1.2 Verbände und boolesche Algebra

Zur Vorlesung Rechenanlagen SS 2019



1.2.1 Partielle Ordnungen

Zur Erinnerung:

Definition

Eine Relation $R \subseteq M \times M$ heißt partielle Ordnung auf M

- \Leftrightarrow 1. $\forall m \in M : (m,m) \in R$ (Reflexivität)
 - 2. mRn und $nRm \Rightarrow n = m$ (Antisymme trie)
 - 3. mRn und $nRp \Rightarrow mRp$ (Transitivität)

Beispiel:

Die Relation Präfix ist eine partielle Ordnung auf A^*

Präfix $\subseteq A^* \times A^*$, mit $(v, w) \in \text{Präfix} \Leftrightarrow \exists u \in A^* : w = vu$

Supremum und Infimum

Definition

Sei M eine Menge, und sei \leq partielle Ordnung. Dann heißt (M, \leq) eine **partiell geordnete Menge** (<u>partially ordered set</u>) oder **Poset**.

Sei $U \subseteq M$. Ein Element $c \in M$ mit

 $\forall u \in U: c \leq u$ heißt **untere Schranke** von *U*

 $\forall u \in U: u \leq c$ heißt **obere Schranke** von *U*

Ein Element $c \in M$ heißt **Supremum (Infimum)** von U (Schreibe $\sup U$ ($\inf U$))

- $:\Leftrightarrow$ (i) c ist obere (untere) Schranke von U
 - (ii) für jede obere (untere) Schranke m von U ist schon $c \le m$ ($m \le c$).

Supremum und Infimum -- ff

Bemerkung:

Das Supremum von U (Infimum) ist also die kleinste obere (größte untere) Schranke einer Menge U.

Existiert zu U ein Supremum (Infimum), so ist es eindeutig bestimmt:

Annahme: c und c' seien beide Suprema von U

Dann ist $c \le c'$, (c ist Supremum, c' obere Schranke)

aber auch $c' \le c$, (c' ist Supremum, c obere Schranke)

also: c' = c. (Antisymmetrie)

1.2.2 Halbverbände

Definition

Eine Poset (M, \leq) heißt oberer (unterer) Halbverband (upper / lower semi lattice)

$$\Leftrightarrow \forall \{a,b\} \subseteq M \exists c \in M : c = \sup\{a,b\}$$
$$(\forall \{a,b\} \subseteq M \exists c \in M : c = \inf\{a,b\})$$

Schreibweisen:

Wir schreiben auch sup(a,b) statt $sup\{a,b\}$ und als Infixoperator $sup(a,b) := a \lor b$ Lies: "oder" Ebenso inf(a,b) statt $inf\{a,b\}$ und als Infixoperator $inf(a,b) := a \cdot b$ Lies: "und"

Halbverbände ff

Mit dieser Schreibweise gilt in einem oberen (unteren) Halbverband für je zwei Elemente *a,b*:

$$a \le b \Leftrightarrow a \lor b = b$$
 $(a \le b \Leftrightarrow a \cdot b = a)$

Definition

Ein Halbverband (M, \leq) heißt **vollständig** (complete) : \Leftrightarrow

Zu jeder (endlichen oder unendlichen) Teilmenge $U \subseteq M$

existiert das Supremum (Infimum).

Bemerkung:

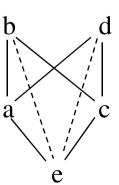
Ein vollständiger oberer (unterer) Halbverband hat stets ein größtes (kleinstes) Element: $T := \sup M \ (\bot := \inf M)$

