

# Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau

Universität Trier

[fernau@informatik.uni-trier.de](mailto:fernau@informatik.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.

## **BAs aus BAs:** Funktionenalgebren

Es sei  $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$  eine Boolesche Algebra.

$B_n := B^{B^n}$  bezeichne die *n-stelligen Booleschen Funktionen*.

Definiere für  $f, g \in B_n$  folgende Operationen:

$$(f \star g)(x_1, \dots, x_n) := f(x_1, \dots, x_n) \oplus g(x_1, \dots, x_n)$$

$$(f \odot g)(x_1, \dots, x_n) := f(x_1, \dots, x_n) \otimes g(x_1, \dots, x_n)$$

$$(\Gamma(f))(x_1, \dots, x_n) := \kappa(f(x_1, \dots, x_n))$$

0 und 1 sollen der Einfachheit halber auch die n-stelligen Funktionen bezeichnen, die konstant 0 bzw. 1 liefern.

**Satz:** Für  $n \in \mathbb{N}$  ist  $\mathcal{B}_n = (B_n, \star, \odot, \Gamma, 0, 1)$  eine Boolesche Algebra. Diese ist für  $n = 0$  zu  $\mathcal{B}$  isomorph.

**Betrachte:** Funktionenalgebra zur Schaltalgebra B: *n-stellige Boolesche Schaltfunktionen*  $B_n$ .  $\leq$  entspricht dem positionsweisen Vergleich der Funktionswerte. Atome sind hier genau die Funktionen, deren Funktionswert nur für genau ein Argument 1 ( $w$ ) ist und sonst immer 0. So gibt es in  $B_2$  genau vier Atome (Tafel).

## BAs, Halbordnungen und Atome

Es sei  $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$  eine Boolesche Algebra.

**Lemma:**  $x \otimes y \leq x$  und  $x \leq x \oplus y$ .

Beweis:  $\kappa(x \otimes y) \oplus x = (\kappa(x) \oplus \kappa(y)) \oplus x = (\kappa(x) \oplus x) \oplus \kappa(y) = 1 \oplus \kappa(y) = 1$ .

$x \oplus (x \otimes y) = (x \oplus x) \oplus y = x \oplus y$ , also  $x \leq x \oplus y$ .

Wegen der Kommutativitäten gilt ferner:

**Lemma:**  $x \otimes y \leq y$  und  $y \leq x \oplus y$ .

**Lemma:** Aus  $x \leq y$  und  $x \leq \kappa(y)$  folgt:  $x = 0$ .

Beweis:  $x = x \otimes \kappa(y) = (x \otimes y) \otimes \kappa(y) = 0$ .

**Satz:** Ist  $a \in B$  Atom und  $x \in B$  beliebig, so gilt:  $a \otimes x = 0$  oder  $a \otimes x = a$ .

Beweis: Aus  $a \otimes x \neq a$  folgt wegen  $a \otimes x \leq a$  (1.Lemma)  $a \otimes x = 0$ , da  $a$  Atom.

## BAs, Halbordnungen und Atome

Es sei  $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$  eine Boolesche Algebra.

**Satz:** Ist  $a \in B$  Atom und  $x \in B$  beliebig, so gilt:  $a \otimes x = 0$  gdw.  $a \otimes \kappa(x) = a$ .

Beweis: Angenommen,  $a \otimes \kappa(x) = a$ , also  $a \leq \kappa(x)$ .

Wäre  $a \otimes x \neq 0$ , so folgt  $a \otimes x = a$ , da  $a$  Atom; also  $a \leq x$ .

3.Lemma  $\leadsto a = 0$  im Widerspruch dazu, dass  $a$  Atom.

Angenommen,  $a \otimes x = 0$ , also  $a \leq \kappa(x)$ .

Gölte außerdem  $a \otimes \kappa(x) \neq a$ , also wegen  $a \otimes \kappa(x) \leq a$  (1.Lemma)  $a \otimes \kappa(x) = 0$ , da  $a$  Atom, so hätten wir  $a \leq x$ .

3.Lemma  $\leadsto a = 0$  im Widerspruch dazu, dass  $a$  Atom.

