2)<(n_1n_2-n_1-n_2)\left\lfloor\frac{n}{n_2}\right\rfloor$ [da v.]

v. $n_1n_2x-n_1-n_2x-n_1n_2x+n_1x+n_2x-n_1n_2+n_1+n_2<(n_1n_2-n_1-n_2)\left\lfloor\frac{n}{n_2}\right\rfloor$ [da vi.]

vi. $n_1x-n_1n_2+n_2<(n_1n_2-n_1-n_2)\left\lfloor\frac{n}{n_2}\right\rfloor$ [da vii.]

vii. $n_1x-n_2(n_1-1)<(n_1n_2-n_1-n_2)\left\lfloor\frac{n}{n_2}\right\rfloor$ [da viii.]

viii. $n_1x-n_2(n_1-1)<(n_1n_2-n_1-n_2+1)\left\lfloor\frac{n}{n_2}\right\rfloor-\left\lfloor\frac{n}{n_2}\right\rfloor$ [da ix.]

ix. $n_1x-n_2(n_1-1)<(n_1-1)(n_2-1)\left\lfloor\frac{n}{n_2}\right\rfloor-\left\lfloor\frac{n}{n_2}\right\rfloor$ [da x.]

x. $n_1x+\left\lfloor\frac{n}{n_2}\right\rfloor<(n_1-1)(n_2-1)\left\lfloor\frac{n}{n_2}\right\rfloor+n_2(n_1-1)$ [da xi.]

xi. $n_1x+\left\lfloor\frac{n}{n_2}\right\rfloor<(n_1-1)\left((n_2-1)\left\lfloor\frac{n}{n_2}\right\rfloor+n_2\right)$ [da xii.]

xii. $n_1x+\left\lfloor\frac{n}{n_2}\right\rfloor<(n_1-1)\left(n-n\bmod n_2-\left\lfloor\frac{n}{n_2}\right\rfloor+n_2\right)$ [da xiii., perché n è soluzione del sistema 8.3]

xiii. $n_1\left(n-\left\lfloor\frac{n}{n_2}\right\rfloor-\left\lfloor\frac{n}{n_1}\right\rfloor\right)+\left\lfloor\frac{n}{n_2}\right\rfloor<(n_1-1)\left(n-n\bmod n_2-\left\lfloor\frac{n}{n_2}\right\rfloor+n_2\right)$ [da xiv.]

xiv. $n_1\left(n-\left\lfloor\frac{n}{n_2}\right\rfloor\right)+\left\lfloor\frac{n}{n_2}\right\rfloor-n_1\left\lfloor\frac{n}{n_1}\right\rfloor<(n_1-1)\left(n-n\bmod n_2-\left\lfloor\frac{n}{n_2}\right\rfloor+n_2\right)$ [da xv.]

xv. $(n_1-1)\left(n-\left\lfloor\frac{n}{n_2}\right\rfloor\right)+n-n_1\left\lfloor\frac{n}{n_1}\right\rfloor<(n_1-1)\left(n-n\bmod n_2-\left\lfloor\frac{n}{n_2}\right\rfloor+n_2\right)$ [da xvi.]

xvi. $n<(n_1-1)(n_2-n\bmod n_2)+n_1\left\lfloor\frac{n}{n_1}\right\rfloor$ [da xvii.]

xvii. $n<(n_1-1)(n_2-n\bmod n_2)+n-n\bmod n_1$ [da xviii.]

xviii. $n\bmod n_1<(n_1-1)(n_2-n\bmod n_2)$ [da xix., xix.–A., xx. e xx.–B.]

xix. Se $n\bmod n_1=n_1-1$

A. $n\bmod n_1<(n_1-1)(n_2-n\bmod n_2)$ [da B. e xix.]

B. $n_1-1<(n_1-1)(n_2-n\bmod n_2)$ [da C., moltiplicando per n_1-1]

C. $1<n_2-n\bmod n_2$ [da D.]

D. $n\bmod n_2<n_2-1$ [da xix., perché $n\bmod n_1\neq n_1-1$ oppure $n\bmod n_2\neq n_2-1$]

xx. Se $n \bmod n_1 < n_1 - 1$

A. $n \bmod n_1 < (n_1 - 1)(n_2 - n \bmod n_2)$ [da B.]

B. $(n_1 - 1)(n_2 - n \bmod n_2) \geq$ [da C.]
$n_1 - 1 >$ [da xx.]
$n \bmod n_1$

C. $n_2 - n \bmod n_2 \geq 1$ [da D.]

D. $n \bmod n_2 \leq n_2 - 1$

□

Si può dimostrare che, se neghiamo l'ipotesi che $n \bmod n_1 \neq n_1 - 1$ oppure $n \bmod n_2 \neq n_2 - 1$, cioè se supponiamo che $n \bmod n_1 = n_1 - 1$ e che $n \bmod n_2 = n_2 - 1$, vale la stessa uguaglianza del lemma con la parte intera per eccesso: $\left\lceil \frac{(n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor}{(n_1-1)(n_2-1)} \right\rceil = x + \left\lfloor \frac{n}{n_2} \right\rfloor$. Lasciamo la dimostrazione al lettore, come esercizio.

Proposizione 8.6. *Siano $n_1 > 1$, $n_2 > 1$, $(n_1, n_2) \neq (2, 2)$. Sia inoltre $x \in \mathbb{N}^\star$. Allora l'intero:*

$$n = \text{t\_spazio}_{(n_1)} \left(\left\lfloor \frac{(n_1 - 1)(n_2 x - 1) - 1}{(n_1 - 1)(n_2 - 1) - 1} \right\rfloor \right)$$

è soluzione del sistema 8.3; se il sistema ammette due soluzioni distinte, esso è la più grande delle due.

Dimostrazione. L'enunciato segue da 1., 1.–(a), 2., 2.–(a).

1. Se il sistema 8.3 ammette una sola soluzione

   (a) $\text{t\_spazio}_{(n_1)} \left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor \right)$ è soluzione del sistema 8.3 [da (b), (c) e (d)]

   (b) Sia n la soluzione del sistema 8.3 [da 1.]

      i. $n \bmod n_1 \neq n_1 - 1 \vee n \bmod n_2 \neq n_2 - 1$ [da ii.]

      ii. $\neg (n \bmod n_1 = n_1 - 1 \wedge n \bmod n_2 = n_2 - 1)$ [da iii.]

      iii. $\neg \exists m \in \mathbb{N} : n = m\text{MCM}(n_1, n_2) - 1$ [da 1. e 1.–(b), per la proposizione 8.5]

   (c) $n = \text{t\_spazio}_{(n_1)} \left(x + \left\lfloor \frac{n}{n_2} \right\rfloor \right)$ [da i. e ii., per la proposizione 8.1]

      i. $\left\lfloor \frac{n}{n_1} \right\rfloor = n - \left(x + \left\lfloor \frac{n}{n_2} \right\rfloor \right)$ [da (b)]

      ii. $n \bmod n_1 \neq 0$ [da (b)]

(d) $x + \left\lfloor \frac{n}{n_2} \right\rfloor = \left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor$ [da i.]

i. $(n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor =$ [da ii. e iii. e iv., per la proposizione 8.1]
t_spazio$_{((n_1-1)(n_2-1))}((n_1-1)(n_2x-1)) =$ [da v., per il corollario 8.1]
$(n_1-1)(n_2x-1) + \left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor$

ii. $\left\lfloor \frac{(n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor}{(n_1-1)(n_2-1)} \right\rfloor = x + \left\lfloor \frac{n}{n_2} \right\rfloor$ [da (b), (b)–i. e dalle ipotesi del teorema, per il lemma 8.2]

iii. Sia $r \equiv \left((n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor\right) \bmod (n_1-1)(n_2-1)$

iv. $r \neq 0$ [perché dall'ipotesi B. si ottiene l'assurdo R.]

A. $(n_1-1)(n_2-1)\left(x+\left\lfloor \frac{n}{n_2} \right\rfloor\right)+r = (n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor$ [da ii. e iii.]

B. Se $r = 0$

C. $(n_1-1)(n_2-1)\left(x+\left\lfloor \frac{n}{n_2} \right\rfloor\right) = (n_1-1)(n_2x-1)+x+\left\lfloor \frac{n}{n_2} \right\rfloor$ [da A. e B.]

D. $\left(x+\left\lfloor \frac{n}{n_2} \right\rfloor\right)((n_1-1)(n_2-1)-1) = (n_1-1)(n_2x-1)$ [da C.]

E. $\left(x+\left\lfloor \frac{n}{n_2} \right\rfloor\right)(n_1n_2-n_1-n_2) = (n_1-1)(n_2x-1)$ [da D.]

F. $\left(x+\left\lfloor \frac{n}{n_2} \right\rfloor\right)(n_1n_2-n_1-n_2) = n_1n_2x-n_2x-(n_1-1)$ [da E.]

G. $(n_1n_2x-n_1x-n_2x)+(n_1n_2-n_1-n_2)\left\lfloor \frac{n}{n_2} \right\rfloor = n_1n_2x-n_2x-(n_1-1)$ [da F.]

H. $(n_1n_2-n_1-n_2)\left\lfloor \frac{n}{n_2} \right\rfloor = n_1x-(n_1-1)$ [da G.]

I. $(n_1n_2-n_1-n_2)\left\lfloor \frac{n}{n_2} \right\rfloor = n_1\left(n-\left\lfloor \frac{n}{n_2} \right\rfloor-\left\lfloor \frac{n}{n_1} \right\rfloor\right)-(n_1-1)$ [da H. e da (c)]

J. $(n_1n_2-n_2)\left\lfloor \frac{n}{n_2} \right\rfloor = n_1\left(n-\left\lfloor \frac{n}{n_1} \right\rfloor\right)-(n_1-1)$ [da I.]

K. $(n_1-1)n_2\frac{n-n \bmod n_2}{n_2} = n_1\left(n-\frac{n-n \bmod n_1}{n_1}\right)-(n_1-1)$ [da J.]

L. $(n_1-1)(n-n \bmod n_2) = n_1n-n+n \bmod n_1-(n_1-1)$ [da K.]

M. $(n_1-1)(n-n \bmod n_2) = n(n_1-1)+n \bmod n_1-(n_1-1)$ [da L.]

N. $(n_1-1)(n-n \bmod n_2-n+1) = n \bmod n_1$ [da M.]

O. $(n_1-1)(-n \bmod n_2+1) = n \bmod n_1$ [da N.]

P. $(n_1-1)(-n \bmod n_2+1) > 0$ [da O. e perché, per (c), $n \bmod n_1 > 0$]

Q. $-n \bmod n_2 + 1 > 0$ [da P. e vi.]

R. $1 \leq$ [perché, per (c), $n \bmod n_2 \neq 0$]

$n \bmod n_2 <$ [da Q.]

1

v. Il tratteggio $((n_1 - 1)(n_2 - 1)) \in \mathcal{L}^1$ ha spazi

A. $(n_1 - 1)(n_2 - 1) \geq$ [perché per ipotesi $n_1 > 2$ o $n_2 > 2$, inoltre $n_1 > 1$ e $n_2 > 1$]

$2 >$

1

2. Se il sistema 8.3 ammette due soluzioni distinte

(a) $\text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right)$ è la più grande soluzione del sistema 8.3 [da (b) e iv.]

(b) Sia n la più grande soluzione del sistema 8.3

i. Siano $s \equiv |\{y \text{ spazio di } T \mid 0 < y \leq \text{MCM}(n_1, n_2)\}|$ e $c \equiv |\{z \text{ classe di } T \mid 0 < |z| \leq \text{MCM}(n_1, n_2)\}|$

ii. $x - 1 = m(s - 1)$, $m \in \mathbb{N}^\star$ [da 2., per la proposizione 8.4]

iii. $\text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right) =$ [da iv.]

$\text{t\_spazio}_{(n_1)}\left(\frac{m(n_1-1)n_2}{\text{MCD}(n_1,n_2)} + 1\right) =$ [per il teorema 8.1]

$\left\lfloor \frac{n_1\left(\frac{m(n_1-1)n_2}{\text{MCD}(n_1,n_2)}+1\right)-1}{n_1-1} \right\rfloor =$

$\left\lfloor \frac{\frac{m(n_1-1)n_1n_2}{\text{MCD}(n_1,n_2)}+n_1-1}{n_1-1} \right\rfloor =$

$\left\lfloor \frac{\frac{m(n_1-1)n_1n_2}{\text{MCD}(n_1,n_2)}}{n_1-1} \right\rfloor + 1 =$

$\left\lfloor \frac{mn_1n_2}{\text{MCD}(n_1,n_2)} \right\rfloor + 1 =$

$\frac{mn_1n_2}{\text{MCD}(n_1,n_2)} + 1 =$

$m\text{MCM}(n_1, n_2) + 1 =$ [da A.]

$m(s + c) + 1 =$

$m(s - 1) + 1 + (c + 1)m =$

$x + (c + 1)m =$

$x + (c + 1)\frac{x-1}{s-1} =$ [da 2., 2.–(b) e 2.–(b)–i., per la proposizione 8.4]

n

A. $c + s = \text{MCM}(n_1, n_2)$ [da 2.–(b)–i., per il corollario 3.1]

iv. $\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor =$ [da A.]

$\left\lfloor \frac{(n_1-1)\left(n_2\left(m\frac{(n_1-1)(n_2-1)-1}{\text{MCD}(n_1,n_2)}+1\right)-1\right)-1}{(n_1-1)(n_2-1)-1} \right\rfloor =$

$$\left\lfloor \frac{(n_1-1)\left(\frac{mn_2}{\mathrm{MCD}(n_1,n_2)}((n_1-1)(n_2-1)-1)+n_2-1\right)-1}{(n_1-1)(n_2-1)-1} \right\rfloor =$$
$$\left\lfloor \frac{(n_1-1)\left(\frac{mn_2}{\mathrm{MCD}(n_1,n_2)}((n_1-1)(n_2-1)-1)\right)+(n_1-1)(n_2-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor =$$
$$\left\lfloor \frac{(n_1-1)\left(\frac{mn_2}{\mathrm{MCD}(n_1,n_2)}((n_1-1)(n_2-1)-1)\right)}{(n_1-1)(n_2-1)-1} \right\rfloor + 1 =$$ [perché il denominatore divide il numeratore]
$$\frac{(n_1-1)\frac{mn_2}{\mathrm{MCD}(n_1,n_2)}((n_1-1)(n_2-1)-1)}{(n_1-1)(n_2-1)-1} + 1 =$$
$$\frac{m(n_1-1)n_2}{\mathrm{MCD}(n_1,n_2)}$$

A. $x =$ [da 2.–(b)–iii.]
$m\,(s-1)+1 =$ [da 2.–(b)–i., per la proposizione 4.7]
$m\left(\frac{(n_1-1)(n_2-1)-1}{\mathrm{MCD}(n_1,n_2)}+1-1\right)+1 =$
$m\frac{(n_1-1)(n_2-1)-1}{\mathrm{MCD}(n_1,n_2)}+1$

□

Si noti che l'ipotesi $(n_1, n_2) \neq (2, 2)$ è fondamentale, altrimenti la parte intera $\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor$ non sarebbe definita perché sarebbe $(n_1-1)(n_2-1)-1=0$.

Corollario 8.3. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$ avente spazi, $T \neq (2, 2)$. Allora per ogni $x \in \mathbb{N}^\star$,*

$$\text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right)$$

è uno spazio di T.

Dimostrazione.

1. Sia $n \equiv \text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right)$
2. n è uno spazio di T [da 1. e (a), per la proprietà 3.15]
   (a) $n \bmod n_1 \neq 0$ e $n \bmod n_2 \neq 0$ [da (b)]
   (b) n è soluzione del sistema 8.3 [da 1., per la proposizione 8.6]

□

Il corollario 8.3 è importante, perché presenta una funzione che genera solo spazi di un tratteggio lineare T. Si noti che essa non può generare tutti gli spazi di T. In particolare, gli unici spazi di T che non possono essere restituiti dalla funzione costituiscono l'insieme, che chiamiamo S, delle più piccole delle due soluzioni del sistema 8.3, nei casi in cui questo abbia due soluzioni. Infatti, nei casi in cui il sistema ha una sola soluzione, essa coincide col valore calcolato dalla funzione, ma

non può appartenere ad S, per la proposizione 8.5; d'altra parte, quando il sistema ha due soluzioni, la funzione calcola la più grande delle due, quindi di nuovo il valore assunto dalla funzione non può appartenere ad S.

Se consideriamo ad esempio il tratteggio $(3,4)$, i suoi spazi minori di $\mathrm{MCM}(3,4) = 12$ sono $1, 2, 5, 7, 10$ e 11. Di questi, solo 11 non può essere restituito dalla funzione, perché corrisponde alla più piccola soluzione del sistema, avente due soluzioni:

$$\begin{cases} n - 6 = \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor \\ n \bmod 3 \neq 0 \\ n \bmod 4 \neq 0 \end{cases}$$

Tutti gli altri spazi, comunque, sono calcolati dalla funzione $\text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right) = \text{t\_spazio}_{(3)}\left(\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor\right) = \left\lfloor \frac{3\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor - 1}{2} \right\rfloor$:

- per $x = 1$: $\left\lfloor \frac{3\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{3\left\lfloor \frac{6-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$
- per $x = 2$: $\left\lfloor \frac{3\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{3\left\lfloor \frac{14-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{6-1}{2} \right\rfloor = 2$
- per $x = 3$: $\left\lfloor \frac{3\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{3\left\lfloor \frac{22-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{12-1}{2} \right\rfloor = 5$
- per $x = 4$: $\left\lfloor \frac{3\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{3\left\lfloor \frac{30-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{15-1}{2} \right\rfloor = 7$
- per $x = 5$: $\left\lfloor \frac{3\left\lfloor \frac{2(4x-1)-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{3\left\lfloor \frac{38-1}{5} \right\rfloor - 1}{2} \right\rfloor = \left\lfloor \frac{21-1}{2} \right\rfloor = 10$

Per $x = 6$ invece si ottiene il valore 13, che è il successivo spazio di $(3,4)$, dopo 11: quest'ultimo è quindi completamente "saltato". Chiudiamo questo paragrafo correggendo questo "difetto" della funzione, ottenendone una simile che calcola esattamente t_spazio nel secondo ordine.

Lemma 8.3. *Sia* $T \equiv (n_1, n_2) \in \mathcal{L}^2$ *avente spazi,* $T \neq (2,2)$. *Sia* $f : \mathbb{N}^\star \to \mathbb{N}$ *tale che* $f(x) = \text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right)$ *per ogni* $x \in \mathbb{N}^\star$. *Sia* $s \equiv |\{y \text{ spazio di } T \mid 0 < y \leq \mathrm{MCM}(n_1, n_2)\}|$. *Allora, per ogni* $x \in \mathbb{N}^\star$, $f(x + s - 1) = f(x) + \mathrm{MCM}(n_1, n_2)$.

Dimostrazione.

1. $f(x + s - 1) = f(x) + \mathrm{MCM}(n_1, n_2)$ [da 2.]
2. $\text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2(x+s-1)-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right) = \text{t\_spazio}_{(n_1)}\left(\left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor\right) + \mathrm{MCM}(n_1, n_2)$ [da 3. e 4.]