1.2.3 Das Hasse Diagramm

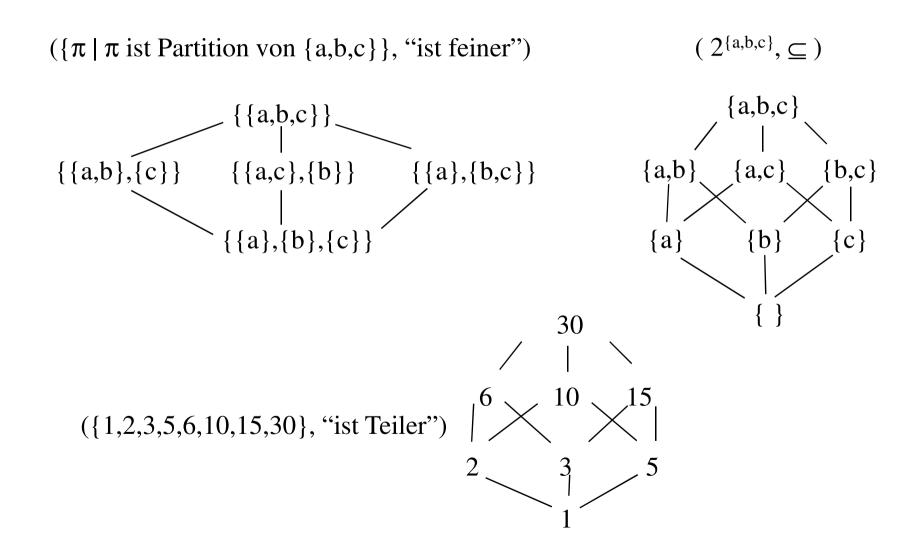
Man kann ein endliches Poset durch folgendes Diagramm, genannt Hasse Diagramm, darstellen:

- \odot Knotenmenge \mathscr{S}
- o gibt es eine Kante zwischen Element a und b, so gilt a ≤ b oder b ≤ a. Der Knoten, der weiter unten liegt, ist kleiner.
- Es wird nur der reduzierte Graph gezeichnet,
 d.h. transitive Kanten lässt man weg

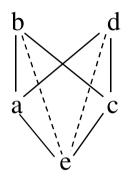
Beispiel:



Hasse Diagramme: Beispiele für weitere Posets



Beispiel:



```
a v d = d
b v d = nicht definiert, da kein gemeinsamer Vorfahre
b d = nicht definiert, da nicht eindeutig
```

1.2.4 Verbände

Definition

Ein Poset *(M*, ≤ *)* heißt (vollständiger) **Verband** (lattice)

: \Leftrightarrow (M, \leq) ist ein (vollständiger) oberer und unterer Halbverband.

Beispiel:

Sei M endliche Menge und $2^M := \{U \mid U \subseteq M\}$

die Potenzmenge von M. Dann gilt für beliebige U, V, W:

$$U \subset U$$

$$U \subseteq V$$
 und $V \subseteq U \Rightarrow U = V$ $(2^M, \subseteq)$ ist also ein Poset

$$U \subseteq V$$
 und $V \subseteq W \Rightarrow U \subseteq W$

Beispiel ff:

Sei *U* beliebige Teilmenge von 2^M

Dann hat U als Supremum die Menge $\bigcup_{u \in U} u$

denn
$$\forall v \in U : v \subseteq \bigcup_{u \in U} u$$
 (obere Schranke!) und gilt $\forall u \in U : u \subseteq y$, so folgt schon $\bigcup_{u \in U} u \subseteq y$ (kleinste o. S.!)

Insbesondere ist

$$\forall a,b \in 2^M : sup(a,b) = a \cup b$$

Also ist die Potenzmenge ein vollständiger, oberer Halbverband.

Beispiel ff:

Analog überzeugt man sich davon, daß für $U \subseteq 2^M$ das Infimum die Menge $\bigcap_{i=1}^{U} U_i$ ist:

$$\begin{cases} \forall v \in U : v \supseteq \bigcap_{u \in U} u \\ \text{gilt } (\forall u \in U : y \subseteq u), \text{ so folgt } y \subseteq \bigcap_{u \in U} u \end{cases}$$

Insbesondere ist $\forall a,b \in 2^M : inf(a,b) = a \cap b$

Also ist die Potenzmenge auch ein vollständiger, unterer Halbverband, und damit ein vollständiger Verband. Wir nennen ihn auch einfach den **Mengenverband über M**.

kleinstes Element: $\bot = \{\}$ größtes Element: T = M

Rechenregeln in Verbänden

Satz

Sei (M, \leq) ein Verband. Dann gilt für alle $a,b,c \in M$

$$(V1) \quad a \lor b = b \lor a$$

(Kommutativität)

$$a \cdot b = b \cdot a$$

(V2)
$$a \lor (b \lor c) = (a \lor b) \lor c$$
 (Assoziativität)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(V3)
$$a \lor (a \cdot b) = a$$

(Absorption)

$$a \cdot (a \lor b) = a$$

Beweis: Wir zeigen nur eine Auswahl der Gleichungen.