## BAs, Halbordnungen und Atome

**Satz:** Ist  $a \in B$  Atom und  $x \in B$  beliebig, so gilt: Entweder  $a \leq x$  oder  $a \leq \kappa(x)$ , aber nicht beides zugleich.

Beweis: Gölte beides zugleich, zu folgte  $a = 0$  mit 3.Lemma, Widerspruch !

Gilt nicht  $a \leq x$ , so gilt nicht  $a \otimes \kappa(x) = 0$ , also gilt mit dem vorigen Satz  $a \otimes \kappa(x) \neq a$ . Da  $a$  Atom und mit 1.Lemma  $a \otimes \kappa(x) \leq a$ , folgt  $a \otimes \kappa(x) = 0$ , also  $a \leq \kappa(x)$ .



## Darstellungssatz durch Atome

Zunächst ein Hilfssatz, den man mit Hilfe des Distributivgesetzes mit Induktion einsieht:

**Lemma:** In einem distributiven Verband gilt:

$$(a \oplus (b_1 \otimes b_2 \otimes \dots \otimes b_\ell)) = (a \oplus b_1) \otimes (a \oplus b_2) \otimes \dots \otimes (a \oplus b_\ell)$$

sowie die duale Aussage.

**Satz:** In einer endlichen Booleschen Algebra  $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$  gilt:  $x \in B$  lässt sich schreiben als:  $x = a_1 \oplus \dots \oplus a_k$ , wobei  $\{a_1, \dots, a_k\}$  die Menge der Atome  $a$  ist, für die  $a \leq x$  gilt.

Beweis: Es bezeichne  $\sigma_x = a_1 \oplus \dots \oplus a_k$ . Wir zeigen  $x \leq \sigma_x$  und  $\sigma_x \leq x$ , woraus die Behauptung aufgrund der Antisymmetrie von  $\leq$  folgt. Mit dem letzten Lemma können wir schreiben:

$$\begin{aligned}
x \otimes \sigma_x &= x \otimes (a_1 \oplus \cdots \oplus a_k) \\
&= (x \otimes a_1) \oplus (x \otimes a_2) \oplus \cdots \oplus (x \otimes a_k) \\
&= a_1 \oplus a_2 \oplus \cdots \oplus a_k \\
&= \sigma_x
\end{aligned}$$

Also gilt:  $\sigma_x \leq x$ .

$$x \otimes \kappa(\sigma_x) = x \otimes \kappa(a_1) \otimes \kappa(a_2) \otimes \cdots \otimes \kappa(a_k)$$

Gölte  $x \otimes \kappa(\sigma_x) \neq 0$ , so gäbe es ein Atom  $a \in B$  mit  $a \leq x \otimes \kappa(\sigma_x)$ , **da  $B$  endlich** (Beweis? Am einfachsten über Irreduzibilitätseigenschaft!). Das bedeutet:  $a = a \otimes x \otimes \kappa(\sigma_x)$ .

Annahme:  $a = a \otimes x$ , also  $a \leq x$ . Dann wäre  $a = a_j$  für einer der Summanden.

Also gölte dann:  $a = a_j = a_j \otimes x \otimes \kappa(\sigma_x) = a_j \otimes x \otimes \kappa(a_j) \otimes \kappa(\sigma_x) = 0$ , denn  $\kappa(a_j)$  steckt ja ausgeschrieben in der Produktdarstellung von  $\kappa(\sigma_x)$ . Dies steht im Widerspruch zu  $a$  Atom.

Mit dem vorigen Satz gilt, da Annahme  $a \leq x$  falsch:  $a \leq \kappa(x)$ , also  $a \otimes \kappa(x) = a$ .

Dies führt ebenfalls zu einem Widerspruch:  $a = a \otimes x \otimes \kappa(\sigma_x) = a \otimes \kappa(x) \otimes x \otimes \kappa(\sigma_x) = 0$ , also kann es solch ein Atom  $a$  nicht geben, d.h.,  $x \otimes \kappa(\sigma_x) = 0$ , also  $x \leq \sigma_x$ .