3. Siano $y \equiv \left\lfloor \frac{(n_1-1)(n_2(x+s-1)-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor$, $x \equiv \left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor$ e $c \equiv \text{MCM}(n_1, n_2)$

4. $\text{t\_spazio}_{(n_1)}(y) = \text{t\_spazio}_{(n_1)}(x) + c \Leftrightarrow$ [per il teorema 8.1]
$\left\lfloor \frac{n_1y-1}{n_1-1} \right\rfloor = \left\lfloor \frac{n_1x-1}{n_1-1} \right\rfloor + c \Leftrightarrow$
$\left\lfloor \frac{n_1y-1}{n_1-1} \right\rfloor - \left\lfloor \frac{n_1x-1}{n_1-1} \right\rfloor = c \Leftrightarrow$
$\left\lfloor \frac{n_1y-1-(n_1x-1)+(n_1x-1) \bmod (n_1-1)}{n_1-1} \right\rfloor = c \Leftrightarrow$
$\left\lfloor \frac{n_1(y-x)+(n_1x-1) \bmod (n_1-1)}{n_1-1} \right\rfloor = c \Leftrightarrow$ [per la proprietà 2.22]
$\left\lfloor \frac{n_1(y-x)}{n_1-1} \right\rfloor + \left\lfloor \frac{(n_1x-1) \bmod (n_1-1)+n_1(y-x) \bmod (n_1-1)}{n_1-1} \right\rfloor = c \Leftrightarrow$ [da (a)]
$\left\lfloor \frac{n_1 \frac{(n_1-1)n_2}{\text{MCD}(n_1,n_2)}}{n_1-1} \right\rfloor + \left\lfloor \frac{(n_1x-1) \bmod (n_1-1)+n_1 \frac{(n_1-1)n_2}{\text{MCD}(n_1,n_2)} \bmod (n_1-1)}{n_1-1} \right\rfloor = c \Leftrightarrow$
$\left\lfloor \frac{(n_1-1) \frac{n_1n_2}{\text{MCD}(n_1,n_2)}}{n_1-1} \right\rfloor + \left\lfloor \frac{(n_1x-1) \bmod (n_1-1)+(n_1-1) \frac{n_1n_2}{\text{MCD}(n_1,n_2)} \bmod (n_1-1)}{n_1-1} \right\rfloor = c \Leftrightarrow$
$\frac{n_1n_2}{\text{MCD}(n_1,n_2)} + \left\lfloor \frac{(n_1x-1) \bmod (n_1-1)}{n_1-1} \right\rfloor = c \Leftrightarrow$
$\frac{n_1n_2}{\text{MCD}(n_1,n_2)} = c \Leftrightarrow$
$\frac{n_1n_2}{\text{MCD}(n_1,n_2)} = \text{MCM}(n_1, n_2)$

   (a) $y - x =$ [da 3.]
   $\left\lfloor \frac{(n_1-1)(n_2(x+s-1)-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor - \left\lfloor \frac{(n_1-1)(n_2x-1)-1}{(n_1-1)(n_2-1)-1} \right\rfloor =$ [per la proprietà 2.22]
   $\left\lfloor \frac{(n_1-1)(n_2(x+s-1)-1)-1-((n_1-1)(n_2x-1)-1)+((n_1-1)(n_2x-1)-1) \bmod ((n_1-1)(n_2-1)-1)}{(n_1-1)(n_2-1)-1} \right\rfloor =$
   $\left\lfloor \frac{(n_1-1)(n_2(x+s-1)-1-(n_2x-1))+((n_1-1)(n_2x-1)-1) \bmod ((n_1-1)(n_2-1)-1)}{(n_1-1)(n_2-1)-1} \right\rfloor =$
   $\left\lfloor \frac{(n_1-1)n_2(s-1)+((n_1-1)(n_2x-1)-1) \bmod ((n_1-1)(n_2-1)-1)}{(n_1-1)(n_2-1)-1} \right\rfloor =$ [da (b)]
   $\left\lfloor \frac{(n_1-1)n_2\left(\frac{(n_1-1)(n_2-1)-1}{\text{MCD}(n_1,n_2)}\right)+((n_1-1)(n_2x-1)-1) \bmod ((n_1-1)(n_2-1)-1)}{(n_1-1)(n_2-1)-1} \right\rfloor =$
   $\frac{(n_1-1)n_2}{\text{MCD}(n_1,n_2)} + \left\lfloor \frac{((n_1-1)(n_2x-1)-1) \bmod ((n_1-1)(n_2-1)-1)}{(n_1-1)(n_2-1)-1} \right\rfloor =$
   $\frac{(n_1-1)n_2}{\text{MCD}(n_1,n_2)}$

   (b) $s = \frac{(n_1-1)(n_2-1)-1}{\text{MCD}(n_1,n_2)} + 1$ [per la proposizione 4.7]

□

Teorema 8.2. *Siano* $T \equiv (n_1, n_2) \in \mathcal{L}^2$ *avente spazi,*
ed $s \equiv |\{y \text{ spazio di } T \mid 0 < y \leq \text{MCM}(n_1, n_2)\}|$. *Per ogni* $i, j \in \{1, 2\}$, $i \neq j$ *e per ogni* $x \in \mathbb{N}^\star$*:*

$$\text{Down}^{T \to T[i]}(\text{t\_spazio}) = \left\{ \lambda x. \left\{ \begin{array}{ll} \frac{x}{s}(n_i - 1)\frac{\text{MCM}(n_i,n_j)}{n_i} & \textit{se } s \mid x \\ \left\lfloor \frac{(n_i-1)\left(n_j\left(x-\left\lfloor \frac{x}{s} \right\rfloor\right)-1\right)-1}{(n_i-1)(n_j-1)-1} \right\rfloor & \textit{altrimenti} \end{array} \right\} \right.$$

Dimostrazione.

1. $\text{Down}^{T\to T[i]}\left(\text{t\_spazio}\right) = \left\{ \lambda x. \left\{ \begin{array}{ll} \frac{x}{s}\left(n_i-1\right)\frac{\text{MCM}(n_i,n_j)}{n_i} & \text{se } s \mid x \\ \left\lfloor \frac{(n_i-1)\left(n_j\left(x-\left\lfloor\frac{x}{s}\right\rfloor\right)-1\right)-1}{(n_i-1)(n_j-1)-1} \right\rfloor & \text{altrimenti} \end{array} \right. \right\}$ [da 2., perché t_spazio lineare è downcast-sicura]

2. $\lambda x. \left\{ \begin{array}{ll} \frac{x}{s}\left(n_i-1\right)n_j & \text{se } s \mid x \\ \left\lfloor \frac{(n_i-1)\left(n_j\left(x-\left\lfloor\frac{x}{s}\right\rfloor\right)-1\right)-1}{(n_i-1)(n_j-1)-1} \right\rfloor & \text{altrimenti} \end{array} \right. \in \text{Down}^{T\to T[i]}\left(\text{t\_spazio}\right)$ [da 3.–(a) e 4.–(a)]

3. Se $s \nmid x$

   (a) Sia $f : \mathbb{N}^\star \to \mathbb{N}$ tale che $f\left(x\right) = \text{t\_spazio}_{T[i]}\left(\left\lfloor \frac{(n_i-1)(n_j x-1)-1}{(n_i-1)(n_j-1)-1} \right\rfloor\right)$ per ogni $x \in \mathbb{N}^\star$

   (b) $\text{t\_spazio}_T\left(x\right) = f\left(x - \left\lfloor\frac{x}{s}\right\rfloor\right)$ [da (c), (c)–ii., (d), (d)–i. e (d)–ii., per induzione]

   (c) Se $\left\lfloor\frac{x}{s}\right\rfloor = 0$

      i. Sia $\text{t\_spazio}_T\left(x\right) \equiv n$

      ii. $\text{t\_spazio}_T\left(x\right) = n \Leftrightarrow$ [per la proposizione 8.3]
      $$\left\{ \begin{array}{l} n - x = \left\lfloor\frac{n}{n_1}\right\rfloor + \left\lfloor\frac{n}{n_2}\right\rfloor - \left\lfloor\frac{n}{\text{MCM}(n_1,n_2)}\right\rfloor \\ n \bmod n_1 \neq 0 \\ n \bmod n_2 \neq 0 \end{array} \right. \Leftrightarrow \text{[da iv.]}$$
      $$\left\{ \begin{array}{l} n - x = \left\lfloor\frac{n}{n_1}\right\rfloor + \left\lfloor\frac{n}{n_2}\right\rfloor \\ n \bmod n_1 \neq 0 \\ n \bmod n_2 \neq 0 \end{array} \right. \Leftrightarrow \text{[da iii., per la proposizione 8.6]}$$
      $n = f\left(x\right)$

      iii. Il sistema $\left\{ \begin{array}{l} n - x = \left\lfloor\frac{n}{n_1}\right\rfloor + \left\lfloor\frac{n}{n_2}\right\rfloor \\ n \bmod n_1 \neq 0 \\ n \bmod n_2 \neq 0 \end{array} \right.$ ha una sola soluzione [da A.]

      A. $\left(s-1\right) \nmid \left(x-1\right)$ [da B.]

      B. $s - 1 > x - 1$ [da v.]

      iv. $\left\lfloor\frac{n}{\text{MCM}(n_1,n_2)}\right\rfloor = 0$

      A. $n \equiv$ [da i.]

      $\text{t\_spazio}_T\left(x\right) <$ [da v., per monotonia di t_spazio]

      $\text{t\_spazio}_T\left(s\right) \leq$ [per definizione di s]

      $\text{MCM}\left(n_1, n_2\right)$

      v. $s > x$ [da (c)]

(d) Se $a \equiv \left\lfloor \frac{x}{s} \right\rfloor > 0$

i. Supponiamo che $\left\lfloor \frac{x'}{s} \right\rfloor < a \Rightarrow \text{t\_spazio}_T(x') = f\left(x' - \left\lfloor \frac{x'}{s} \right\rfloor\right)$ [ipotesi induttiva]

ii. $\text{t\_spazio}_T(x) =$ [da 5., per il corollario 3.6]
$\text{t\_spazio}_T(x - s) + \text{MCM}(n_1, n_2) =$ [da i.]
$f\left(x - s - \left\lfloor \frac{x-s}{s} \right\rfloor\right) + \text{MCM}(n_1, n_2) =$
$f\left(x - s - \left(\left\lfloor \frac{x}{s} \right\rfloor - 1\right)\right) + \text{MCM}(n_1, n_2) =$
$f\left(x - \left\lfloor \frac{x}{s} \right\rfloor - s + 1\right) + \text{MCM}(n_1, n_2) =$ [per la proposizione 8.3]
$f\left(x - \left\lfloor \frac{x}{s} \right\rfloor\right) - \text{MCM}(n_1, n_2) + \text{MCM}(n_1, n_2) =$
$f\left(x - \left\lfloor \frac{x}{s} \right\rfloor\right)$

4. Se $s \mid x$

(a) $\text{t\_spazio}_T(x) =$ [da (b), (b)–i., (c), (c)–i. e (c)–ii., per induzione]
$\text{MCM}(n_1, n_2) \frac{x}{s} - 1 =$
$\left\lceil \frac{n_i \frac{x}{s} (n_i - 1) \frac{\text{MCM}\left(n_i, n_j\right)}{n_i}}{n_i - 1} \right\rceil - 1 =$ [per la proprietà 2.21]
$\left\lfloor \frac{n_i \frac{x}{s} (n_i - 1) \frac{\text{MCM}\left(n_i, n_j\right)}{n_i} - 1}{n_i - 1} \right\rfloor =$ [per il teorema 8.1]
$\text{t\_spazio}_{T[i]}\left(\frac{x}{s}(n_i - 1) \frac{\text{MCM}(n_i, n_j)}{n_i}\right)$

(b) Se $\frac{x}{s} = 1$

i. $\text{t\_spazio}_T(x) =$ [da (b)]
$\text{t\_spazio}_T(s) =$ [per definizione di s e perché $\text{MCM}(n_1, n_2) - 1$ è uno spazio di T]
$\text{MCM}(n_1, n_2) - 1$

(c) Se $\frac{x}{s} > 1$

i. Supponiamo che per ogni y multiplo di s: $\frac{y}{s} < \frac{x}{s} \Rightarrow \text{t\_spazio}_T(y) = \text{MCM}(n_1, n_2) \frac{y}{s} - 1$

ii. $\text{t\_spazio}_T(x) =$[da 5., per il corollario 3.6]
$\text{t\_spazio}_T(x - s) + \text{MCM}(n_1, n_2) =$ [da i.]
$\text{MCM}(n_1, n_2) \frac{x-s}{s} + \text{MCM}(n_1, n_2) - 1 =$
$\text{MCM}(n_1, n_2) \frac{x}{s} - 1$

5. T è un tratteggio periodico finito con lunghezza di un periodo fondamentale pari a $\text{MCM}(n_1, n_2)$ [per la proposizione 4.8]

□

Appendice I - Calcolo di t_valore senza conoscere t

Finora l'unico modo che abbiamo per calcolare $\text{t\_valore}_T(x)$ è calcolando prima $\text{t}_T(x)$, essendo $\text{t\_valore}_T(x) = T(\text{t}_T(x))$. Tuttavia, si può concepire la funzione $\text{t\_valore}_T(x)$ svincolata da t_T, nel senso che si potrebbe calcolare la prima senza saper calcolare la seconda: in quest'appendice esploriamo proprio questa possibilità.

Notiamo anche che uno studio di $\text{t\_valore}_T(x)$ aggiungerebbe qualcosa di nuovo rispetto allo studio di t dei capitoli 6 e 7. Infatti t_valore_T, a differenza di t_T, non è iniettiva, dunque $\text{Down}_x^{T\to T'}(\text{t\_valore})$ e $\text{Up}_x^{T'\to T}(\text{t\_valore})$ possono contenere più di un elemento, per particolari scelte di x, T e T'. Di conseguenza, t_valore non è né downcast-sicura, né upcast-sicura (a differenza di t, che non è downcast-sicura ma è upcast-sicura).

La seguente congettura si può inquadrare nell'ambito del paragrafo 6.5, in quanto l'intento è di esprimere $\text{t\_valore}_T(x)$ come somma della stima del teorema 6.3 e di una opportuna correzione, qui indicata come $a(T,x)$:

Congettura 8.1. *Sia $T \equiv (n_1, n_2) \in \mathcal{L}^2$, con $n_1 < n_2$. Per ogni $x \in \mathbb{N}^\star$:*

$$\text{t\_valore}_T(x) = \left\lfloor \frac{n_1 n_2 x}{n_1 + n_2} \right\rfloor + a(T,x)$$

dove $a : \mathcal{L}^2 \times \mathbb{N}^\star \to \mathbb{N}$ è definita nel modo seguente:

$$a((m_1,m_2),x) = b((m_1,m_2), x \bmod s)$$

dove s è il numero di spazi di (m_1,m_2) minori di $\text{MCM}(n_1,n_2)$ e $b : \mathcal{L}^2 \times \mathbb{N}^\star \to \mathbb{N}$ è definita nel modo seguente:

$$b((m_1,m_2),x) = \begin{cases} c((m_1,m_2),x) & \text{se } m_2 \geq m_1(m_1-1) \\ d((m_1,m_2),x) & \text{altrimenti} \end{cases}$$

dove $c : \mathcal{L}^2 \times \mathbb{N}^\star \to \mathbb{N}$ *e* $d : \mathcal{L}^2 \times \mathbb{N}^\star \to \mathbb{N}$ *sono definite come segue:*

$$c\left((m_1, m_2), x\right) = \begin{cases} (k-1) \bmod m_1 + 1 & \text{se } \exists y \in \mathbb{N} : \left\lfloor \frac{(l-p)y}{l} \right\rfloor = r \\ \left(\begin{cases} \bar{n} \left\lfloor \frac{k}{n} \right\rfloor \bmod m_1 & \text{se } k \bmod n = 1 \\ (k-1) \bmod m_1 & \text{altrimenti} \end{cases} \right) & \text{altrimenti} \end{cases}$$

$$d\left((m_1, m_2), x\right) = \begin{cases} m \equiv c\left((m_1, m_2 + m_1^2), x + \left\lfloor \frac{\bar{n}(x-1)}{m_1^2} \right\rfloor\right) & \text{se } m \leq m_1 - \left\lfloor \frac{\bar{n}x}{m_1^2} \right\rfloor \\ c\left((m_1, m_2 + m_1^2), x + \left\lfloor \frac{\bar{n}(x-1)}{m_1^2} \right\rfloor + m_1 - m\right) - m_1 + m & \text{altrimenti} \end{cases}$$

dove:

- $n = \text{t\_valore}_{(m_1, m_2)}(x)$
- $r = \frac{\text{MCM}(m_1, m_2)}{m_2} - x + 1$
- $\bar{n} \equiv (m_2 - m_1 (m_1 - 1)) \bmod m_1^2$
- $p \equiv \frac{\text{MCM}\left(n_1^2, \bar{n}\right)}{\bar{n}}$
- $l \equiv \left\lceil \frac{n_2 - n_1(n_1-1)}{n_1^2} \right\rceil p + \frac{\text{MCM}\left(n_1^2, \bar{n}\right)}{n_1^2}$
- $k \equiv x - \left| \left\{ y \in \left[0, \frac{\text{MCM}(m_1, m_2)}{m_2}\right] \mid \left\lfloor \frac{(l-p)y}{l} \right\rfloor > x \right\} \right|$

Parte III

Tratteggi dei quozienti

Capitolo 9

L'algoritmo per il calcolo del M.C.M.

Se cerchi cose complicate, osserva meglio quelle semplici.

L'algoritmo per il calcolo del minimo comune multiplo (M.C.M. o MCM) è alla base della teoria dei tratteggi. Nato attraverso lo studio dei tratteggi lineari, ha portato in modo naturale alla definizione di un'altra classe di tratteggi, quelli dei quozienti. In questo capitolo vedremo alcune proprietà dell'algoritmo in sé; le proprietà dei tratteggi dei quozienti che da esso traggono origine sono oggetto della terza parte del libro.

L'algoritmo ha una forma "base" ed una generalizzata. Cominciamo dalla prima, perché è quella che fa emergere tutte le idee essenziali.

9.1 L'algoritmo per il calcolo del M.C.M. - forma base

L'algoritmo per il calcolo del M.C.M. ha come input due numeri $n_1, n_2 \in \mathbb{N}^\star$ e come output una terna $\left(k, (q_n)_{n=1,\dots,k}, (r_n)_{n=1,\dots,k}\right)$, dove $k \in \mathbb{N}^\star$ e $q_n, r_n \in \mathbb{N}$ per ogni $n \in \{1, \dots, k\}$. Lo pseudocodice è presente nel riquadro Algoritmo 9.1.

