

Come istituire una biiezione ‘effettiva’ fra le sequenze di parole (dell’alfabeto proposizionale) e i numeri naturali

Eugenio G. Omodeo

a.a. 2015/16

Cominciamo con porre gli elementi dell’*alfabeto proposizionale* in corrispondenza con gli interi positivi:

$$\begin{array}{cccccccc} (,) , & \rightarrow , & \mathbf{p}_0 , & \mathbf{p}_1 , & \mathbf{p}_2 , & \mathbf{p}_3 , & \dots \\ \color{red}{1} & \color{red}{2} & \color{red}{3} & \color{red}{4} & \color{red}{5} & \color{red}{6} & \color{red}{7} \end{array}$$

e associamo al numero **0** un simbolo ‘fuori alfabeto’: lo *spazio vuoto*.

Per il teorema fondamentale dell’aritmetica, dato un qualsiasi numero naturale d , possiamo scomporre il successivo $d + 1$ così:

$$d + 1 = \prod_{i=1}^{k_d} p_i^{m_i} ,$$

dove

$$p_1 , p_2 , p_3 , p_4 , p_5 , p_6 , \dots$$

è la successione $2, 3, 5, 7, 11, 13, \dots$ dei numeri *primi* disposti in ordine crescente e dove $m_{k_d} \neq 0$ vale quando $k_d \neq 0$. Pertanto in d possiamo ‘leggere’ una sequenza

$$w_0 , \dots , w_{\ell_d}$$

di parole w sull’alfabeto proposizionale, intercalate da singoli spazi vuoti.

A partire dalla scomposizione univoca di $d + 1$ descritta sopra, possiamo ottenerne infinite, una per ogni numero naturale h :

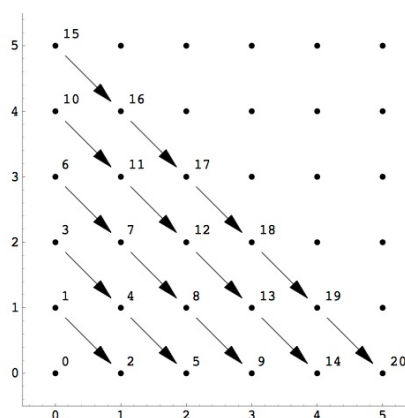
$$d + 1 = \prod_{i=1}^{k_d+h} p_i^{m_i} , \text{ semplicemente ponendo } m_{k_d+1} = \dots = m_{k_d+h} = 0.$$

Ciò rappresenta l’inserimento di h parole vuote dopo w_{ℓ_d} .

All'inverso, qualsiasi sequenza W di parole è individuata da quell'unica coppia $\langle d, h \rangle$ in cui possiamo leggere W nel modo accennato sopra.

A questo punto abbiamo istituito una corrispondenza biunivoca fra le sequenze di parole e le coppie di numeri naturali; a sua volta, ogni coppia di naturali può essere codificata con un naturale singolo tramite la corrispondenza di Cantor (vedi figura):

$$\langle d, h \rangle \mapsto \frac{(d+h)^2 + 3d + h}{2}.$$



Ora posso proporvi un nuovo esercizio dello stesso tipo, ma piú impegnativo: Ideare un procedimento che controlli *che* $A \vdash \vartheta$ vale nella logica proposizionale standard \mathbb{P} , e che fornisca come certificazione una catena di passaggi d'inferenza che porti dalle premesse A alla conclusione ϑ . Notate il 'che': non vi sto chiedendo che il procedimento stabilisca 'se $A \vdash \vartheta$ valga o meno'. Quindi, nel caso che $A \not\vdash \vartheta$, il procedimento può dilungarsi all'infinito.

'standard'?

Quanto ad A , potete assumere che sia un insieme finito dato esplicitamente o, piú in generale, che per ogni enunciato α si possa stabilire, tramite apposito algoritmo "*decisore*", se α appartenga o meno ad A . Sotto l'ipotesi piú generale, A potrebbe anche essere infinito.

Come controllare *che* $A \vdash \vartheta$ nella logica \mathbb{P}

Soluzione dell'esercizio. Consideriamo un insieme $A \subseteq \mathcal{P}$ tale che per ogni enunciato α si possa stabilire, tramite apposito algoritmo, se α appartenga o

meno ad A (un esempio scontato è $A = \emptyset$). Sia dato inoltre un enunciato ϑ .

Ecco come si può controllare—purché ciò corrisponda al vero—che, ai sensi della nozione di DIMOSTRABILITÀ della logica \mathbb{P} , vale

$$A \vdash \vartheta .$$

Per $d = 1, 2, 3, 4, \dots$

- si ottenga da d la corrispondente sequenza w_0, \dots, w_{ℓ_d} di parole sull'alfabeto proposizionale (con w_{ℓ_d} non vuota);
- si accerti che ciascuna di tali parole appartenga a \mathcal{P} e, in caso contrario, si passi subito al d successivo; altrimenti
- si accerti se l'ultima di tali parole soddisfi l'identità

$$w_{\ell_d} = \vartheta$$

e, se così non è, si passi subito al d successivo; altrimenti

- si accerti che per ciascuna w_j vale almeno una delle tre condizioni:
 - w_j appartiene ad A ,
 - w_j ricade in uno schema d'assioma logico,
 - w_j risulta da due passi w_h, w_k tali che $h < j$ e $k < j$, tramite *modus ponens*;

se qualche w_j viola tutte e tre queste condizioni, si passi al d successivo; altrimenti

- arrivando qui, siamo sicuri che tutti i controlli hanno avuto successo; dunque interrompiamo il ciclo segnalando che $A \vdash \vartheta$ in \mathbb{P} .

e la 'certificazione' dov'è?

Si osservi che il metodo appena visto non è in grado di *decidere* ma solo di *semi-decidere*. Dunque la sua prestazione è incomparabilmente peggiore, per lo meno quando A è un insieme finito, di quella di un metodo SEMANTICO, che invece delle dimostrazioni consideri direttamente gli assegnamenti di valore di verità, per accertare se $A \models \vartheta$ valga o meno. (E quando A è infinito? Viene comunque in aiuto la compattezza; ma anche la semantica può condurci, in questo caso, a un procedimento perpetuo...).