

# Bool'sche Algebra

# Fahrplan

Recap

Einleitung

Erfüllbarkeit & Äquivalenz

Beweisstrategien

Strukturelle Induktion

Normalformdarstellungen

# Aussagenlogik

## Definition (Aussagenlogik)

**Aussagenlogik**, als Teilgebiet der Logik, befasst sich mit Aussagen und der Verknüpfung von Aussagen mittels *Junktoren*.

- ▶ Junktoren sind logische Verknüpfungen
- ▶ Klassische Junktoren:
  - ▶ Negation  $\neg P$
  - ▶ Implikation/Subjunktion/Konditional  $P \Rightarrow Q$
  - ▶ Äquivalenz/Bikonditional/Bisubjunktion  $P \Leftrightarrow Q$
  - ▶ Konjunktion  $P \wedge Q$
  - ▶ Disjunktion  $P \vee Q$

[Rau08]

# Bool'sche Algebra nach Huntington (Wichtig!)

## Definition

Die bool'sche Algebra nach Huntington ist definiert als Menge  $\mathcal{V} : \{0, 1\}$  mit den Verknüpfungen  $\cdot (\wedge), + (\vee)$ , sodass  $\mathcal{V} \times \mathcal{V} \rightarrow \mathcal{V}$ , also  $\{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$ .

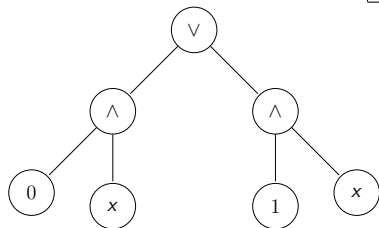
- ▶ Kommutativgesetze (K):  $a \cdot b = b \cdot a$  bzw.  $a + b = b + a$
- ▶ Distributivgesetze (D):  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  bzw.  
 $a + (b \cdot c) = (a + b) \cdot (a + c)$
- ▶ Neutrale Elemente (N):  $\exists e, n \in \mathcal{V}$  mit  $a \cdot e = a$  und  $a + n = a$
- ▶ Inverse Elemente (I):  $\forall a \in \mathcal{V}$  existiert ein  $a'$  mit  $a \cdot a' = n$  und  $a + a' = e$

Übernommen von [Bar13] bzw. [Hof20]

# Darstellungen & Bool'sche Funktionen

## ► Wahrheitstabelle

$a$	$b$	$a \Rightarrow b$
0	0	1
0	1	1
1	0	0
1	1	1



## ► Algebraische Darstellung: $y = ((0 \wedge x) \vee (1 \vee x))$

# Notation und Operatorenbindung

- ▶ Syntactic Sugar (Ableitungen aus Basisverknüpfungen)
  - ▶  $(a \Rightarrow b)$  für  $(\neg a \vee b)$  – Implikation
  - ▶  $(a \Leftarrow b)$  für  $(b \Rightarrow a)$  – Inversion der Implikation
  - ▶  $(a \Leftrightarrow b)$  für  $(a \Rightarrow b) \wedge (a \Leftarrow b)$  – Äquivalenz
  - ▶  $(a \oplus b)$  für  $\neg(a \Leftrightarrow b)$  – Antivalenz oder Exklusiv-ODER/XOR
  - ▶  $\neg(a \vee b)$  – NOR
  - ▶  $\neg(a \wedge b)$  – NAND
- ▶ Bindung der Operatoren
  - ▶  $\wedge$  bindet stärker als  $\vee$
  - ▶  $\neg$  bindet stärker als  $\wedge$
- ▶ Klammerung
  - ▶ Gleiche Verknüpfungen: linksassoziativ zusammengefasst

# Beispiel

$$Y = (A \vee B) \wedge (\neg A \vee B) \wedge (A \vee \neg B)$$

# Beispiel

Umformulieren:

$$\begin{aligned} Y &= (A \vee B) \wedge (\neg A \vee B) \wedge (A \vee \neg B) \\ &= ((A + B) \cdot (\overline{A} + B) \cdot (A + \overline{B})) \\ &= ((A \cdot B \cdot B) + (B \cdot A \cdot A) + (A \cdot A \cdot \overline{A}) + (B \cdot B \cdot \overline{B}) \\ &\quad + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B})) \end{aligned}$$