Kommutativität:

 $a \lor b := \sup\{a,b\} = \sup\{b,a\} =: b \lor a$

Beweis ff

Assoziativität:

```
Es ist:
\left. \begin{array}{l} \sup\{a,b\} \leq \sup\{a,b,c\} \\ c \leq \sup\{a,b,c\} \end{array} \right\} \Rightarrow \sup\{\sup\{a,b\},c\} \leq \sup\{a,b,c\}
Umgekehrt ist:
a,b,c \leq \sup\{\sup\{a,b\},c\} \Rightarrow \sup\{a,b,c\} \leq \sup\{\sup\{a,b\},c\}
Damit ist: sup\{sup\{a,b\},c\} = sup\{a,b,c\} = sup\{a,sup\{b,c\}\}
                          (Antisymmetrie)
                                                                     (analog)
 Also: (a \lor b) \lor c = \sup\{\sup\{a,b\},c\}
                           = sup\{a,b,c\}
                           = \sup\{a, \sup\{b,c\}\} = a \lor (b \lor c)
```

Beweis ff

Absorption:

Hier ist:
$$a \le \sup\{a, \inf\{a, b\}\}\}$$

Andererseits ist: $\Rightarrow \sup\{a, \inf\{a, b\}\} = a$
 $\inf\{a, b\} \le a$
 $a \le a$ $\Rightarrow \sup\{a, \inf\{a, b\}\} \le a$ (Antisymmetrie)

Also:
$$a \lor (a \cdot b) = \sup\{a, \inf\{a, b\}\}\$$

= a

Die anderen Beziehungen zeigt man analog!

Dualität

Beobachtung:

Die Regeln (V1), (V2), (V3) sind **dual** unter der Vertauschung von "und" und "oder". Damit gilt für jede Formel, die man mit (V1), (V2), (V3) herleiten kann, auch zugleich die **duale Formel**, die man durch Tauschen von "und" mit "oder" erhält.

Grund:

Da man in der Herleitung stets Regeln aus (V1), (V2), (V3) benutzt, kann man durch Anwendung der dualen Regeln die duale Formel herleiten.

Bei einem dualen Axiomensystem werden wir stets nur einen Beweis führen.

Eigenschaften von Verbänden

Satz

 (M_1, \leq_1) und (M_2, \leq_2) seien (vollständige) Verbände. Dann sind auch

(a)
$$(M_1 \times M_2, \leq_{1,2})$$
 mit
 $(a,b) \leq_{1,2} (c,d) \Leftrightarrow a \leq_1 c \text{ und } b \leq_2 d$
(b) $(Abb(X, M_1), \leq)$ mit
 $f \leq g \Leftrightarrow \forall x \in X : f(x) \leq_1 g(x)$

vollständige Verbände.

Beweis: Übung.

Distributiver Verband

Definition

Ein Verband (M, \vee, \cdot) heißt **distributiver Verband**, dann und nur dann, wenn für alle a,b,c aus M gilt

$$(V4) \ a \lor (b \cdot c) = (a \lor b) \cdot (a \lor c)$$
 (Distributivität)
 $a \cdot (b \lor c) = (a \cdot b) \lor (a \cdot c)$

Bemerkung:

Die Regel (V4) ist auch dual.

Wir vereinbaren für die Operatoren von nun an:

'·' bindet stärker als 'v'.

D.h. der Ausdruck $a \cdot b \lor c$ ist zu lesen als $(a \cdot b) \lor c$.

Wir lassen '.' auch häufig weg.

