Diskrete Strukturen und Logik

WiSe 2007/08 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Diskrete Strukturen und Logik Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

Boolesche Algebren und Ordnungen

Erinnerung: Eine *Boolesche Algebra* $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ erfüllt folgende Eigenschaften:

$0 \neq 1$

Kommutativgesetze: (1) $\forall a, b \in B : a \oplus b = b \oplus a$, (2) $\forall a, b \in B : a \otimes b = b \otimes a$.

Distributivgesetze: (1) $\forall a, b, c \in B : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und (2) $\forall a, b, c \in B : a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$

Neutralitätsgesetze: (1) 0 ist *rechtsneutrales Element* bzgl. $\oplus$, d.h.: $a \oplus 0 = a$ und (2) 1 ist *rechtsneutrales Element* bzgl. $\otimes$, d.h.: $a \otimes 1 = a$

Komplementgesetze: (1) $\kappa(a)$ ist das *Komplement* von a, d.h.: (1) $a \oplus \kappa(a) = 1$ und (2) $a \otimes \kappa(a) = 0$.

Boolesche Algebren und Ordnungen

Satz: Auf einer B.A. $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ kann durch $a \leq b$ gdw. $a \oplus b = b$ eine Halbordnung auf B definiert werden (*von B.A. induzierte Halbordnung*).

Satz: In der von einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ induzierten Halbordnung $\leq$ gibt es stets ein kleinstes und ein größtes Element, nämlich 0 und 1.
Satz: $x \leq y$ gdw. $\kappa(y) \leq \kappa(x)$ gdw. $x \otimes y = x$ gdw. $x \otimes \kappa(y) = 0$ gdw. $\kappa(x) \oplus y = 1$.
Begriffe: Atom und irreduzibles Element (bei B.A. dasselbe); dual: Hyperatom
$p \neq 0$, heißt *Atom* gdw. $\forall a : 0 \leq a \leq p \Rightarrow (a = 0 \vee a = p)$.
Im Hasse-Diagramm einer B.A. sind die Atome genau die direkten Nachfolger des Nullelements.
Primzahlen sind Hyperatome in der Teileralgebra.
Folgerung: In einer endlichen B.A. gibt es stets Atome.

Darstellungssatz durch (Hyper-)Atome

Satz: In einer endlichen Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gilt: $x \in B$ lässt sich (bis auf die Reihenfolge sogar in eindeutiger Weise) schreiben als:
(1) $x = b_1 \oplus \cdots \oplus b_\ell$, wobei $\{b_1, \ldots, b_\ell\}$ die Menge der Atome b ist, für die $b \leq x$ gilt.
(2) $x = a_1 \otimes \cdots \otimes a_k$, wobei $\{a_1, \ldots, a_k\}$ die Menge der Hyperatome a ist, für die $a \geq x$ gilt.
Ferner sind die Hyper-Atome von $\mathcal{B}$ gerade die Komplemente der Atome von $\mathcal{B}$.
Daher hat $\mathcal{B}$ genauso viele Atome wie Hyperatome, sagen wir n Stück.
Damit gilt dann $|B| = 2^n$.
Eine endliche Boolesche Algebra ist also das Erzeugnis ihrer Atome (bzw. Hyper-Atome).

Aussagenlogische Folgerungen

Folgerung: Jeder Boolesche Ausdruck ist äquivalent zu einer Summe vollständiger Minterme.
Folgerung: Zu jedem w.a.A. existiert ein äquivalenter in disjunktiver Normalform.
Folgerung: Jeder Boolesche Ausdruck ist äquivalent zu einem Produkt vollständiger Maxterme.
Folgerung: Zu jedem w.a.A. existiert ein äquivalenter in konjunktiver Normalform.

Problem: Wie gelangt man zu kurzen Darstellungen ?
Bislang: Karnaugh-Diagramme (visuelle Methode), gut für kleine Variablenmengen
Heute: Systematische, allgemeine Vorgehensweise

Resolventen

Sind α und α' zwei verschiedene Minterme mit den gleichen Variablen, die sich hinsichtlich ihrer Literale nur in einem unterscheiden, z.B. ℓ in α bzw. $\bar{\ell}$ in α', so entsteht die *Resolvente* $\rho(\alpha, \alpha')$ als Minterm aus α durch Streichen von ℓ; alternativ entsteht sie aus α' durch Streichen von $\bar{\ell}$. In solch einer Situation heißen α und α' auch *resolvierbar*. Spezialfall: $\rho(x, \bar{x}) = 1$.

Lemma: Sind α und α' resolvierbar, so gilt: $\rho(\alpha, \alpha') \equiv (\alpha \vee \alpha')$.

Beweis: Distributivgesetz nebst Kommutativitäts- und Assoziativitätsgesetzen.

Der Resolventengraph (alternativ Quine/McCluskey (RS 1), Ausgang von vollständigen Mintermen)

Genauer definieren wir induktiv eine Folge von Graphen zu einer gegebenen Summe α von Mintermen:

Basis: $G_0 = (V_0, E_0)$;

V_0: Menge der Minterme, die in α vorkommen.

$E_0 = \emptyset$.

Sind $G_0, \ldots, G_i$ bereits definiert, so beschreiben wir jetzt $G_{i+1} = (V_{i+1}, E_{i+1})$.

