Il teorema di Davis-Putnam-Robinson

Eugenio G. Omodeo

6 aprile 2022

Indice

"We prove that every recursively enumerable set can be existentially defined in terms of exponentiation. Hence, there is no general algorithm for deciding whether or not an exponential diophantine equation has a solution in positive integers. We also obtain a general theorem about bounds for solutions of diophantine equations with a finite number of solutions.[2]

$[\cdots]$

[2] The result that every recursively enumerable set can be existentially defined in terms of exponentiation was obtained by Davis and Putnam, basing themselves on their [3], using the unproved number-theoretical hypothesis that there are arbitrarily long progressions containing only prime numbers. They wish to acknowledge useful suggestions, made in conversation, by H. S. Shapiro. Their results $[\cdots]$ were presented to the American Mathematical Society, October 31, 1959. $[\cdots]$ Julia Robinson showed that the use of this hypothesis can be avoided. This result was presented to the American Mathematical Society, January 27, 1960."

[DPR61][1]

1 Asserto che verrà dimostrato

Teorema 1 (Davis-Putnam-Robinson)**.** *Sia* $g(a_1, \ldots, a_{\boldsymbol{m}})$ *una funzione computabile (anche solo parzialmente). Allora la relazione*

$$\mathcal{G}(a_1, \ldots, a_{\boldsymbol{m}}, a_0) \quad \leftrightarrow_{Def} \quad g(a_1, \ldots, a_{\boldsymbol{m}}) = a_0$$

è diofantea esponenziale. □

Tutta questa dispensa si riferirà all'insieme $\mathbb{N}$ dei numeri naturali.

Dunque $\mathcal{G}$ è quella relazione $\boldsymbol{m}+1$-aria su $\mathbb{N}$—di qui in poi chiamata GRAFO di g—che è formata dalle sequenze $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}}, \boldsymbol{a}_0 \rangle$ tali che: (1) $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}} \rangle$ appartiene al dominio di g; (2) $\boldsymbol{a}_0$ è il valore in cui g manda $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}} \rangle$. Per dimostrare il teorema, occorre definire $\mathcal{G}$ tramite un sistema di equazioni diofantee esponenziali. Nel fare e discutere questo, ci avvarremo di quanto già sappiamo su tali equazioni; in particolare dei seguenti fatti:

- La proprietà $a \equiv 1$ (**mod** 2) che a soddisfa quando è un numero naturale dispari è diofantea, in quanto definita dall'equazione $a = 2\,x + 1$.

  Diofantea, ovvio, anche la $a \equiv 0$ (**mod** 2).

- Il confronto $a < b$ tra numeri naturali è relazione diofantea, in quanto definito dall'equazione: $a + x + 1 = b$.

- La relazione triadica $a \max b = c$ è relazione diofantea, in quanto definita dall'equazione $(c - a - x)^2 + (c - b - y)^2 + \big((c - b) \cdot (c - a)\big)^2 = 0$.

- Il quoziente $a = b \div c$ tra naturali è diofanteo: possiamo definirlo come $c\,a \leqslant b < c\,(a + 1)$, cioè tramite il sistema $c\,a + x = b$, $b + y + 1 = c\,a + c$.

  Esercizio: specificare $a = b \div c$ con un'equazione sola.

[1] Due progressioni aritmetiche formate da primi: $5, 53, 101, 149, 197$ e $7, 37, 67, 97, 127, 157$. Quello che [DPR61] riportava in bibliografia come voce [3] era il [DP58]; la congettura di Davis e Putnam menzionata in [DPR61] diceva che "per ogni intero positivo q, esistono numeri naturali r, s tali che $s > 0$ ed $r + ks$ è primo per $k = 0, 1, \ldots, q$" ed è stata dimostrata vera (da Ben Green e Terence Tao) solo nel 2004. Per una generalizzazione successiva, vedi [TZ08], reperibile alla URL `http://link.springer.com/article/10.1007%2Fs11511-008-0032-5`.

- È diofantea esponenziale la relazione di DOMINANZA $a \sqsubseteq b$ che intercorre fra $a = \sum_{i=0}^{k} a_i 2^i$ e $b = \sum_{i=0}^{k} b_i 2^i$ con $a_0, b_0, \ldots, a_k, b_k \in \{0,1\}$ se e solo se $a_i \leqslant b_i$ per $i = 0, \ldots, k$. Essa, infatti, sussiste se e solo se $\binom{b}{a}$ è dispari[2] e dunque—in virtú della specifica del coefficiente binomiale data altrove—è definita dal sistema di equazioni

$$\begin{array}{rcl} u & = & 2^b + 1\,, \\ (u+1)^b & = & w\,u\,u^a + z\,u^a + v\,, \\ v & < & u^a\,, \\ z & < & u\,, \\ z & = & 2\,t + 1\,. \end{array}$$

Difatti $2^b+1 > \binom{b}{k}$ e, per il *teor. binomiale*:

$$\begin{array}{c} \left(\left(2^b+1\right)+1\right)^b = \left(2^b+1\right)^{a+1} \\ \Sigma_{h=a+1}^{b} \binom{b}{h} \left(2^b+1\right)^{h-a-1} + \\ \binom{b}{a} \left(2^b+1\right)^a + \\ \Sigma_{h=0}^{a-1} \binom{b}{h} \left(2^b+1\right)^h\,. \end{array}$$

Esercizio 1. *Si può sostituire* $2^b + 1$ *con* 2^{b+1} *nella specifica, mostrata or ora, della dominanza? Possiamo sostituirvi* $2^b + 1$ *con* 2^b*?*

Esercizio 2. *Specificare la proprietà* $a \equiv 1$ (**mod** 2) *tramite la dominanza.*

2 Cenni essenziali di teoria della computabilità

Nel dimostrare il teorema di Davis-Putnam-Robinson ci atterremo a una variante delle nozioni di computabilità introdotte in [DSW94, Cap. 2] e in [Cut80, Cap. 1], a loro volta eredi di quella di [SS63]: variante che equivale alle altre, ma che calza meglio coi nostri presenti scopi.

2.1 Programmazione di una macchina a registri

Introduciamo un LINGUAGGIO DI PROGRAMMAZIONE che comprende un'infinità numerabile $\mathsf{R}_0\,,\ \mathsf{R}_1\,,\ \mathsf{R}_2\,, \cdots$ di variabili a valori in $\mathbb{N}$.

Vi sono istruzioni di cinque sorte:

$\mathsf{R}_j \leftarrow \mathsf{R}_j + 1$	incremento
$\mathsf{R}_j \leftarrow \mathsf{R}_j - 1$	decremento
IF $\mathsf{R}_j = 0$ **GOTO** k	salto condizionato
GOTO k	salto incondizionato
STOP	arresto

Istruzioni di un linguaggio programmativo Turing-completo.

ove $j, k \in \mathbb{N}$. Per PROGRAMMA intendiamo una lista $\Im_0, \ldots, \Im_{\boldsymbol{\ell}}$ d'istruzioni di queste sorte, con $\boldsymbol{\ell} \in \mathbb{N}$, soggetta alle seguenti limitazioni:

1. Quando un'istruzione $\Im_i$ della lista ha la forma **IF** $\mathsf{R}_j = 0$ **GOTO** k

$k = i$, *non* vietato, potrebbe causare iterazione perpetua.

[2] Ciò segue dalla congruenza di Lucas $\left(\begin{array}{c} \sum_{i=0}^{k} b_i\, p^i \\ \sum_{i=0}^{k} a_i\, p^i \end{array}\right) \equiv \prod_{i=0}^{k} \left(\begin{array}{c} b_i \\ a_i \end{array}\right)$ (**mod** p) che vale quando p è un numero primo ed $\{a_0, b_0, \ldots, a_k, b_k\} \subseteq \{0, \ldots, p-1\}$. Tener presente che $\binom{0}{1} = 0$ ed $1 = \binom{0}{0} = \binom{1}{0} = \binom{1}{1}$.

oppure la forma **GOTO** k , deve aversi $0 \leqslant k \leqslant \boldsymbol{\ell}$ e $k \neq i+1$; inoltre $\Im_k$ non dev'essere un'istruzione di decremento.