## Darstellungssatz durch Atome

**Satz:** Die im vorigen Satz erklärte Darstellung ist sogar eindeutig.

Beweis: Angenommen,  $x$  könne man durch zwei Atom-Summen  $\sigma$  und  $\sigma' = a_1 \oplus \dots \oplus a_k$  darstellen. Dann gäbe es in einer der beiden Summen, z.B.  $\sigma$  ein Atom  $a \leq x = \sigma'$ , das in der anderen,  $\sigma'$ , nicht vorkäme. Daher gilt:

$$a = a \otimes \sigma' = (a \otimes a_1) \oplus \dots \oplus (a \otimes a_k), \quad k \geq 2$$

Mit erstem Satz dieser VL haben wir  $a \otimes a_j = 0$  für alle  $j$ , denn sonst wäre ja  $a$  in der Atom-Summe  $\sigma'$  enthalten. Daher ist die rechte Seite eine Summe von Nullen.

$\leadsto a = 0$  im Widerspruch dazu, dass  $a$  Atom ist.

Aus dem Idempotenzgesetz folgt mit ein wenig Kombinatorik (Bit-Vektoren !):

**Folgerung:** Besitzt eine Boolesche Algebra  $n$  Atome, so hat sie genau  $2^n$  Elemente.

## Darstellungssatz durch Hyper-Atome

Mit der Auffassung von  $\kappa$  als B.A.-Isomorphismus folgt sofort.

**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:  $x = a_1 \otimes \cdots \otimes a_k$ , wobei  $\{a_1, \dots, a_k\}$  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  $|B| = 2^n$ .

Hyper-Atome heißen daher auch *Atomkomplemente*.

## **Algebraische Deutung:** Erzeugnisse

Unsere Darstellungssätze erlauben noch eine weitere Deutung:

**Satz:** Eine endliche Boolesche Algebra ist das Erzeugnis ihrer Atome (bzw. Hyper-Atome).

Daher übernimmt die Menge der Atome die Rolle einer Basis (wie sie aus der Linearen Algebra bekannt sein sollte).

Insbesondere gilt:

**Folgerung:** Ein B.A.-Morphismus von einer endlichen B.A. in eine andere B.A. ist schon eindeutig durch die Angabe seiner Werte bei den Atomen (oder auch bei den Hyper-Atomen) festgelegt.

## **Zahlentheoretische Deutung:** Teileralgebra

Hyper-Atome sind hier gerade die Primzahlen.

Man mache sich klar, was Hyper-Atom bzw. dual unzerlegbar genau bedeutet.

Damit folgt eine eingeschränkte Version des bekannten Satzes, demzufolge eine Primfaktorenzerlegung eindeutig ist.

Worin besteht die Einschränkung ?

Und dürfen wir dies hier eigentlich wirklich folgern ?

## n-stellige Boolesche Schaltfunktionen und Boolesche Ausdrücke

**Satz:**  $\forall n : A_n$  und  $B_n$  sind isomorph.

Beweis: Da die Mengen  $A_n$  durch äquivalente w.a.A. bestimmt sind und diese Äquivalenz wiederum durch die Gleichheit der Werte definiert ist, die sich beim Einsetzen gleicher Variablenbelegungen ergeben, ist klar, dass jeder w.a.A.  $\alpha \in A_n$  eine n-stellige Boolesche Schaltfunktion beschreibt.

Umgekehrt lässt sich jede Boolesche Schaltfunktion als Summe von Atomen in der Funktionenalgebra ausdrücken. Ein Atom lässt sich durch einen Ausdruck der Form  $\ell_1 \wedge \dots \wedge \ell_n$  beschreiben mit  $\ell_i = x_i$  oder  $\ell_i = \bar{x}_i$ : genau für eine Variablenbelegung wird der Ausdruck wahr.

Man mache sich klar, dass hierdurch tatsächlich ein Isomorphismus beschrieben wird.

**Jargon:** Die  $\ell_i$  nennt man auch *Literale*; ein Produkt (also eine Konjunktion) von Literalen heißt auch *Minterm*; taucht in einem Minterm jede Variable genau einmal vor, spricht man auch von einem *vollständigen Minterm*.

## Aussagenlogische Folgerungen I

**Folgerung:** Jeder Boolesche Ausdruck ist äquivalent zu einer Summe vollständiger Minterme.

Eine Konjunktion von Literalen heißt auch manchmal *Konjunktionsterm*, und ein Ausdruck, der eine Disjunktion von Konjunktionstermen ist, heißt in *disjunktiver Normalform (DNF)*.