$V_{i+1} = V_i \cup \{\rho(\alpha, \alpha') \mid \alpha, \alpha' \in V_i, \alpha, \alpha' \text{ resolvierbar.}\}$

$E_{i+1} = E_i \cup \{(\alpha, r), (\alpha', r) \mid r = \rho(\alpha, \alpha'), \alpha, \alpha' \in V_i\}$

Die Graphenfolge ändert sich höchstens # Variablen oft und strebt daher gegen einen Graphen $G = (V, E)$.

Die Summe über diejenigen Minterme, die die Knoten vom Ausgangsgrad 0 in G bilden (*Primterme* oder *Primimplikanten*), ist äquivalent zu der vorgelegten Summe α.

Der schwierigste Teil: kleinstmögliche Auswahl von Primtermen. (*Mengenüberdeckungsproblem*)

Exkurs Das Mengenüberdeckungsproblem als *Entscheidungsproblem*

Eingabe: Grundmenge M, $S \subseteq 2^M$, $k \in \mathbb{N}$
Frage: Gibt es ein Mengensystem $C \subseteq S$, $|C| \leq k$, mit $\bigcup_{N \in C} N = M$?
(Natürlich ist man dann auch daran interessiert, eine solche kleine *Mengenüberdeckung* zu bekommen.)

Das Mengenüberdeckungsproblem ist (ebenso wie das schon erwähnte Erfüllbarkeitsproblem) NP-hart, d.h., man erwartet gemeinhin nicht, dafür einen Algorithmus angeben zu können, der in Polynomzeit läuft. Genaueres später ! (siehe Ber.&Kompl.-Vorl.)

Exkurs Das Mengenüberdeckungsproblem als *Optimierungsproblem*

Eingabe: Grundmenge M, $S \subseteq 2^M$
Ausgabe: Ein Mengensystem $C \subseteq S$ mit $\bigcup_{N \in C} N = M$ kleinstmöglicher Mächtigkeit

Hinweis: Könnte man das Entscheidungsproblem in Polynomzeit lösen, so auch das Optimierungsproblem, denn k liegt sinnvollerweise zwischen 0 und $2^{|M|}$ und lässt sich so in linear viel Bits (gemessen in $|M|$) aufschreiben.
Könnte man das Optimierungsproblem in Polynomzeit lösen, so auch das Entscheidungsproblem, denn man müsste ja nur testen, wie die Größe der kleinstmöglichen Lösung sich zum Eingabeparameter k verhält.
In gewissem Sinne sind also beide Problemarten “gleich schwer”.

Exkurs Das Mengenüberdeckungsproblem und die Primtermauswahl

Frage: Was hat das mit der Primtermauswahl zu tun ?

Dazu formalisieren wir das *Primtermauswahlproblem* zunächst geeignet als *Entscheidungsproblem*:
Eingabe: Boolescher Ausdruck α, Menge S von Primtermen, $k \in \mathbb{N}$
Frage: Gibt es eine Teilmenge $C \subseteq S$, $|C| \leq k$ mit $\bigvee_{r \in C} r \equiv \alpha$?
(Natürlich ist man dann auch daran interessiert, eine solche kleine *Primtermüberdeckung* zu bekommen.)

Exkurs Das Mengenüberdeckungsproblem und die Primtermauswahl

Lemma: Könnte man das Mengenüberdeckungsproblem in Polynomzeit lösen, so auch das Primtermüberdeckungsproblem.

Beweis: Assoziiere zu α die Menge $M(\alpha)$ der vollständigen Minterme, deren Summe zu α äquivalent ist.

Fasse Primterm $r \in S$ auf als Menge $N(r)$ derjenigen vollständigen Minterme auf, deren Summe zu r äquivalent ist. So gelangt man von S nach $S' = \{N(r) \mid r \in S\}$.

Dann ist $C \subseteq S$ eine Lösung des Primtermüberdeckungsproblems (α, S, k) gdw. $C' := \{N(r) \mid r \in C\}$ eine Lösung des Mengenüberdeckungsproblems $(M(\alpha), S', k)$ ist.

Hinweis: Eigentlich ist Argument "nur" richtig, wenn von α gegeben als Summe vollständiger Minterme ausgegangen wird.

Exkurs Das Mengenüberdeckungsproblem und die Primtermauswahl

Lemma: Könnte man das Primtermüberdeckungsproblem in Polynomzeit lösen, so auch das Mengenüberdeckungsproblem.

Beweis: Betrachte eine Mengenüberdeckungsinstanz (M, S, k). Wir können davon ausgehen (*), dass keine zwei verschiedenen Mengen aus dem System S einander enthalten, da wir sonst stets die größere wählen könnten.

Fasse Grundmenge $M = \{x_1, \ldots, x_n\}$ auf als Menge von Booleschen Variablen.

Konstruiere daraus $\alpha(M) = \bigvee_{1 \leq i \leq n} x_i$.

Wir können $N = \{x_{i_1}, \ldots, x_{i_j}\} \in S$ durch den Minterm $t(N) = \bigwedge_{1 \leq \ell \leq j} x_{i_\ell} \bigwedge_{x \notin N} \bar{x}$ beschreiben.

$S' = \{t(N) \mid N \in S\}$ ist eine Menge von Primtermen wegen (*).

C ist eine Mengenüberdeckung zu (M, S, k) gdw. $C' = \{t(N) \mid N \in C\}$ ist eine Primtermüberdeckung zu $(\alpha(M), S', k)$.

Hinweis: Reduktionsbegriffe in Ber.&Kompl.

Hinweis: Bitvektorinterpretation an der Tafel mit Rückblick auf Karnaugh / englische Folien.