2. Ogni istruzione $\mathsf{R}_j \leftarrow \mathsf{R}_j - 1$ di decremento dev'essere immediatamente preceduta da un enunciato **IF** $\mathsf{R}_j = 0$ **GOTO** k , dove il numero k è tenuto, ovviamente, a soddisfare le restrizioni del punto 1.

3. $\Im_{\boldsymbol{\ell}}$ è una **STOP**, l'unica che compare nella lista.

2.2 Esecuzione di un programma

Un programma del genere può essere utilizzato per COMPUTARE una funzione

$$g: \quad \mathbb{N}^{\boldsymbol{m}} \quad \rightharpoonup \quad \mathbb{N},$$

totale *o parziale* (di qui la mezza freccia), ad $\boldsymbol{m}$ operandi, come segue:

preavvio: prima dell'avvio del programma,

- alle variabili $\mathsf{R}_1, \ldots, \mathsf{R}_{\boldsymbol{m}}$ vengono assegnati i rispettivi valori $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}}$ degli OPERANDI;
- tutte le altre variabili vengono inizialmente poste a 0;

avvio: il programma viene avviato dall'istruzione $\Im_0$;

passi:

- quando viene eseguita un'istruzione $\Im_i$ della forma

  $$\mathsf{R}_j \leftarrow \mathsf{R}_j \pm 1 ,$$

  il valore corrente della variabile R_j subisce un incr-/decr-emento unitario, dopodiché si attiva la $\Im_{i+1}$;
- quando viene eseguita un'istruzione $\Im_i$ della forma

  $$\textbf{IF} \quad \mathsf{R}_j = 0 \quad \textbf{GOTO} \quad k ,$$

  essa non modifica alcun valore di variabile; subito dopo si attiverà l'istruzione $\Im_k$ o la $\Im_{i+1}$ a seconda che al momento R_j detenga, o no, il valore 0;
- anche l'istruzione **GOTO** k non modifica alcun valore di variabile; le sussegue l'istruzione $\Im_k$;

arresto: se e quando il programma giunge all'istruzione **STOP**, il valore conservato nella variabile R_0 viene preso come RISULTATO $g(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}})$; ($g$ non associa alcun valore alla $\boldsymbol{m}$-upla $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}}$ se e solo se, quando avviato su tali valori, il programma prosegue per sempre).

Esempio 3. *Il seguente programma computa la moltiplicazione di due numeri:*

0	**IF** $\mathsf{R}_2 = 0$ **GOTO** 11
1	$\mathsf{R}_2 \leftarrow \mathsf{R}_2 - 1$
2	**IF** $\mathsf{R}_1 = 0$ **GOTO** 7
3	$\mathsf{R}_1 \leftarrow \mathsf{R}_1 - 1$
4	$\mathsf{R}_3 \leftarrow \mathsf{R}_3 + 1$
5	$\mathsf{R}_0 \leftarrow \mathsf{R}_0 + 1$
6	**GOTO** 2
7	**IF** $\mathsf{R}_3 = 0$ **GOTO** 0
8	$\mathsf{R}_3 \leftarrow \mathsf{R}_3 - 1$
9	$\mathsf{R}_1 \leftarrow \mathsf{R}_1 + 1$
10	**GOTO** 7
$\boldsymbol{\ell} = 11$	**STOP**

$\boldsymbol{m} = 2$, $\boldsymbol{r} = 3$

```
while R2 > 0
  R2 −−
  while R1 > 0
    R1 −−
    R3 ++
    R0 ++
  while R3 > 0
    R3 −−
    R1 ++
```

Esercizio 4. *Scrivere un programma che computi l'addizione di due numeri.*

Esercizio 5. *Che funzione computa il programma di un'istruzione sola?*

Esercizio 6. *Quale funzione a 3 operandi viene computata dal programma dell'Esempio 3 se anche* R_3 *viene considerata variabile d'ingresso?*

Esercizio 7. *Mostrare che se c'è un programma* π *che computa una certa funzione* g*, allora ce n'è uno che computa la stessa* g *e che, quando (e se) termina, lascia a* 0 *tutte le variabili distinte dalla* R_0*.*

Esercizio 8. *Mostrare che non sarebbe restrittivo imporre che la prima istruzione di un programma non sia mai un'istruzione di salto (condizionato o meno).*

Esercizio 9. *Mostrare che l'aggiunta di una nuova sorta d'istruzione, la*

$$\textbf{\textit{IF}} \quad \mathsf{R}_j \neq 0 \quad \textbf{\textit{GOTO}} \quad k \qquad \textit{(di ovvio significato),}$$

non aumenterebbe il potere espressivo del linguaggio di programmazione e che anche l'istruzione di salto incondizionato è—in un modo che dipende da $\boldsymbol{m}$*—eliminabile.*

3 Dimostrazione del teorema DPR

Dimostrazione (James Jones e Yuri Matiyasevich [JM84], cfr. [Dav93, pagg. 66–73]). Supponiamo che π sia un programma che computa la funzione g, ad $\boldsymbol{m}$ operandi, che qui c'interessa. Come la Fig. 1 vuol suggerire, la dimostrazione consisterà nel tradurre la coppia $\pi, \boldsymbol{m}$ in un sistema di equazioni diofantee esponenziali definente il grafo di g.

Cominciamo col porre:

- $\boldsymbol{\ell} + 1 \;=\;$ il numero delle istruzioni $\Im_0, \ldots, \Im_{\boldsymbol{\ell}}$ di π ;
- $\boldsymbol{r} \;=\;$ il primo r tale che R_{r+1} *non* compare in π.

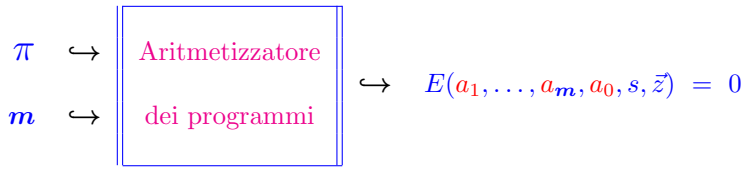

Figura 1: *Costruzione che dimostrerà, alla Jones-Matiyasevich, il teorema DPR. L'equazione E sarà risolubile, per $a_0 = \boldsymbol{a}_0, a_1 = \boldsymbol{a}_1, \ldots, a_{\boldsymbol{m}} = \boldsymbol{a}_{\boldsymbol{m}}$, se e solo se l'esecuzione di π, avviata sui dati $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\boldsymbol{m}}$, giunge a* **STOP** *in un numero finito s di passi fornendo, a conclusione, il risultato $\boldsymbol{a}_0$.*

Facciamo l'assunzione di comodo che tutte le variabili a parte R_0 conservino, a fine computazione, il valore 0. Essa non comporta perdita di generalità (v. Esercizio 7) e ci assicura che $\boldsymbol{r} \geqslant \boldsymbol{m}$.

Le incognite principali del sistema di equazioni che stiamo per vedere sono / rappresentano:

s il numero tale che al termine di $s+1$ passi di computazione il programma π dà il risultato $g(a_1, \ldots, a_{\boldsymbol{m}})$;

$\mathfrak{r}_j$ l'intero decorso dei valori di ciascuna variabile R_j del programma;[3]

$\mathfrak{l}_i$ il tracciato delle attivazioni di ciascuna istruzione $\mathfrak{I}_i$.