**Folgerung:** Zu jedem w.a.A. existiert ein äquivalenter in disjunktiver Normalform.



## Aussagenlogische Folgerungen II

Eine Summe (Disjunktion) von Literalen heißt auch *Maxterm* oder *Disjunktionsterm* oder *Klausel*; taucht in einem Maxterm jede Variable genau einmal vor, spricht man auch von einem *vollständigen Maxterm*; ein Ausdruck, der eine Konjunktion von Disjunktionstermen ist, heißt in *konjunktiver Normalform (KNF)*.

**Folgerung:** Zu jedem w.a.A. existiert ein äquivalenter in konjunktiver Normalform. (siehe VL 18)

Genauer: **Folgerung:** Jeder Boolesche Ausdruck ist äquivalent zu einem Produkt vollständiger Maxterme.

Ein ausführliches Beispiel  $(x_1 + x_2) \cdot (\bar{x}_1 \cdot \bar{x}_2) + (x_2 \cdot x_3)$  wird an der Tafel gerechnet, siehe M/M S. 216/217.

## Aussagenlogische Folgerungen III

Unsere allgemeinen Aussagen ergeben weiter:

**Folgerung:** Jeder Boolesche Ausdruck ist äquivalent zu einer Summe vollständiger Minterme, und diese Darstellung ist *kanonisch* in dem Sinne, dass sie bis auf Anwenden des Kommutativitätsgesetzes bei Summe und Produkt eindeutig ist, sobald man z.B. positive Literale stets vor negative sortiert.

Eine entsprechende Aussage gilt für die Darstellung durch Produkte vollständiger Maxterme.

Beide kanonischen Darstellungen gestatten sodann einen einfachen Äquivalenz-Test für Boolesche Ausdrücke.

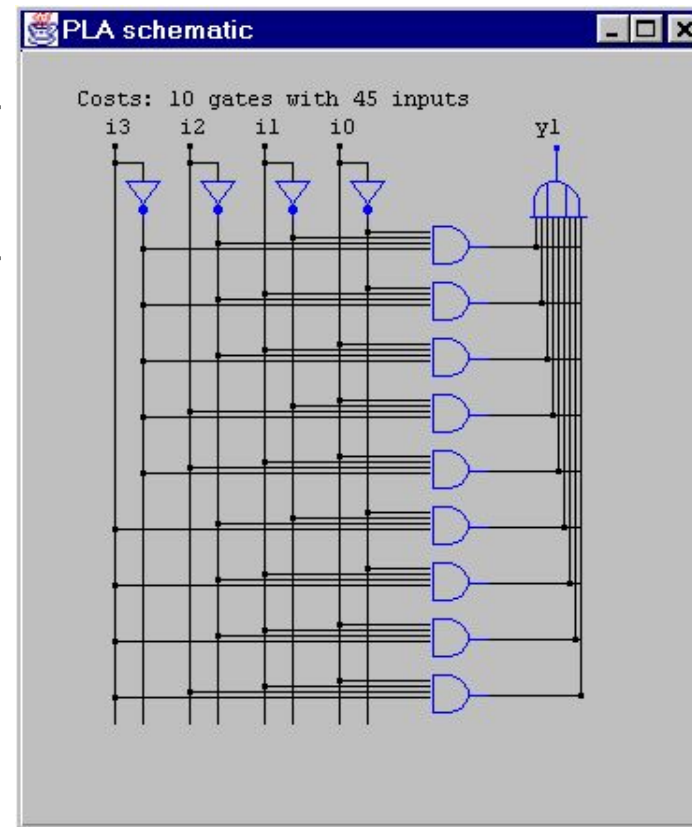
## Programmable Logic Arrays (PLAs): Die technische Seite

Ein Schaltnetz ist die Realisierung einer Schaltfunktion; in DNF wird die Schaltfunktion als *zweistufiges Schaltnetz* verwirklicht.

\* Die Inverter sorgen für die Negierung der Eingangsvariablen. Wie üblich werden die Inverter nicht als eigene Stufe angesehen.