Esempio 9.1. *Applichiamo l'algoritmo con* $n_1 = 6$ *e* $n_2 = 8$*.*

Nella prima iterazione del ciclo si ha $n = 1$ *e dobbiamo dividere* $n_2 + r_0 = 8 + 0$ *per* $n_1 = 6$*:*

$$8 = 6 \cdot 1 + 2$$

da cui $q_1 = 1$ *ed* $r_1 = 2$*.*

Algoritmo 9.1 $\left(k, (q_n)_{n=1,\dots,k}, (r_n)_{n=1,\dots,k}\right) = \text{algoritmo\_MCM}\,(n_1, n_2)$

Input $n_1, n_2 \in \mathbb{N}^\star$
Output $k \in \mathbb{N}^\star$, $q_n, r_n \in \mathbb{N}$ per ogni $n \in \{1, \dots, k\}$
  $r_0 \leftarrow 0$
  $n \leftarrow 0$
  ripeti
    $n \leftarrow n + 1$
    $q_n \leftarrow \left\lfloor \frac{n_2 + r_{n-1}}{n_1} \right\rfloor$
    $r_n \leftarrow (n_2 + r_{n-1}) \bmod n_1$
  finché $r_n = 0$
  restituisci $\left(n, (q_n)_{n=1,\dots,k}, (r_n)_{n=1,\dots,k}\right)$

Nella seconda iterazione si ha $n = 2$ *e dobbiamo dividere* $n_2 + r_1 = 8 + 2 = 10$ *per* $n_1 = 6$*:*

$$10 = 6 \cdot 1 + 4$$

da cui $q_2 = 1$ *ed* $r_2 = 4$*.*

Nella terza iterazione si ha $n = 3$ *e dobbiamo dividere* $n_2 + r_2 = 8 + 4 = 12$ *per* $n_1 = 6$*:*

$$12 = 6 \cdot 2 + 0$$

da cui $q_3 = 2$ *ed* $r_3 = 0$*.*

Ora $r_n = r_3 = 0$*, quindi il ciclo termina e l'algoritmo restituisce l'intero* 3 *e le terne* $(r_1, r_2, r_3) = (2, 4, 0)$ *e* $(q_1, q_2, q_3) = (1, 1, 2)$*.*

Notazione 9.1. *Sia* $\left(k, (q_n)_{n=1,\dots,k}, (r_n)_{n=1,\dots,k}\right)$ *l'output dell'algoritmo per il calcolo del MCM con input* n_1*e* n_2*, e sia* $n \in \mathbb{N}^\star$*. Allora poniamo:*

$$\begin{aligned} k^{n_1,n_2} &\equiv k \\ q_n^{n_1,n_2} &\equiv \begin{cases} q_n & \text{se } 1 \le n \le k \\ q_{n \bmod^\star k} & \text{altrimenti} \end{cases} \end{aligned}$$

Inoltre, per $n \in \mathbb{N}$*, poniamo:*

$$r_n^{n_1,n_2} \equiv \begin{cases} 0 & \text{se } n = 0 \\ r_n & \text{se } 1 \le n \le k \\ r_{n \bmod^\star k} & \text{altrimenti} \end{cases}$$

Utilizzando le notazioni appena introdotte, dall'algoritmo segue che:

Osservazione 9.1. $\forall n \in \mathbb{N}^\star$*:*

- $q_n^{n_1,n_2} = \left\lfloor \frac{n_2 + r_{n-1}^{n_1,n_2}}{n_1} \right\rfloor$
- $r_n^{n_1,n_2} = \left(n_2 + r_{n-1}^{n_1,n_2}\right) \bmod n_1$
  - *In particolare,* $r_1^{n_1,n_2} = n_2 \bmod n_1$
- $r_n^{n_1,n_2} = 0 \Leftrightarrow k^{n_1,n_2} \mid n$

Dimostrazione. I primi due punti derivano rispettivamente dall'istruzione 7[1] e dall'istruzione 8.

Dimostriamo che $r_n^{n_1,n_2} = 0 \Leftrightarrow k^{n_1,n_2} \mid n$:

- Se $n = k^{n_1,n_2}$, vuol dire che l'algoritmo è appena terminato (perché k^{n_1,n_2} è per definizione l'ultimo valore assunto dalla variabile `n`), quindi la condizione `r_n > 0` è falsa, dunque `r_n = 0`. Allora, usando la notazione 9.1, `n` $= k^{n_1,n_2}$ e $0 =$ `r_n` $= r_n^{n_1,n_2} = r_{k^{n_1,n_2}}^{n_1,n_2}$
- Se $n < k^{n_1,n_2}$, ci vogliono altre iterazioni prima che l'algoritmo termini (perché il valore finale assunto da `n` è per definizione k^{n_1,n_2}), quindi la condizione `r_n > 0` è vera, cioè $r_n^{n_1,n_2} > 0$
- Se $n > k^{n_1,n_2}$ e $k^{n_1,n_2} \mid n$, $r_n^{n_1,n_2} = r_{n \bmod^\star k^{n_1,n_2}}^{n_1,n_2} = r_{k^{n_1,n_2}}^{n_1,n_2} = 0$
- Se $n > k^{n_1,n_2}$ e $k^{n_1,n_2} \nmid n$, $r_n^{n_1,n_2} = r_{n \bmod^\star k^{n_1,n_2}}^{n_1,n_2} = r_t^{n_1,n_2}$, con $0 < t < k$, dunque $r_n^{n_1,n_2} = r_t^{n_1,n_2} > 0$

□

Proposizione 9.1. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} \geq n_1 \Leftrightarrow r_n^{n_1,n_2} < r_1^{n_1,n_2}$.

Dimostrazione.

1. $r_n^{n_1,n_2} =$ [per l'osservazione 9.1]
   $\left(a_1 + r_{n-1}^{n_1,n_2}\right) \bmod n_1 =$ [per la proprietà 2.2]
   $\left(n_2 \bmod n_1 + r_{n-1}^{n_1,n_2}\right) \bmod n_1 =$ [per l'osservazione 9.1]
   $\left(r_1^{n_1,n_2} + r_{n-1}^{n_1,n_2}\right) \bmod n_1$
2. $r_{n-1}^{n_1,n_2} = r_{n-1}^{n_1,n_2} \bmod n_1$ [da $r_{n-1}^{n_1,n_2} < n_1$, perché si tratta di un resto modulo n_1]
3. $r_1^{n_1,n_2} = r_1^{n_1,n_2} \bmod n_1$ [da $r_1^{n_1,n_2} < n_1$, perché si tratta di un resto modulo n_1]
4. Se $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} \geq n_1$:

[1] Si intende: l'istruzione alla riga 7

(a) $r_{n-1}^{n_1,n_2} \bmod n_1 + r_1^{n_1,n_2} \bmod n_1 \geq n_1$ [da 2., 3. e 4.]

(b) $r_n^{n_1,n_2} =$ [da 1.]
$\left(r_1^{n_1,n_2} + r_{n-1}^{n_1,n_2}\right) \bmod n_1 =$ [da (a), per la proprietà 2.4]
$r_1^{n_1,n_2} \bmod n_1 + r_{n-1}^{n_1,n_2} \bmod n_1 - n_1 =$ [da 2. e 3.]
$r_1^{n_1,n_2} + r_{n-1}^{n_1,n_2} - n_1 <$ [da $r_{n-1}^{n_1,n_2} < n_1$]
$r_1^{n_1,n_2}$

5. Se $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} < n_1$

(a) $r_{n-1}^{n_1,n_2} \bmod n_1 + r_1^{n_1,n_2} \bmod n_1 < n_1$ [da 2., 3. e 5.]

(b) $r_n^{n_1,n_2} =$ [da 1.]
$\left(r_1^{n_1,n_2} + r_{n-1}^{n_1,n_2}\right) \bmod n_1 =$ [da (a), per la proprietà 2.4]
$r_1^{n_1,n_2} \bmod n_1 + r_{n-1}^{n_1,n_2} \bmod n_1 =$ [da 2. e 3.]
$r_1^{n_1,n_2} + r_{n-1}^{n_1,n_2} \geq$ [da $r_{n-1}^{n_1,n_2} \geq 0$]
$r_1^{n_1,n_2}$

6. $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} \geq n_1 \Leftrightarrow r_n^{n_1,n_2} < r_1^{n_1,n_2}$ [da 4.–(b) e 5.–(b)]

□

Proposizione 9.2. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $r_n^{n_1,n_2} = n_2 n \bmod n_1$.

Dimostrazione. Siano $n_1, n_2 \in \mathbb{N}^\star$ arbitrari.

La dimostrazione è per induzione su n.

1. Se $n = 1$

(a) $r_n^{n_1,n_2} = n_2 n \bmod n_1$ [da 1. per l'osservazione 9.1]

2. Se $n > 1$ e $r_{n-1}^{n_1,n_2} = n_2 (n-1) \bmod n_1$

(a) $r_n^{n_1,n_2} =$ [per l'osservazione 9.1]
$\left(n_2 + r_{n-1}^{n_1,n_2}\right) \bmod n_1 =$ [da 2.]
$(n_2 + n_2 (n-1) \bmod n_1) \bmod n_1 =$ [aggiunto e sottratto $n_2 (n-1)$]
$(n_2 n - n_2 (n-1) + n_2 (n-1) \bmod n_1) \bmod n_1 =$
$(n_2 n - (n_2 (n-1) - n_2 (n-1) \bmod n_1)) \bmod n_1 =$
$\left(n_2 n - n_1 \left\lfloor \frac{n_2 (n-1)}{n_1} \right\rfloor\right) \bmod n_1 =$ [per la proprietà 2.1]
$n_2 n \bmod n_1$

3. $\forall n \in \mathbb{N}^\star : r_n^{n_1,n_2} = n_2 n \bmod n_1$ [da 1.–(a) e 2.–(a), per il principio di induzione]

□

Corollario 9.1. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $r_n^{n_1,n_2} = r_1^{n_1,n_2} n \bmod n_1$.

Dimostrazione.

1. $r_n^{n_1,n_2} =$ [per la proposizione 9.2]
   $n_2 n \bmod n_1 =$ [divisione di n_2 per n_1 in $\mathbb{N}$]
   $\left(n_1 \left\lfloor \frac{n_2}{n_1} \right\rfloor + n_2 \bmod n_1\right) n \bmod n_1 =$
   $\left(n_1 \left\lfloor \frac{n_2}{n_1} \right\rfloor n + (n_2 \bmod n_1)\, n\right) \bmod n_1 =$ [per la proprietà 2.1]
   $(n_2 \bmod n_1)\, n \bmod n_1 =$ [per l'osservazione 9.1]
   $r_1^{n_1,n_2} n \bmod n_1$

□

Osservazione 9.2. *Applicando l'algoritmo per il calcolo del M.C.M. con input* n_1 *ed* n_2*, ed applicandolo con input* $r_1^{n_1,n_2}$ *ed* n_2*, si ottiene la stessa sequenza di resti.*

Dimostrazione. Il corollario 9.1 afferma che $r_n^{n_1,n_2} = r_1^{n_1,n_2} n \bmod n_1$. Applicando la proposizione 9.2, otteniamo che $r_1^{n_1,n_2} n \bmod n_1 = r_n^{r_1^{n_1,n_2},n_2}$. In definitiva, per transitività, $r_n^{n_1,n_2} = r_n^{r_1^{n_1,n_2},n_2}$ per ogni n, cioè la sequenza dei resti che si ottengono con input n_1 e n_2 è la stessa di quella che si ottiene con input $r_1^{n_1,n_2}$ ed n_1.

□

Corollario 9.2. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $q_n^{n_1,n_2} = \left\lfloor \frac{n_2 + n_2(n-1) \bmod n_1}{n_1} \right\rfloor$.

Dimostrazione.

1. $q_n^{n_1,n_2} =$ [per l'osservazione 9.1]
   $\left\lfloor \frac{n_2 + r_{n-1}^{n_1,n_2}}{n_1} \right\rfloor =$ [per la proposizione 9.2]
   $\left\lfloor \frac{n_2 + n_2(n-1) \bmod n_1}{n_1} \right\rfloor$

□

Proposizione 9.3. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $\sum_{i=1}^{n} q_i^{n_1,n_2} = \left\lfloor \frac{n_2 n}{n_1} \right\rfloor$.

Dimostrazione. Siano $n_1, n_2 \in \mathbb{N}^\star$ arbitrari. Procediamo per induzione su n.

1. Se $n = 1$

   (a) $\sum_{i=1}^{n} q_i^{n_1,n_2} =$ [da 1.]
   $q_1^{n_1,n_2} =$ [per l'osservazione 9.1]
   $\left\lfloor \frac{n_2 + r_0^{n_1,n_2}}{n_1} \right\rfloor =$
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor =$ [da 1.]
   $\left\lfloor \frac{n_2 n}{n_1} \right\rfloor$

2. Se $n > 1$ e $\sum_{i=1}^{n-1} q_i^{n_1,n_2} = \left\lfloor \frac{n_2(n-1)}{n_1} \right\rfloor$

   (a) $\sum_{i=1}^{n} q_i^{n_1,n_2} =$ [da 2., in particolare da $n > 1$]
   $\left(\sum_{i=1}^{n-1} q_i^{n_1,n_2}\right) + q_n^{n_1,n_2} =$ [da 2. (ipotesi di induzione)]
   $\left\lfloor \frac{n_2(n-1)}{n_1} \right\rfloor + q_n^{n_1,n_2} =$
   $\frac{n_2(n-1) - n_2(n-1) \bmod n_1}{n_1} + q_n^{n_1,n_2} =$ [per la 9.2]
   $\frac{n_2(n-1) - r_{n-1}^{n_1,n_2}}{n_1} + q_n^{n_1,n_2} =$ [per il corollario 9.2]
   $\frac{n_2(n-1) - r_{n-1}^{n_1,n_2}}{n_1} + \left\lfloor \frac{n_2 + n_2(n-1) \bmod n_1}{n_1} \right\rfloor =$
   $\frac{n_2(n-1) - r_{n-1}^{n_1,n_2}}{n_1} + \frac{n_2 + n_2(n-1) \bmod n_1 - (n_2 + n_2(n-1) \bmod n_1) \bmod n_1}{n_1} =$ [per la 9.2]
   $\frac{n_2(n-1) - r_{n-1}^{n_1,n_2}}{n_1} + \frac{n_2 + r_{n-1}^{n_1,n_2} - \left(n_2 + r_{n-1}^{n_1,n_2}\right) \bmod n_1}{n_1} =$ [per l'osservazione 9.1]
   $\frac{n_2(n-1) - r_{n-1}^{n_1,n_2}}{n_1} + \frac{n_2 + r_{n-1}^{n_1,n_2} - r_n^{n_1,n_2}}{n_1} =$
   $\frac{n_2 n - r_n^{n_1,n_2}}{n_1} =$ [per la 9.2]
   $\frac{n_2 n - n_2 n \bmod n_1}{n_1} =$
   $\left\lfloor \frac{n_2 n}{n_1} \right\rfloor$

3. $\forall n \in \mathbb{N}^\star : \sum_{i=1}^{n} q_i^{n_1,n_2} = \left\lfloor \frac{n_1 n}{n_2} \right\rfloor$ [da 1.–(a) e 2.–(a), per il principio di induzione]

□

Corollario 9.3. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $q_n^{n_1,n_2} = \left\lfloor \frac{n_2 n}{n_1} \right\rfloor - \left\lfloor \frac{n_2(n-1)}{n_1} \right\rfloor$.

Dimostrazione.

1. $q_n^{n_1,n_2} =$
   $\sum_{i=1}^{n} q_i^{n_1,n_2} - \sum_{i=1}^{n-1} q_i^{n_1,n_2} =$ [per la proposizione 9.3]
   $\left\lfloor \frac{n_2 n}{n_1} \right\rfloor - \left\lfloor \frac{n_2(n-1)}{n_1} \right\rfloor$

□

È interessante notare che, dai corollari 9.2 e 9.3 si ottiene che per ogni $n_1, n_2, n \in \mathbb{N}^\star$: $\left\lfloor \frac{n_2 n}{n_1} \right\rfloor - \left\lfloor \frac{n_2(n-1)}{n_1} \right\rfloor = \left\lfloor \frac{n_2 + n_2(n-1) \bmod n_1}{n_1} \right\rfloor$, poiché entrambi sono uguali a $q_n^{n_1,n_2}$. Sarebbe un buon esercizio dimostrare questa proprietà facendo uso di quelle viste nel paragrafo 2.2.

Proposizione 9.4. *Siano* $n_1, n_2, n \in \mathbb{N}^\star$. $q_n^{n_1,n_2} = \left\lfloor \frac{n_2}{n_1} \right\rfloor + (r_n^{n_1,n_2} < r_1^{n_1,n_2})$.

Dimostrazione.

1. $q_n^{n_1,n_2} =$ [per l'osservazione 9.1]
   $\left\lfloor \frac{n_2 + r_{n-1}^{n_1,n_2}}{n_1} \right\rfloor =$ [per la proprietà 2.21]
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor + \left\lfloor \frac{r_{n-1}^{n_1,n_2} + n_2 \bmod n_1}{n_1} \right\rfloor =$ [per l'osservazione 9.1]
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor + \left\lfloor \frac{r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2}}{n_1} \right\rfloor =$ [da 4. e 2.]
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor + \begin{cases} 0 & \text{se } r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} < n_1 \\ 1 & \text{altrimenti} \end{cases} \equiv$
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor + \left(r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} \geq n_1\right) =$ [per la proposizione 9.1]
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor + \left(r_n^{n_2,n_1} < r_1^{n_2,n_1}\right)$

2. $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} \geq n_1 \Rightarrow$

   (a) $1 =$
   $\left\lfloor \frac{n_1}{n_1} \right\rfloor \leq$ [da 2., per monotonia]
   $\left\lfloor \frac{r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2}}{n_1} \right\rfloor <$ [da 3., per la proprietà 2.25]
   $\left\lfloor \frac{2n_1}{n_1} \right\rfloor =$
   2

   (b) $\left\lfloor \frac{r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2}}{n_1} \right\rfloor = 1$ [da (a)]

3. $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} \leq$ [da $r_{n-1}^{n_1,n_2} < n_1$ e $r_1^{n_1,n_2} < n_1$]
   $n_1 - 1 + n_1 - 1 <$
   $2n_1 - 1 =$ [poiché $2n_1 \bmod n_1 = 0$]
   $2n_1 - 2n_1 \bmod n_1 - 1 =$ [divisione e moltiplicazione per n_1]
   $n_1 \frac{2n_1 - 2n_1 \bmod n_1}{n_1} - 1 =$
   $n_1 \left\lfloor \frac{2n_1}{n_1} \right\rfloor - 1$

4. $r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2} < n_1 \Rightarrow \left\lfloor \frac{r_{n-1}^{n_1,n_2} + r_1^{n_1,n_2}}{n_1} \right\rfloor = 0$

□

Proposizione 9.5. *Siano $n_1, n_2 \in \mathbb{N}^\star, k \in \mathbb{N}$. Allora:*

1. $kn_1 < n_2 < (k+1)\, n_1 \Rightarrow \begin{cases} \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \in \{k, k+1\} \\ \exists n' \in \mathbb{N}^\star : q_{n'}^{n_1,n_2} = k \\ \exists n'' \in \mathbb{N}^\star : q_{n''}^{n_1,n_2} = k+1 \end{cases}$
2. $n_2 = kn_1 \Rightarrow \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} = k$

Dimostrazione.