1.2.5 Boolesche Algebra

Definition

```
(M,\lor,\cdot,\lnot) heißt boolesche Algebra, dann und nur dann, wenn (A1) (M,\lor,\cdot) ist distributiver Verband (A2) \forall a,b\in M: a\lor b\cdot\lnot b=a \forall a,b\in M: a\cdot(b\lor\lnot b)=a
```

Notation: Wir schreiben in Formeln statt $\neg b$ (lies nicht b) einfacher \overline{b} (lies b quer)

Bemerkung: Auch in der booleschen Algebra sind die Axiome dual!

Eigenschaften boolescher Algebren

Lemma

In einer booleschen Algebra gilt (Idempotenz):

$$a \lor a = a$$
; dual : $a \cdot a = a$

Beweis:

$$X \vee X = X \vee X \cdot (X \vee X)$$

$$= X$$

Dualer Beweis

$$x \cdot x = x \cdot (x \lor x \cdot x)$$
$$= x$$

Eigenschaften boolescher Algebren

Lemma

Jede boolesche Algebra besitzt genau ein "0" und ein "1" Element, die zueinander dual sind, und es gilt:

$$a \lor 0 = a$$
; dual : $a \cdot 1 = a$

$$a \cdot 0 = 0$$
; dual: $a \lor 1 = 1$

Beweis:

Höchstens eins: Seien 0, 0' zwei Nullelemente, dann gilt:

$$0 = 0 \lor 0' = 0'$$
 Dual: $1 = 1 \cdot 1' = 1'$
 $(0 \text{ ist Nullelement})$

(0' ist Nullelement)

Beweis ff

Mindestens eins: Setze für beliebiges b aus M

$$0 := b\overline{b}$$

Dann gilt für alle *a* aus *M*:

$$a \lor 0 = a \lor b\overline{b} = a$$

Ferner gilt:

$$a \cdot 0 = a \cdot b\overline{b}$$

$$= a \cdot a\overline{a}$$

$$= (aa)\overline{a}$$

$$= a\overline{a} = 0$$
da *b* beliebig
Assoziativität
$$= (aa)a$$
Idempotenz und Def. 0

Eigenschaften boolescher Algebren

Lemma

In einer booleschen Algebra *M* gibt es zu jedem Element *a* genau ein Element *b*, mit

$$a \lor b = 1$$
 und $a \cdot b = 0$

Beweis:

Man nehme an, dass *b* und *b* obigen Gleichungen genügen: dann ist

$$b = (a \lor b')b = ab \lor bb' = bb' = ab' \lor bb' = (a \lor b)b' = b'$$
 $\uparrow \qquad \uparrow \qquad \uparrow \qquad \uparrow \qquad \uparrow$
 $(a \lor b' = 1) (ab = 0) \qquad (ab' = 0) \qquad (a \lor b = 1)$

Eigenschaften boolescher Algebren

Korollar

Die Gleichungen $a \lor b = 1$ und $a \cdot b = 0$ gelten nur für $b = \overline{a}$

Wir nennen dieses Element $b = \overline{a}$ auch **das Komplement** von a.

Satz (de Morgan'sche Regel)

In einer booleschen Algebra M gilt für alle Elemente a,b:

$$\overline{a \lor b} = \overline{a} \cdot \overline{b}$$
 und dual $\overline{a \cdot b} = \overline{a} \lor \overline{b}$

Beweis der de Morgan Regel

Wir zeigen nach dem letzten Korollar, dass

$$ab \cdot (\overline{a} \vee \overline{b}) = 0$$
 und $ab \vee (\overline{a} \vee \overline{b}) = 1$

Dann folgt die erste Regel. Der Beweis der dualen Regel ist dual.

$$ab \cdot (\overline{a} \vee \overline{b}) = \overline{aba} \vee \overline{abb}$$