\* Die erste Stufe besteht aus UND-Verknüpfungen zur Bildung der Minterme aus den negierten oder nicht negierten Eingangsvariablen.

\* Die zweite und letzte Stufe besteht aus einer ODER-Verknüpfungen zur disjunktiven Verknüpfung der Minterme.



## Ist kanonisch immer gut ?

Kanonische Ausdrücke sind oft von beträchtlicher Länge.

**Beispiel:** Betrachte:  $(x_1 + x_2 + x_3) \cdot (x_1 + x_2 + \bar{x}_3) \cdot (x_1 + \bar{x}_2 + x_3)$ .

Offenkundig könnte man hier doch (in B.A.-Jargon) das Gesetz zur Vereinfachung von Gleichungen bemühen und somit zur Darstellung

$(x_1 + x_2) \cdot (x_1 + \bar{x}_2 + x_3)$  gelangen.

Mit dem Zwischenschritt über den offensichtlich äquivalenten Ausdruck

$(x_1 + x_2) \cdot (x_1 + x_2 + x_3) \cdot (x_1 + \bar{x}_2 + x_3)$

kommen wir zu (wieder mit dem Gesetz zur Vereinfachung von Gleichungen):

$(x_1 + x_2) \cdot (x_1 + x_3)$

Vielleicht gibt es noch kürzere Darstellungen in KNF ?

## Karnaugh-Diagramme (am Beispiel)

Function y1

<u>i0</u>			
0	1	1	1
0	0	1	0
<u>          </u> i2			

| i1

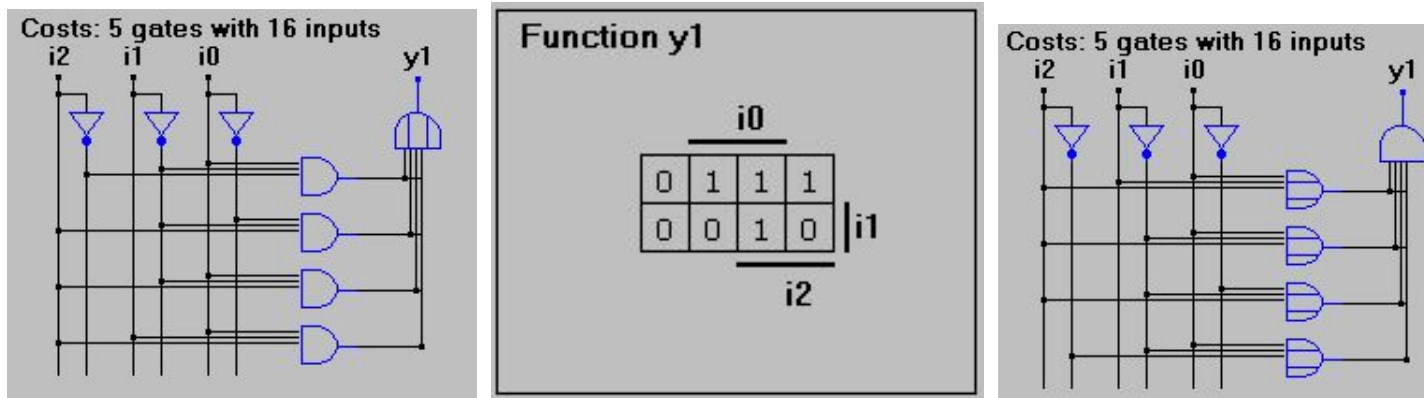
In dem Beispiel handelt es sich um eine 3-stellige Boolesche Funktion.

Die Tabelle enthält lediglich die Ausgabewerte.

Der Balken mit der Beschriftung  $i_0$  oben deutet an, dass die mittleren vier Felder die Werte für den Fall enthalten, dass das Eingangssignal  $i_0 = 1$  gilt.

Das Feld oben links z.B. beschreibt den Ausgabewert für  $i_0 = i_1 = i_2 = 0$ .