1. $kn_1 < n_2 < (k+1)\, n_1 \Rightarrow \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \in \{k, k+1\}$ [da (a) e (b)]

(a) Sia $kn_1 < n_2 < (k+1)\,n_1$, $n \in \mathbb{N}^\star$

(b) $k \leq q_n^{n_1,n_2} \leq k+1$ [da (c) e (d)]

(c) $q_n^{n_1,n_2} =$ [per la proposizione 9.4]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + (r_n^{n_1,n_2} < r_1^{n_1,n_2}) =$ [da (a), per la proprietà 2.23]
$k + (r_n^{n_1,n_2} < r_1^{n_1,n_2})$

(d) $0 \leq (r_n^{n_1,n_2} < r_1^{n_1,n_2}) \leq 1$ [per la notazione introdotta nel paragrafo 1.1.2]

2. $kn_1 < n_2 < (k+1)\,n_1 \Rightarrow \exists n' \in \mathbb{N}^\star : q_{n'}^{n_1,n_2} = k$ [da (a) e (b), ponendo $n' = 1$]

(a) Sia $kn_1 < n_2 < (k+1)\,n_1$

(b) $q_1^{n_1,n_2} =$ [per la proposizione 9.4]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + (r_1^{n_1,n_2} < r_1^{n_1,n_2}) =$ [banale, e per la notazione introdotta nel paragrafo 1.1.2]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor =$ [da (a), per la proprietà 2.23]
k

3. $kn_1 < n_2 < (k+1)\,n_1 \Rightarrow \exists n'' \in \mathbb{N}^\star : q_{n''}^{n_1,n_2} = k+1$ [da (a) e (b), ponendo $n'' = n_1$]

(a) Sia $kn_1 < n_2 < (k+1)\,n_1$

(b) $q_{n_1}^{n_1,n_2} =$ [per la proposizione 9.4]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + \left(r_{n_1}^{n_1,n_2} < r_1^{n_1,n_2}\right) =$ [banale, e per la notazione introdotta nel paragrafo 1.1.2]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + (r_1^{n_1,n_2} n_1 \bmod n_1 < r_1^{n_1,n_2}) =$ [per la proposizione 9.1]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + (0 < r_1^{n_1,n_2}) =$ [per la proposizione 9.2]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + (0 < n_2 \bmod n_1) =$ [da (a) si ha che $n_1 \nmid n_2$]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1 =$ [da (a), per la proprietà 2.23]
$k+1$

4. $n_2 = kn_1 \Rightarrow \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} = k$ [da (a) e (b)]

(a) Siano $n_2 = kn_1$, $n \in \mathbb{N}^\star$

(b) $q_n^{n_1,n_2} =$ [per la proposizione 9.2]
$\left\lfloor \frac{n_2 + n_2(x-1) \bmod n_1}{n_1} \right\rfloor =$ [da (a)]
$\left\lfloor \frac{kn_1 + kn_1(x-1) \bmod n_1}{n_1} \right\rfloor =$ [perché $n_1 \mid kn_1\,(x-1)$]
$\left\lfloor \frac{kn_1}{n_1} \right\rfloor =$
k

□

Corollario 9.4. *Siano $n_1, n_2 \in \mathbb{N}^\star, k \in \mathbb{N}$. Allora:*

- $\forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \leq k \Leftrightarrow n_2 \leq kn_1$
- $\forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \geq k \Leftrightarrow n_2 \geq kn_1$

Dimostrazione.

1. $\forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \leq k \Leftrightarrow n_2 \leq kn_1$ [da (a), (b) e 3.]
   (a) $n_2 < kn_1 \Rightarrow \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \leq k$ [da i. e ii.]
      i. Siano $n_2 < kn_1$, $n \in \mathbb{N}^\star$
      ii. $q_n^{n_1,n_2} \leq$ [per la proposizione 9.5]
      $\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1 \leq$ [da i., per la proprietà 2.25]
      $k - 1 + 1 =$ [calcoli]
      k
   (b) $n_2 > kn_1 \Rightarrow \exists n \in \mathbb{N}^\star : q_n^{n_1,n_2} > k$ [da i. e ii.]
      i. Sia $n_2 > kn_1$
      ii. $\exists n \in \mathbb{N}^\star : q_n^{n_1,n_2} > k$ [da A. e B.]
         A. $\exists n \in \mathbb{N}^\star : q_n^{n_1,n_2} = \left\lfloor \frac{n_2}{n_1} \right\rfloor + 1$ [per la proposizione 9.5]
         B. $\left\lfloor \frac{n_2}{n_1} \right\rfloor > k - 1$ [da i., per la proprietà 2.24]
2. $\forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \geq k \Leftrightarrow n_2 \geq kn_1$ [da (a), (b) e 3.]
   (a) $n_2 > kn_1 \Rightarrow \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} \geq k$ [da i. e ii.]
      i. Siano $n_2 > kn_1$, $n \in \mathbb{N}^\star$
      ii. $q_n^{n_1,n_2} \geq$ [per la proposizione 9.5]
      $\left\lfloor \frac{n_2}{n_1} \right\rfloor \geq$ [da i., per la proprietà 2.24]
      k
   (b) $n_2 < kn_1 \Rightarrow \exists n \in \mathbb{N}^\star : q_n^{n_1,n_2} < k$ [da i. e ii.]
      i. Sia $n_2 < kn_1$
      ii. $\exists n \in \mathbb{N}^\star : q_n^{n_1,n_2} < k$ [da A. e B.]
         A. $\exists n \in \mathbb{N}^\star : q_n^{n_1,n_2} = \left\lfloor \frac{n_2}{n_1} \right\rfloor$ [per la proposizione 9.5]
         B. $\left\lfloor \frac{n_2}{n_1} \right\rfloor < k$ [da i., per la proprietà 2.25]
3. $n_2 = kn_1 \Rightarrow \forall n \in \mathbb{N}^\star : q_n^{n_1,n_2} = k$

□

Vediamo ora il teorema che dà il nome all'algoritmo:

Teorema 9.1. *Siano* $n_1, n_2 \in \mathbb{N}^\star$. $k^{n_1,n_2} = \frac{\text{MCM}(n_1,n_2)}{n_2}$ *e* $\sum_{i=1}^{k^{n_1,n_2}} q_i^{n_1,n_2} = \frac{\text{MCM}(n_1,n_2)}{n_1}$.

Dimostrazione.

1. $n_2 k^{n_1,n_2} \bmod n_1 =$ [per la proposizione 9.2]
   $r_{k^{n_1,n_2}}^{n_1,n_2} =$ [per l'osservazione 9.1]
   0

2. $n_1 \mid n_2 k^{n_1,n_2}$ [da 1.]

3. $n_2 \mid n_2 k^{n_1,n_2}$

4. Se $\exists c \in \mathbb{N}$ tale che $n_2 \mid c$ e $n_1 \mid c$:

   (a) $c = n_2 h$ [da 4.]

   (b) $n_1 \mid n_2 h$ [da (a) e 4.]

   (c) $0 =$ [da (b)]
   $n_2 h \bmod n_1 =$ [per la proposizione 9.2]
   r_h

   (d) $k^{n_1,n_2} \mid h$ [da (c), per l'osservazione 9.1]

   (e) $n_2 k^{n_1,n_2} \mid$ [da (d)]
   $n_2 h =$ [da (a)]
   c

5. $n_2 k^{n_1,n_2} = \text{MCM}(n_1, n_2)$ [da 2., 3. e 4.–(e), per definizione di MCM]

6. $k^{n_1,n_2} = \frac{\text{MCM}(n_1,n_2)}{n_2}$ [da 5.]

7. $\sum_{i=1}^{k^{n_1,n_2}} q_i^{n_1,n_2} =$ [per la proposizione 9.3]
   $\left\lfloor \frac{n_2 k^{n_1,n_2}}{n_1} \right\rfloor =$
   $\frac{n_2 k^{n_1,n_2} - n_2 k^{n_1,n_2} \bmod n_1}{n_1} =$ [da 1.]
   $\frac{n_2 k^{n_1,n_2}}{n_1} =$ [da 5.]
   $\frac{\text{MCM}(n_1,n_2)}{n_1}$

□

Esempio 9.2. *Verifichiamo il teorema con gli stessi dati dell'esempio 9.3, ossia* $n_1 = 6$ *e* $n_2 = 8$. *Applicando l'algoritmo abbiamo ottenuto che* $k^{6,8} = 3$, $\left(r_1^{6,8}, r_2^{6,8}, r_3^{6,8}\right) = (2, 4, 0)$ *e* $\left(q_1^{6,8}, q_2^{6,8}, q_3^{6,8}\right) = (1, 1, 2)$. *Questi risultati sono in accordo col teorema 9.1. Infatti* $3 = k^{6,8} = \frac{\text{MCM}(6,8)}{8}$ *e* $4 = 1 + 1 + 2 = \sum_{i=1}^{3} q_i^{6,8} = \sum_{i=1}^{k^{6,8}} q_i^{6,8} = \frac{\text{MCM}(6,8)}{6}$.

Il teorema 9.1 fornisce un modo semplice per calcolare il minimo comune multiplo di due numeri naturali n_1 e n_2: basta applicare l'algoritmo e considerare $n_2 k^{n_1,n_2}$ o $n_1 \sum_{i=1}^{k^{n_1,n_2}} q_i^{n_1,n_2}$.

L'algoritmo per il calcolo del minimo comune multiplo assomiglia molto a quello di Euclide per il calcolo del massimo comun divisore. Dal punto di vista pratico, se si volesse davvero calcolare il minimo comune multiplo tra due numeri, conviene calcolare il massimo comun divisore con l'algoritmo di Euclide e ricavare da questo il minimo comune multiplo, grazie alla nota uguaglianza $\text{MCM}(n_1, n_2) = \frac{n_1 n_2}{\text{MCD}(n_1, n_2)}$, perché l'algoritmo di Euclide compie molte meno iterazioni di quante ne compirebbe il nostro algoritmo a parità di input. Tuttavia, il nostro algoritmo ha una grande importanza teorica nella teoria dei tratteggi, come vedremo a partire dal prossimo capitolo.

9.1.1 Approfondimenti

Per concretizzare quest'aspetto, applichiamo l'algoritmo con input $n_1 \equiv 5$ e $n_2 \equiv 8$ (il lettore può provare in seguito anche con l'esempio 9.1, che è un caso abbastanza degenere e perciò non lo consideriamo adesso):

$$\begin{aligned} 8 &= 1 \cdot 5 + 3 \\ 11 &= 2 \cdot 5 + 1 \\ 9 &= 1 \cdot 5 + 4 \\ 12 &= 2 \cdot 5 + 2 \\ 10 &= 2 \cdot 5 + 0 \end{aligned}$$

Quindi le sequenze dei resti e dei quozienti che si ottengono sono, rispettivamente,

$(r_1, r_2, r_3, r_4, r_5) = (3, 1, 4, 2, 0)$ e $(q_1, q_2, q_3, q_4, q_5) = (1, 2, 1, 2, 2)$

$$\begin{aligned} 5 &= 8 \cdot 0 + 5 \\ 10 &= 8 \cdot 1 + 2 \\ 7 &= 8 \cdot 0 + 7 \\ 12 &= 8 \cdot 1 + 4 \\ 9 &= 8 \cdot 1 + 1 \\ 6 &= 8 \cdot 0 + 6 \\ 11 &= 8 \cdot 1 + 3 \\ 8 &= 8 \cdot 1 + 0 \end{aligned}$$

Proposizione 9.6. *Siano $n_1, n_2, x \in \mathbb{N}^\star$. Allora, usando la notazione 9.1:*

$$\left|\{n \in \{1, \ldots, x\} \mid r_n^{n_1,n_2} < n_2 \bmod n_1\}\right| = \left\lfloor \frac{x\,(n_2 \bmod n_1)}{n_1} \right\rfloor$$

Dimostrazione.

1. $|\{n \in \{1, \ldots, x\} \mid r_n^{n_1,n_2} < n_2 \bmod n_1\}| =$ [per il corollario 9.1]
   $|\{n \in \{1, \ldots, x\} \mid r_n^{n_1,n_2} < r_1^{n_1,n_2}\}| =$ [usando la notazione 9.1]
   $|\{n \in \{1, \ldots, x\} \mid r_1^{n_1,n_2} n \bmod n_1 < r_1^{n_1,n_2}\}| =$ [da 2., 3., 4. e 5.]
   $\left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor =$ [usando la notazione 9.1]
   $\left\lfloor \frac{x(n_2 \bmod n_1)}{n_1} \right\rfloor$
2. Sia $A \equiv \{n \in \{1, \ldots, x\} \mid r_1^{n_1,n_2} n \bmod n_1 < r_1^{n_1,n_2}\}$
3. $|A| =$ [da 4. e 5.]
   $\left|\left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right]\right| =$ [per defninizione di intervallo]
   $\left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor$
4. Sia $f : \left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right] \to \mathbb{N}$ tale che per ogni $k \in \left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right]$ $f(k) = \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil$
5. f è una biezione tra $\left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right]$ e A [da (a), (b) e (c)]
   (a) f è iniettiva
      i. Siano $a, b \in \left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right]$
      ii. $f(a) = f(b) \Leftrightarrow$ [da 4.]
      $\left\lceil \frac{n_1 a}{r_1^{n_1,n_2}} \right\rceil = \left\lceil \frac{n_1 b}{r_1^{n_1,n_2}} \right\rceil \Leftrightarrow$ [per la proprietà 2.23]
      $r_1^{n_1,n_2} \left(\left\lceil \frac{n_1 b}{r_1^{n_1,n_2}} \right\rceil - 1 \right) < n_1 a \leq r_1^{n_1,n_2} \left\lceil \frac{n_1 b}{r_1^{n_1,n_2}} \right\rceil \Leftrightarrow$

$r_1^{n_1,n_2}\left(\frac{n_1b-n_1b \bmod^\star r_1^{n_1,n_2}}{r_1^{n_1,n_2}}+1-1\right)<n_1a\leq r_1^{n_1,n_2}\left(\frac{n_1b-n_1b \bmod^\star r_1^{n_1,n_2}}{r_1^{n_1,n_2}}+1\right)\Leftrightarrow$
$n_1b-n_1b \bmod^\star r_1^{n_1,n_2}<n_1a\leq n_1b-n_1b \bmod^\star r_1^{n_1,n_2}+r_1^{n_1,n_2}\Leftrightarrow$ [sottraendo $n_1b-n_1b \bmod^\star r_1^{n_1,n_2}$]
$-n_1b \bmod^\star r_1^{n_1,n_2}<n_1a-n_1b\leq -n_1b \bmod^\star r_1^{n_1,n_2}+r_1^{n_1,n_2}\Leftrightarrow$
$n_1b \bmod^\star r_1^{n_1,n_2}>n_1b-n_1a\geq n_1b \bmod^\star r_1^{n_1,n_2}-r_1^{n_1,n_2}\Rightarrow$ [da iii., iii–A., iv., iv.–A., v., v.–A.]
$a=b$

iii. Se $a=b$

A. $n_1b \bmod^\star r_1^{n_1,n_2}>n_1b-n_1a\geq n_1b \bmod^\star r_1^{n_1,n_2}-r_1^{n_1,n_2}\Leftrightarrow$ [da iii.]
$n_1b \bmod^\star r_1^{n_1,n_2}>0\geq n_1b \bmod^\star r_1^{n_1,n_2}-r_1^{n_1,n_2}\Leftrightarrow$ [perché $0<n_1b \bmod^\star r_1^{n_1,n_2}\leq r_1^{n_1,n_2}$]
T

iv. Se $a<b$

A. $n_1b \bmod^\star r_1^{n_1,n_2}>n_1b-n_1a\geq n_1b \bmod^\star r_1^{n_1,n_2}-r_1^{n_1,n_2}\Rightarrow$
$n_1b \bmod^\star r_1^{n_1,n_2}>n_1b-n_1a\Leftrightarrow$
$n_1b \bmod^\star r_1^{n_1,n_2}>n_1(b-a)\Rightarrow$ [da iv.]
$n_1b \bmod^\star r_1^{n_1,n_2}\geq n_1\Leftrightarrow$ [perché $n_1b \bmod^\star r_1^{n_1,n_2}\leq r_1^{n_1,n_2}=n_2 \bmod n_1<n_1$]
F

v. Se $a>b$

A. $n_1b \bmod^\star r_1^{n_1,n_2}>n_1b-n_1a\geq n_1b \bmod^\star r_1^{n_1,n_2}-r_1^{n_1,n_2}\Rightarrow$
$n_1b-n_1a\geq n_1b \bmod^\star r_1^{n_1,n_2}-r_1^{n_1,n_2}\Leftrightarrow$
$n_1(a-b)\geq r_1^{n_1,n_2}-n_1b \bmod^\star r_1^{n_1,n_2}\Leftrightarrow$ [da v.]
$n_1\geq r_1^{n_1,n_2}-n_1b \bmod^\star r_1^{n_1,n_2}\Rightarrow$
$n_1\geq r_1^{n_1,n_2}\Leftrightarrow$ [perché $r_1^{n_1,n_2}=n_2 \bmod n_1<n_1$]
F

(b) $f\left(\left[1,\left\lfloor\frac{xr_1^{n_1,n_2}}{n_1}\right\rfloor\right]\right)\subseteq A$

i. Sia $k\in\left[1,\left\lfloor\frac{xr_1^{n_1,n_2}}{n_1}\right\rfloor\right]$

ii. $f(k)\in A$ [da iii. e iv.]

iii. $f(k)\in\{1,\ldots,x\}$ [da i. e A.]

A. $1\leq k\leq\left\lfloor\frac{xr_1^{n_1,n_2}}{n_1}\right\rfloor\Leftrightarrow$ [per monotonia della parte intera]
$\left\lceil\frac{n_1}{r_1^{n_1,n_2}}\right\rceil\leq\left\lceil\frac{n_1k}{r_1^{n_1,n_2}}\right\rceil\leq\left\lceil\frac{n_1\left\lfloor\frac{xr_1^{n_1,n_2}}{n_1}\right\rfloor}{r_1^{n_1,n_2}}\right\rceil\Leftrightarrow$ [perché $n_1>n_2 \bmod n_1=r_1^{n_1,n_2}$]

$1 \leq \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil \leq \left\lceil \frac{n_1 \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor}{r_1^{n_1,n_2}} \right\rceil \Leftrightarrow$

$1 \leq \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil \leq \left\lceil \frac{n_1 \frac{x r_1^{n_1,n_2} - x r_1^{n_1,n_2} \bmod n_1}{n_1}}{r_1^{n_1,n_2}} \right\rceil \Leftrightarrow$

$1 \leq \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil \leq \left\lceil \frac{x r_1^{n_1,n_2} - x r_1^{n_1,n_2} \bmod n_1}{r_1^{n_1,n_2}} \right\rceil \Rightarrow$ [per monotonia della parte intera]

$1 \leq \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil \leq \left\lceil \frac{x r_1^{n_1,n_2}}{r_1^{n_1,n_2}} \right\rceil \Leftrightarrow$

$1 \leq \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil \leq x \Leftrightarrow$ [da 4.]

$1 \leq f(k) \leq x$

iv. $r_1^{n_1,n_2} f(k) \bmod n_1 =$ [da 4.]

$r_1^{n_1,n_2} \left\lceil \frac{n_1 k}{r_1^{n_1,n_2}} \right\rceil \bmod n_1 =$

$r_1^{n_1,n_2} \left(\frac{n_1 k - n_1 k \bmod^\star r_1^{n_1,n_2}}{r_1^{n_1,n_2}} + 1 \right) \bmod n_1 =$

$(n_1 k - n_1 k \bmod^\star r_1^{n_1,n_2} + r_1^{n_1,n_2}) \bmod n_1 =$ [per la proprietà 2.1]

$(r_1^{n_1,n_2} - n_1 k \bmod^\star r_1^{n_1,n_2}) \bmod n_1 =$ [per la proprietà 2.14]

$((n_1 k r_1^{n_1,n_2} - n_1 k) \bmod r_1^{n_1,n_2}) \bmod n_1 =$ [perché $(n_1 k r_1^{n_1,n_2} - n_1 k) \bmod r_1^{n_1,n_2} < r_1^{n_1,n_2} = n_2 \bmod n_1 < n_1$]

$(n_1 k r_1^{n_1,n_2} - n_1 k) \bmod r_1^{n_1,n_2} < r_1^{n_1,n_2}$

(c) $f\left(\left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right]\right) \supseteq A$

i. Sia $n \in A$

ii. $f\left(\left\lfloor \frac{n r_1^{n_1,n_2}}{n_1} \right\rfloor\right) =$ [da 4.]

