

Estratto da

R. Ferro e A. Zanardo (a cura di), *Atti degli incontri di logica matematica*
Volume 3, Siena 8-11 gennaio 1985, Padova 24-27 ottobre 1985, Siena 2-5
aprile 1986.

Disponibile in rete su <http://www.ailalogica.it>

ABC: UNA TEORIA ALGEBRICA PER RIDURRE CODICE INTERMEDIO

STEFANO STEFANI
Siena

Lo sviluppo di sempre piu' numerosi linguaggi di programmazione e, dall'altro lato, di sempre nuove architetture dei dispositivi di calcolo, ha reso sempre piu' opportuno manipolare e trasformare i programmi rappresentandoli sotto forma di "codice intermedio".

L'indipendenza di questa rappresentazione sia dal particolare linguaggio sorgente che dall'hardware utilizzato, rende possibile, oltreche' opportuno, definire in astratto una semantica che le trasformazioni del programma, espresso in codice intermedio, devono rispettare per essere corrette.

Nel seguito presenteremo due teorie algebriche (ABC ed A,B,C) che cercano di catturare il comportamento delle operazioni aritmetiche e Booleane che ogni calcolatore e' in grado di eseguire.

Per la teoria A,B,C , ottenuta da ABC indebolendo i legami tra "parte aritmetica" e "parte Booleana" e' stato formulato un sistema di riduzione mediante

regole di riscrittura, che unifica termini algebricamente equivalenti in forme canoniche definite in modo sufficientemente naturale (tale ad esempio da comportare il così detto "constants folding"). La formulazione di un sistema di riduzione per ABC sarebbe di utilità per ottimizzare il calcolo delle espressioni adattandone il codice a diversi dispositivi di calcolo. Questo sembra un passo preliminare e promettente in vista di uno studio sistematico che affronti trasformazioni che coinvolgono sott'espressioni ripetute ed eventualmente interessino il controllo non solo del flusso dei dati ma del flusso del programma.

LA VARIETA' ALGEBRICA "ABC"

La definizione seguente intende "catturare" una struttura algebrica che rifletta il comportamento di un anello (intero) e di un anello booleano collegati da una serie di operazioni, da intendersi come pseudo predicati.

ABC è una varietà di algebre di tipo

$$T = \langle 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2 \rangle$$

le cui operazioni base sono denotate rispettivamente da

0, U (supremo booleano), I (unita'),

M (massimo intero), ! (differenza simmetrica),

&, +, *, ? (uguaglianza), <, > ,

definita dai seguenti assiomi:

- A1 $x+(y+z) = (x+y)+z$
 A2 $0+x = x$
 A3 $M+M = 0$
 A4 $I+U = 0$
 A5 $x*y = y*x$
 A6 $x*(y*z) = (x*y)*z$
 A7 $x*I = x$
 A8 $x*(y+z) = (x*y)+(x*z)$
 B1 $x!(y!z) = (x!y)!z$
 B2 $x!x = 0$
 B3 $x!y = y!x$
 B4 $x&(y&z) = (x&y)&z$
 B5 $x&x = x$
 B6 $x&U = x$
 B7 $x&(y!z) = (x&y)!(x&z)$
 AB $x+y = ((x&y)+(x&y))+(x!y)$
 C1 $x<y = y>x$
 C2 $(x<y)&(y<x) = 0$
 C3 $((x<y)!(x?y))!(x>y) = U$
 C4 $x&(x?0) = 0$
 C5 $(x!t)?(y!t) = (x+z)?(y+z)$
 C6 $((x<y)&I)*U = x<y$
 C7 $((U!(x<y))&I)*U = U!(x<y)$
 C8 $(x<(x+I))!((x&(M?0))&((x+I)&M)?M))!(M?0) = U$
 C9 $(x<y)&(y<z) = ((x<y)&(y<z))&(x<z)$

Si può facilmente osservare che il ridotto di un'algebra A della varietà ABC ottenuto considerando solamente le operazioni +, *, 0, I, U è un anello, mentre se si considerano le operazioni !, &, 0, U si avrà a che fare con un anello booleano.

Si ottiene inoltre che ogni algebra finita A della varietà ABC deve avere come cardinalità una potenza di due e che il gruppo (A, +, 0) deve essere somma diretta di gruppi ciclici; se quindi A non è scomponibile in prodotti diretti deve essere isomorfa al gruppo additivo degli interi modulo la cardinalità di A. Non è difficile vedere che i quozienti degli interi modulo una potenza di due (con

le operazioni booleane opportunamente definite) sono, a meno di isomorfismi, le uniche algebre di ABC non direttamente scomponibili non banali.

Un modello e' particolarmente significativo tra le algebre infinite di ABC, quello ottenuto considerando i sottoinsiemi finiti e cofiniti dei numeri naturali e su essi le operazioni aritmetiche definite in "complemento due". In questo caso il ridotto aritmetico sara' isomorfo agli interi e la costante M sara' zero.

LE VARIETA' ABC(2N) ED A,B,C

Dato che ci interessano particolarmente le algebre finite e' utile introdurre una famiglia di costanti (operazioni 0-arie) che possano essere interpretate su elementi dell'algebra.

Dato una potenza intera di due N, aggiungiamo al tipo 2N costanti denotate

$$\#-N, \#(-N+1), \dots, \#(N-2), \#(N-1).$$

La varieta' ABC(2N) di questo nuovo tipo e' ottenuta aggiungendo ad ABC gli assiomi che corrispondono a considerare sulle costanti le operazioni che vi sono definite considerando gli elementi rappresentati in complemento due.

Le principali congetture che emergono dallo studio di tali varieta' sono: 1) Il modello di ABC(2N) con 2N elementi genera la varieta' stessa; 2) La classe di

tali modelli, al variare di N, genera ABC.

Il verificarsi di queste congetture mostrerebbe che gli assiomi scelti sono adeguati a caratterizzare i "modelli standard", almeno per quello che riguarda l'aspetto equazionale.

Per cominciare ad affrontare la formulazione di un sistema di regole di riduzione per ABC(2N), e' parso opportuno indebolire l'insieme degli assiomi nel modo seguente: la costante M, le operazioni \langle e \rangle e gli assiomi che le riguardano vengono eliminati; cosi' pure gli assiomi AB e C4. Occorre inoltre aggiungere gli assiomi $x+y = y+x$ e $x!0 = x$. La varieta' cosi' definita e' detta A,B,C. Per queste varieta' e' possibile unificare termini equivalenti attraverso un sistema di regole di riscrittura ed un tale sistema di regole e' stato effettivamente formulato. Tuttavia, a causa della particolare complessita' della struttura algebrica che ci si trova di fronte, pare inevitabile dover ricorrere ad una formulazione piu' ampia delle regole stesse, suddividendo ad esempio le regole di riduzione in piu' gruppi ed introducendo la nozione di "relativamente normale"; aggiungendo oltre ad un buon ordine dei termini nuove operazioni ausiliarie; e mettendosi in grado, infine, di condizionare l'applicazione di una riscrittura ad alcuni predicati primitivi che completano l'azione di pattern matching.

BIBLIOGRAFIA

- [1] BIRKHOFF, G. The role of modern algebra in computing, SIAM-AMS Proc IV, 1981.
- [2] HUET, G. Confluent reductions: abstract properties and applications to term rewriting systems, J.ACM (27)4 (1980).
- [3] KNUTH, D.B. - BENDIX, F.B. Simple word problems in universal algebra, In "Computational Problems in abstract algebras" (J. Leech Ed.) Pergamon Press 1970, 263-297.