# Beispiel

Anwenden der Idempotenz:  $X \cdot X = X$  für  $X = B$

$$\begin{aligned} &= (A \cdot (B \cdot B)) + (B \cdot A \cdot A) + (A \cdot A \cdot \bar{A}) + (B \cdot B \cdot \bar{B}) \\ &+ (A \cdot B \cdot \bar{A}) + (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \\ &= (A \cdot (B)) + (B \cdot A \cdot A) + (A \cdot A \cdot \bar{A}) + (B \cdot B \cdot \bar{B}) \\ &+ (A \cdot B \cdot \bar{A}) + (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \end{aligned}$$

# Beispiel

Anwenden der Idempotenz:  $X \cdot X = X$  für  $X = A$

$$\begin{aligned} &= (A \cdot B) + (B \cdot (A \cdot A)) + (A \cdot A \cdot \bar{A}) + (B \cdot B \cdot \bar{B}) \\ &+ (A \cdot B \cdot \bar{A}) + (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \\ &= (A \cdot B) + (B \cdot (A)) + (A \cdot A \cdot \bar{A}) + (B \cdot B \cdot \bar{B}) \\ &+ (A \cdot B \cdot \bar{A}) + (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \end{aligned}$$

# Beispiel

Anwenden des Kommutativgesetz:

$$\begin{aligned} &= (A \cdot B) + (B \cdot A) + (A \cdot A \cdot \overline{A}) + (B \cdot B \cdot \overline{B}) + (A \cdot B \cdot \overline{A}) \\ &+ (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (A \cdot B) + (A \cdot A \cdot \overline{A}) + (B \cdot B \cdot \overline{B}) + (A \cdot B \cdot \overline{A}) \\ &+ (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \end{aligned}$$

# Beispiel

Anwenden der Idempotenz:  $X \cdot X = X$  für  $X = A \cdot B$

$$\begin{aligned} &= ((A \cdot B) + (B \cdot A)) + (A \cdot A \cdot \bar{A}) + (B \cdot B \cdot \bar{B}) + (A \cdot B \cdot \bar{A}) \\ &+ (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \\ &= (A \cdot B) + (A \cdot A \cdot \bar{A}) + (B \cdot B \cdot \bar{B}) + (A \cdot B \cdot \bar{A}) \\ &+ (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \end{aligned}$$

# Beispiel

Anwenden der Idempotenz:  $X \cdot X = X$  für  $X = A$  und  $X = B$  (Nicht dargestellt)

Anwenden des Komplements

$$\begin{aligned} &= (A \cdot B) + (A \cdot \bar{A}) + (B \cdot \bar{B}) + (A \cdot B \cdot \bar{A}) + (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \\ &= (A \cdot B) + (0) + (B \cdot \bar{B}) + (A \cdot B \cdot \bar{A}) + (A \cdot B \cdot \bar{B}) + (A \cdot \bar{A} \cdot \bar{B}) + (B \cdot \bar{A} \cdot \bar{B}) \end{aligned}$$

# Beispiel

Anwenden der Identität:

$$\begin{aligned} &= (((A \cdot B) + 0) + (B \cdot \overline{B}) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B})) \\ &= (A \cdot B) + (B \cdot \overline{B}) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (B \cdot \overline{B}) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (0) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \end{aligned}$$

# Beispiel

Anwenden des Komplements und Identität:

$$\begin{aligned} &= (A \cdot B) + (B \cdot \overline{B}) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (0) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= ((A \cdot B) + 0) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \end{aligned}$$

# Beispiel

Anwenden des Kommutativgesetz und Komplements:

$$\begin{aligned} &= (A \cdot B) + (A \cdot B \cdot \overline{A}) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (A \cdot \overline{A} \cdot B) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (0 \cdot B) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (B \cdot 0) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \end{aligned}$$



# Beispiel

Anwenden der Dominanz und Identität:

$$\begin{aligned} &= (A \cdot B) + (B \cdot 0) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (0) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= ((A \cdot B) + 0) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \\ &= (A \cdot B) + (A \cdot B \cdot \overline{B}) + (A \cdot \overline{A} \cdot \overline{B}) + (B \cdot \overline{A} \cdot \overline{B}) \end{aligned}$$

# Beispiel

... Wiederholung Identität und Dominanz durch 0 und Anwenden der Identität

$$\begin{aligned} &= (A \cdot B) + (\overline{A} \cdot 0) = (A \cdot B) + (0) \\ &= ((A \cdot B) + 0) = (A \cdot B) \end{aligned}$$