$\left\lceil \frac{n_1 \left\lfloor \frac{n r_1^{n_1,n_2}}{n_1} \right\rfloor}{r_1^{n_1,n_2}} \right\rceil =$

$\left\lceil \frac{n_1 \frac{n r_1^{n_1,n_2} - n r_1^{n_1,n_2} \bmod n_1}{n_1}}{r_1^{n_1,n_2}} \right\rceil =$

$\left\lceil \frac{n r_1^{n_1,n_2} - n r_1^{n_1,n_2} \bmod n_1}{r_1^{n_1,n_2}} \right\rceil =$ [per la proprietà 2.20]

$n - \left\lfloor \frac{n r_1^{n_1,n_2} \bmod n_1}{r_1^{n_1,n_2}} \right\rfloor =$ [da A.]

n

A. $n r_1^{n_1,n_2} \bmod n_1 < r_1^{n_1,n_2}$ [da i.]

iii. $\left\lfloor \frac{n r_1^{n_1,n_2}}{n_1} \right\rfloor \in \left[1, \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor\right]$

A. $\left\lfloor \frac{n r_1^{n_1,n_2}}{n_1} \right\rfloor \leq \left\lfloor \frac{x r_1^{n_1,n_2}}{n_1} \right\rfloor$ [per monotonia della parte intera e da B.]

B. $1 \leq n \leq x$ [da i.]

C. $\left\lfloor \frac{n r_1^{n_1,n_2}}{n_1} \right\rfloor \geq 1$ [perché $\left\lfloor \frac{n r_1^{n_1,n_2}}{n_1} \right\rfloor \geq 0$ e da D.]

D. $\left\lfloor \frac{nr_1^{n_1,n_2}}{n_1} \right\rfloor = 0 \Leftrightarrow$
$nr_1^{n_1,n_2} < n_1 \Leftrightarrow$
$r_1^{n_1,n_2} n < n_1 \Rightarrow$
$r_1^{n_1,n_2} n \bmod n_1 = r_1^{n_1,n_2} n \Rightarrow$ [da B.]
$r_1^{n_1,n_2} n \bmod n_1 \geq r_1^{n_1,n_2} \Rightarrow$ [perché $n \in A \Rightarrow r_1^{n_1,n_2} n \bmod n_1 < r_1^{n_1,n_2}$]
$n \notin A$

□

Corollario 9.5. *Siano $n_1, n_2, x \in \mathbb{N}^\star$. Allora, usando la notazione 9.1:*

$$|\{n \in \{1, \ldots, k^{n_1,n_2}\} \mid r_n^{n_1,n_2} < n_2 \bmod n_1\}| = \left\lfloor \frac{n_2 \bmod n_1}{\mathrm{MCD}\,(n_1, n_2)} \right\rfloor$$

Dimostrazione. Basta porre $x = k^{n_1,n_2}$ nella proposizione 9.6, ottenendo:

1. $|\{n \in \{1, \ldots, k^{n_1,n_2}\} \mid r_n^{n_1,n_2} < n_2 \bmod n_1\}| =$ [per la proposizione 9.6]
$\left\lfloor \frac{k^{n_1,n_2}(n_2 \bmod n_1)}{n_1} \right\rfloor =$ [per il teorema 9.1]
$\left\lfloor \frac{\frac{\mathrm{MCM}(n_1,n_2)}{n_2}(n_2 \bmod n_1)}{n_1} \right\rfloor =$
$\left\lfloor \frac{\mathrm{MCM}(n_1,n_2)(n_2 \bmod n_1)}{n_1 n_2} \right\rfloor =$ [perché $\mathrm{MCD}\,(n_1, n_2)\,\mathrm{MCM}\,(n_1, n_2) = n_1 n_2$]
$\left\lfloor \frac{n_2 \bmod n_1}{\mathrm{MCD}(n_1,n_2)} \right\rfloor$

□

Mediante la proposizione 9.6 possiamo dimostrare in modo più elegante la proposizione 9.3:

Dimostrazione. 1. $\sum_{i=1}^{n} q_i^{n_1,n_2} =$ [per la proposizione 9.4]
$\sum_{i=1}^{n} \left(\left\lfloor \frac{n_2}{n_1} \right\rfloor + (r_i^{n_1,n_2} < r_1^{n_1,n_2}) \right) =$
$\sum_{i=1}^{n} \left\lfloor \frac{n_2}{n_1} \right\rfloor + \sum_{i=1}^{n} (r_i^{n_1,n_2} < r_1^{n_1,n_2}) =$
$n \left\lfloor \frac{n_2}{n_1} \right\rfloor + \sum_{i=1}^{n} (r_i^{n_1,n_2} < r_1^{n_1,n_2}) =$
$n \left\lfloor \frac{n_2}{n_1} \right\rfloor + |\{i \in \{1, \ldots, n\} \mid r_i^{n_1,n_2} < r_1^{n_1,n_2}\}| =$ [per la proposizione 9.6, ricordando che $r_1^{n_1,n_2} = n_2 \bmod n_1$]
$n \left\lfloor \frac{n_2}{n_1} \right\rfloor + \left\lfloor \frac{n(n_2 \bmod n_1)}{n_1} \right\rfloor =$ [per la proprietà 2.27]
$\left\lfloor \frac{n_2 n}{n_1} \right\rfloor$

□

Proposizione 9.7. *Siano $n_1, n_2, x \in \mathbb{N}^\star$. Allora, usando la notazione 9.1, l'x-esimo $y \in \mathbb{N}^\star$ tale che $r_y^{n_1,n_2} < n_2 \bmod n_1$ è:*

$$\left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil$$

Dimostrazione.

1. L'x-esimo $y \in \mathbb{N}^\star$ tale che $r_y^{n_1,n_2} < n_2 \bmod n_1$ è $\left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil$ [da 2.]
2. n è l'x-esimo $y \in \mathbb{N}^\star$ tale che $r_y^{n_1,n_2} < n_2 \bmod n_1$ se e solo se $n = \left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil$ [da 3., per il lemma del conteggio (lemma 3.1)]
3. $\begin{cases} \left|\left\{y \in \{1,\dots,n\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x \\ \left|\left\{y \in \{1,\dots,n-1\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x-1 \end{cases} \Leftrightarrow n = \left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil$ [da 4. e 5.]
4. $\begin{cases} \left|\left\{y \in \{1,\dots,n\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x \\ \left|\left\{y \in \{1,\dots,n-1\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x-1 \end{cases} \Rightarrow n = \left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil$ [da (a), (b) e (c)]
   (a) Sia $\left|\left\{y \in \{1,\dots,n\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x$
   (b) Sia $\left|\left\{y \in \{1,\dots,n-1\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x-1$
   (c) $n = \left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil$ [da i., per la proprietà 2.23]
      i. $(n_2 \bmod n_1)(n-1) < n_1 x \le (n_2 \bmod n_1)\, n$ [da ii. e iii.]
      ii. $n_1 (x-1) \le (n-1)(n_2 \bmod n_1) < n_1 x$ [da A., per la proprietà 2.23]
         A. $x - 1 = \left\lfloor \frac{(n-1)(n_2 \bmod n_1)}{n_1} \right\rfloor$ [da (a), per la proposizione 9.6]
      iii. $n_1 x \le n\,(n_2 \bmod n_1) < n_1 (x+1)$ [da A., per la proprietà 2.23]
         A. $x = \left\lfloor \frac{n(n_2 \bmod n_1)}{n_1} \right\rfloor$ [da (b), per la proposizione 9.6]
5. $n = \left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil \Rightarrow \begin{cases} \left|\left\{y \in \{1,\dots,n\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x \\ \left|\left\{y \in \{1,\dots,n-1\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x-1 \end{cases}$ [da (a)]
   (a) $\begin{cases} \left|\left\{y \in \left\{1,\dots,\left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil\right\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x \\ \left|\left\{y \in \left\{1,\dots,\left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil - 1\right\} \mid r_y^{n_1,n_2} < n_2 \bmod n_1\right\}\right| = x-1 \end{cases}$ [da (b), per la proposizione 9.6]
   (b) $\begin{cases} \left\lfloor \frac{\left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil (n_2 \bmod n_1)}{n_1} \right\rfloor = x \\ \left\lfloor \frac{\left(\left\lceil \frac{n_1 x}{n_2 \bmod n_1} \right\rceil - 1\right)(n_2 \bmod n_1)}{n_1} \right\rfloor = x-1 \end{cases}$ [da (c), per definizione]

(c) $\begin{cases} \left\lfloor \frac{\left(\frac{n_1 x - n_1 x \bmod^\star (n_2 \bmod n_1)}{n_2 \bmod n_1} + 1\right)(n_2 \bmod n_1)}{n_1} \right\rfloor = x \\ \left\lfloor \frac{\frac{n_1 x - n_1 x \bmod^\star (n_2 \bmod n_1)}{n_2 \bmod n_1}(n_2 \bmod n_1)}{n_1} \right\rfloor = x - 1 \end{cases}$ [da (d), calcoli algebrici]

(d) $\begin{cases} \left\lfloor \frac{n_1 x - n_1 x \bmod^\star (n_2 \bmod n_1) + n_2 \bmod n_1}{n_1} \right\rfloor = x \\ \left\lfloor \frac{n_1 x - n_1 x \bmod^\star (n_2 \bmod n_1)}{n_1} \right\rfloor = x - 1 \end{cases}$ [da (e), per la proprietà 2.23]

(e) $\begin{cases} n_1 x \leq n_1 x - n_1 x \bmod^\star (n_2 \bmod n_1) + n_2 \bmod n_1 < n_1 (x+1) \\ n_1 (x-1) \leq n_1 x - n_1 x \bmod^\star (n_2 \bmod n_1) < n_1 x \end{cases}$ [da (f), calcoli algebrici]

(f) $\begin{cases} 0 \leq n_2 \bmod n_1 - n_1 x \bmod^\star (n_2 \bmod n_1) < n_1 \\ 0 \leq n_1 - n_1 x \bmod^\star (n_2 \bmod n_1) < n_1 \end{cases}$ [da (g), (h), (i) ed (l)]

(g) $0 \leq n_2 \bmod n_1 - n_1 x \bmod^\star (n_2 \bmod n_1)$ [da i.]

i. $n_1 x \bmod^\star (n_2 \bmod n_1) \leq n_2 \bmod n_1$

(h) $n_2 \bmod n_1 - n_1 x \bmod^\star (n_2 \bmod n_1) <$ [perché $n_1 x \bmod^\star (n_2 \bmod n_1) > 0$]
$n_2 \bmod n_1 <$
n_1

(i) $0 \leq n_1 - n_1 x \bmod^\star (n_2 \bmod n_1)$ [da i.]

i. $n_1 x \bmod^\star (n_2 \bmod n_1) \leq$
$n_2 \bmod n_1 \leq$
n_1

(j) $n_1 - n_1 x \bmod^\star (n_2 \bmod n_1) < n_1$ [perché $n_1 x \bmod^\star (n_2 \bmod n_1) > 0$]

□

Concludiamo questo paragrafo di approfondimento con un'osservazione sulle sequenze dei resti e dei quozienti che si ottengono applicando l'algoritmo. Considerando ad esempio gli input $n_1 \equiv 8$ e $n_2 \equiv 5$, come abbiamo visto prima, si ottengono le sequenza $(r_1, \ldots, r_8) = (5, 2, 7, 4, 1, 6, 3, 0)$ e $(q_1, \ldots, q_8) = (0, 1, 0, 1, 1, 0, 1, 1)$.

La prima osservazione è che la sequenza dei quozienti è simmetrica, a parte il primo e l'ultimo quoziente, che, se $n_1 \neq n_2$, sono sempre rispettivamente $\left\lfloor \frac{n_2}{n_1} \right\rfloor$ e $\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1$. Nell'esempio, $q_1 = 0 = \left\lfloor \frac{5}{8} \right\rfloor$, $q_2 = q_7 = 1$, $q_3 = q_6 = 0$, $q_4 = q_5 = 1$, $q_8 = 1 = \left\lfloor \frac{5}{8} \right\rfloor + 1$.

La seconda osservazione è che sommando i resti in posizione simmetrica, si ottiene un numero del tipo $n_2 \bmod n_1 + k n_1$, $k \in \mathbb{N}$. Nell'esempio, si ha $r_1 + r_8 = 5 + 0 = 5 = 5 \bmod 8$, $r_2 + r_7 = 2 + 3 = 5$, $r_3 + r_6 = 7 + 6 = 13 = 5 + 8 = 5 \bmod 8 + 8$, $r_4 + r_5 = 4 + 1 = 5$.

Proponiamo come esercizio per il lettore la dimostrazione delle seguenti proposizioni:

Proposizione 9.8. *Siano $n_1, n_2 \in \mathbb{N}^\star$. Allora, usando la notazione 9.1, per ogni $i, j \in \mathbb{N}^\star$:*

$$i + j = k^{n_1,n_2} + 1 \Rightarrow \left(r_i^{n_1,n_2} + r_j^{n_1,n_2}\right) \bmod n_1 = n_2 \bmod n_1$$

Proposizione 9.9. *Siano $n_1, n_2 \in \mathbb{N}^\star$, $n_1 \neq n_2$. Allora, usando la notazione 9.1, per ogni $i, j \in \mathbb{N}^\star$:*

$$i + j = k^{n_1,n_2} + 1 \Rightarrow q_i + q_j = 2\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1$$

Riguardo la seconda proposizione, si osservi che, poiché, per la proposizione 9.4, tutti i quozienti possono essere uguali o a $\left\lfloor \frac{n_2}{n_1} \right\rfloor$ o a $\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1$, dire che la somma di due quozienti è $2\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1$ equivale a dire che uno è $\left\lfloor \frac{n_2}{n_1} \right\rfloor$ e l'altro è $\left\lfloor \frac{n_2}{n_1} \right\rfloor + 1$.

9.2 L'algoritmo per il calcolo del M.C.M. - forma generalizzata

Vediamo ora una forma generalizzata dell'algoritmo per il calcolo del MCM, che come caso particolare ha l'algoritmo già analizzato. L'algoritmo generalizzato ha come input $m > 1$ numeri $n_1, \ldots, n_m \in \mathbb{N}^\star$ e come output una terna

$$\left(k, Q \equiv \begin{pmatrix} q_{1,1} & \cdots & q_{1,k} \\ \vdots & \ddots & \vdots \\ q_{m-1,1} & \cdots & q_{m-1,k} \end{pmatrix}, R \equiv \begin{pmatrix} r_{1,1} & \cdots & r_{1,k} \\ \vdots & \ddots & \vdots \\ r_{m-1,1} & \cdots & r_{m-1,k} \end{pmatrix} \right)$$

dove $k \in \mathbb{N}^\star$ e $Q \in \mathbb{N}^{m-1\times k}$,$R \in \mathbb{N}^{m-1\times k}$. Lo pseudocodice è presente nel riquadro Algoritmo 9.2.

Esempio 9.3. *Applichiamo l'algoritmo con $a_1 = 5$ e $a_2 = 4$ e $a_3 = 6$.*

Nella prima iterazione del ciclo si ha $n = 1$ e dobbiamo dividere $a_3 + r_{1,0} = 6 + 0$ per $a_1 = 5$ e $a_3 + r_{2,0} = 6 + 0$ per $a_2 = 4$:

$$\begin{cases} 6 = 5 \cdot 1 + 1 \\ 6 = 4 \cdot 1 + 2 \end{cases}$$

da cui $q_{1,1} = 1$, $q_{2,1} = 1$, $r_{1,1} = 1$ ed $r_{2,1} = 2$.

Algoritmo 9.2 $\left(k, Q \equiv \begin{pmatrix} q_{1,1} & \cdots & q_{1,k} \\ \vdots & \ddots & \vdots \\ q_{m-1,1} & \cdots & q_{m-1,k} \end{pmatrix}, R \equiv \begin{pmatrix} r_{1,1} & \cdots & r_{1,k} \\ \vdots & \ddots & \vdots \\ r_{m-1,1} & \cdots & r_{m-1,k} \end{pmatrix}\right) =$ algoritmo_MCM $(n_1, \ldots, n_m)$

Input $n_1, \ldots, n_m \in \mathbb{N}^\star$
Output $k \in \mathbb{N}^\star$, $Q \in \mathbb{N}^{m-1\times k}$,$R \in \mathbb{N}^{m-1\times k}$
  per $i = 1m-1$ **esegui**
    $r_{i,0} \leftarrow 0$
  fine per
  $n \leftarrow 0$
  ripeti
    $n \leftarrow n+1$
    per $i = 1m-1$ **esegui**
      $q_{i,n} \leftarrow \left\lfloor \frac{n_m + r_{i,n-1}}{n_i} \right\rfloor$
      $r_{i,n} \leftarrow (n_m + r_{i,n-1}) \bmod n_i$
    fine per
  finché $\forall i \in \{1, \ldots, m-1\} : r_{i,n} = 0$
  restituisci (n, Q, R)

Nella seconda iterazione si ha $n = 2$ *e dobbiamo dividere* $a_3 + r_{1,1} = 6 + 1 = 7$ *per* $a_1 = 5$ *e* $a_3 + r_{2,1} = 6 + 2 = 8$ *per* $a_2 = 4$*:*

$$\begin{cases} 7 = 5 \cdot 1 + 2 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

da cui $q_{1,2} = 1$*,* $q_{2,2} = 2$*,* $r_{1,2} = 2$ *ed* $r_{2,2} = 0$*.*

Procedendo in questo modo fino ad ottenere $r_{1,n} = r_{2,n} = 0$ *per qualche* n*, si effettuano le seguenti divisioni:*

$$\begin{cases} 8 = 5 \cdot 1 + 3 \\ 6 = 4 \cdot 1 + 2 \end{cases}$$

$$\begin{cases} 9 = 5 \cdot 1 + 4 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

$$\begin{cases} 10 = 5 \cdot 2 + 0 \\ 6 = 4 \cdot 1 + 2 \end{cases}$$

$$\begin{cases} 6 = 5 \cdot 1 + 1 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

$$\begin{cases} 7 = 5 \cdot 1 + 2 \\ 6 = 4 \cdot 1 + 2 \end{cases}$$

$$\begin{cases} 8 = 5 \cdot 1 + 3 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

$$\begin{cases} 9 = 5 \cdot 1 + 4 \\ 6 = 4 \cdot 1 + 2 \end{cases}$$

$$\begin{cases} 10 = 5 \cdot 2 + 0 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

Siamo usciti dal ciclo principale con $n = 10$, quindi l'algoritmo restituisce l'intero 10 e le matrici

$$\begin{pmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} & r_{1,5} & r_{1,6} & r_{1,7} & r_{1,8} & r_{1,9} & r_{1,10} \\ r_{2,1} & r_{2,2} & r_{2,3} & r_{2,4} & r_{2,5} & r_{2,6} & r_{2,7} & r_{2,8} & r_{2,9} & r_{2,10} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} q_{1,1} & q_{1,2} & q_{1,3} & q_{1,4} & q_{1,5} & q_{1,6} & q_{1,7} & q_{1,8} & q_{1,9} & q_{1,10} \\ q_{2,1} & q_{2,2} & q_{2,3} & q_{2,4} & q_{2,5} & q_{2,6} & q_{2,7} & q_{2,8} & q_{2,9} & q_{2,10} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \end{pmatrix}$$

D'ora in poi chiamaremo l'algoritmo della definizione 9.2 "algoritmo generalizzato" e l'algoritmo della definizione 9.1 "algoritmo base". Se $m = 2$, l'algoritmo generalizzato si comporta esattamente come quello base.