= $0 \vee 0 = 0$

$$ab \lor (\overline{a} \lor \overline{b}) = (ab \lor \overline{a}) \lor \overline{b}$$
(Distributivität) = $(a \lor \overline{a})(b \lor \overline{a}) \lor \overline{b}$

$$= 1 = (b \lor \overline{a}) \lor \overline{b} = 1$$

Korollar

$$\overline{0} = 1$$
 und $\overline{1} = 0$

Beweis:

$$\overline{0} = \overline{aa} = \overline{a} \lor \overline{a} = 1$$

$$\bar{1} = \overline{a \lor a} = \overline{a \cdot a} = 0$$

Eigenschaften boolescher Algebren

Satz

Seien M_1 , M_2 boolesche Algebren und sei A eine Menge. Dann sind auch

(a)
$$(2^{A}, \cup, \cap, \neg)$$

(b) $(M_{1} \times M_{2}, \vee, \cdot, \neg)$ mit
 $(a,b) \vee (c,d) := (a \vee c, b \vee d);$
 $(a,b) \cdot (c,d) := (a \cdot c, b \cdot d);$ $\overline{(a,b)} := (\overline{a},\overline{b})$
(c) $Abb(A,M_{1})$ mit
 $(f \vee g)(a) := f(a) \vee g(a);$
 $(f \cdot g)(a) := f(a) \cdot g(a);$ $\overline{f}(a) := \overline{f(a)}$
jeweils boolesche Algebren.

Beweis: Übung

Beispiele:

Was hat das alles nun mit Digitaltechnik zu tun?

Die Menge **B** ist eine boolesche Algebra, die nur aus der 0 und der 1 besteht (sie ist die kleinste b.A. überhaupt).

Nach dem letzten Satz bilden dann aber auch die Mengen

$$\mathbf{B}^n := \underbrace{\mathbf{B} \times \cdots \times \mathbf{B}}_{n-mal}$$

unter komponentenweiser Verknüpfung, sowie die Mengen

$$S_{n,k} := Abb(B^n, B^k)$$

eine boolesche Algebra. Wir nennen $S_{n,k}$ auch die Menge der (totalen) k-stelligen **Schaltfunktionen**.

Beispiele ff:

Ebenso bildet die Menge der partiellen Funktionen mit gleichem Definitionsbereich *D*:

$$F(\boldsymbol{B}^n, \boldsymbol{B}^k) \supseteq \boldsymbol{S}_{n,k}^D := Abb(D, \boldsymbol{B}^k)$$

eine boolesche Algebra. Die 0 und 1 der Algebra sind gerade die konstanten Funktionen.

Die Grundbausteine der Digitaltechnik berechnen Schaltfunktionen. Da Schaltfunktionen eine boolesche Algebra bilden, ist diese Theorie also ein wichtiges Fundament zur Analyse von digitalen Schaltkreisen.

Atome

Definition

Ein Element a einer boolesche Algebra M heißt Atom genau dann, wenn

```
(At1) a \neq 0
(At2) \forall b \in M : a \cdot b \in \{a,0\}
```

Bemerkung: Atome sind kleinste, von *0* verschiedene Elemente in der booleschen Algebra. Sie sind nicht weiter aufspaltbar, daher der Name "Atom".

Eigenschaften von Atomen

Lemma

 $a \in M$ ist Atom $\Leftrightarrow \forall b \in M : b \le a \Rightarrow (b = 0 \text{ oder } b = a)$

Beweis:

⇒: Sei a Atom und sei $b \le a$

$$b \le a :\Leftrightarrow b = ba = ab \in \{0,a\}$$

 \Leftarrow : Es gelte nun: $\forall b \in M : b \le a \Rightarrow (b = 0 \text{ oder } b = a)$

Sei c aus M beliebig, dann ist $ac \le a$.

Insbesondere gilt also für b = ac: ac = 0 oder ac = a, also ist a Atom.

Eigenschaften von Atomen ff

Lemma

a,b Atome mit $a \neq b$, dann gilt ab = 0

Beweis:

 $ab \in \{a,0\}$, da a Atom

$$\Rightarrow$$
 ab $\in \{a,0\} \cap \{b,0\} = \{0\}$

 $ab \in \{b,0\}$, da b Atom

Beispiele:

- 1. Die Atome von $(2^A, \cup, \cap, \neg)$ sind $At(2^A) = \{\{a\} \mid a \in A\}$
- 2. Die Atome von $\boldsymbol{S}_n := \boldsymbol{S}_{n,1}$

Für einen Punkt $p \in \mathbf{B}^n$ sei $x^p : \mathbf{B}^n \mapsto \mathbf{B}$ die Funktion, die nur auf p den Wert 1 hat, d.h.

$$x^{p}(q) := \begin{cases} 1 & \text{für } p = q \\ 0 & \text{für } p \neq q \end{cases}$$

Wir nennen diese Funktion auch einfach **Minterm** zu *p* oder **Punkt** *p*.

