Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau
Universität Trier
fernau@informatik.uni-trier.de

$\boxed{\text{Diskrete Strukturen und Logik}}$ 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) $a \otimes \kappa(a) = 0$.

Der Isomorphiesatz von Stones für Boolesche Algebren

Satz: Jede endliche B.A. $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ ist isomorph zu einer Potenzmengenalgebra $\mathcal{P} = (2^A, \cup, \cap, ^-, \emptyset, A)$ für a eine endliche Menge A .

Beweis: Idee: Wähle $A = \{a_1, \ldots, a_n\}$ als Menge der Atome von $\mathcal{B}$.

Da $\mathcal{B}$ endlich ist, gilt $A \neq \emptyset$.

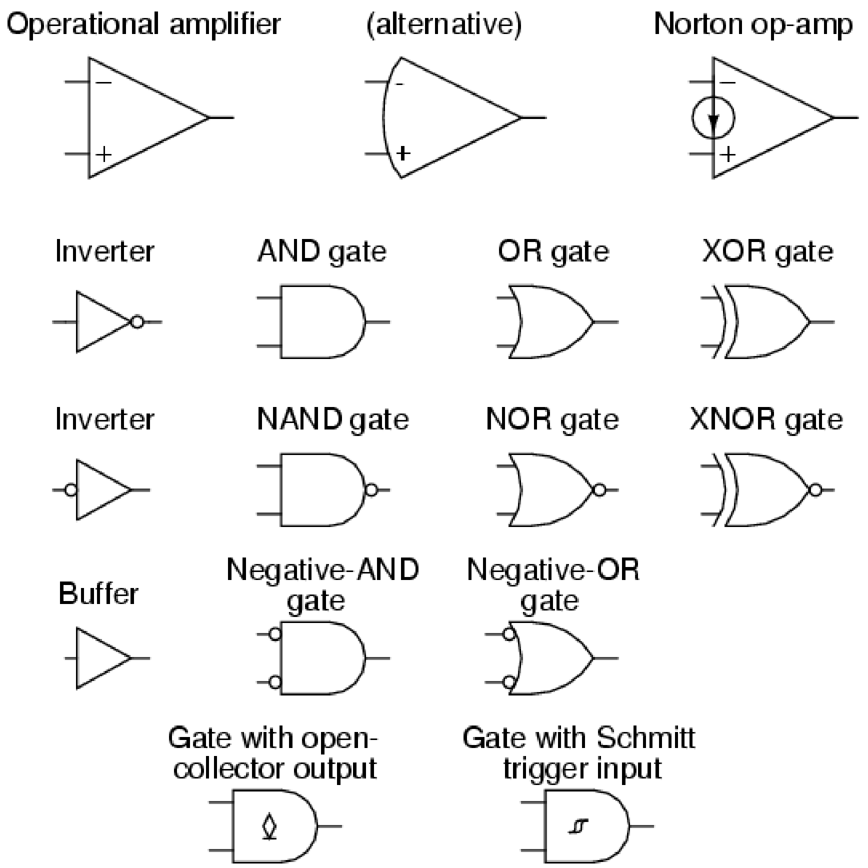
Der Morphismus $h : B \to 2^A$ ist festgelegt durch $a_i \mapsto \{a_i\}$ für Atome a_i. Damit gilt die Strukturverträglichkeit automatisch.

Jedes $b \in B$ lässt sich in eindeutiger Weise als Summe $\sum_{a \in A, a \leq b} a$ darstellen. Gleichermaßen ist jede Menge $C \subseteq A$ eindeutig durch Angabe ihrer Elemente festgelegt. Daher ist h bijektiv.

Beispiel: Teileralgebra $\mathcal{T}(30) = (\{1, 2, 3, 5, 6, 10, 15, 30\}, \mathrm{ggT}, \mathrm{kgV}, 30, 1)$:
Hasse-Diagramm an der Tafel
Atome: $A = \{6, 10, 15\}$
Hyperatome: $\{2, 3, 5\}$
Wie sieht h konkret aus ?

