Riduzione al 4º grado di un'equazione polinomiale diofantea $P = 0$

Eugenio Omodeo

18 marzo 2019

Partendo dall'equazione $P = 0$ con P polinomio multivariato su $\mathbb{Z}$, otterremo un sistema $\mathcal{S}$ di equazioni S_i delle tre forme $u = 1$, $s = v + w$, $q = p^2$ (ove u, s, v, w, q, p indicano variabili) che avrà soluzione se e solo se $P = 0$ ne ha. A sua volta $\mathcal{S}$ può venir riscritto come $\sum_i (Q_i)^2 = 0$, ove ciascuna Q_i risulta dalla corrispondente S_i mediante la riscrittura:

$$\begin{array}{rcl} u = 1 & \rightsquigarrow & u - 1 \\ s = v + w & \rightsquigarrow & v + w - s \\ q = p^2 & \rightsquigarrow & p^2 - q \end{array}$$

Poniamo $Q = \sum_i (Q_i)^2$. La trasformazione di $P = 0$ in $Q = 0$ amplierà l'insieme di variabili in gioco, in compenso riducendo a 4 il grado dell'equazione. Ogni soluzione di $P = 0$ si potrà estendere a soluzione di $Q = 0$; viceversa ogni soluzione di $Q = 0$, una volta ristretta alle variabili di P, darà luogo a una soluzione di $P = 0$.

Procedimento:

i. Introduco due nuove variabili, u e z; parto con $\mathcal{S}$ costituito dalle equazioni $u = 1$, $u = z + u$; sostituisco in P:

- ogni presenza di 0 con la z,
- ogni costante numerica $\boldsymbol{\kappa}(\geqslant 0)$ con $\underbrace{u + \cdots + u}_{\boldsymbol{\kappa} \text{ volte}}$.

ii. Finché trovo, entro P, un'espressione di una delle tre forme $x \pm y$, $x \cdot y$, ove x e y indicano variabili, la rimpiazzo con una nuova variabile t. Aggiungo ad $\mathcal{S}$, nei tre rispettivi casi:

- l'equazione $t = x + y$,
- l'equazione $y = x + t$,
- le equazioni $f = x^2$, $g = y^2$, $h = f + g$, $k = t + t$, $p = x + y$, $q = h + k$, $q = p^2$, ove f, g, h, k, p, q sono ulteriori nuove variabili.

iii. Ora che P si è ridotta a una singola variabile r, corono $\mathcal{S}$ con l'equazione $r = z + z$ (ove z è la stessa variabile introdotta al passo **i.**).

Riduzione a forma 3CNF di un enunciato E della logica proposizionale

Eugenio Omodeo

18 marzo 2019

Partendo da un enunciato proposizionale E nei connettivi logici diadici $\&, \vee, \rightarrow, \leftrightarrow$ (piú eventuali altri), otterremo un insieme $\mathcal{S}$ di disgiunzioni D_i di letterali (i.e., lettere proposizionali asserite o negate) tale che $\&_i\, D_i$ sarà *soddisfacibile*—cioè vera in qualche interpretazione $\Im$—se e solo se tale è E. Ciascuna D_i sarà costituita da tre letterali; la lunghezza complessiva di $\mathcal{S}$ sarà linearmente correlata alla lunghezza di E.

Poniamo $K = \&_i\, D_i$. La trasformazione di E in K amplierà l'insieme di lettere proposizionali in gioco. Ogni interpretazione soddisfacente E si potrà estendere in modo da soddisfare K; viceversa ogni interpretazione soddisfacente K, una volta ristretta alle lettere presenti in E, soddisferà E.

Procedimento:

- poniamo, anzitutto, $i := 0$, $\mathcal{S}_0 := \emptyset$ ed $E_0 := E$;
- poi, fino a quando E_i non è una lettera o una lettera negata:
  - selezioniamo in E_i un sotto-enunciato della forma $\neg\neg G$ oppure della forma $X \star Y$, dove X, come pure Y, rappresenta una lettera o una lettera negata e $\star$ rappresenta un connettivo;
  - nel primo caso otteniamo E_{i+1} sostituendo $\neg\neg G$ in E_i con G, e manteniamo $\mathcal{S}_{i+1} := \mathcal{S}_i$;
  - nell'altro caso, otteniamo E_{i+1} sostituendo $X \star Y$ in E_i con una lettera Z nuova di zecca, ed otteniamo $\mathcal{S}_{i+1}$ aggiungendo a $\mathcal{S}_i$ tre o quattro nuovi congiunti esprimenti la bi-implicazione $Z \leftrightarrow (\, X \star Y\,)$,

in base alla seguente tabella:

$Z \leftrightarrow X \mathbin{\&} Y$	$(Z \rightarrow X) \mathbin{\&} (Z \rightarrow Y) \mathbin{\&} (X \mathbin{\&} Y \rightarrow Z)$ $\rightsquigarrow (\neg Z \vee X) \mathbin{\&} (\neg Z \vee Y) \mathbin{\&} (\neg X \vee \neg Y \vee Z)$
$Z \leftrightarrow X \vee Y$	$(X \rightarrow Z) \mathbin{\&} (Y \rightarrow Z) \mathbin{\&} (Z \rightarrow X \vee Y)$ $\rightsquigarrow (\neg X \vee Z) \mathbin{\&} (\neg Y \vee Z) \mathbin{\&} (\neg Z \vee X \vee Y)$
$Z \leftrightarrow (X \leftrightarrow Y)$	$(Z \mathbin{\&} X \rightarrow Y) \mathbin{\&} (Z \mathbin{\&} Y \rightarrow X)$ $\mathbin{\&} (X \mathbin{\&} Y \rightarrow Z) \mathbin{\&} (\neg X \mathbin{\&} \neg Y \rightarrow Z)$ $\rightsquigarrow (\neg Z \vee \neg X \vee Y) \mathbin{\&} (\neg Z \vee \neg Y \vee X)$ $\mathbin{\&} (\neg X \vee \neg Y \vee Z) \mathbin{\&} (X \vee Y \vee Z)$
.....	.....