Notazione 9.2. *Sia* $\left(k, \begin{pmatrix} q_{1,1} & \cdots & q_{1,k} \\ \vdots & \ddots & \vdots \\ q_{m-1,1} & \cdots & q_{m-1,k} \end{pmatrix}, \begin{pmatrix} r_{1,1} & \cdots & r_{1,k} \\ \vdots & \ddots & \vdots \\ r_{m-1,1} & \cdots & r_{m-1,k} \end{pmatrix}\right)$ *l'output dell'algoritmo con input $n_1, \ldots, n_m$ e sia $n \in \mathbb{N}^\star$. Allora poniamo:*

- $k^{n_1,\ldots,n_m} \equiv k$
- $q_{i,n}^{n_1,\ldots,n_m} \equiv \begin{cases} q_{i,n} & \text{se } 1 \leq n \leq k \\ q_{i,n \bmod^\star k} & \text{altrimenti} \end{cases}$ *per ogni* $i \in \{1, \ldots, m-1\}$
- $r_{i,n}^{n_1,\ldots,n_m} \equiv \begin{cases} 0 & \text{se } n = 0 \\ r_{i,n} & \text{se } 1 \leq n \leq k \\ r_{i,n \bmod^\star k} & \text{altrimenti} \end{cases}$ *per ogni* $i \in \{1, \ldots, m-1\}$

La cosa più importante da osservare sull'algoritmo generalizzato è che esso, con input $n_1, \ldots, n_m$, non fa altro che calcolare *in parallelo* $m - 1$ algoritmi "base", ciascuno con input n_i e n_m, per $i \in \{1, \ldots, m-1\}$, e fermarsi quando *tutti* gli $m-1$ algoritmi base si fermano.

Ciò è evidente nell'esempio precedente, dove $m = 3$ e $(n_1, n_2, n_3) = (5, 4, 6)$. Ad esempio, il primo passo è:

$$\begin{cases} 6 = 5 \cdot 1 + 1 \\ 6 = 4 \cdot 1 + 2 \end{cases}$$

Ma $6 = 5 \cdot 1 + 1$ è il primo passo dell'algoritmo base con input $n_3 = 6$ e $n_1 = 5$, e $6 = 4 \cdot 1 + 2$ è il primo passo dello stesso con input $n_3 = 6$ e $n_2 = 4$.

Questa situazione si verifica per ogni passo dell'algoritmo generalizzato: la prima e la seconda riga sono rispettivamente passi dell'algoritmo base con input n_1 e n_3, e con input n_2 e n_3. Si può verificare il caso in cui uno degli algoritmi base termina e l'altro no, come nel secondo passo:

$$\begin{cases} 7 = 5 \cdot 1 + 2 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

Ma l'algoritmo generalizzato prosegue fin quando entrambi (in generale, tutti) gli algoritmi base terminano:

$$\begin{cases} 10 = 5 \cdot 2 + 0 \\ 8 = 4 \cdot 2 + 0 \end{cases}$$

Formalizzando quanto abbiamo detto, si può dire che:

Osservazione 9.3. *Per ogni $i \in \{1, \dots, m-1\}$, con $m > 1$:*

- $q_{i,n}^{n_1,\dots,n_m} = q_n^{n_i,n_m}$
- $r_{i,n}^{n_1,\dots,n_m} = r_n^{n_i,n_m}$
- $k^{n_1,\dots,n_m}$ *può essere diverso da* k^{n_i,n_m} *(cioè: quando un algoritmo base termina, non è detto che termini anche l'algoritmo generalizzato)*

Dimostrazione. I primi due punti sono una conseguenza diretta della definizione dell'algoritmo, in particolare delle istruzioni 10 e 11.

Non dimostriamo l'ultimo punto, perché dimostreremo un risultato più forte, che stabilisce quanto vale esattamente $k^{n_1,\dots,n_m}$.

□

Dall'osservazione 9.3 si può concludere che sui quozienti e sui resti dell'algoritmo generalizzato non possiamo dire nulla che non sia immediatamente riconducibile a proprietà dei quozienti e sui resti dell'algoritmo base, perciò non annoieremo il lettore con proprietà dalla dimostrazione banale.

Non ci resta allora che parlare di $k^{n_1,\dots,n_m}$. Le uniche proprietà dell'algoritmo base connesse a k^{n_1,n_2} sono l'ultimo punto dell'osservazione 9.1 ed il teorema 9.1. Ora li generalizziamo entrambi.

Osservazione 9.4. $\forall i \in \{1,\dots,m-1\} : r_{i,n}^{n_1,\dots n_m} = 0 \Leftrightarrow k^{n_1,\dots,n_m} \mid n$

Dimostrazione.

- Se $n = k^{n_1,\dots,n_m}$, vuol dire che l'algoritmo è appena terminato (perché $k^{n_1,\dots,n_m}$ è per definizione l'ultimo valore assunto dalla variabile `n`), quindi la condizione `esiste un t tale che r_t_n > 0` è falsa, dunque per ogni $i \in \{1,\dots,m-1\}$ si ha `r_i_n = 0`. Allora, usando la notazione 9.2, per ogni $i \in \{1,\dots,m-1\}$ si ha $0 = \texttt{r\_i\_n} = r_{i,n}^{n_1,\dots,n_m} = r_{i,k^{n_1,\dots,n_m}}^{n_1,\dots,n_m}$
- Se $n < k^{n_1,\dots,n_m}$, ci vogliono altre iterazioni prima che l'algoritmo termini (perché il valore finale assunto da `n` è per definizione $k^{n_1,\dots,n_m}$), quindi la condizione `esiste un t tale che r_t_n > 0` è vera, cioè $\forall i \in \{1,\dots,m-1\} : r_{i,n}^{n_1,\dots n_m} = 0$ è falsa
- Se $n > k^{n_1,\dots,n_m}$ e $k^{n_1,\dots,n_m} \mid n$, allora per ogni $i \in \{1,\dots,m-1\}$ si ha $r_{i,n}^{n_1,\dots,n_m} = r_{i,n \bmod^\star k^{n_1,\dots,n_m}}^{n_1,\dots,n_m} = r_{i,k^{n_1,\dots,n_m}}^{n_1,\dots,n_m} = 0$
- Se $n > k^{n_1,\dots,n_m}$ e $k^{n_1,\dots,n_m} \nmid n$, allora per ogni $i \in \{1,\dots,m-1\}$ si ha $r_{i,n}^{n_1,\dots,n_m} = r_{i,n \bmod^\star k^{n_1,\dots,n_m}}^{n_1,\dots,n_m} = r_{i,t}^{n_1,\dots,n_m}$, con $0 < t < k^{n_1,\dots,n_m}$, dunque $r_{i,n}^{n_1,\dots,n_m} = r_{i,t}^{n_1,\dots,n_m} > 0$

□

Il seguente lemma, abbastanza intuitivo, viene utilizzato per generalizzare il teorema 9.1.

Lemma 9.1. *Siano* $m \in \mathbb{N}, m > 1$, *e* $n_1,\dots,n_m \in \mathbb{N}^\star$. $\mathrm{MCM}(n_1,\dots,n_m) = \mathrm{MCM}(\mathrm{MCM}(n_1,n_m),\dots,\mathrm{MCM}(n_{m-1},n_m))$, *cioè, per definizione di minimo comune multiplo:*

- $\forall i \in \{1,\dots,m-1\} : \mathrm{MCM}(n_i,n_m) \mid \mathrm{MCM}(n_1,\dots,n_m)$
- $\forall i \in \{1,\dots,m-1\} : \mathrm{MCM}(n_i,n_m) \mid n \Rightarrow \mathrm{MCM}(n_1,\dots,n_m) \mid n$

Dimostrazione. 1. $n_m \mid \mathrm{MCM}(n_1,\dots,n_m)$ [per definizione di MCM]

2. Sia $i \in \{1,\dots,m-1\}$

   (a) $n_i \mid \mathrm{MCM}(n_1,\dots,n_m)$ [da 2., per definizione di MCM]

   (b) $\mathrm{MCM}(n_i, n_m) \mid \mathrm{MCM}(n_1, \ldots, n_m)$ [da 1. e 2.–(a), per definizione di MCM]

3. $\forall i \in \{1, \ldots, m-1\} : \mathrm{MCM}(n_i, n_m) \mid \mathrm{MCM}(n_1, \ldots, n_m)$ [da 2.–(b)]

4. Sia $i \in \{1, \ldots, m-1\}$, $\mathrm{MCM}(n_i, n_m) \mid n$

   (a) $n_m \mid$ [per definizione di MCM]
   $\mathrm{MCM}(n_i, n_m) \mid$ [da 4.]
   n

   (b) $n_i \mid$ [per definizione di MCM]
   $\mathrm{MCM}(n_i, n_m) \mid$ [da 4.]
   n

5. $\forall i \in \{1, \ldots, m-1\} : \mathrm{MCM}(n_i, n_m) \mid n \Rightarrow$ [da 4.–(a) e 4.–(b)]
   $\forall i \in \{1, \ldots, m-1\} : n_m \mid n \Rightarrow$ [per definizione di MCM]
   $\mathrm{MCM}(n_1, \ldots, n_m) \mid n$

6. $\mathrm{MCM}(n_1, \ldots, n_m) = \mathrm{MCM}(\mathrm{MCM}(n_1, n_m), ..., \mathrm{MCM}(n_{m-1}, n_m))$ [da 3. e 5., per definizione di MCM]

□

Teorema 9.2. *Siano* $m \in \mathbb{N}, m > 1$, *e* $n_1, \ldots, n_m \in \mathbb{N}^\star$. $k^{n_1,\ldots,n_m} = \frac{\mathrm{MCM}(n_1,\ldots,n_m)}{n_m}$ *e* $\forall i \in \{1, \ldots, m-1\} : \sum_{n=1}^{k^{n_1,\ldots,n_m}} q_{i,n}^{n_1,\ldots,n_m} = \frac{\mathrm{MCM}(n_1,\ldots,n_m)}{n_i}$.

Dimostrazione.

Dimostriamo che $k^{a_1,\ldots,a_m} = \frac{\mathrm{MCM}(a_1,\ldots,a_m)}{a_1}$:

1. $\forall i \in \{1, \ldots, m-1\} : r_{i,k^{n_1,\ldots,n_m}}^{n_1,\ldots n_m} = 0$ [per l'osservazione 9.3]

2. $\forall i \in \{1, \ldots, m-1\} : r_{k^{n_1,\ldots,n_m}}^{n_i,n_m} = 0$ [da 1., per la notazione 9.2]

3. $\forall i \in \{1, \ldots, m-1\} : k^{n_i,n_m} \mid k^{n_1,\ldots,n_m}$ [da 2., per l'osservazione 9.1]

4. $\forall i \in \{1, \ldots, m-1\} : \frac{\mathrm{MCM}(n_i,n_m)}{n_m} \mid k^{n_1,\ldots,n_m}$ [da 3., per il teorema 9.1]

5. $\frac{\mathrm{MCM}(n_1,\ldots,n_m)}{n_m} \mid k^{n_1,\ldots,n_m}$ [da 4., per il lemma 9.1]

6. $\forall i \in \{1, \ldots, m-1\} : k^{n_i,n_m} =$ [per il teorema 9.1]
   $\frac{\mathrm{MCM}(n_i,n_m)}{n_m} \mid$ [per il lemma 9.1]
   $\frac{\mathrm{MCM}(n_1,\ldots,n_m)}{n_m}$

7. $\forall i \in \{1, \ldots, m-1\} : r_{i,\frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}}^{n_1,\ldots,n_m} =$ [per l'osservazione 9.3]
   $r_{\frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}}^{n_i,n_m} =$ [da 6., per l'osservazione 9.1]
   0

8. $k^{n_1,\ldots,n_m} \mid \frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}$ [da 7., per l'osservazione 9.4]

9. $k^{n_1,\ldots,n_m} = \frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}$ [da 5. e 8.]

Ora dimostriamo che $\forall i \in \{1, \ldots, m-1\} : \sum_{n=1}^{k^{n_1,\ldots,n_m}} q_{i,n}^{n_1,\ldots,n_m} = \frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}$:

1. $\sum_{n=1}^{k^{n_1,\ldots,n_m}} q_{i,n}^{n_1,\ldots,n_m} =$ [per l'osservazione 9.3]
   $\sum_{n=1}^{k^{n_1,\ldots,n_m}} q_n^{n_i,n_m} =$ [per la parte precedente della dimostrazione]
   $\sum_{n=1}^{\frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}} q_n^{n_i,n_m} =$ [per la proposizione 9.3]
   $\left\lfloor \frac{n_m \frac{\text{MCM}(n_1,\ldots,n_m)}{n_m}}{n_i} \right\rfloor =$
   $\left\lfloor \frac{\text{MCM}(n_1,\ldots,n_m)}{n_i} \right\rfloor =$ [da $\text{MCM}(n_1, \ldots, n_m) \bmod n_i = 0$]
   $\frac{\text{MCM}(n_1,\ldots,n_m)}{n_i}$

□

9.3 Un'interpretazione dell'algoritmo per il calcolo del M.C.M.

I tratteggi lineari sono un ottimo modello per interpretare l'algoritmo per il calcolo del M.C.M. del capitolo 9, che in questo modo dovrebbe risultare più intuitivo e meno asettico. Consideriamo per semplicità solo la forma base (definizione 9.1), essendo il discorso facilmente estendibile alla forma generalizzata (anzi, ciò può costituire un utile esercizio per il lettore). Utilizziamo la notazione 9.1.

Siano $n_1, n_2, n \in \mathbb{N}^\star$. La proposizione 9.2 afferma che:

$$r_n^{n_1,n_2} = n_2 n \bmod n_1$$

Consideriamo il tratteggio $(n_1, n_2) \in \mathcal{L}^2$. $n_2 n \bmod n_1$ è la differenza tra $n_2 n$, il valore dell'n-esimo trattino di indice 2, e $n_1 \left\lfloor \frac{n_2 n}{n_1} \right\rfloor$, il valore del più grande trattino di indice 1 minore o uguale all'n-esimo trattino di indice 2 (proposizione 4.1). La situazione, nei casi $(n_1, n_2) = (7, 4)$ e $(n_1, n_2) = (4, 7)$, è visualizzata, rispettivamente, nelle figure 9.3 e 9.3.

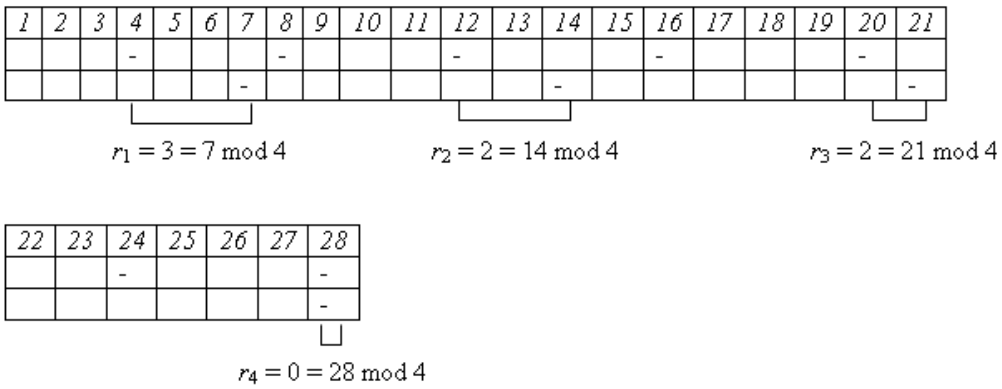

Figura 9.1: Interpretazione della proposizione 9.2, con $(n_1, n_2) = (7, 4)$.

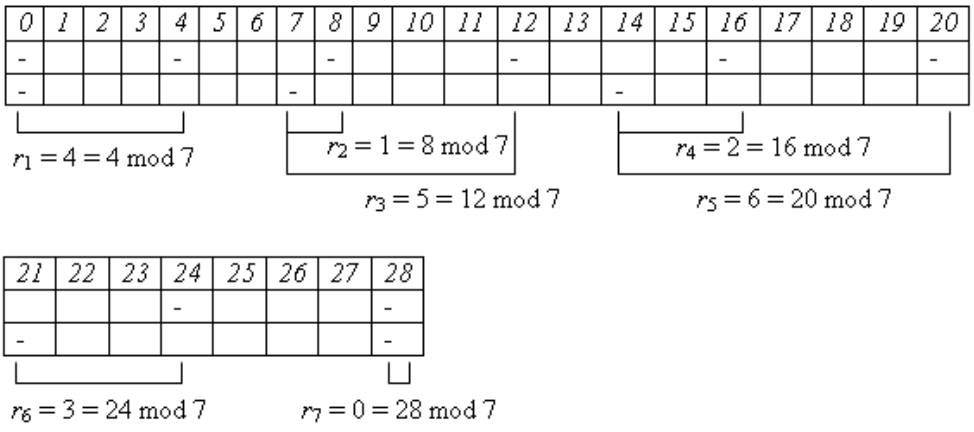

Figura 9.2: Interpretazione della proposizione 9.2, con $(n_1, n_2) = (4, 7)$.

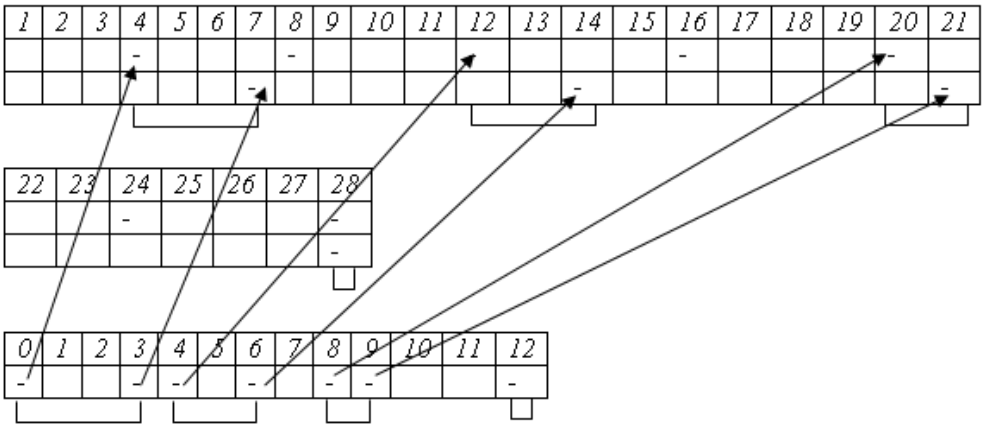

Figura 9.3: Interpretazione dell'osservazione 9.2, con $(n_1, n_2) = (4, 7)$.