Beispiel: Schaltfunktionenalgebra zu zweistelligen Schaltfunktionen (Tafel)

Schaltkreisalgebra



Schaltkreisalgebra

Ein *Schaltkreis* $S = (V, E, X)$ ist ein gerichteter kreisfreier Graph (V, E) (DAG: directed acyclic graph) zusammen mit einer Variablenmenge $X = \{x_1, \ldots, x_n\}$.
Knoten mit Eingangsgrad 0, sogenannte *Eingabegatter*, sind mit Variablen $x_i \in X$ oder mit Konstanten $0, 1$ markiert.
Knoten mit Eingangsgrad ≥ 1 (*Gatter*) sind mit Schaltfunktionen markiert, deren Stelligkeit dem Eingangsgrad entspricht.
Gatter mit Ausgangsgrad 0 sind *Ausgabegatter*.

Was berechnet ein Schaltkreis ?

Da (V, E) kreisfrei, kann die an einem Gatter g mit Markierung m berechnete Funktion $f_g(x_1, \ldots, x_n)$ induktiv beschrieben werden:
$f_g(x_1, \ldots, x_n) = m$, falls g ein mit m markiertes Eingabegatter ist.
$f_g(x_1, \ldots, x_n) = m(f_{g_1}(x_1, \ldots, x_n), \ldots, f_{g_\ell}(x_1, \ldots, x_n))$, falls g den Eingangsgrad $\ell > 0$ besitzt und $g_1, \ldots, g_\ell$ die Vorgängergatter sind.
Besitzt S nur ein Ausgabegatter, so berechnet S die Schaltfunktion am Ausgabegatter.

Warum Schaltkreise ?

Satz: Es gibt eine Familie von Schaltfunktionen, die sich mit essentiell kleineren Schaltkreisen darstellen lässt, verglichen mit der Größe der Repräsentation durch Boolesche Ausdrücke.

Beweis: Betrachte die *Paritätsfunktion* $P_n(x_1, \ldots, x_n) = 1$ gdw. eine ungerade Anzahl von x_i hat Wert 1.
Für die Normalformdarstellung mit vollständigen Mintermen benötigt man 2^{n-1} Minterme, die sich paarweise an mindestens zwei Stellen unterscheiden und daher paarweise nicht resolvierbar sind.
Hingegen genügen Schaltkreise linearer Größe (Tafel).

Paritätsfunktion(en) und Boolesche Ausdrücke

Wenn wir auf Normalformen verzichten, gibt es kleinere Darstellungen für P_n mit Booleschen Ausdrücken:

Lemma: P_n lässt sich durch Boolesche Ausdrücke mit n^2 Operatoren beschreiben (also der *Größe* n^2).

<u>Beweis:</u> Wir zeigen die Behauptung induktiv.

P_2 lässt sich beschreiben durch: $(x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2)$.

Rekursiv kann man P_{2^k} für $k > 1$ berechnen durch Boolesche Ausdrücke b_1 und b_2 der Größe jeweils 4^{k-1} für die Paritätsfunktion $P_{2^{k-1}}$ der ersten 2^{k-1} Variablen sowie für die der letzten 2^{k-1} Variablen. Der gesamte Ausdruck ergibt sich als $(b_1 \wedge \bar{b}_2) \vee (\bar{b}_1 \wedge b_2)$.

Daher gilt: P_{2^k} lässt sich durch B.A. der vierfachen Größe der B.A. für die $P_{2^{k-1}}$ ausdrücken.

Also lässt sich P_{2^k} durch Boolesche Ausdrücke der Größe 4^k beschreiben.

Daraus folgt die Behauptung. (Warum ?)

Folgerung: Lineare Größe für Schaltkreise ! (Warum ? Fast dieselbe Idee. . .)