## Karnaugh-Diagramme (am Beispiel)

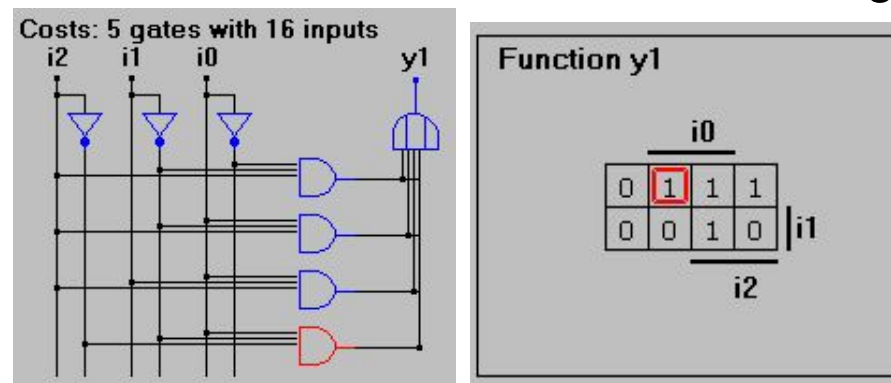


(kan.) DNF:  $y_1 = (i_0 \cdot \bar{i}_1 \cdot \bar{i}_2) + (\bar{i}_0 \cdot \bar{i}_1 \cdot i_2) + (i_0 \cdot \bar{i}_1 \cdot i_2) + (i_0 \cdot i_1 \cdot i_2)$

(kan.) KNF:  $y_1 = (i_0 + i_1 + i_2) \cdot (i_0 + \bar{i}_1 + i_2) \cdot (\bar{i}_0 + \bar{i}_1 + i_2) \cdot (i_0 + \bar{i}_1 + \bar{i}_2)$ .

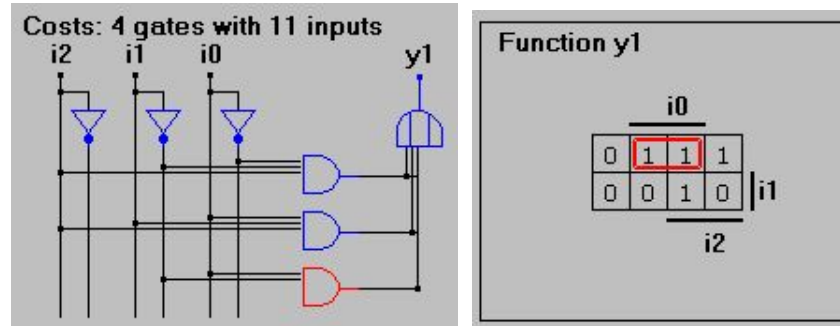
## Karnaugh-Diagramme (am Beispiel)

In dem JAVA Applet, das im Rahmen einer Studienarbeit an der Universität Hamburg entstand, kann man sodann einzelne Felder des Karnaugh-Diagramms farblich mit entsprechenden Gattern im PLA in Verbindung bringen.



## Karnaugh-Diagramme (am Beispiel)

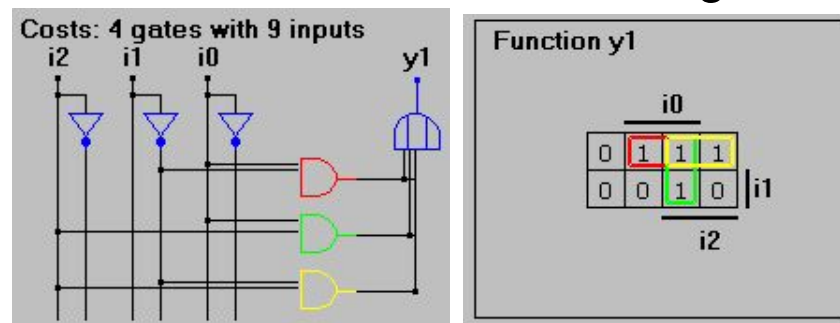
Mehrere Felder des Karnaugh-Diagramms mit gleicher Farbe kann man wieder mit entsprechenden Gattern im PLA in Verbindung bringen.





## Karnaugh-Diagramme (am Beispiel)

Diese Zusammenfassungen kann man mit mehreren Farben wiederholen. Man beobachte, wie die Größe des PLA sich verringert.



Ein weiteres Applet finden Sie hier.

# Karnaugh-Diagramme (allgemein): Der Mensch als Mustererkenner