Intendiamo, cioè, rappresentare con

$\mathfrak{r}_j$ **:** la sequenza $\mathfrak{r}_{j,0}, \ldots, \mathfrak{r}_{j,s}$ costituita dall'iniziale $\mathfrak{r}_{j,0}$ e dai susseguenti valori $\mathfrak{r}_{j,t}$ di R_j, nella quale $\mathfrak{r}_{j,t}$ è il valore súbito dopo l'esecuzione del t-esimo passo. $\substack{t=1,\ldots,s \\ j=0,\ldots,\boldsymbol{r}}$ e

$\mathfrak{l}_i$ **:** la sequenza $\mathfrak{l}_{i,0}, \ldots, \mathfrak{l}_{i,s}$ di 0 / 1 che soddisfa $\mathfrak{l}_{i,t} = 1$ in corrispondenza di quei t per cui $\mathfrak{I}_i$ è l'istruzione eseguita al $t+1$-esimo passo di π. $\substack{t=0,\ldots,s \\ i=0,\ldots,\boldsymbol{\ell}}$ ed

Per riuscire a rappresentare ognuna di queste sequenze tramite un numero, ricorreremo a una Q *tanto grande* da consentirci di assimilare ogni componente di ogni $\mathfrak{r}_j$ a una cifra del sistema di numerazione posizionale che ha base Q. Cosí potremo utilizzare, semplicemente: come $\mathfrak{r}_j$ quel numero che in base Q risulta espresso dalla sequenza di cifre $\mathfrak{r}_{j,s} \cdots \mathfrak{r}_{j,1}\, \mathfrak{r}_{j,0}$; come $\mathfrak{l}_i$, in modo analogo, il numero espresso da $\mathfrak{l}_{i,s} \cdots \mathfrak{l}_{i,1}\, \mathfrak{l}_{i,0}$. Anche la quantità Q avrà titolo ad entrare come incognita nel nostro sistema di equazioni, per quanto non bastino a determinarla univocamente né il criterio che dev'essere 'grande', né il requisito ulteriore—cui portano considerazioni di semplicità concettuale—che Q sia una potenza positiva del numero 2. Quest'ultimo criterio tira in ballo un altro valore incognito $\mathfrak{b}$, pure lui sotto-determinato:[4] quel numero tale che $Q = 2^{\mathfrak{b}+1}$.

[3] Qui le minuscole $\mathfrak{r}$ ed $\mathfrak{l}$ dell'alfabeto Fraktur sono, rispettivamente, 'r' ed 'l'.
[4] Su come imporre l'unicità di Q e di $\mathfrak{b}$, v. Esercizio 12.

Verificheremo che il grafo $\mathcal{G}$ di g risulta correttamente descritto dal seguente sistema di equazioni parametriche nelle incognite $s, Q, I, \flat, \mathfrak{r}_0, \ldots, \mathfrak{r}_{\boldsymbol{r}}, \mathfrak{l}_0, \ldots, \mathfrak{l}_{\boldsymbol{\ell}}$:[5]

(I) $2\,(a_1 + \cdots + a_{\boldsymbol{m}} + s) < Q$;

(II) $\boldsymbol{\ell} + 1 < Q$;

(III) $Q = 2 \cdot 2^{\flat}$;

(IV) $1 + (Q-1)\,I = Q^{s+1}$;

(V) $\mathfrak{r}_j \sqsubseteq (Q \div 2 - 1)I$, per $j = 0, 1, \ldots, \boldsymbol{r}$;

(VI) $\mathfrak{l}_i \sqsubseteq I = \sum_{h=0}^{\boldsymbol{\ell}} \mathfrak{l}_h$, per $i = 0, 1, \ldots, \boldsymbol{\ell} - 1$;

(VII) $\mathfrak{l}_0 \;\equiv\; 1 \pmod 2$;

(VIII) $\mathfrak{l}_{\boldsymbol{\ell}} = Q^s$;

(IX) $\mathfrak{r}_j \;=\; Q\left(\mathfrak{r}_j + \sum_{i=0}^{\boldsymbol{\ell}} \Delta_{j,i}\mathfrak{l}_i\right) + \begin{cases} -Q^{s+1}a_0 & \text{se } \; j = 0\,, \\ a_j & \text{se } \; 0 < j \leqslant \boldsymbol{m}\,, \\ 0 & \text{se } \; \boldsymbol{m} < j\,, \end{cases}$

per $j = 0, \ldots, \boldsymbol{r}$, dove:

$$\Delta_{j,i} \;=_{\text{Def}}\; \begin{cases} 0 & \text{quando } \Im_i \text{ non modifica } \mathsf{R}_j\,, \text{ altrimenti} \\ \pm 1 & \text{a seconda che } \Im_i \text{ sia } \mathsf{R}_j \leftarrow \mathsf{R}_j \pm 1\,; \end{cases}$$

(X) $Q\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1}$ ogniqualvolta $\Im_i$ è un'istruzione di inc-/dec-remento;

(XI) $Q\mathfrak{l}_i \sqsubseteq \mathfrak{l}_k$ ogniqualvolta $\Im_i$ è un'istruzione **GOTO** k di salto incondizionato;

(XII) $Q\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1} + \mathfrak{l}_k$ ogniqualvolta $\Im_i$ è un'istruzione di salto condizionato **IF** $\mathsf{R}_j = 0$ **GOTO** k ;[6]

(XIII) $Q\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1} + QI - 2\mathfrak{r}_j$ ogniqualvolta $\Im_i$ è un'istruzione di salto condizionato **IF** $\mathsf{R}_j = 0$ **GOTO** k.

Le condizioni **(III)**, **(II)**, **(I)** ci dicono che Q deve:

- essere potenza del 2;
- superare l'1;
- superare—di oltre il doppio—la somma dei valori degli operandi piú il numero d'"istanti' che misura la durata dell'esecuzione.

Analoga a: $1 + 9 \cdot \underbrace{111}_{3\text{ uni}} = 10^3$.

Ogni cifra Q-aria di $\mathfrak{r}_i$ ha il bit piú significativo a 0.

0/1 sole cifre Q-arie nei $\mathfrak{l}_i$; ogni posizione è occupata da un 1 in esattamente un $\mathfrak{l}_h$.

Ossia: $\mathfrak{l}_0$ è dispari.

La posizione piú significativa contraddistingue l'arresto.

$$\Xi = Q\,(\Xi + \Delta\Lambda) + \begin{pmatrix} -Q^{s+1}a_0 \\ a_1 \\ \vdots \\ a_{\boldsymbol{m}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

[5] Il numero complessivo c delle condizioni soddisferà alla fine $9 + 2\boldsymbol{r} + 2\boldsymbol{\ell} \leqslant c \leqslant 9 + 2\boldsymbol{r} + 3\boldsymbol{\ell}$.

[6] Ricordare che in questo caso si ha $i + 1 \neq k$, o $\overline{\Pi}$ sarebbe scorretto.

Con ciò, grazie alla **(II)**, Q può essere utilizzato come base per una rappresentazione posizionale dei naturali. Inoltre, grazie alla **(I)**, tenendo conto che il valore $\mathfrak{r}_{j,t}$ che si trova nella variabile R_j all'istante t non può mai superare il valore $t+a_j$ per $j=1,\ldots,\boldsymbol{m}$, né può superare t per $j=0$ e per $j=\boldsymbol{m}+1,\ldots,\boldsymbol{r}$, possiamo rappresentare in base Q il decorso di R_j come

$$\mathfrak{r}_j \quad =_{\text{Def}} \quad \textstyle\sum_{t=0}^{s} \mathfrak{r}_{j,t} Q^t \ ,$$

dove $\mathfrak{r}_{j,t} < Q/2 = Q \div 2$. Infine, dall'aver richiesto **(III)** ci proverrà il vantaggio che se esprimiamo posizionalmente due numeri qualsiasi u, v come

$$u \ = \ \textstyle\sum_{i=0}^{K} u_i Q^i \ , \qquad v \ = \ \textstyle\sum_{i=0}^{K} v_i Q^i$$

(equiparandone il numero K di cifre Q-arie), allora varrà[7]

$$u \ \sqsubseteq \ v \qquad \text{se e solo se} \qquad u_i \ \sqsubseteq \ v_i \quad \text{per} \quad i = 0, 1, \ldots, K.$$

La condizione **(IV)** ci dice che $I = \sum_{t=0}^{s} Q^t$ per cui I, rappresentato nelle basi d'interesse Q e 2, è

$$\underbrace{1\ldots11}_{s+1} \qquad \text{e} \qquad \underbrace{\underbrace{0\ldots0}_{\flat}1\ldots\underbrace{0\ldots0}_{\flat}1}_{s+1} \ ,$$

Rappresentaz. di I in base Q e in base 2.

donde la **(V)**, che vuol riflettere in parte il nostro modo d'intendere le $\mathfrak{r}_j$: ognuna delle $s+1$ cifre di $(Q \div 2 - 1)I$, infatti, è rappresentata in base 2 da $0\underbrace{1\ldots1}_{\flat}$.