Ein hilfreiches kleines Lemma

Lemma: $\frac{n^2}{a} + \frac{m^2}{b} \geq \frac{(n+m)^2}{a+b}$ für nichtverschwindende Nenner.

Beweis: Wir bringen auf die Hauptnenner:

links: $b(a+b)n^2 + a(a+b)m^2 = abn^2 + abm^2 + b^2n^2 + a^2m^2$.

rechts: $ab(n+m)^2 = abn^2 + abm^2 + 2abnm$.

links minus rechts liefert also:

$b^2n^2 + a^2m^2 - 2abnm = (am - bn)^2 \geq 0$.

Beweisziel: Die untere Schranke von Kraptschenko (Krapchenko)

Erinnerung: Wohlgeformte aussagenlogische Ausdrücke, also Boolesche Ausdrücke, sind rekursiv definiert.
Daher lässt sich jedem w.a.A. ein (Rekursions-)baum zuordnen.
Die Zahl der Blätter dieses Rekursionsbaums heißt auch *Blattkomplexität* des Booleschen Ausdrucks B, kurz $\mathrm{BK}(\mathrm{B})$.
Unter der Blattkomplexität einer Schaltfunktion f, kurz $\mathrm{BK}(\mathrm{f})$, verstehen wir entsprechend die kleinste Blattkomplexität eines f beschreibenen Booleschen Ausdrucks.
Da für diesen Komplexitätsbegriff wesentlich ist, welche Operationen wir gestatten, wollen wir im Folgenden von Ausdrücken ausgehen, die in unserer früheren Begriffsbildung *vereinfachte w.a.A.* hießen, d.h., wir gestatten lediglich $\wedge$, $\vee$ und Negation.

Alternativ könnte man die Anzahl der verwendeten Operatoren als Komplexitätmaß zugrunde legen. Beide Maße wären eng verwandt (wie genau ?).

Satz: Jeder Boolesche Ausdruck, der nur mit $\wedge$, $\vee$ und Negation als Operatoren auskommt, und welcher P_n beschreibt, hat eine Blattkomplexität von wenigstens n^2.

Dieser Satz ist einer der ersten Bestandteile einer ganz eigenen Komplexitäts-theorie, nämlich der Schaltkreiskomplexität (Circuit Complexity).

Ähnliche Sachverhalte sind für andere Grundoperationen bekannt, aber nicht für beliebige.

Hinführung zum Beweis

Sind $x, y \in \{0,1\}^n$ zwei n-Bitvektoren, so ist ihr *Hamming-Abstand* $H(x,y)$ die Anzahl der Bits, an denen x und y sich unterscheiden.

Die *gemeinsame Nachbarschaft* von $A, B \subseteq \{0,1\}^n$ ist die Menge $N(A,B)$ aller Paare von n-Bitvektoren $(x,y) \in A \times B$ mit $H(x,y) = 1$.

Eigentlich zeigen wir nun im Folgenden eine Verallgemeinerung:

Satz: Ist $f : \{0,1\}^n \to \{0,1\}$ eine Schaltfunktion und $\mathrm{BK}(f)$ die Größe des kleinsten f beschreibenen Booleschen Ausdrucks mit Operatoren $\wedge$, $\vee$ und der Negation, so gilt für alle $\emptyset \subset A \subseteq f^{-}(0)$ und alle $\emptyset \subset B \subseteq f^{-}(1)$: $\mathrm{BK}(f) \geq \frac{|N(A,B)|^2}{|A|\cdot|B|}$.

Speziell für $f = P_n$, $A = f^{-}(0)$ und $B = f^{-}(1)$ ergibt sich die gesuchte Beziehung $\mathrm{BK}(P_n) \geq n^2$, denn $|A| = |B| = 2^{n-1}$ und $|N(A,B)| = n|A| = n2^{n-1}$.

Der Beweis von Kraptschenko Der Beweis der Verallgemeinerung gelingt durch Induktion über die Blattkomplexität von Schaltfunktionen.