# Heute

- ▶ Erfüllbarkeit & Äquivalenz
- ▶ Beweisstrategien & Induktion – Strukturelle Induktion
- ▶ Negationstheorem
- ▶ De Morgan Regeln & Dualitätsprinzip
- ▶ Universelle Operatoren
- ▶ Normalformen
- ▶ Bitweise logische Operationen, Bit-Maskierung
- ▶ (Einführung Logikgatter)

# Erfüllbarkeit

## Definition (Erfüllbarkeit)

Sei  $\varphi$  ein beliebiger boolescher Ausdruck.  $\varphi$  heißt

- ▶ erfüllbar, wenn es Werte  $x_1, \dots, x_n$  gibt, mit  $\varphi(x_1, \dots, x_n) = 1$ .
- ▶ widerlegbar, wenn es Werte  $x_1, \dots, x_n$  gibt, mit  $\varphi(x_1, \dots, x_n) = 0$ .
- ▶ unerfüllbar, wenn  $\varphi(x_1, \dots, x_n)$  immer gleich 0 ist.
- ▶ allgemeingültig, wenn  $\varphi(x_1, \dots, x_n)$  immer gleich 1 ist.

Einen allgemeingültigen Ausdruck bezeichnen wir auch als **Tautologie**.

# Erfüllbarkeit/Unerfüllbar/Allgemeingültig

## ► Erfüllbare Funktionen

- $\varphi_1 = \neg x$
- $\varphi_2 = x \wedge y$
- $\varphi_3 = x \vee y$

## ► Unerfüllbare Funktionen

- $\varphi_1 = 0$
- $\varphi_2 = x \wedge \neg x$
- $\varphi_3 = \neg(x \vee \neg x)$

## ► Allgemeingültige Funktionen

- $\varphi_1 = 1$
- $\varphi_2 = x \vee \neg x$
- $\varphi_3 = \neg(x \wedge \neg x)$

# Äquivalenz

## Definition (Äquivalenz)

Zwei bool'sche Ausdrücke  $\varphi$  und  $\psi$  sind äquivalent, falls sie dieselbe Funktion repräsentieren. In anderen Worten:  $\varphi$  und  $\psi$  sind genau dann äquivalent, wenn für alle Variablenbelegungen  $x_1, \dots, x_n$  die folgende Beziehung gilt:

$$\varphi(x_1, \dots, x_n) = \psi(x_1, \dots, x_n)$$

D.h. Zwei bool'sche Ausdrücke  $\phi$  und  $\psi$  sind genau dann äquivalent, wenn der Ausdruck  $\phi \Leftrightarrow \psi$  eine Tautologie ist.

Mithilfe von Wahrheitstafeln, algebraischer Umformung oder durch Erzeugen einer Normalform können wir die Äquivalenz feststellen.

# Beweisstrategien

- ▶ Direkter Beweis
  - ▶ Annahme:  $A$  ist allgemeingültig, durch richtiges Schließen:  $A \Rightarrow B$
- ▶ Indirekter Beweis:
  - ▶ Negation der Annahme darf zu keinem korrekten Ergebnis führen
- ▶ Vollständige Induktion
  - ▶ Beweise für Aussagen über die natürlichen Zahlen  $\mathbb{N}$
  - ▶ Basierend auf den Peano-Axiomen für  $\mathbb{N}$

# Beweisregeln

- ▶ Abtrennungsregel:
  - ▶ Sind  $A$  und  $A \Rightarrow B$  allgemeingültig, so ist  $B$  allgemeingültig
  - ▶ Korrektheit folgt aus der Allgemeingültigkeit von  $(A \wedge (A \Rightarrow B)) \Rightarrow B$
- ▶ Fallunterscheidung
  - ▶ Sind  $A \Rightarrow B$  und  $\neg A \Rightarrow B$  allgemeingültig, so ist  $B$  allgemeingültig
  - ▶ Korrektheit folgt aus der Allgemeingültigkeit von  $((A \Rightarrow B) \wedge ((\neg A) \Rightarrow B)) \Rightarrow B$
- ▶ Kettenschluss
  - ▶ Sind  $A \Rightarrow B$  und  $B \Rightarrow C$  allgemeingültig, so ist  $A \Rightarrow C$  allgemeingültig
  - ▶ Korrektheit folgt aus der Allgemeingültigkeit von  $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$