Non si può prescindere da altri aspetti dell'esecuzione, nel trattare il decorso

$$\begin{pmatrix} \mathfrak{r}_0 \\ \mathfrak{r}_1 \\ \vdots \\ \mathfrak{r}_{\boldsymbol{r}} \end{pmatrix} = \begin{pmatrix} \mathfrak{r}_{0,s} & \ldots & \mathfrak{r}_{0,1} & \mathfrak{r}_{0,0} \\ \mathfrak{r}_{1,s} & \ldots & \mathfrak{r}_{1,1} & \mathfrak{r}_{1,0} \\ \vdots & \ddots & \vdots & \vdots \\ \mathfrak{r}_{\boldsymbol{r},s} & \ldots & \mathfrak{r}_{\boldsymbol{r},1} & \mathfrak{r}_{\boldsymbol{r},0} \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{r}_{0,s} & \mathfrak{r}_{0,s-1} & \ldots & \mathfrak{r}_{0,1} & 0 \\ 0 & \mathfrak{r}_{1,s-1} & \ldots & \mathfrak{r}_{1,1} & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \mathfrak{r}_{\boldsymbol{m},s-1} & \ldots & \mathfrak{r}_{\boldsymbol{m},1} & a_{\boldsymbol{m}} \\ 0 & \mathfrak{r}_{\boldsymbol{m}+1,s-1} & \ldots & \mathfrak{r}_{\boldsymbol{m}+1,1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \mathfrak{r}_{\boldsymbol{r},s-1} & \ldots & \mathfrak{r}_{\boldsymbol{r},1} & 0 \end{pmatrix}$$

Istantanee della memoria còlte nell'imminenza degli $s+1$ passi dell'esecuzione. Ogni componente è un naturale $\mathfrak{r}_{j,t}$ inferiore a $Q/2$. L'eventuale discostamento fra $t+1$-esima e t-esima colonna riguarda un solo $\mathfrak{r}_{i,t+1} = \mathfrak{r}_{i,t} \pm 1$.

complessivo della 'memoria' di π. Passiamo per un po' a modellare il 'controllo', per poi collegare—sempre tramite equazioni—le due prospettive tra di loro.

[7] Conviene pensare alle cifre u_i di un numero u rappresentato in base Q come a delle sequenze, ognuna di $\flat+1$ bit (da leggersi da destra). Nelle cifre Q-arie di ogni decorso $\mathfrak{r}_j$, il $(\flat+1)$-esimo bit (i.e., quello che occupa la posizione piú significativa) è immancabilmente 0.

Per spiegare le condizioni **(VI)**, **(VII)**, **(VIII)**, consideriamo la matrice

$$\begin{pmatrix} \mathfrak{l}_0 \\ \mathfrak{l}_1 \\ \vdots \\ \mathfrak{l}_{\boldsymbol{\ell}} \end{pmatrix} = \begin{pmatrix} \mathfrak{l}_{0,s} & \cdots & \mathfrak{l}_{0,1} & \mathfrak{l}_{0,0} \\ \mathfrak{l}_{1,s} & \cdots & \mathfrak{l}_{1,1} & \mathfrak{l}_{1,0} \\ \vdots & \ddots & \vdots & \vdots \\ \mathfrak{l}_{\boldsymbol{\ell},s} & \cdots & \mathfrak{l}_{\boldsymbol{\ell},1} & \mathfrak{l}_{\boldsymbol{\ell},0} \end{pmatrix}$$

'Bit' delle attivazioni di $\Im_0, \ldots, \Im_{\boldsymbol{\ell}}$ ai passi $0, \ldots, s$ (esattamente un 1 per colonna).

di '*bit*', che ci dice, per ogni coppia i, t con $0 \leqslant i \leqslant \boldsymbol{\ell}$ e $0 \leqslant t \leqslant s$, se l'istruzione eseguita all'istante t è la $\Im_i$ (nel qual caso $\mathfrak{l}_{i,t} = 1$) oppure un'altra. Sulla riga d'indice i, che letta come numero in base Q rappresenta $\mathfrak{l}_i =_{\text{Def}} \sum_{t=0}^{s} \mathfrak{l}_{i,t} Q^t$, troviamo dunque indicazione di tutti gli istanti in cui l'istruzione eseguita è la i-esima. Con ciò, il senso delle **(VI)** è che ad ogni istante viene eseguita una e una sola istruzione;[8] il senso della **(VII)** e della **(VIII)**, implicanti $\mathfrak{l}_{0,0} = \mathfrak{l}_{\boldsymbol{\ell},s} = 1$, è che $\Im_0$ ed $\Im_{\boldsymbol{\ell}}$ sono, cronologicamente, la prima e l'ultima istruzione:

Piuttosto che veri bit, gli $\mathfrak{l}_{i,t}$ assumono le prime due cifre del sistema di numerazione $2^{\flat+1}$-ario.

$$\begin{pmatrix} 0 & \mathfrak{l}_{0,s-1} & \cdots & \mathfrak{l}_{0,1} & 1 \\ 0 & \mathfrak{l}_{1,s-1} & \cdots & \mathfrak{l}_{1,1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \mathfrak{l}_{\boldsymbol{\ell}-1,s-1} & \cdots & \mathfrak{l}_{\boldsymbol{\ell}-1,1} & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

I bit delle attivazioni, meglio messi a fuoco.

Le condizioni **(IX)** richiederebbero una spiegazione algebrica accurata che qui tralasciamo (v. sotto, Esercizio 10); intuitivamente, dicono che se moltiplichiamo per Q il decorso di valori di una variabile R_j, di ciò risentono per difetto (rispettivam. per eccesso) le cifre Q-arie corrispondenti alle azioni d'incremento (rispettivam. di decremento[9]) di R_j. Qualora R_j sia una variabile d'ingresso, occorrerà inoltre tener conto di a_j come sfasamento iniziale. Non c'è da preoccuparsi della cifra corrispondente all'arresto dell'esecuzione—che di proposito abbiamo azzerato—se non per la variabile d'uscita R_0: per questa lo sfasamento ha segno contrario agli sfasamenti iniziali e peso massimo (intendendo come 'peso' l'esponente di Q associato a ciascuna cifra), anziché minimo.

Le condizioni **(X)** dicono che se l'istruzione $\Im_i$ è di inc-/dec-remento—e dunque non altera il flusso di controllo—, subito dopo ogni istante in cui va ad effetto la $\Im_i$ andrà ad effetto la $\Im_{i+1}$. Le **(XI)** sono del tutto analoghe.

Similmente le condizioni **(XII)** dicono che se $\Im_i$ è un'istruzione di salto condizionato **IF** $\mathsf{R}_j = 0$ **GOTO** k, subito dopo ogni istante in cui va ad effetto la $\Im_i$ andrà ad effetto o la $\Im_{i+1}$ o la $\Im_k$ (dove vige $k \neq i+1$): quale delle due, lo stabiliranno le condizioni **(XIII)**.

Per concludere, va dunque mostrato che le **(XIII)**, richiedendo che nella stessa situazione or ora considerata valga $Q\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1} + QI - 2\mathfrak{r}_j$, instradano il controllo proprio come serve. La guida che ci aiuterà:

[8] Ragionando per assurdo: valga **(VI)** ma vi sia un primo t tale che il numero di 1 presenti sulla colonna t sia $\neq 1$; ma allora, per la **(II)**, la t-esima cifra Q-aria di $\sum_{h=0}^{\boldsymbol{\ell}} \mathfrak{l}_h$ sarebbe $\neq 1$.

[9] Rammentare: abbiamo supposto che le operazioni di decremento siano sempre effettive, cioè che non trovino mai a 0 la variabile di programma da decrementare.

