Strutture algebriche, algebre di Boole

Lezione 13 di Fondamenti di informatica

Docente: Giuseppe Scollo

Università di Catania
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica, I livello, AA 2009-10

Indice

logica matematica e algebra astratta

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**

le **equazioni** sono non meno fondamentali nell'**algebra astratta** (XX secolo):

incognite: i **simboli di operazione**

operazioni, proprietà, relazioni

cos'è un'**operazione**?

una **regola** applicabile a un **argomento** per produrre un **risultato**

questa definizione corrisponde al concetto **intensionale** di funzione, dove è rilevante il **modo** in cui si determina l'immagine di ciascun elemento del dominio di definizione

due operazioni sono **estensionalmente equivalenti** se producono sempre (seppure in modi diversi) uguali risultati per uguali argomenti

un'operazione di **arietà *k*, o *k*-aria**, ha argomenti nel prodotto cartesiano di ***k*** insiemi

non necessariamente distinti: un'operazione ***k*-aria** su S ha S^k per dominio

una **proprietà** è un'operazione che produce risultati in un insieme di due valori, usualmente detti **valori di verità** ({0,1}, o {T,F}, etc.)

ogni proprietà **caratterizza** un sottoinsieme del suo dominio di definizione: quello costituito dagli elementi per i quali essa "vale" (dà risultato 1)

la versione estensionale del concetto di proprietà corrisponde al concetto insiemistico di **relazione *k*-aria**: sottoinsieme del prodotto cartesiano di ***k*** insiemi

una **relazione binaria su** S è caratterizzata da una proprietà su S^2

ordinamenti

quasi-ordine (o preordine): una relazione binaria $\preccurlyeq$ su un insieme la quale soddisfi:
- **riflessività:** $x \preccurlyeq x$
- **transitività:** $x \preccurlyeq y$, $y \preccurlyeq z \rightarrow x \preccurlyeq z$

N.B. la relazione conversa di un quasi-ordine è anch'essa un quasi-ordine

relazione di equivalenza: un quasi-ordine $\approx$ su un insieme che inoltre soddisfi:
- **simmetria:** $x \approx y \rightarrow y \approx x$

N.B.: la congiunzione (o, insiemisticamente, intersezione) di un quasi-ordine e della sua conversa è una relazione di equivalenza: il ***kernel*** del quasi-ordine

una relazione binaria su un insieme è un **ordinamento stretto** se è **irriflessiva** (cioè non vale mai per una coppia di elementi identici) e **transitiva**

ordinamento parziale: un quasi-ordine $\leq$ su un insieme che inoltre soddisfi:
- **antisimmetria:** $x \leq y$, $y \leq x \rightarrow x = y$

terminologia: se $\leq$ è un ordinamento parziale:
- se $a \leq b$, allora a è un **minorante** di b, e b è un **maggiorante** di a
- a è un **minorante** (risp. **maggiorante**) dell'insieme S se è un minorante (risp. maggiorante) di ogni elemento in S

strutture algebriche

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, sul quale sono definite:
- le **operazioni e/o relazioni** di cui la struttura è dotata

una **ridotta** di una struttura $\mathcal{A}$ è una struttura costituita da un sottoinsieme delle operazioni e relazioni di $\mathcal{A}$, definite sullo stesso sostegno

una struttura si dice **omogenea** se il sostegno consta di un solo insieme, **eterogenea** altrimenti (**N.B.: il sostegno di una ridotta di una struttura eterogenea $\mathcal{A}$ può essere costituito da un sottoinsieme proprio della collezione di insiemi che costituisce il sostegno di $\mathcal{A}$, 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 la sua operazione binaria

monoide: $(A; e, \cdot)$, un semigruppo $(A; \cdot)$ con e costante **neutra** rispetto a $\cdot$
il monoide è detto **commutativo** se tale 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* $\tau(t_1) = \tau(t_2)$

rimpiazzamento: *se* $t_1 = t_2$ *allora* $t[u \leftarrow t_1] = t[u \leftarrow t_2]$

dove il termine $\tau(t)$ è ottenuto dal termine t per sostituzione simultanea di tutte le occorrenze di ciascuna variabile con uno stesso termine, mentre il termine $t[u \leftarrow t']$ è ottenuto dal termine t rimpiazzando il suo sottotermine al posto u con il termine t'

reticoli

def.: un **reticolo** è un ordinamento parziale in cui ogni **coppia** di elementi abbia:
un **minimo maggiorante** (ingl. ***join***, o ***l.u.b.***: *least upper bound*) e
un **massimo minorante** (ingl. ***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 · è espressa dall'equazione $x \cdot x = x$)
un reticolo è un'algebra $(A; \vee, \wedge)$ tale che le sue due **algebre ridotte** $(A; \vee)$, $(A; \wedge)$ sono semireticoli, e inoltre valgono gli assiomi di **assorbimento:**

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

che fine ha fatto l'ordinamento del reticolo? può essere definito algebricamente come **abbreviazione** di equazioni nelle due operazioni binarie:

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

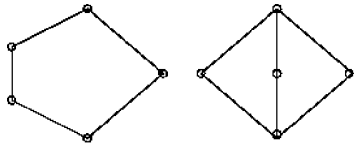
N.B.: si veda in proposito l'esercizio sull'ordinamento nei reticoli algebrici

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

temi per ulteriori 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/investigationofl00boolrich
   (attenzione: la versione PDF dell'originale "pesa" 44MB).
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. Informazioni sulla storia del Problema e sulla sua soluzione sono reperibili al sito http://www.cs.unm.edu/~mccune/papers/robbins