Induktionsanfang: Blattkomplexität null haben Konstanten (jedenfalls bei manchen Autoren; B.K. eins würde am folgenden Argument aber nichts ändern).
$f = 0$: Dann ist $B = \emptyset$ und die Behauptung gilt leer.
$f = 1$: analog
Blattkomplexität eins haben einzelne Variablen (und ihre Negation).
$f = x_1$: Dann ist $A = \{0\}$ und $B = \{1\}$, und man braucht wirklich ein Eingabegatter.
$f = \bar{x}_1$: analog.

Induktionsvoraussetzung: Es werde also angenommen, die Aussage gelte für alle Schaltfunktionen einer Blattkomplexität $\leq n-1$.
Induktionsschritt: Es sei f eine Schaltfunktion mit $\mathrm{BK}(f) = n$. Wir gehen davon aus, dass α ein Ausdruck kleinster Blattkomplexität für f ist.
Wir argumentieren jetzt aufgrund der rekursiven Definition der w.a.A.
Gilt $\alpha = \bar{\alpha}'$, so könnten wir das folgende Argument mit α' statt α durchführen.
Wir diskutieren jetzt den Fall: $\alpha = (\alpha_1 \wedge \alpha_2)$.
(Der Fall der Disjuktion als äußerster Operation lässt sich entsprechend erörtern.)
Es gilt also: $f = f_1 \wedge f_2$, wobei die Schaltfunktion f_i durch den Ausdruck α_i beschrieben wird.
Wir gehen von der Optimalität der α_i aus, d.h., $\mathrm{BK}(\alpha_i) = \mathrm{BK}(f_i)$.
$\rightsquigarrow \mathrm{BK}(\alpha) = \mathrm{BK}(f) = \mathrm{BK}(\alpha_1) + \mathrm{BK}(\alpha_2) = \mathrm{BK}(f_1) + \mathrm{BK}(f_2)$.
Ferner gilt: $\mathrm{BK}(f_i) \leq n-1$, sodass wir hier IV anwenden könnten.
Wir schließen hierbei den Fall aus, dass eines der f_i konstant ist.

Betrachte $\emptyset \neq A \subseteq f^{-}(0)$ und $\emptyset \neq B \subseteq f^{-}(1)$.
Da wir die Konjunktion diskutieren, gilt: $f^{-}(1) \subseteq f_i^{-}(1)$ für $i = 1, 2$.
$\rightsquigarrow B \subseteq f_1^{-}(1) \cap f_2^{-}(1)$.
Setze im Folgenden: $B_1 = B_2 = B$.
Setze außerdem $A_1 = A \cap f_1^{-}(0)$ und $A_2 = A \setminus A_1$.
Nach Konstruktion gilt $f_1(x) = 1$ für $x \in A_2$.
Da $f(x) = 0$, muss wegen $f(x) = f_1(x) \wedge f_2(x)$ gelten: $f_2(x) = 0$.
$\rightsquigarrow A_2 \subseteq f_2^{-}(0)$.
Mit A sind A_1 und A_2 nicht leer, da wir konstante Funktionen ausschlossen.
Also ist die IV für f_1 und f_2 und die gerade konstruierten Mengen A_i und B_i anwendbar und liefert:
$\mathrm{BK}(f_1) \geq \frac{|N(A_1,B_1)|^2}{|A_1|\cdot|B_1|}$ und $\mathrm{BK}(f_2) \geq \frac{|N(A_2,B_2)|^2}{|A_2|\cdot|B_2|}$.
$\rightsquigarrow \mathrm{BK}(f) = \mathrm{BK}(f_1) + \mathrm{BK}(f_2) \geq \frac{|N(A_1,B_1)|^2}{|A_1|\cdot|B_1|} + \frac{|N(A_2,B_2)|^2}{|A_2|\cdot|B_2|}$.
Das hilfreiche Lemma liefert nun die Behauptung, denn $N(A, B)$ lässt sich zerlegen in $N(A_1, B_1)$ und $N(A_2, B_2)$.