	$s+1$	s	$\cdots$	t	$\cdots$	2	1	0
$Q\mathfrak{l}_i$	0	$\mathfrak{l}_{i,s-1}$	$\cdots$	$\mathfrak{l}_{i,t-1}$	$\cdots$	$\mathfrak{l}_{i,1}$	$\mathfrak{l}_{i,0}$	0
$\mathfrak{l}_{i+1}$	0	$\mathfrak{l}_{i+1,s}$	$\cdots$	$\mathfrak{l}_{i+1,t}$	$\cdots$	$\mathfrak{l}_{i+1,2}$	$\mathfrak{l}_{i+1,1}$	0
QI	1	1	$\cdots$	1	$\cdots$	1	1	0
$-2\,\mathfrak{r}_j$	-0	$2\,\mathfrak{r}_{j,s}$	$\cdots$	$2\,\mathfrak{r}_{j,t}$	$\cdots$	$2\,\mathfrak{r}_{j,2}$	$2\,\mathfrak{r}_{j,1}$	$2\,\mathfrak{r}_{j,0}$

ha quattro righe, ciascuna di $(s+2)(\flat+1)$ bit. Eventuali bit 1 sulla riga $Q\mathfrak{l}_i$ si affacciano all'estremità destra delle colonne t tali che all'istante $t-1$ è attiva la $\Im_i$ ($\mathfrak{l}_{i,t-1}=1$). Va mostrato che in questi casi, a seconda che valga o no $\mathfrak{r}_{j,t-1}=0$, la successiva istruzione non sarà $\Im_{i+1}$, o invece sí.

Preliminarmente si osservi che la sottrazione produce una sequenza

Ricordiamo: $\mathfrak{r}_{j,t} < Q/2$.

$QI-2\mathfrak{r}_j$	d_{s+1}	d_s	$\cdots$	d_t	$\cdots$	d_2	d_1	d_0

di cifre Q-arie dove la parità di d_t è disciplinata, per $t>0$, dalla regola:[10]

$$d_t \quad\equiv\quad 0 \pmod 2 \quad \text{se e solo se} \quad \mathfrak{r}_{j,t-1} \quad\neq\quad 0\ .$$

Questa regola si semplifica in

$$d_t \quad\equiv\quad 0 \pmod 2 \quad \text{se e solo se} \quad \mathfrak{r}_{j,t} \quad\neq\quad 0$$

quando $\mathfrak{l}_{i,t-1}=1$, visto che la $\Im_i$ non modifica la memoria.

Consideriamo un istante $t-1<s$ in cui $\mathfrak{l}_{i,t-1}=1$. Se $\mathfrak{r}_{j,t}=0$ (condizione del salto), la parità di $(\mathfrak{l}_{i+1}+QI-2\mathfrak{r}_j)_t$, cioè di $\mathfrak{l}_{i+1,t}+d_t$, è dunque data da

$$\mathfrak{l}_{i+1,t}+d_t \quad\not\equiv\quad \mathfrak{l}_{i+1,t} \pmod 2\ ;$$

cosí, richiedendo che $\mathfrak{l}_{i+1,t}+d_t$ sia dispari la **(XIII)** impone che $\mathfrak{l}_{i+1,t}=0$, cioè che il salto abbia luogo. Viceversa, se $\mathfrak{r}_{j,t}\neq 0$, abbiamo

$$\mathfrak{l}_{i+1,t}+d_t \quad\equiv\quad \mathfrak{l}_{i+1,t} \pmod 2\ ;$$

cosí la richiesta che $\mathfrak{l}_{i+1,t}+d_t$ sia dispari comporta che debba valere $\mathfrak{l}_{i+1,t}=1$, che il salto non abbia luogo. In ogni caso, la **(XIII)** ben modella l'instradamento esercitato dall'istruzione in esame $\Im_i$, di tipo **IF**. ⊣

Esercizio 10. *Spiegate in dettaglio algebrico le condizioni **(IX)**.*

Esercizio 11. *Dimostrate che la **(VIII)** potrebbe venir attenuata in: $\mathfrak{l}_\ell \sqsubseteq Q^s$.*

Esercizio 12. *Il sistema di equazioni **(I)**–**(XIII)** è sotto-determinato. Come rafforzarlo in modo che quando ammette soluzione ne abbia solo una?*

Esercizio 13. *Delineate come costruire un'equazione diofantea esponenziale $G=0$ che manca di soluzione se e solo se la congettura di Christian Goldbach (ca. 1742), "ogni numero pari maggiore di 2 può essere scritto come somma di due primi", è vera.*

Esercizio 14. *Si dimostri il seguente corollario de Teor. 1. Il dominio*

$$\left\{\, \langle a_1,\ldots,a_{\boldsymbol{m}}\rangle \in \mathbb{N}^{\boldsymbol{m}} \mid g(a_1,\ldots,a_{\boldsymbol{m}}) \in \mathbb{N} \,\right\}$$

di qualsiasi funzione parzialmente computabile $g(a_1,\ldots,a_{\boldsymbol{m}})$ è una relazione (ovvero una proprietà, nel caso $\boldsymbol{m}=1$) diofantea esponenziale.

[10] Banalmente vale anche $d_0 \quad\equiv\quad 0 \pmod 2$; fatto che però non ci serve.

4 (∗) H10 riferito ad eq. diofantee esponenziali

Indichiamo per comodità con ψ_π la funzione monadica

$$\psi_\pi : \quad \mathbb{N} \quad \rightharpoonup \quad \mathbb{N} \,,$$

totale o parziale, computata da un programma π.

La teoria dell'enumerabilità ricorsiva ci permette di scrivere un programma κ tale che per ogni altro programma π accade che

$$\{\, x : \langle x, y\rangle \in \psi_\pi \,\} \quad \neq \quad \mathbb{N} \setminus \{\, x : \langle x, y\rangle \in \psi_\kappa \,\} \,;$$

cioè, i dominî delle funzioni computate non sono mai complementari. In altre parole, l'insieme $\mathcal{K} =_{\text{Def}} \{\, x : \langle x, y\rangle \in \psi_\kappa \,\}$ è semidecidibile ma non decidibile.

Il Teor. 1 ci permette, poi, di costruire un polinomio diofanteo esponenziale parametrico K tale che

$$\psi_\kappa(a) \quad = \quad b \quad \leftrightarrow \quad \exists\, \vec{z} \quad K(a, b, \vec{z}) \quad = \quad 0 \,;$$

cosí $\mathcal{K}$ risulta esistenzialmente definito dall'equazione

$$K(a, y, \vec{z}) \quad = \quad 0 \,,$$

dove il secondo parametro è stato 'declassato' a nuova incognita.

Discende di qui l'insolubilità algoritmica del X problema di Hilbert riferito alle equazioni diofantee esponenziali—anziché a quelle polinomiali. Riuscissimo a risolvere quel problema in totale generalità, potremmo infatti, per qualsiasi assegnato valore $\boldsymbol{a}$, stabilire se l'equazione $K(\boldsymbol{a}, x, \vec{z}) = 0$ abbia o no soluzione. In altre parole, potremmo stabilire se $\boldsymbol{a}$ stia in $\mathcal{K}$ oppure no; situazione che contrasterebbe con l'indecidibilità di $\mathcal{K}$.

[DPR61, pagg. 429–430] raffinava questo risultato negativo rifacendosi a un risultato di [Rob52], in base al quale la relazione $b^c = a$ può essere definita esistenzialmente in termini di addizione, moltiplicazione e di una qualsiasi relazione $\mathcal{J}(u, v)$ che soddisfi, per qualche numero h, le seguenti due condizioni:

1. ogniqualvolta vale $\mathcal{J}(u, v)$, si ha che

$$v \quad < \quad u^{u^{\cdot^{\cdot^{\cdot^{u}}}}} \,, \qquad \text{dove la torre di esponenti ha altezza } h \,;$$

2. per ogni k, esistono u e v tali che $\mathcal{J}(u, v)$ ed $u^k < v$.