– effettuiamo l'incremento $i := i + 1$;

- da ultimo poniamo $\mathcal{S} := \mathcal{S}_i \cup \{E_i\}$. ⊣

Esempio. L'enunciato $\neg r \mathbin{\&} (p \rightarrow (q \vee r))$ è tautologicamente equivalente all'enunciato $\neg r \mathbin{\&} (\neg p \vee q \vee r)$ in FNC, ed anche al piú semplice $\neg r \mathbin{\&} (\neg p \vee q)$, e all'enunciato $(\neg r \mathbin{\&} \neg p) \vee (\neg r \mathbin{\&} q)$ in FND. Il procedimento di riduzione in FNC produrrà il seguente enunciato che, pur non essendo equivalente ai precedenti, è equi-soddisfacibile con loro:

$$\begin{array}{llllllll} (\neg q \vee p') & \mathbin{\&} & (\neg r \vee p') & \mathbin{\&} & (\neg p' \vee q \vee r) & \mathbin{\&} \\ (p \vee p'') & \mathbin{\&} & (\neg p' \vee p'') & \mathbin{\&} & (\neg p'' \vee \neg p \vee p') & \mathbin{\&} \\ (\neg p''' \vee \neg r) & \mathbin{\&} & (\neg p''' \vee p'') & \mathbin{\&} & (r \vee \neg p'' \vee p''') & \mathbin{\&} \\ p''' \,. & & & & & & & \end{array}$$

⊣

Esercizio 1. Modificare il procedimento descritto sopra per far sí che ciascuno dei congiunti D_i della forma normale congiuntiva $\mathcal{S}$ sia disgiunzione di esattamente tre letterali uno diverso dall'altro. ⊣

Esercizio 2. Mostrare che per soddisfare la congiunzione

$$\begin{array}{llllllll} (\neg p \vee \neg q \vee \neg r) & \mathbin{\&} & & & & & & \\ (\neg p \vee r \vee \neg t) & \mathbin{\&} & (\neg r \vee q \vee \neg t) & \mathbin{\&} & (\neg q \vee p \vee \neg t) & \mathbin{\&} \\ (\neg p \vee r \vee t) & \mathbin{\&} & (\neg r \vee q \vee t) & \mathbin{\&} & (\neg q \vee p \vee t) & & \end{array}$$

è indispensabile attribuire il valore falso tanto a p che a q che ad r. ⊣

Soddisfacibilità di forme normali congiuntive

Definiamo qui due operazioni su un generico dominio d'integrità ordinato:

$$\begin{aligned} \neg x &=_{\text{Def}} (x-1)^2, \\ y \vee z &=_{\text{Def}} y + z - y\,z \end{aligned}$$

(cosicché $x \vee y \vee z = x\,y\,z - x\,y - x\,z - y\,z + x + y + z$). Consideriamo poi un'equazione della forma

$$\sum_{i=1}^{\ell} \neg(\, p_i^2 + \neg p_i \,) + \sum_{j=1}^{\kappa} \neg(\, x_j \vee y_j \vee z_j) \;=\; 0\,, \qquad (*)$$

dove $p_1, \ldots, p_\ell$ sono incognite distinte e

$$\{\, x_1, y_1, z_1, \ldots, x_\kappa, y_\kappa, z_\kappa \,\} \subseteq \{\, p_1, \ldots, p_\ell,\ \neg p_1, \ldots, \neg p_\ell \,\}\,.$$

Nel risolvere l'equazione polinomiale (∗) occorre soddisfare ciascuna delle

$$\neg(\, p_i^2 + \neg p_i \,) \;=\; 0\,,$$

in altre parole richiedere che $p_i = 0$ o $p_i = 1$, per ogni i . È chiaro che alle istanze del decimo problema di Hilbert della particolarissima forma (∗) (per la cui risoluzione è indifferente che ci si riferisca a $\mathbb{N}$, a $\mathbb{Z}$, a $\mathbb{Q}$, o ad $\mathbb{R}$) si può dare risposta tramite un algoritmo decisionale. Tuttavia rimane un grande problema insoluto dei giorni nostri stabilire se vi sia un algoritmo di complessità polinomiale in grado di rispondere a tutte le istanze di questo tipo (vedi [Garey and Johnson(1979)]).

Esercizio 3 (**Terzo escluso**)**.** Dimostrare che l'equazione $\neg(\, p^2 + \neg p \,) = 0$ ha come soluzioni: $p = 0$, $p = 1$ e nessun'altra. Quante e quali soluzioni ha l'equazione $\neg(\, p \vee \neg p \,) = 0$? È risolubile un'equazione della forma $x \vee y \vee 2 = 1$ con $\{x, y\} \subseteq \{p, q, \neg p, \neg q\}$, se richiediamo che $\{p, q\} \subseteq \{0, 1, 2\}$? ⊣

Riferimenti bibliografici

[Garey and Johnson(1979)] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Series of Books in the Mathematical Sciences. W. H. Freeman, 1979. ISBN 0716710455.