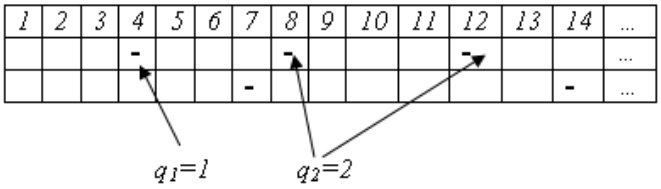

Figura 9.4: Interpretazione grafica del corollario 9.3, con $(n_1, n_2) = (4, 7)$.

Grazie a quest'interpretazione dell'n-esimo resto, possiamo visualizzare graficamente l'osservazione 9.2, secondo cui applicando l'algoritmo per il calcolo del M.C.M. con input n_1 ed n_2, ed applicandolo con input $r_1^{n_1,n_2}$ ed n_1, si ottiene la stessa sequenza di resti. Ciò significa che la differenza tra l'n-esimo trattino di indice 2 ed il precedente trattino di indice 1, nel tratteggio (n_1, n_2), è pari alla differenza tra l'n-esimo trattino di indice 1 ed il precedente trattino di indice 2, nel tratteggio $(r_1^{n_1,n_2}, n_1)$, per ogni n. Ciò è mostrato in figura 9.3.

Finora abbiamo dato un significato all'n-esimo resto. Ora analizziamo i corollari 9.2 e 9.3, che permettono di dare un significato all'n-esimo quoziente, affermando che:

$$q_n^{n_1,n_2} = \left\lfloor \frac{n_2 n}{n_1} \right\rfloor - \left\lfloor \frac{n_2 (n-1)}{n_1} \right\rfloor = \left\lfloor \frac{n_2 + n_2 (n-1) \bmod n_1}{n_1} \right\rfloor$$

Dall'espressione centrale (corollario 9.3), alla luce del corollario 4.2, si ottiene che $q_n^{n_1,n_2}$ è pari alla differenza tra il numero di trattini positivi minori o uguali ad $\langle 2, n \rangle$ ed il numero di trattini positivi minori o uguali a $\langle 2, n-1 \rangle$; in altri termini, $q_n^{n_1,n_2}$ è pari al numero di trattini maggiori di $\langle 2, n-1 \rangle$ e minori o uguali a $\langle 2, n \rangle$. Ciò è rappresentato graficamente in figura 9.3.
Si può anche osservare che $\left\lfloor \frac{n_2 n}{n_1} \right\rfloor - \left\lfloor \frac{n_2 (n-1)}{n_1} \right\rfloor$, se si sostituisce n_2 con $n_1' n_2'$ e n_1 con $n_1' + n_2'$, è pari all'ampiezza dell'intervallo che contiene $\mathrm{t}_{(n_1', n_2')}(n-1)$ (si veda il

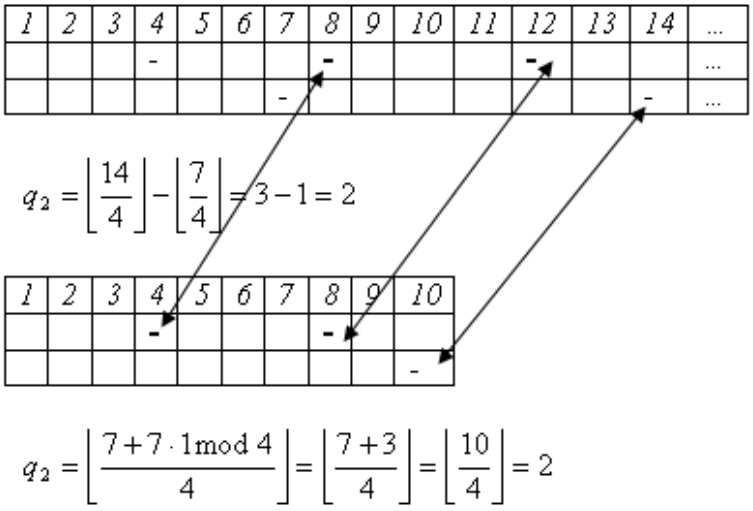

Figura 9.5: Interpretazione grafica dei corollari 9.3 e 9.2, con $(n_1, n_2) = (4, 7)$.

paragrafo 6.5).
L'espressione $\left\lfloor \frac{n_2 + n_2(n-1) \bmod n_1}{n_1} \right\rfloor$ può essere guardata, sempre alla luce del corollario 4.2, come il numero di trattini positivi di indice 1 di valore minore o uguale a $n_2 + n_2 (n-1) \bmod n_1$. Ricordando quanto abbiamo appena detto, possiamo dire quindi che ci sono tanti trattini positivi di indice 1 di valore minore o uguale a $n_2 + n_2 (n-1) \bmod n_1$, quanti ce ne sono tra $\langle 2, n-1 \rangle$, non compreso, e $\langle 2, n \rangle$, compreso. Potremmo in effetti definire una corrispondenza biunivoca tra i due insiemi di trattini: una possibile corrispondenza è visualizzata in figura 9.3.

Capitolo 10

Tratteggi dei quozienti di primo ordine

In questo capitolo trattiamo in dettaglio i tratteggi dei quozienti di primo ordine (definiti, ricordiamo, come metatratteggi di un tratteggio lineare di secondo ordine). Questo caso, pur essendo semplice, non è banale come quello dei tratteggi lineari di primo ordine (tranne che per la funzione t, ovviamente). Infatti, la funzione t_valore dei tratteggi di $\mathcal{Q}^1$, anziché data per definizione come in $\mathcal{L}^1$, è ricavata dalla definizione di metatratteggio e, come vedremo, è una funzione più complessa di un semplice prodotto. Una volta ricavata la funzione t_valore, questa sarà utilizzata per ottenere la funzione t_spazio.

10.1 t_valore dei quozienti di primo ordine

La funzione t_valore_Q, $Q \in \mathcal{Q}^1$, è strettamente legata all'algoritmo per il calcolo del M.C.M.. Per concretizzare quest'aspetto, applichiamo l'algoritmo con input $n_1 \equiv 5$ e $n_2 \equiv 8$ (il lettore può provare in seguito anche con l'esempio 9.1, che è un caso abbastanza degenere e perciò non lo consideriamo adesso):

$$\begin{aligned} 8 &= 1 \cdot 5 + 3 \\ 11 &= 2 \cdot 5 + 1 \\ 9 &= 1 \cdot 5 + 4 \\ 12 &= 2 \cdot 5 + 2 \\ 10 &= 2 \cdot 5 + 0 \end{aligned}$$

Quindi le sequenze dei resti e dei quozienti che si ottengono sono, rispettivamente, $(r_1, r_2, r_3, r_4, r_5) = (3, 1, 4, 2, 0)$ e $(q_1, q_2, q_3, q_4, q_5) = (1, 2, 1, 2, 2)$. A par-

tire da questi, seguendo la notazione 9.1, sono definiti $r_n^{5,8}$ e $q_n^{5,8}$ in modo tale che $\left(r_1^{5,8}, r_2^{5,8}, \ldots, r_{11}^{5,8}, \ldots\right) = (3,1,4,2,0,3,1,4,2,0,3\ldots)$ e $\left(q_1^{5,8}, q_2^{5,8}, \ldots, q_{11}^{5,8}, \ldots\right) = (1,2,1,2,2,1,2,1,2,2,1,\ldots)$.

Ora analizziamo, d'altra parte, il tratteggio $Q \equiv q\,(T)$, con $T \equiv (n_1, n_2) \equiv (5,8)$. Esso è definito (definizione 3.9) come il metatratteggio di (8) generato da $\left(\lambda x.\, \left\lfloor \frac{x}{5} \right\rfloor\right)$ e dalla funzione identica definita su $\{1\}$. La partizione di $\mathbb{N}$ indotta dalla funzione di ripartizione $f \equiv \lambda x.\, \left\lfloor \frac{x}{5} \right\rfloor$ è la seguente:

$$\left\{f_1^{-1}\,(0)\,,\ f_1^{-1}\,(1)\,,\ f_1^{-1}\,(2)\,,\ \ldots\right\} = \left\{\{0,1,2,3,4\}\,,\ \{5,6,7,8,9\}\,,\ \{10,11,12,13,14\}\,,\ \ldots\right\}$$

Partizionando in questo modo le colonne di (8), si ottiene la seguente tabella:

	0					1					2					3					...
1	**0**	1	2	3	4	5	6	7	**8**	9	10	11	12	13	14	15	**16**	17	18	19	...

da cui si ottiene la tabella di Q:

	0	1	2	3	4	5	6	7	8	9	10	11	12	...
1	-	-		-	-		-		-	-		-	-	...

Per come è stata ottenuta la tabella, si può associare l'x-esimo trattino di Q dopo l'origine all'x-esimo multiplo positivo di n_2 (nell'esempio, 8, 16, ...) ed il suo valore nel tratteggio corrisponde al numero di intervalli disgiunti di cardinalità n_1 che si devono considerare, partendo da zero, per raggiungere tale numero. Alla luce di questo si può interpretare il seguente teorema:

Teorema 10.1. *Sia $Q \equiv q\,(T)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$. Allora, per ogni $x \in \mathbb{N}^\star$:*

$$\text{t\_valore}_Q\,(x) = \left\lfloor \frac{n_2 x}{n_1} \right\rfloor$$

Dimostrazione.

1. $Q \equiv q\,((n_1, n_2))$ è il metatratteggio di (n_2) generato dalla funzione di ripartizione $f_1 \equiv \lambda x.\, \left\lfloor \frac{x}{n_1} \right\rfloor$ e dalla funzione identica f definita sull'insieme $\{1\}$ [per definizione di tratteggio dei quozienti (definizione 3.9)]

2. $\text{t\_valore}_Q\,(x) =$ [per definizione di t_valore e perché Q è di primo ordine]
   $Q\,(\langle 1, x\rangle) =$ [da 1. per definizione di metatratteggio (definizione 3.7)]
   $f_1\left(\text{t\_valore}_{(n_2)[f^{-1}(1)]}\,(x)\right) =$ [da 1. (in particolare, perché $f_1 \equiv \lambda x.\, \left\lfloor \frac{x}{n_1} \right\rfloor$ e f è

la funzione identica definita sull'insieme $\{1\}$)]
$\left(\lambda x. \left\lfloor \frac{x}{n_1} \right\rfloor\right) \left(\text{t\_valore}_{(n_2)[1]}\left(x\right)\right)$ = [dalle definizioni di tratteggio e di sottotratteggio]
$\left(\lambda x. \left\lfloor \frac{x}{n_1} \right\rfloor\right) \left(\text{t\_valore}_{(n_2)}\left(x\right)\right)$ = [applicazione della funzione $\lambda x. \left\lfloor \frac{x}{n_1} \right\rfloor$ a $\text{t\_valore}_{T[1]}\left(x\right)$]
$\left\lfloor \frac{\text{t\_valore}_{(n_2)}(x)}{n_1} \right\rfloor$ = [per definizione di (n_2)]
$\left\lfloor \frac{n_2 x}{n_1} \right\rfloor$

□

In questo modo abbiamo ricavato l'equazione della funzione t_valore direttamente dalla definizione del tratteggio. In alternativa, sarebbe stato possibile fare il contrario, ossia dare il teorema 10.1 come definizione di tratteggio dei quozienti, e successivamente dimostrare che un tratteggio definito in tal modo è un metatratteggio di un tratteggio lineare.

Proposizione 10.1. *Sia $Q \equiv q\left(T\right)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$. Allora, usando la notazione 9.1, per ogni $x \in \mathbb{N}^\star$:*

$$\text{t\_valore\_diff}_Q\left(x\right) = q_x^{n_1,n_2}$$

Dimostrazione.

1. $\text{t\_valore\_diff}_Q\left(x\right) = q_x^{n_1,n_2}$ [da 2., 2.–(a), 3. e 3.–(a)]

2. Se $x = 1$

   (a) $\text{t\_valore\_diff}_Q\left(x\right)$ = [da 2., per definizione]
   $\text{t\_valore}_T\left(x\right)$ = [per il teorema 10.1]
   $\left\lfloor \frac{n_2 x}{n_1} \right\rfloor$ = [da 2.]
   $\left\lfloor \frac{n_2}{n_1} \right\rfloor$ = [per la proposizione 9.3]
   $q_1^{n_1,n_2}$ = [da 2.]
   $q_x^{n_1,n_2}$

3. Se $x > 1$

   (a) $\text{t\_valore\_diff}_Q\left(x\right)$ = [da 2., per definizione]
   $\text{t\_valore}_T\left(x\right) - \text{t\_valore}_T\left(x-1\right)$ = [per il teorema 10.1]
   $\left\lfloor \frac{n_2 x}{n_1} \right\rfloor - \left\lfloor \frac{n_2 (x-1)}{n_1} \right\rfloor$ = [per il corollario 9.3]
   $q_x^{n_1,n_2}$

□

Ad esempio, osservando la tabella di Q si ottiene che $\text{t\_valore\_diff}_Q(1) = 1 - 0 = 1 = q_1^{5,8}$ e $\text{t\_valore\_diff}_Q(2) = 3 - 1 = 2 = q_2^{5,8}$.

Notiamo anche che, se fosse nota in partenza l'espressione di t_valore_diff_Q, sarebbe possibile ottenere t_valore_Q in modo molto semplice, sfruttando alcuni risultati dei capitoli precedenti:

1. $\text{t\_valore}_Q(x) =$ [proprietà 3.1]
   $\sum_{i=1}^{x} \text{t\_valore\_diff}_Q(x) =$ [per la proposizione 10.1]
   $\sum_{i=1}^{x} q_x^{n_1,n_2} =$ [per la proposizione 9.3]
   $\left\lfloor \frac{n_2 x}{n_1} \right\rfloor$

Proposizione 10.2. *Sia $Q \equiv q(T)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$. Allora, per ogni $x \in \mathbb{N}^\star$, il più grande trattino di Q di valore minore o uguale a x è $\left\langle 1, \left\lfloor \frac{n_1(x+1)-1}{n_2} \right\rfloor \right\rangle$. In altri termini:*

$$\arg\max_{u \in Q | Q(u) \leq x} Q(u) = \left\langle 1, \left\lfloor \frac{n_1(x+1) - 1}{n_2} \right\rfloor \right\rangle$$

Dimostrazione.

1. Il più grande trattino di Q di valore minore o uguale a x è $\left\langle 1, \left\lfloor \frac{n_1(x+1)-1}{n_2} \right\rfloor \right\rangle$ [da 2. e 3.]

2. Sia $t \equiv \langle 1, k \rangle = \arg\max_{u \in Q | Q(u) \leq x} Q(u)$

3. $k =$ [da 2. e per il lemma 3.8]
   $\arg\max_{n \in \mathbb{N},\, Q(\langle 1,n \rangle) \leq x} Q(\langle 1, n \rangle) =$ [per il teorema 10.1]
   $\arg\max_{n \in \mathbb{N},\, \left\lfloor \frac{n_2 n}{n_1} \right\rfloor \leq x} \left\lfloor \frac{n_2 n}{n_1} \right\rfloor =$ [per la proprietà 2.25]
   $\arg\max_{n \in \mathbb{N},\, n_2 n \leq n_1(x+1)-1} \left\lfloor \frac{n_2 n}{n_1} \right\rfloor =$ [per la proprietà 2.24]
   $\arg\max_{n \in \mathbb{N},\, n \leq \left\lfloor \frac{n_1(x+1)-1}{n_2} \right\rfloor} \left\lfloor \frac{n_2 n}{n_1} \right\rfloor =$ [per monotonia della parte intera]
   $\left\lfloor \frac{n_1(x+1)-1}{n_2} \right\rfloor$

□

10.2 t_spazio dei quozienti di primo ordine

In questo paragrafo ricaviamo la funzione t_spazio per un tratteggio dei quozienti di primo ordine, partendo dalla conoscenza della sua funzione valore, espressa dal teorema 10.1.

Si presenta subito un problema: un tratteggio dei quozienti può non avere spazi! Consideriamo ad esempio il tratteggio $R \equiv q\,(U)$, con $U \equiv (n_1, n_2) \equiv (8, 5)$. Si noti che n_1 e n_2 sono scambiati rispetto a quelli del tratteggio Q del paragrafo precedente: invitiamo il lettore a confrontare quest'ultimo col tratteggio R appena definito. R, per la definizione 3.9, è il metatratteggio di (5) generato da $\left(\lambda x.\, \left\lfloor \frac{x}{8} \right\rfloor\right)$ e dalla funzione identica definita su $\{1\}$. La partizione di $\mathbb{N}$ indotta dalla funzione di ripartizione $f \equiv \lambda x.\, \left\lfloor \frac{x}{8} \right\rfloor$ è la seguente:

$$\left\{f^{-1}\,(0)\,,\ f^{-1}\,(1)\,,\ f^{-1}\,(2)\,,\ \ldots\right\} = \left\{ \begin{array}{l} \{0,1,2,3,4,5,6,7\}\,,\ \{8,9,10,11,12,13,14,15\}\,, \\ \{16,17,18,19,20,21,22,23\}\,,\ \ldots \end{array} \right\}$$

Partizionando in questo modo le colonne di (5), si ottiene la seguente tabella:

	0								1							
1	**0**	1	2	3	4	**5**	6	7	8	9	**10**	11	12	13	14	**15**

	2								...
1	16	17	18	19	**20**	21	22	23	...

da cui, aggiungendo più colonne, si ottiene la seguente tabella:

	0	1	2	3	4	5	6	7	8	9	10	...
1	–	–	-	–	-	–	–	-	–	-	–	...

Evidentemente R non ha spazi. È interessante notare, però, come la proposizione 10.1 valga anche in questo caso. Infatti, applicando l'algoritmo per il calcolo del M.C.M. con input 8 e 5 si ottiene:

$$\begin{aligned} 5 &= 0 \cdot 8 + 5 \\ 10 &= 1 \cdot 8 + 2 \\ 7 &= 0 \cdot 8 + 7 \\ 12 &= 1 \cdot 8 + 4 \\ 9 &= 1 \cdot 8 + 1 \\ 6 &= 0 \cdot 8 + 6 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 1 \cdot 8 + 0 \end{aligned}$$

Quindi la sequenza dei quozienti è $(q_1, \ldots, q_8) = (0, 1, 0, 1, 1, 0, 1, 1)$. I quozienti nulli indicano appunto che due trattini consecutivi hanno lo stesso valore, cioè stanno nella stessa cella della tabella. Ad esempio, $\text{t\_valore\_diff}_Q(3) = \text{t\_valore}_Q(3) - \text{t\_valore}_Q(2) = 1 - 1 = 0$; d'altra parte, applicando la proposizione 10.1 si ha che $\text{t\_valore\_diff}_Q(3) = q_3^{8,5} = 0$. Si può osservare, inoltre, che tutti i quozienti sono minori o uguali a 1: ciò, sempre alla luce della proposizione 10.1, non consente la presenza di spazi in Q, perché se esistesse uno spazio, allora esisterebbero due trattini consecutivi i cui valori differiscono di almeno 2. Dunque il fatto che R non contenga spazi è dovuto al fatto che i quozienti ottenuti con l'algoritmo sono tutti minori o uguali a 1, che a sua volta è dovuto al fatto che il secondo input (5 nell'esempio) è minore o uguale al primo (8). Più formalmente:

Proposizione 10.3. *Sia $Q \equiv q(T)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$. Allora Q non ha spazi (cioè la funzione t_spazio_Q non è definita) se e solo se $n_2 \leq n_1$.*

Dimostrazione.