È di questo tipo, ad esempio (per $h = 3$), la relazione $2^u = v$ con $u \geqslant 2$. Discende quindi—esercizio che lasciamo al lettore—, grazie al Teor. 1, che per ogni funzione parziale computabile

$$g : \quad \mathbb{N} \quad \rightharpoonup \quad \mathbb{N}$$

c'è un polinomio P a coefficienti interi in un numero dispari $2\,m+1$ di variabili per cui vale

$$\exists\, x\,\big(x = g(\boldsymbol{a})\big) \quad\longleftrightarrow\quad \exists\, y_1 \cdots \exists\, y_m\; P(\boldsymbol{a}, y_1, \ldots, y_m, 2^{y_1}, \ldots, 2^{y_m}) = 0$$

per ogni $\boldsymbol{a} \in \mathbb{N}$. Di qui l'insolubilità algoritmica del X problema di Hilbert riferito alle equazioni della particolare forma $Q(y_1, \ldots, y_m, 2^{y_1}, \ldots, 2^{y_m}) = 0$, dove $Q(y_1, \ldots, y_m, z_1, \ldots, z_m)$ è un polinomio diofanteo.

Esercizio 15. *Mostrate che per ogni funzione parziale computabile $g : \mathbb{N} \rightharpoonup \mathbb{N}$ c'è un polinomio diofanteo $P(a, y_0, \ldots, y_m, z_0, \ldots, z_m)$, in un sol parametro a, tale che l'equazione esponenziale $P(a, y_0, \ldots, y_m, 2^{y_0}, \ldots, 2^{y_m}) = 0$ definisca esistenzialmente la proprietà $\exists\, x\, g(a) = x$, ossia: "a sta nel dominio di g".*

5 Equazione diofantea esponenziale *universale*

Nella recensione [Kre62] di [DPR61], l'illustre logico Georg Kreisel prendeva un celebre abbaglio asserendo che i risultati di quel lavoro erano solo superficialmente correlati al decimo problema di Hilbert riguardante le equazioni diofantee *ordinarie* (i.e., non esponenziali). Merita qui chiarire quale fosse il motivo di tanto sconcerto di Kreisel di fronte al teorema DPR.

Un risultato centrale della teoria della computabilità asserisce l'esistenza di un programma universale:[11]

Teorema 2 (Universalità)**.** *Per ogni $n \in \mathbb{N}$ si può esibire un programma $\mathcal{U}_n$ tale che, indicati con*

- *$\#\pi$ il numero di Gödel che compete a un generico programma π, con*
- *$\psi_\pi^{(n)}(x_1, \ldots, x_n)$ la funzione n-aria computata da π e con*
- *$\psi_{\mathcal{U}_n}^{(n+1)}(x_1, \ldots, x_n, \mathfrak{r}_{n+1})$ la funzione $n+1$-aria computata da $\mathcal{U}_n$,*

risulti

$$\psi_\pi^{(n)}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \;=\; \psi_{\mathcal{U}_n}^{(n+1)}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, \#\pi)$$

per ogni sequenza $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \rangle \in \mathbb{N}^n$ ed ogni programma π. ⊣

Questo teorema ha un'importante conseguenza:

Corollario 3. *Per ogni $n \in \mathbb{N}$, esiste un'equazione diofantea esponenziale*

$$U(a_1, \ldots, a_n, a_{n+1}, x_1, \ldots, x_m) \;=\; 0$$

tale che gli insiemi diofantei esponenziali di dimensione n sono tutti e soli gli insiemi definiti da una delle equazioni

$$U(a_1, \ldots, a_n, \boldsymbol{a}, x_1, \ldots, x_m) \;=\; 0$$

che risultano dal variare di $\boldsymbol{a}$ in $\mathbb{N}$.

[11] Tale scoperta viene prescelta, nel 2013, come "the most important British innovation of the last 100 years", v. `https://webarchive.nationalarchives.gov.uk/20170405141542/http://www.topbritishinnovations.org/pastinnovations`.

Dimostrazione. Alla stregua della dimostrazione del Teor. 1, si ricavi da $\mathcal{U}_n$ un sistema diofanteo esponenziale definente il grafo $\psi^{(n+1)}_{\mathcal{U}_n}(a_1, \ldots, a_{n+1}) = a_0$ di $\psi^{(n+1)}_{\mathcal{U}_n}$; poi si riscriva tale sistema come singola equazione $W(a_0, \ldots, a_{n+1}, \vec{x}) = 0$ e si ponga $U(a_1, \ldots, a_{n+1}, \vec{x}) =_{\text{Def}} W(0, a_1, \ldots, a_{n+1}, \vec{x})$. Per ogni fissato valore $\boldsymbol{a} \in \mathbb{N}$, la $U(a_1, \ldots, a_n, \boldsymbol{a}, \vec{x}) = 0$ è un'equazione diofantea esponenziale e dunque definisce un insieme diofanteo esponenziale.

D'altronde, a partire da qualsiasi equazione diofantea esponenziale

$$E(a_1, \ldots, a_n, y_1, \ldots, y_k) \quad = \quad 0$$

ci venga data, possiamo con facilità ricavarne un programma π che

- ricevendo all'avvio una sequenza $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ di naturali...
- ...passi in rassegna in modo sistematico i valori $E(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_k)$ ottenibili prendendo $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_k \in \mathbb{N}$, fino a imbattersi—se c'è—nel val. 0,
- in tal caso emettendo appunto, come risultato, lo 0.

Ma allora è facile vedere che l'insieme descritto da E è lo stesso definito dall'equazione $U(a_1, \ldots, a_n, \#\pi, \vec{x}) \quad = \quad 0$. ⊣

Esercizio 16. *Spiegare quanto asserito alla fine del Cor. 3: che le equazioni* $E(a_1, \ldots, a_n, y_1, \ldots, y_k) = 0$ *ed* $U(a_1, \ldots, a_n, \#\pi, \vec{x}) = 0$ *definiscono lo stesso insieme di sequenze di lunghezza* n.

Per concludere notiamo, in analogia a quanto osservato alla fine del § 4, che possiamo attribuire all'equazione universale del Cor. 3 una forma particolarissima: per limitarci al caso $n = 1$, si tratta della forma

$$\mathrm{U}(a_1, a_2, x_1, \ldots, x_m, 2^{x_1}, \ldots, 2^{x_m}) \quad = \quad 0\,,$$

dove $\mathrm{U}(a_1, a_2, x_1, \ldots, x_m, y_1, \ldots, y_m)$ è un *polinomio* diofanteo.

Esercizio 17. *Spiegare quest'ultima osservazione.*

6 Svolgimento degli esercizi

Soluzione Es. 1. Sí: al fine che $u > \binom{b}{h}$ per $h = 0, 1, \ldots, b$ basta che $u > 2^b$. Il caso $\binom{b}{h} = 2^b$ si verifica solo quando $b = h = 0$; perciò, semplificando $2^b + 1$ in 2^b definiamo ancora la dominanza, però omettendone la coppia $\langle 0,\, 0\rangle$. ⊣

Soluzione Es. 2. $1 \sqsubseteq a$ specifica la proprietà 'a è dispari'. ⊣

Soluzione Es. 4. Il seguente programma computa l'addizione di due numeri:

$$
\begin{array}{rl}
0 & \mathbf{IF}\ \ \mathsf{R}_1 = 0\ \ \mathbf{GOTO}\ \ 4 \\
1 & \mathsf{R}_1 \ \leftarrow\ \ \mathsf{R}_1 - 1 \\
2 & \mathsf{R}_0 \ \leftarrow\ \ \mathsf{R}_0 + 1 \\
3 & \mathbf{GOTO}\ \ 0 \\
4 & \mathbf{IF}\ \ \mathsf{R}_2 = 0\ \ \mathbf{GOTO}\ \ 8 \\
5 & \mathsf{R}_2 \ \leftarrow\ \ \mathsf{R}_2 - 1 \\
6 & \mathsf{R}_0 \ \leftarrow\ \ \mathsf{R}_0 + 1 \\
7 & \mathbf{GOTO}\ \ 4 \\
\boldsymbol{\ell} = 8 & \mathbf{STOP}
\end{array}
\qquad \boldsymbol{r} = \boldsymbol{m} = 2
$$

```
while R1 > 0
    R1 − −
    R0 + +
while R2 > 0
    R2 − −
    R0 + +
```

