Strutture algebriche, algebre di Boole

Lezione 04 di Architettura degli elaboratori

Docente: Giuseppe Scollo

Università di Catania
Dipartimento di Matematica e Informatica
Corso di Laurea in Informatica, I livello, AA 2014-15

Indice

precursori della formalizzazione logica: da Aristotele a Leibniz

- teoria del sillogismo: forme valide del ragionamento
- la visione di Leibniz: *Mathesis Rationis*

Leibniz anticipa di un paio di secoli l'intuizione di George Boole: le leggi di un'algebra del pensiero

ma cos'è un'*algebra*?

in prima approssimazione: un insieme + operazioni su di esso

esempi: l'aritmetica dei naturali, degli interi, dei reali, ...

le equazioni giocano un ruolo fondamentale nell'algebra tradizionale:

incognite: le variabili

sono non meno fondamentali nell'algebra astratta (XX secolo), dove però:

incognite: i simboli di operazione

il concetto di algebra, nella prima approssimazione introdotta sopra, si generalizza a quello di struttura algebrica, in cui si distingue:

- il sostegno, costituito da uno o più insiemi, su cui sono definite:
- le operazioni e/o relazioni di cui la struttura è dotata

una ridotta di una struttura A è una struttura costituita da un sottoinsieme delle operazioni e relazioni di A, definite sullo stesso sostegno

una struttura si dice omogenea se il sostegno consta di un solo insieme

- altrimenti si dice eterogenea

  N.B.: il sostegno di una ridotta di una struttura eterogenea A può essere costituito da un sottoinsieme proprio della famiglia di insiemi sostegno di A, purché tutte le operazioni della ridotta siano definite nel suo sostegno

una struttura dotata solo di operazioni totali è detta algebra in senso stretto, altrimenti è un'algebra in senso lato

tali sono anche le strutture relazionali, dotate solo di relazioni

N.B.: è sempre possibile rappresentare una struttura algebrica come

- un'algebra (eterogenea) in senso stretto, rappresentando le relazioni per il tramite delle loro proprietà caratteristiche, intese come operazioni
- una struttura relazionale, rappresentando le operazioni k-arie come relazioni $(k+1)$-arie

assiomi di strutture algebriche

semigruppo: $(A; \cdot)$, con $\cdot$ un'operazione binaria associativa

il semigruppo è detto commutativo se tale è l'operazione binaria

monoide: $(A; e, \cdot)$, un semigruppo $(A; \cdot)$ con e costante neutra rispetto a $\cdot$

il monoide è detto commutativo se lo è il suo ridotto semigruppo

gruppo [commutativo]: $(A; e, \cdot, -)$, un monoide [commutativo] $(A; e, \cdot)$ con un'operazione unaria $-$ che dà l'inverso rispetto a $\cdot$ ed e: $x \cdot -x = -x \cdot x = e$

semianello [commutativo]: $(A; 0, 1, +, \cdot)$, un monoide commutativo $(A; 0, +)$, detto additivo, e un monoide [commutativo] $(A; 1, \cdot)$, detto moltiplicativo, tali da soddisfare:

1. distributività: $x \cdot (y+z) = (x \cdot y)+(x \cdot z)$, $(x+y) \cdot z = (x \cdot z)+(y \cdot z)$
2. cancellazione: $0 \cdot x = x \cdot 0 = 0$

anello [commutativo]: $(A; 0, 1, +, \cdot, -)$, un semianello [commutativo] $(A; 0, 1, +, \cdot)$, con il monoide additivo esteso a un gruppo commutativo $(A; 0, +, -)$

deduzione equazionale

classi di algebre in senso stretto quali quelle viste in precedenza sono caratterizzate da assiomi di forma molto semplice:

equazioni di termini, costituiti da simboli di operazione e variabili: $t_1 = t_2$ (con implicita quantificazione universale)

quando una classe di algebre è caratterizzata da un insieme di equazioni, che ne costituisce la base assiomatica, è possibile dedurre da tale base tutte le equazioni valide in ogni algebra della classe mediante le regole del calcolo equazionale di Garrett Birkhoff:

- riflessività: $t = t$
- simmetria: *se* $t_1 = t_2$ *allora* $t_2 = t_1$
- transitività: *se* $t_1 = t_2$, $t_2 = t_3$ *allora* $t_1 = t_3$
- sostituzione: *se* $t_1 = t_2$ *allora* $\tau(t_1) = \tau(t_2)$

  il termine $\tau(t)$ è ottenuto dal termine t per sostituzione simultanea di tutte le occorrenze di ciascuna variabile con uno stesso termine
- rimpiazzamento: *se* $t_1 = t_2$ *allora* $t[u \leftarrow t_1] = t[u \leftarrow t_2]$

  il termine $t[u \leftarrow t']$ è ottenuto dal termine t rimpiazzando il suo sottotermine al posto u con il termine t'

reticoli

un reticolo è un ordinamento parziale in cui ogni coppia di elementi abbia:

un minimo maggiorante (*join*, o *l.u.b.*: *least upper bound*) e
un massimo minorante (*meet*, o *g.l.b.*: *greatest lower bound*)

alternativamente, per via strettamente algebrica:

- un semireticolo è un semigruppo commutativo idempotente (assiomi ACI: l'idempotenza di un'operazione binaria $\cdot$ è espressa dall'equazione $x \cdot x = x$)
- un reticolo è un'algebra $(A; \vee, \wedge)$ tale che le sue due ridotte $(A; \vee)$, $(A; \wedge)$ sono semireticoli, e inoltre valgono gli assiomi di assorbimento:

$$x \vee (x \wedge y) = x \qquad x \wedge (x \vee y) = x$$

reticoli algebrici

occorrono dunque 8 equazioni per la base assiomatica dei reticoli?

no, ne bastano 6: l'idempotenza è deducibile dagli altri, v. l'esercizio sugli assiomi indipendenti per i reticoli algebrici

che fine ha fatto l'ordinamento del reticolo? lo si può definire algebricamente come abbreviazione di equazioni (equivalenti) in ciascuna delle due operazioni binarie:

$$x \leq y \equiv x \vee y = y \qquad \text{oppure: } x \leq y \equiv x \wedge y = x$$

N.B.: v. l'esercizio sull'ordinamento nei reticoli algebrici

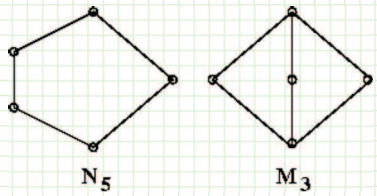
un reticolo è completo se ogni insieme di suoi elementi ha minimo maggiorante e massimo minorante

algebre di Boole

un reticolo è detto distributivo se ciascuna delle sue due operazioni è distributiva rispetto all'altra

caratterizzazione M_3-N_5 dei reticoli non distributivi:

un reticolo è non distributivo sse ha almeno un sottoreticolo con diagramma di Hasse M_3 o N_5



un reticolo è detto limitato se ha un massimo 1 e un minimo 0

un reticolo limitato è detto complementato se ammette un'operazione unaria di complemento - tale da soddisfare: $x \vee -x = 1$ e: $x \wedge -x = 0$

e finalmente ...:

un'algebra di Boole (o booleana) è un reticolo distributivo complementato

un'algebra di Boole è completa se tale è il suo ridotto reticolo

assiomi delle algebre di Boole

mettendo assieme le equazioni che caratterizzano i reticoli distributivi complementati, si ottiene una base assiomatica di 12 equazioni per le algebre di Boole

reticoli: 6, distributività: 2, limiti: 2, complemento: 2

un paio di domande si sono presto imposte all'attenzione:

- tale base costituisce un sistema di assiomi indipendenti?
- qual è il minimo numero di assiomi atti a caratterizzare le algebre di Boole?

alla risposta (negativa) alla prima domanda ha fatto seguito la ricerca di una risposta alla seconda:

- con riferimento alla ridotta costituita da una delle due operazioni di reticolo e dal complemento
  ciò perché è possibile definire l'altra operazione di reticolo mediante una delle leggi di De Morgan (dualità Booleana), e usare le due equazioni imposte al complemento come definizioni delle costanti 0, 1
- una celebre assiomatizzazione delle algebre di Boole $(A; +, -)$ così ridotte, dovuta a E.V. Huntington (1933), consta di solo 3 equazioni: associatività e commutatività di + e assioma di Huntington: $-(-x + y) + -(-x + -y) = x$
  è l'assiomatizzazione più economica? v. il tema di approfondimento 2

algebre booleane di insiemi

su qualsiasi insieme S possono costruirsi algebre booleane di insiemi, ciascuna così fatta:

- il sostegno è una famiglia di sottoinsiemi di S, che contenga S e l'insieme vuoto, e sia chiusa rispetto alle operazioni seguenti
- gli operatori join, meet e complemento sono risp. interpretati dalle operazioni di unione, intersezione e complemento in S
- l'insieme vuoto e S sono risp. il minimo (0) e il massimo (1)

si verifica che l'ordinamento booleano è l'inclusione di insiemi nella famiglia

Teorema di rappresentazione di Stone:

ogni algebra booleana è isomorfa a un'algebra booleana di insiemi

algebra di Lindenbaum-Tarski

qualsiasi sistema di assiomi completo per le algebre di Boole fornisce un calcolo deduttivo completo per la logica proposizionale: $\vdash \varphi = 1$ sse $\models \varphi$

inoltre $\vdash \varphi = \psi$ sse $\models \varphi \leftrightarrow \psi$ sse φ, ψ logicamente equivalenti

possiamo costruire un'algebra booleana delle formule proposizionali, dove si identifichino formule equivalenti? (semantica algebrica della logica proposizionale)

sì, perché l'equivalenza logica proposizionale è decidibile

infatti, gli assiomi booleani bastano a trasformare ogni formula in una equivalente DNF, che determina la tavola di verità della formula

l'algebra di Lindenbaum-Tarski è una tal costruzione; fissato un insieme V di variabili proposizionali:

- dominio: il quoziente dell'insieme delle formule proposizionali con variabili in V per la relazione di equivalenza logica proposizionale
- operazioni booleane sulle classi di equivalenza: definite per il tramite dei connettivi proposizionali su rappresentanti delle classi

si veda l'esercizio sulla definizione dell'algebra di Lindenbaum-Tarski

algebra booleana minimale

di particolare interesse per la realizzazione di macchine da calcolo fisiche è l'algebra booleana minimale, o algebra binaria di commutazione (*Switching Algebra*), caratterizzata dal fatto che il sostegno consta solo delle due costanti booleane (distinte)

> N.B. tale algebra, unica a meno di isomorfismo, è detta minimale perché tale è l'insieme di equazioni che soddisfa: ogni equazione booleana valida in essa lo è in qualsiasi algebra booleana

l'algebra booleana minimale è isomorfa all'algebra di Lindenbaum-Tarski generata dall'insieme vuoto di variabili

completezza funzionale di operatori booleani

l'algebra booleana minimale offre un'interpretazione dei simboli di costante come valori di verità e degli operatori booleani come connettivi proposizionali

i due operatori $(\vee, -)$ sono sufficienti a definire qualsiasi funzione booleana, cioè funzione n-aria su $\{0,1\}$

> basta infatti "leggere" la definizione della funzione come una DNF proposizionale, ed eliminare $\wedge$ con una legge di De Morgan

Un insieme di operatori booleani si dice funzionalmente completo se ogni funzione booleana è rappresentabile da un termine contenente solo variabili e operatori nell'insieme

> altri insiemi funzionalmente completi sono: $(\wedge, -)$, e i singoli $\overline{\vee}$ e $\overline{\wedge}$

porte logiche e circuiti logici

si possono definire funzioni numeriche finite mediante funzioni booleane grazie alla rappresentazione binaria dei numeri (già intuita da Leibniz)

se occorrono k bit per rappresentare il massimo valore assunto dalla funzione, questa è rappresentabile mediante una sequenza di k funzioni booleane (una per ogni bit dell'immagine)

sono detti porte logiche (*gate*) componenti fisici con vie di ingresso e di uscita che esibiscano il comportamento di ingresso/uscita proprio di operatori booleani

la composizione di operatori booleani è realizzata fisicamente da corrispondenti collegamenti di uscite a ingressi di porte logiche

si realizzano in tal modo circuiti logici, classificabili in due categorie:

- reti combinatorie: circuiti logici privi di cicli
  le reti combinatorie sono prive di memoria
- circuiti sequenziali: circuiti logici con cicli (*feedback*)
  con i circuiti sequenziali si possono realizzare memorie di capacità finita

in una rete combinatoria l'output a un dato istante dipende solo dai valori in input a quell'istante, mentre in un circuito sequenziale si ha la dipendenza dell'output dalla precedente sequenza temporale degli input

fonti per approfondimenti

1. Il lavoro originale di George Boole
   Il testo fondamentale del 1854: An investigation of the laws of thought, on which are founded the mathematical theories of logic and probabilities, è liberamente disponibile in rete:
   http://www.archive.org/details/investigationof100boolrich

2. Assiomatizzazione di Robbins delle algebre di Boole
   Un'assiomatizzazione delle algebre di Boole alternativa a quella di Huntington, e non meno concisa, è stata proposta da H. Robbins nel 1933. Il problema di dimostrare l'equivalenza degli assiomi di Robbins a quelli di Huntington si è rivelato difficile, ed è stato risolto da McCune nel 1996, grazie ad un uso molto accorto di vari sistemi di deduzione automatica. Per informazioni sulla storia del Problema e sulla sua soluzione v.
   http://www.cs.unm.edu/~mccune/papers/robbins