Dann ist x^p Atom, denn für eine beliebige Funktion

$$f \in \mathbf{S}_n$$
 gilt:

$$f \cdot x^p(q) = \begin{cases} f(p) \cdot 1 & \text{für } p = q \\ 0 & \text{für } p \neq q \end{cases} = \begin{cases} x^p(q) & \text{für } f(p) = 1 \\ 0 & \text{für } f(p) = 0 \end{cases}$$

Weitere Eigenschaften

Atome spielen eine wichtige Rolle. Man kann zeigen, dass jedes Element einer endlichen booleschen Algebra aus Atomen eindeutig zusammengesetzt ist:

Satz

Sei *M* eine endliche boolesche Algebra. Dann gilt für ein beliebiges Element *f* stets:

$$f = \bigvee_{a \in At(M)} a$$

$$a \cdot f \neq 0$$

Wir zeigen den Beweis über einige Hilfsbehauptungen:

Beweis:

Behauptung 1: Sei $b \neq 0$ beliebig, dann gibt es stets ein Atom a_0 mit $a_0 \leq b$

Fall 1: $\forall a \in M, a \neq b : ab \in \{0, b\}$ Dann ist b schon ein Atom, insbesondere ist $a_0 := b \leq b$

Fall 2: $\exists a \in M : ab \notin \{0, b\}$ Dann ist aber $0 \neq ab \leq b$

Setze $b_2 = ab$ und wiederhole die

Falldiskussion für *b*₂

Wir erhalten also eine Folge, $b=b_1 \ge b_2 \ge ... \ge b_n = a_0$ die irgendwann mit Fall 1 abbricht (M endlich).

Also gilt Behauptung 1.

Beweis ff:

Behauptung 2:
$$\bigvee_{a \in At(M)} a = 1$$

Annahme: $x := \bigvee_{a \in At(M)} a \neq 1$

Dann ist $x \neq 0$

Also gibt es mit Behauptung 1 ein Atom $a_0 \leq x$

Nun ist aber $a_0 \cdot x = a_0 \cdot \bigvee_{a \in At(M)} a$

$$= \bigvee_{a \in At(M)} a_0 a = a_0$$

da ja $a_0 \in At(M)$

Damit ist aber $a_0 = a_0 x$, da $a_0 \leq x$

$$= a_0 x x$$
, da $a_0 x = a_0$

 $= a_0 0 = 0$ $\qquad \qquad \qquad = a_0 \text{ Atom}$

Beweis ff:

Mit Behauptung 2 rechnet man nun ganz leicht nach:

$$f = f \cdot 1$$

$$= f \cdot \left(\bigvee_{a \in At(M)} a \right)$$

$$= \bigvee_{a \in At(M)} f \cdot a$$

$$= \bigvee_{a \in At(M)} a$$

$$f \cdot a \neq 0$$

Weitere Eigenschaften

Korollar

Sei *M* eine endliche boolesche Algebra. Dann gibt es eine natürliche Zahl *n*, so dass:

$$\#M = 2^n$$

Beweis: Für ein beliebiges Element f von M gilt nach

unserem Satz:
$$f = \bigvee_{a \in At(M)} a$$

Damit bestimmt die Menge

$$ON(f) := \{a \in At(M) \mid f \cdot a \neq 0\} \subseteq At(M)$$

jedes Element f eindeutig (ON(f) heißt ON-Set von f)

Es gibt aber genau 2^{#At(M)} verschiedene Teilmengen.

Beobachtung und Beispiel

Beobachtung

Aus dem Korollar folgt nun auch, dass man, sofern man alle Atome berechnen kann, mit der "oder" Operation dann auch alle Elemente als Veroderung ihres ON-Sets darstellen kann.