⊣

Soluzione Es. 5. Quale che sia il numero $\boldsymbol{m}$ degli operandi, il programma formato dalla sola **STOP** computa la funzione che vale costantemente 0. ⊣

Soluzione Es. 6. $g(x_1, x_2, x_3) \quad = \quad \begin{cases} 0 & \text{se } x_2 = 0, \\ x_1 + (x_2 - 1)\,(x_1 + x_3) & \text{altrimenti.} \end{cases}$

⊣

Soluzione Es. 7. Se la lista $\mathsf{R}_0, \mathsf{R}_1, \ldots, \mathsf{R}_{\boldsymbol{r}}$ include tutte le variabili di π ed $\boldsymbol{\ell} + 1$ è il numero d'istruzioni che formano π, posto $\boldsymbol{\ell}_k =_{\text{Def}} \boldsymbol{\ell} + 3\,(k-1)$, basta inserire subito prima della **STOP** di π i blocchetti di istruzioni:

$$
\begin{array}{rl}
\boldsymbol{\ell}_k & \mathbf{IF}\ \ \mathsf{R}_k = 0\ \ \mathbf{GOTO}\ \ \boldsymbol{\ell}_{k+1} \\
& \mathsf{R}_k \ \leftarrow\ \ \mathsf{R}_k - 1 \\
& \mathbf{GOTO}\ \ \boldsymbol{\ell}_k
\end{array}
\quad , \text{ con } k = 1, \ldots, \boldsymbol{r}. \qquad \dashv
$$

Soluzione Es. 8. Anteponendo a un programma il blocchetto

$$
\begin{array}{l}
\mathsf{R}_0 \ \leftarrow\ \ \mathsf{R}_0 + 1 \\
\mathbf{IF}\ \ \mathsf{R}_0 = 0\ \ \mathbf{GOTO}\ \ 0 \\
\mathsf{R}_0 \ \leftarrow\ \ \mathsf{R}_0 - 1
\end{array}
$$

d'istruzioni, dopo avervi incrementato di 3 tutti i numeri che seguivano la parola **GOTO**, non se ne altera il funzionamento. ⊣

Soluzione Es. 9. Sia π un programma nel linguaggio arricchito con la nuova sorta d'istruzione di salto condizionato e sia $\boldsymbol{\ell} + 1$ il numero delle istruzioni che lo compongono; per ogni $h \in \{0, \ldots, \boldsymbol{\ell}\}$, indichiamo con h' il numero delle istruzioni della nuova sorta che precedono l'istruzione $\Im_h$ sita in posizione h.

Consideriamo quindi il primo numero, $\boldsymbol{t}$, tale che la variabile $\mathsf{R}_{\boldsymbol{t}}$ non compaia in π. Introduciamo in π, a mo' di segnaposto, immediatamente dopo ogni istruzione della nuova sorta, una

$$\mathsf{R}_{\boldsymbol{t}} \ \leftarrow\ \ \mathsf{R}_{\boldsymbol{t}} + 1\ ;$$

poi sostituiamo, per tutto π, ogni numero h che compare subito dopo la parola chiave **GOTO** con il numero $h + h'$ dove h' è come detto sopra.

Sostituiamo ora, per tutto π, le coppie d'istruzioni

$$i \quad \boxed{\begin{array}{l} \textbf{IF} \quad \mathsf{R}_j \neq 0 \quad \textbf{GOTO} \quad k \\ \mathsf{R}_{\boldsymbol{t}} \quad \leftarrow \quad \mathsf{R}_{\boldsymbol{t}} + 1 \end{array}}$$

con

$$i \quad \boxed{\begin{array}{l} \textbf{IF} \quad \mathsf{R}_j = 0 \quad \textbf{GOTO} \quad i+2 \\ \textbf{GOTO} \quad k \end{array}} \; .$$

Per finire, sostituiamo ogni istruzione **GOTO** k di salto condizionato con la **IF** $\mathsf{R}_{\boldsymbol{t}} = 0$ **GOTO** k o con la **IF** $\mathsf{R}_{\boldsymbol{m}+1} = 0$ **GOTO** k a seconda che $\boldsymbol{t} > \boldsymbol{m}$ o meno. ⊣

Soluzione Es. 10. Direttamente dalla definizione $\mathfrak{r}_j \;=_{\text{Def}}\; \sum_{t=0}^{s} \mathfrak{r}_{j,t} Q^t$ è facile ricavare

$$\mathfrak{r}_j - Q\mathfrak{r}_j \;=\; \mathfrak{r}_{j,0} + \textstyle\sum_{t=1}^{s} (\mathfrak{r}_{j,t} - \mathfrak{r}_{j,t-1})\; Q^t - \mathfrak{r}_{j,s}\, Q^{s+1} \,,$$

dove

$$\begin{array}{rcll} \mathfrak{r}_{j,t} - \mathfrak{r}_{j,t-1} & = & \Delta_{j,i} & \text{se } i \text{ è l'indice per cui vale } \mathfrak{l}_{i,t-1} = 1 \\ \therefore \quad \mathfrak{r}_{j,t} - \mathfrak{r}_{j,t-1} & = & \sum_{i=0}^{\boldsymbol{\ell}} \Delta_{j,i}\, \mathfrak{l}_{i,t-1} \,. & \end{array}$$

Pertanto

$$\mathfrak{r}_j - Q\mathfrak{r}_j \;=\; \mathfrak{r}_{j,0} - \mathfrak{r}_{j,s} Q^{s+1} + \textstyle\sum_{i=0}^{\boldsymbol{\ell}} \sum_{t=1}^{s} \Delta_{j,i}\, \mathfrak{l}_{i,t-1}\, Q^t$$

e, considerato che quando $\Delta_{j,i} \neq 0$ vale $\mathfrak{l}_{i,s} = 0$, onde

$$\textstyle\sum_{t=1}^{s} \mathfrak{l}_{i,t-1} Q^t \;=\; \sum_{t=0}^{s} \mathfrak{l}_{i,t} Q^{t+1} \;=\; Q\mathfrak{l}_i \;\; ,$$

possiamo riscrivere

$$\mathfrak{r}_j - Q\mathfrak{r}_j \;=\; \mathfrak{r}_{j,0} - \mathfrak{r}_{j,s}\, Q^{s+1} + Q \textstyle\sum_{i=0}^{\boldsymbol{\ell}} \Delta_{j,i} \mathfrak{l}_i \,.$$

A questo punto, per tirar le somme, basta richiamare che:

$$\begin{array}{rcl} \mathfrak{r}_{j,0} & = & \begin{cases} 0 & \text{se} \quad j = 0 \vee j > n \,, \\ a_j & \text{se} \quad 0 < j \leqslant n \,; \end{cases} \\ \mathfrak{r}_{j,s} & = & \begin{cases} 0 & \text{se} \quad j \neq 0 \,, \\ a_0 & \text{se} \quad j = 0 \,. \end{cases} \end{array}$$ ⊣

Soluzione Es. 11. Segue dalle condizioni **(VI)** che ciascun $\mathfrak{l}_i$ è rappresentato, in base Q, da una sequenza formata da al piú $s+1$ cifre 0 / 1; inoltre, visto che dalla somma di $m+1$ ($< Q$) numeri di questo tipo risulta la sequenza formata da $s+1$ uni consecutivi, esattamente uno degli $\mathfrak{l}_i$ avrà un 1 in ciascuna posizione t con $0 \leqslant t \leqslant s$.