1. Q non ha spazi $\Leftrightarrow$ [per la proprietà 3.3]
   $\forall x \in \mathbb{N}^\star : \text{t\_valore\_diff}_Q(x) \leq 1 \Leftrightarrow$ [per la proposizione 10.1]
   $\forall x \in \mathbb{N}^\star : q_x^{n_1,n_2} \leq 1 \Leftrightarrow$ [per la proposizione 9.4]
   $n_2 \leq n_1$

□

Parecchie semplici proprietà dei tratteggi dei quozienti si possono ricondurre a proprietà dell'algoritmo per il calcolo del M.C.M., ad esempio:

Proposizione 10.4. *Sia $Q \equiv q(T)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$. Q è periodico, con periodo $\frac{\text{MCM}(n_1,n_2)}{n_2}$ e lunghezza di un dominio fondamentale $\frac{\text{MCM}(n_1,n_2)}{n_1}$.*

Dimostrazione.

1. Q è periodico, con periodo $\frac{\text{MCM}(n_1,n_2)}{n_2}$ e lunghezza di un dominio fondamentale $\frac{\text{MCM}(n_1,n_2)}{n_1}$ [da 2., 3. e 4., per la definizione 1.15]
2. Siano $n \equiv \frac{\text{MCM}(n_1,n_2)}{n_2}$ e $m \equiv \frac{\text{MCM}(n_1,n_2)}{n_1}$; sia, per ogni $t \in Q$, t_n l'n-esimo trattino successivo a t
3. $\forall t \in Q : Q(t) = Q(t_n) - m \wedge \text{ind}(t) = \text{ind}(t_n)$ [da 2., (a), (b), (c) e (d)]
   (a) Sia $t \equiv \langle 1, k \rangle \in Q$
   (b) Sia $v \equiv \left\langle 1, k + \frac{\text{MCM}(n_1,n_2)}{n_2} \right\rangle$ [k definito in (a)]

(c) $v = t_n$ [da (a), (b) e 2., per il corollario 3.3]

(d) $Q(t) =$ [da (a), per definizione di T]
$\left\lfloor \frac{n_2 k}{n_1} \right\rfloor =$
$\left\lfloor \frac{n_2 k}{n_1} \right\rfloor + \frac{\mathrm{MCM}(n_1,n_2)}{n_1} - \frac{\mathrm{MCM}(n_1,n_2)}{n_1} =$ [per la proprietà 2.19]
$\left\lfloor \frac{n_2 k + \mathrm{MCM}(n_1,n_2)}{n_1} \right\rfloor - \frac{\mathrm{MCM}(n_1,n_2)}{n_1} =$
$\left\lfloor \frac{n_2\left(k + \frac{\mathrm{MCM}(n_1,n_2)}{n_2}\right)}{n_1} \right\rfloor - \frac{\mathrm{MCM}(n_1,n_2)}{n_1} =$ [da (b), per definizione di T]
$Q(v) - \frac{\mathrm{MCM}(n_1,n_2)}{n_1} =$ [da 2.]
$Q(v) - m$

4. $n' \in \mathbb{N}^\star,\ n' < n \Rightarrow \forall m \in \mathbb{N}^\star \exists t \in Q :\ Q(t) \neq Q(t_{n'}) - m \ \vee\ \mathrm{ind}(t) \neq \mathrm{ind}(t_{n'})$ [da (a)]

(a) $n' \in \mathbb{N}^\star,\ n' < n \Rightarrow \forall m \in \mathbb{N}^\star \exists t \in Q :\ Q(t) \neq Q(t_{n'}) - m$ [da (b) e (b)–i.]

(b) Siano $n' \in \mathbb{N}^\star$, $n' < n$, ed $m \in \mathbb{N}^\star$

i. $\exists t \in Q :\ Q(t) \neq Q(t_{n'}) - m$

ii. Sia $x \in \mathbb{N}^\star$ tale che $q_x^{n_1,n_2n'} = \begin{cases} \left\lfloor \frac{n_2n'}{n_1} \right\rfloor + 1 & \text{se } m = \left\lfloor \frac{n_2n'}{n_1} \right\rfloor \\ \left\lfloor \frac{n_2n'}{n_1} \right\rfloor & \text{altrimenti} \end{cases}$ [x è ben definito, per A.]

A. $\exists x \in \mathbb{N}^\star : q_x^{n_1,n_2n'} = \left\lfloor \frac{n_2n'}{n_1} \right\rfloor \wedge \exists x' \in \mathbb{N}^\star : q_{x'}^{n_1,n_2n'} = \left\lfloor \frac{n_2n'}{n_1} \right\rfloor + 1$ [da B., per la proposizione 9.5]

B. $\left\lfloor \frac{n_2n'}{n_1} \right\rfloor n_1 < n_2n' < \left(\left\lfloor \frac{n_2n'}{n_1} \right\rfloor + 1 \right) n_1$ [da C. e H.]

C. $\left\lfloor \frac{n_2n'}{n_1} \right\rfloor n_1 < n_2n'$ [da D.]

D. $n_2n' - n_2n' \bmod n_1 < n_2n'$ [da E.]

E. $n_2n' \bmod n_1 > 0$ [da F.; se infatti fosse $n_2n' \bmod n_1 = 0$, sarebbe $\mathrm{MCM}(n_1,n_2) \mid n_2n'$]

F. $0 < n_2n' < \mathrm{MCM}(n_1,n_2)$ [da G.]

G. $0 < n' < \frac{\mathrm{MCM}(n_1,n_2)}{n_2}$ [da (b) e 2.]

H. $n_2n' < \left(\left\lfloor \frac{n_2n'}{n_1} \right\rfloor + 1 \right) n_1$ [da I.]

I. $n_2n' < n_2n' - n_2n' \bmod n_1 + n_1$ [da J.]

J. $n_2n' \bmod n_1 < n_1$

iii. Sia $t = \langle 1, n'x \rangle \in Q$

iv. $Q(t) \neq Q(t_{n'}) - m$ [da B. e D.]

v. $m \neq q_x^{n_1,n_2n'}$

vi. $Q(t) \neq Q(t_{n'}) - m \Leftrightarrow$
$\left\lfloor \frac{n_2 n' x}{n_1} \right\rfloor \neq \left\lfloor \frac{n_2(n'x+n')}{n_1} \right\rfloor - m \Leftrightarrow$
$\left\lfloor \frac{n_2 n' x}{n_1} \right\rfloor \neq \left\lfloor \frac{n_2 n' x}{n_1} \right\rfloor + \left\lfloor \frac{n_2 n' + n_2 n' x \bmod n_1}{n_1} \right\rfloor - m \Leftrightarrow$
$m \neq \left\lfloor \frac{n_2 n' + n_2 n' x \bmod n_1}{n_1} \right\rfloor \Leftrightarrow$
$m \neq q_x^{n_1, n_2 n'}$

vii. $t_{n'} = \langle 1, k + n' \rangle$ [da ii., per il corollario 3.3]

□

Proposizione 10.5. *Sia $Q \equiv q(T)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$. Q è strettamente monotono se e solo se $n_2 \geq n_1$.*

Dimostrazione.

1. Q è strettamente monotono $\Leftrightarrow$
$\forall x \in \mathbb{N}^\star : \text{t\_valore\_diff}_Q(x) \geq 1 \Leftrightarrow$ [per la proposizione 10.1]
$\forall x \in \mathbb{N}^\star : q_x^{n_1, n_2} \geq 1 \Leftrightarrow$ [per la proposizione 9.4]
$n_2 \geq n_1$

□

Per la proposizione 10.4, i tratteggi dei quozienti sono periodici. Quindi, per il corollario 3.4, se un tratteggio dei quozienti ha uno spazio, allora ha infiniti spazi; in altri termini, un tratteggio dei quozienti o non ha spazi (e ciò accade se e solo se $n_2 \leq n_1$, in base alla proposizione 10.3), o ne ha infiniti. Quindi, nel caso $n_2 > n_1$, è senz'altro definita la funzione t_spazio, che esplicitiamo nel teorema seguente.

Teorema 10.2. *Sia $Q \equiv q(T)$, con $T \in \mathcal{L}^2$, $T \equiv (n_1, n_2)$, con $n_2 > n_1$. Allora, per ogni $x \in \mathbb{N}^\star$:*

$$\text{t\_spazio}_Q(x) = \left\lfloor \frac{n_2 x - 1}{n_2 - n_1} \right\rfloor$$

Dimostrazione.

1. $n = \text{t\_spazio}_Q(x) \Leftrightarrow$ [per il lemma del conteggio (lemma 3.1)]
$$\begin{cases} |\{y \in \{1, \ldots, n\} \mid y \text{ è uno spazio di } Q\}| = x \\ |\{y \in \{1, \ldots, n-1\} \mid y \text{ è uno spazio di } Q\}| = x - 1 \end{cases} \Leftrightarrow$$
$$\begin{cases} |\{y \in \{1, \ldots, n\} \mid y \text{ è uno spazio di } Q\}| + \\ + |\{y \in \{1, \ldots, n\} \mid y \text{ non è uno spazio di } Q\}| = \\ x + |\{y \in \{1, \ldots, n\} \mid y \text{ non è uno spazio di } Q\}| \\ |\{y \in \{1, \ldots, n-1\} \mid y \text{ è uno spazio di } Q\}| + \\ + |\{y \in \{1, \ldots, n-1\} \mid y \text{ non è uno spazio di } Q\}| = \\ x - 1 + |\{y \in \{1, \ldots, n-1\} \mid y \text{ non è uno spazio di } Q\}| \end{cases} \Leftrightarrow$$

$$\begin{cases} n = x + |\{y \in \{1,\dots,n\} \mid y \text{ non è uno spazio di } Q\}| \\ n-1 = x-1 + |\{y \in \{1,\dots,n-1\} \mid y \text{ non è uno spazio di } Q\}| \end{cases} \Leftrightarrow$$ [per definizione di spazio]

$$\begin{cases} n = x + |\{y \in \{1,\dots,n\} \mid \exists t \in Q : Q(t) = y\}| \\ n-1 = x-1 + |\{y \in \{1,\dots,n-1\} \mid \exists t \in Q : Q(t) = y\}| \end{cases} \Leftrightarrow$$ [per il lemma 3.5 e per (a)]

$$\begin{cases} n = x + |\{t \in Q \mid Q(t) \in [\mathcal{O}_Q + 1, n]\}| \\ n-1 = x-1 + |\{t \in Q \mid Q(t) \in [\mathcal{O}_Q + 1, n-1]\}| \end{cases} \Leftrightarrow$$ [per il lemma 3.7 e per (b)]

$$\begin{cases} n = x + \underset{y \in \mathbb{N} \mid Q(\langle 1,y\rangle) \le n}{\arg\max} Q(\langle 1,y\rangle) \\ n-1 = x-1 + \underset{y \in \mathbb{N} \mid Q(\langle 1,y\rangle) \le n-1}{\arg\max} Q(\langle 1,y\rangle) \end{cases} \Leftrightarrow$$ [per il lemma 3.8]

$$\begin{cases} n = x + \underset{t \in Q \mid Q(t) \le n}{\arg\max} Q(t) \\ n-1 = x-1 + \underset{t \in Q \mid Q(t) \le n-1}{\arg\max} Q(t) \end{cases} \Leftrightarrow$$ [per la proposizione 10.2]

$$\begin{cases} n = x + \left\lfloor \frac{n_1(n+1)-1}{n_2} \right\rfloor \\ n-1 = x-1 + \left\lfloor \frac{n_1 n - 1}{n_2} \right\rfloor \end{cases} \Leftrightarrow$$

$$\begin{cases} \left\lfloor \frac{n_1(n+1)-1}{n_2} \right\rfloor = n-x \\ \left\lfloor \frac{n_1 n - 1}{n_2} \right\rfloor = n-x \end{cases} \Leftrightarrow$$ [per la proprietà 2.23]

$$\begin{cases} n_2(n-x) \le n_1(n+1) - 1 < n_2(n-x+1) \\ n_2(n-x) \le n_1 n - 1 < n_2(n-x+1) \end{cases} \Leftrightarrow$$

[perché $n_1 n - 1 < n_1(n+1) - 1 < n_2(n-x+1) \Rightarrow n_1 n - 1 < n_2(n-x+1)$]

$$\begin{cases} n_2(n-x) \le n_1(n+1) - 1 < n_2(n-x+1) \\ n_2(n-x) \le n_1 n - 1 \end{cases} \Leftrightarrow$$

[perché $n_2(n-x) \le n_1 n - 1 < n_1(n+1) - 1 \Rightarrow n_2(n-x) \le n_1(n+1) - 1$]

$$\begin{cases} n_1(n+1) - 1 < n_2(n-x+1) \\ n_2(n-x) \le n_1 n - 1 \end{cases} \Leftrightarrow$$ [calcoli algebrici, separatamente sulle due disuguaglianze]

$$\begin{cases} n_2 x - 1 < (n_2 - n_1)(n+1) \\ (n_2 - n_1) n \le n_2 x - 1 \end{cases} \Leftrightarrow$$

$(n_2 - n_1) n \le n_2 x - 1 < (n_2 - n_1)(n+1) \Leftrightarrow$ [per la proprietà 2.23]

$n = \left\lfloor \frac{n_2 x - 1}{n_2 - n_1} \right\rfloor$

(a) Q è strettamente monotono [da $n_2 > n_1$, per la proposizione 10.5]

(b) $Q(\langle 1,1\rangle) =$ [per il teorema 10.1]
$\left\lfloor \frac{n_2}{n_1} \right\rfloor \ge$ [da $n_2 > n_1$]
$1 >$ [perché l'origine di un tratteggio dei quozienti è 0]
$\mathcal{O}_Q$

□

10.3 $\mathcal{Q}^1$ come estensione di $\mathcal{L}^1$

Un modo interessante di analizzare i tratteggi dei quozienti è interpretarli come generalizzazione dei tratteggi lineari. Infatti, soffermandosi sul primo ordine, si ha che ogni tratteggio lineare (n_1) è un tratteggio dei quozienti: in particolare, $(n_1) = q((1, n_1))$. Possiamo dire, in generale:

Proposizione 10.6. *Sia* $T \equiv (n_1) \in \mathcal{L}^1$. *Allora* $T = q((1, n_1)) \in \mathcal{Q}^1$.

Dimostrazione.

1. Sia $T \equiv (n_1) \in \mathcal{L}^1$
   (a) Sia $Q \equiv q((1, n_1)) \in \mathcal{Q}^1$ [n_1 definito in (a)]
   (b) $T = Q$ [da (d) ed (e)]
   (c) $\text{ord}(T) = \text{ord}(Q) = 1$ [da (a) e (b)]
   (d) $\forall \langle 1, k\rangle \in \text{Tratt}_{\{1\}} : T(\langle 1, k\rangle) = Q(\langle 1, k\rangle)$
      i. Se $k = 0$
         A. $T(\langle 1, k\rangle) =$ [da i., per definizione di origine]
            $\mathcal{O}_T =$ [per la proprietà 3.16]
            $\mathcal{O}_Q =$ [da i., per definizione di origine]
            $Q(\langle 1, k\rangle)$
      ii. Se $k > 0$
         A. $T(\langle 1, k\rangle) =$ [per l'osservazione 1.2]
            $T(\text{t}_T(k)) =$
            $\text{t\_valore}_T(k) =$ [da (a)]
            $n_1 k =$
            $\left\lfloor \frac{n_1 k}{1} \right\rfloor =$ [da (b), per il teorema 10.1]
            $\text{t\_valore}_Q(k) =$
            $Q(\text{t}_Q(k)) =$ [per l'osservazione 1.2]
            $Q(\langle 1, k\rangle)$

□

Corollario 10.1. $\mathcal{L}^1 \subset \mathcal{Q}^1$.

Dimostrazione.

1. $\mathcal{L}^1 \subset \mathcal{Q}^1$ [da 2. e 3.]
2. $\forall T \in \mathcal{L}^1 : T \in \mathcal{Q}^1$ [per la proposizione 10.6]
3. $\exists Q \in \mathcal{Q}^1 : Q \notin \mathcal{L}^1$ [da (a) e (b)]
   (a) Sia $Q \equiv q\left((5,8)\right)$
   (b) $Q \notin \mathcal{L}^1$ [da (a), (c) e (d); infatti nei tratteggi lineari t_valore_diff è una funzione costante]
   (c) $\text{t\_valore\_diff}_Q\left(1\right) = q_1^{5,8} = 1$ [da (a), per la proposizione 10.1]
   (d) $\text{t\_valore\_diff}_Q\left(2\right) = q_2^{5,8} = 2$ [da (a), per la proposizione 10.1]

□

Stabilito dunque che un tratteggio lineare è un tratteggio dei quozienti, in particolare $(n_1) = q\left((1,n_1)\right)$, si deve avere che tutti i teoremi validi tratteggi lineari del tipo (n_1) si possono ottenere come casi particolari di teoremi validi per un generico tratteggio dei quozienti $Q \equiv q\left((n_1,n_2)\right)$, ponendo $n_1 \equiv 1$ e $n_2 \equiv n_1$. Facciamo tre esempi, sempre ponendo $Q \equiv q\left((n_1,n_2)\right)$:

- Per il teorema 10.1, $\text{t\_valore}_Q\left(x\right) = \left\lfloor \frac{n_2 x}{n_1} \right\rfloor$. Ponendo $n_1 \equiv 1$ e $n_2 \equiv n_1$, si ottiene che $\text{t\_valore}_{q((1,n_1))}\left(x\right) = \text{t\_valore}_T\left(x\right) = \left\lfloor \frac{n_1 x}{1} \right\rfloor = n_1 x$, come sappiamo per definizione di tratteggio lineare.

- Secondo il teorema 10.2, il più grande trattino di Q di valore minore o uguale a x è $\left\langle 1, \left\lfloor \frac{n_1(x+1)-1}{n_2} \right\rfloor \right\rangle$. Ponendo $n_1 \equiv 1$ e $n_2 \equiv n_1$, si ottiene che il più grande trattino di $q\left((1,n_1)\right) = (n_1)$ è $\left\langle 1, \left\lfloor \frac{(x+1)-1}{n_1} \right\rfloor \right\rangle = \left\langle 1, \left\lfloor \frac{x}{n_1} \right\rfloor \right\rangle$, come affermato dal teorema 4.1.

- Per il teorema 10.1, $\text{t\_spazio}_Q\left(x\right) = \left\lfloor \frac{n_2 x - 1}{n_2 - n_1} \right\rfloor$. Ponendo $n_1 \equiv 1$ e $n_2 \equiv n_1$, si ottiene che $\text{t\_spazio}_{q((1,n_1))}\left(x\right) = \text{t\_spazio}_T\left(x\right) = \left\lfloor \frac{n_1 x - 1}{n_1 - 1} \right\rfloor$, come stabilito dal teorema 8.1.

Ringraziamenti

Vorrei ringraziare tutte le persone che, pur in minima parte, hanno contribuito a questo lavoro: Mariangela per i preziosi consigli sul primo capitolo, Vito per i consigli sulla formattazione e per la segnalazione di LyX come editor per LaTeX, Myriam riguardo alla vignetta di Woodstock. Ringrazio anche tutti quelli che, pur senza dare un contributo, si sono interessati a questo lavoro: il prof. Danese e il prof. Borzacchini per avermi preso seriamente in considerazione, i miei genitori, Simone, Manuela, Eugenia, Antonio e Salvatore.