Beispiel: Betrachten wir wieder die Schaltfunktionen. Die Minterme bilden Atome. Da nun für alle $q \in \mathbf{B}^n$

$$\left(\bigvee_{p\in\mathbf{B}^n} x^p\right)(q) = \bigvee_{p\in\mathbf{B}^n} x^p(q)$$
$$= x^q(q)$$
$$= 1$$

folgt nach obigem Satz sogar $At(\mathbf{S}_n) = \{x^p \mid p \in \mathbf{B}^n\}$

$$At(\mathbf{S}_n) = \{x^p \mid p \in \mathbf{B}^n\}$$

Beispiel ff:

Die Minterme sind damit genau die Atome der Algebra der einstelligen Schaltfunktionen und es gilt für eine beliebige Funktion f stets, dass f darstellbar ist durch

$$f = f \cdot 1$$

$$= f \cdot \left(\bigvee_{p \in \mathbf{B}^n} x^p\right)$$

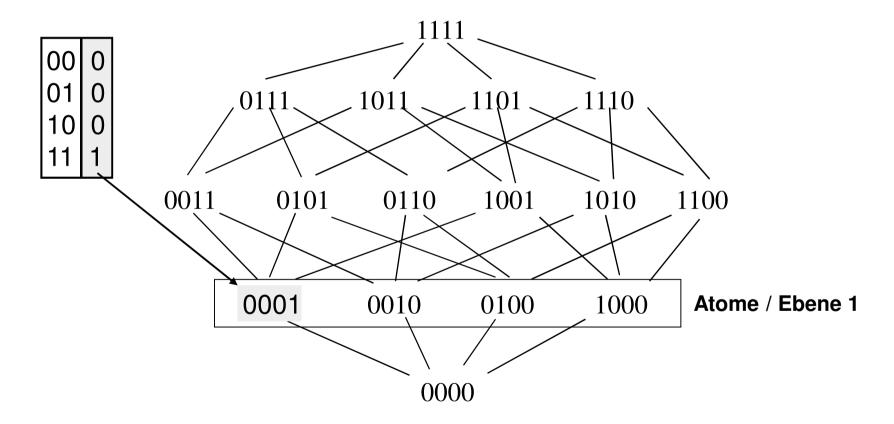
$$= \bigvee_{p \in \mathbf{B}^n} f \cdot x^p$$

$$= \bigvee_{p \in \mathbf{B}^n} f(p) \cdot x^p$$

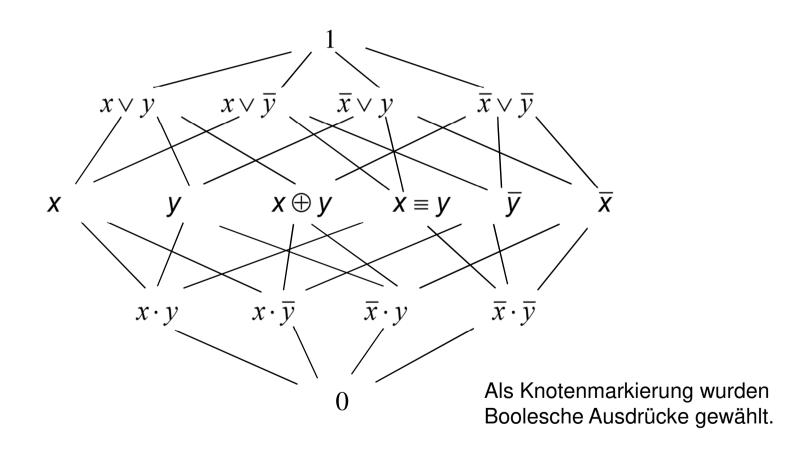
$$= \bigvee_{p, f(p) = 1} x^p \quad \text{disjunktive Normalform von } f$$

Hassediagramm der Booleschen Funktionen in 2 Variablen

Als Knotenmarkierung wurden die Funktionstafel gewählt.



Hassediagramm der Booleschen Funktionen in 2 Variablen ff



Hassediagramm der Booleschen Funktionen in 2 Variablen ff