Nel caso di $\mathfrak{l}_{\boldsymbol{\ell}}$, dalla condizione $\mathfrak{l}_{\boldsymbol{\ell}} \sqsubseteq Q^s$ con cui stiamo rimpiazzando la **(VIII)** segue che se $\Im_{\boldsymbol{\ell}}$ si attiva almeno una volta, allora si attiva all'istante s; per ricavare la **(VIII)** occorre semplicemente accertare che quest'attivazione avvenga davvero. Notiamo in effetti che, per ogni $i < \boldsymbol{\ell}$, la cifra in posizione

s di $\mathfrak{l}_i$ dev'essere 0, altrimenti verrebbe contraddetta una delle condizioni **(X)**, **(XI)**, **(XII)**; pertanto $\Im_{\boldsymbol{\ell}}$ è la sola istruzione qualificata ad attivarsi all'istante s: almeno una lo deve fare e quindi tocca a lei. ⊣

Soluzione Es. 12. Per rendere uniche la $\flat$ e la Q basta richiedere, oltre ad **(I)**–**(XIII)**, anche: $2^{\flat} \leqslant (2\,a_1 + \cdots + 2\,a_{\boldsymbol{m}} + 2\,s)\ \max\,(\boldsymbol{\ell}+1)$. ⊣

Soluzione Es. 13. Si scriva un programma γ che computi la funzione

$$g(a) \quad =_{\text{Def}} \quad \begin{cases} 1 & \text{se vi sono numeri primi } p,q \text{ tali che } 2\,a+4 = p+q, \\ 0 & \text{altrimenti,} \end{cases}$$

ricorrendo a un procedimento che determini i numeri primi, ad es. tramite lo storico *crivello di Eratostene* (cfr. `http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes`.

Quindi, alla stregua della dimostrazione del Teor. 1, si ricavi da γ un sistema di equazioni diofantee esponenziali definente il grafo $\mathcal{G}(a,b)$ di g; poi si riscriva tale sistema come singola equazione $G(a,b,\vec{y}) = 0$. La specifica richiesta è $G(x,0,\vec{y}) = 0$. ⊣

Soluzione Es. 14. Il Teor. 1 ci dà un'equazione diofantea esponenziale $E_{\mathsf{sn}} = E_{\mathsf{dx}}$ tale che

$$g(a_1,\ldots,a_{\boldsymbol{m}}) = a_0 \quad \leftrightarrow \quad \exists\, z_1 \cdots \exists\, z_{\boldsymbol{r}+\boldsymbol{\ell}+6}$$
$$E_{\mathsf{sn}}(a_1,\ldots,a_{\boldsymbol{m}},a_0,z_1,\ldots,z_{\boldsymbol{r}+\boldsymbol{\ell}+6}) \quad = \quad E_{\mathsf{dx}}(a_1,\ldots,a_{\boldsymbol{m}},a_0,z_1,\ldots,z_{\boldsymbol{r}+\boldsymbol{\ell}+6})\,;$$

dunque $\langle a_1,\ldots,a_{\boldsymbol{m}}\rangle$ starà nel dominio di g se e solo se

$$\exists\, z_0 \cdots \exists\, z_{\boldsymbol{r}+\boldsymbol{\ell}+6} \quad E_{\mathsf{sn}}(a_1,\ldots,a_{\boldsymbol{m}},z_0,\ldots,z_{\boldsymbol{r}+\boldsymbol{\ell}+6}) \quad = \quad E_{\mathsf{dx}}(a_1,\ldots,a_{\boldsymbol{m}},z_0,\ldots,z_{\boldsymbol{r}+\boldsymbol{\ell}+6})\,.$$ ⊣

Soluzione Es. 15. Avvalendoci del Teor. 1 possiamo definire esistenzialmente, a partire da un programma che computi g, la relazione diadica $g(a) = b$ tramite un'equazione esponenziale $E(a,b,y_2,\ldots,y_h) = 0$. Sostituiamo i parametri di quest'equazione con due nuove incognite y_0, y_1; poi appiattiamo alla Skolem la $E(y_0,y_1,y_2,\ldots,y_h) = 0$ estroflettendone le sottoespressioni, fino a ridurla a sistema (=congiunzione) di condizioni delle forme

$$x \;=\; y\,z\,, \qquad x \;=\; y+z\,, \qquad x \;=\; 2^y\,, \qquad y = 0\,, \qquad y = z\,,$$

dove x,y,z rappresentano variabili—da riguardarsi, quelle nuove al pari di $y_0,y_1,\ldots,y_h$, come incognite su $\mathbb{N}$. (Qui entra in gioco il fatto che la relazione $u \geqslant 2 \wedge y = 2^u$ ha crescita grosso modo esponenziale e dunque ci permette di eliminare l'esponenziazione).

Tornando ora a comprimere il sistema, otteniamo un'equazione

$$D(y_0,\ldots,y_m,2^{y_0},\ldots,2^{y_m}) \;=\; 0$$

dove $D(y_0,\ldots,y_m,z_0,\ldots,z_m)$ è un polinomio diofanteo in cui figura la y_0 rappresentativa del parametro d'interesse. Il polinomio P cercato è semplicemente:

$$P(a,y_0,\ldots,y_m,z_0,\ldots,z_m) \quad =_{\text{Def}} \quad (a+1) - (y_0+1)\big(1 - D^2(y_0,\ldots,y_m,z_0,\ldots,z_m)\big)\,.$$

Soluzione Es. 16. Abbiamo la seguente catena di doppie implicazioni:

$$\begin{array}{rcll}
\vec{\boldsymbol{a}} & \text{sta nell'insieme descritto da} & E(\vec{a},\vec{y}) & \leftrightarrow \\
E(\vec{\boldsymbol{a}},\vec{y}) & = \; 0 \quad \text{ha soluzione} & & \leftrightarrow \\
\psi_{\pi}^{(n)}(\vec{\boldsymbol{a}}) & \neq \; \perp & & \leftrightarrow \\
\psi_{\pi}^{(n)}(\vec{\boldsymbol{a}}) & = \; 0 & & \leftrightarrow \\
0 & = \; \psi_{U_n}^{(n+1)}(\vec{\boldsymbol{a}},\#\pi) & & \leftrightarrow \\
0 & = \; W(0,\vec{\boldsymbol{a}},\#\pi,\vec{x}) \quad \text{ha sol.} & & \leftrightarrow \\
0 & = \; U(\vec{\boldsymbol{a}},\#\pi,\vec{x}) \quad \text{ha sol.} & & \leftrightarrow \\
\vec{\boldsymbol{a}} & \text{sta nell'insieme descritto da} & U(\vec{a},\#\pi,\vec{x})\,. &
\end{array}$$

Riferimenti bibliografici

[Cut80] Nigel Cutland. *Computability: An Introduction to Recursive Function Theory*. Cambridge University Press, 1980.

[Dav93] Martin Davis. *Lecture Notes in Logic*. Courant Institute of Mathematical Sciences, New York University, 1993.

[DP58] Martin Davis and Hilary Putnam. Reduction of Hilbert's tenth problem. *The Journal of Symbolic Logic*, 23(2):183–187, 1958.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential Diophantine equations. *Ann. of Math., Second Series*, 74(3):425–436, 1961.

[DSW94] Martin D. Davis, Ron Sigal, and Elaine J. Weyuker. *Computability, complexity, and languages - Fundamentals of theoretical computer science*. Computer Science ad scientific computing. Academic Press, 1994.

[JM84] J. P. Jones and Y. V. Matijasevič. Register machine proof of the theorem on exponential Diophantine representation of enumerable sets. *The Journal of Symbolic Logic*, 49(3):818–829, 1984.

[Kre62] Georg Kreisel. A3061: Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations. *Mathematical Reviews*, 24A(6A):573, 1962.

[Rob52] Julia Robinson. Existential definability in arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. Reprinted in [Rob96, p. 47ff.].

[Rob96] Julia Robinson. *The collected works of Julia Robinson*, volume 6 of *Collected Works*. American Mathematical Society, Providence, RI, 1996. ISBN 0-8218-0575-4. With an introduction by Constance Reid. Edited and with a foreword by Solomon Feferman. xliv+338 pp.

[SS63] John C. Shepherdson and Howard E. Sturgis. Computability of recursive functions. *J. ACM*, 10(2):217–255, 1963.

[TZ08] Terence Tao and Tamar Ziegler. The primes contain arbitrarily long polynomial progressions. *Acta Mathematica*, 201:213–305, 2008.