# Beweisregeln

- ▶ Indirekter Beweis
  - ▶ Sind  $A \Rightarrow B$  und  $A \Rightarrow \neg B$  allgemeingültig, so ist  $\neg A$  allgemeingültig
  - ▶ Korrektheit folgt aus der Allgemeingültigkeit von
$$((A \Rightarrow B) \wedge (A \Rightarrow (\neg B))) \Rightarrow (\neg A)$$
- ▶ Kontraposition: Ist  $A \Rightarrow B$  allgemeingültig, so ist  $(\neg B) \Rightarrow (\neg A)$  allgemeingültig
  - ▶ Korrektheit folgt aus der Allgemeingültigkeit von
$$(A \Rightarrow B) \Rightarrow ((\neg B) \Rightarrow (\neg A)).$$

# Beispiel: Direkter Beweis

## Theorem

*Quadrate ungerader Zahlen sind ungerade Das Quadrat einer ungeraden Zahl  $n$ , wobei  $n \in \mathbb{N}_0$ , sei immer ungerade.*

## Beispiel: Direkter Beweis

Beweis.

$n$  sei eine ungerade Zahl. Dann lässt sich  $n$  als  $n = 2 \cdot k + 1, k \in \mathbb{N}_0$  schreiben. Hieraus folgert:

$$n^2 = (2 \cdot k + 1)^2$$

$$\Leftrightarrow = 4 \cdot k^2 + 4 \cdot k + 1$$

$$\Leftrightarrow = 2 \cdot (2k^2 + 2k) + 1$$

Nun ist  $n^2$  ungerade, da aus  $k \in \mathbb{N}_0$  und  $(2k^2 + 2k) \in \mathbb{N}_0$  und eine Vielfaches von 2 immer eine gerade Zahl folgt. Die Addition der 1 ergibt eben die ungerade Zahl. □

# Beispiel: Indirekter Beweis

Theorem (Größte Primzahlen)

*Es gibt keine größte Primzahl  $p$ .*

# Beispiel: Indirekter Beweis

## Größte Primzahlen.

Annahme: Es gebe nur endlich viele Primzahlen. D.h. es gibt eine endliche Menge von Primzahlen  $\mathbb{P} = \{p_1, p_2, \dots, p_r\}$ . Konstruieren wir eine neue Primzahl aus allen Faktoren von  $\mathbb{P}$  und addieren 1 hinzu. Die neue Zahl sei also  $p_{r+} := p_1 \cdot \dots \cdot p_r + 1$  und  $p$  sei ein Primteiler von  $p_{r+}$ . Dann ist  $p$  aber verschieden der  $p_i \in \mathbb{P}$ , da sonst  $p|p_{r+}$  oder  $p|p_1 \cdot \dots \cdot p_r$  gelten würde. Dies steht im Widerspruch zur Annahme des Satzes! Es kann also nicht endlich viele Primzahlen geben. □

# Vollständige Induktion

- ▶ Drei Teile:
  - ▶ Induktionsanfang (IA) & Induktionsannahme
  - ▶ Induktionsschritt (IS)
  - ▶ Induktionsschluss

# Beispiel: Vollständige Induktion

## Theorem

$$\forall n (n \in \mathbb{N}_0 \rightarrow 2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1)$$

## Beweis.

Prädikat:  $\varphi(n) \equiv (2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1)$

1. Induktionsanfang (IA):  $\varphi(0)$  soll gelten  $2^0 = 2^{0+1} - 1 \Leftrightarrow 1 = 1 \checkmark$
2. Induktionsschritt (IS):

$$\varphi(n) \Rightarrow \varphi(n^+)$$

$$2^0 + 2^1 + \dots + 2^n + 2^{n+1} = 2^{n+2} - 1 \quad \text{nach Voraussetzung wahr}$$

$$\Leftrightarrow 2^{n+1} - 1 + 2^{n+1} = 2^{(n+1)+1} - 1 \quad \text{Einsetzen der Voraussetzung}$$

$$\text{Anm.: } a^n \cdot a^m = a^{n+m}$$

$$\Leftrightarrow 2^1 \cdot 2^{n+1} - 1 = 2^{(n+1)+1} - 1$$

$$\Leftrightarrow 2^{(n+2)} - 1 = 2^{(n+2)} - 1 \checkmark$$





## Beweis.

Prädikat:  $\varphi(n) \equiv (2^0 + 2^1 + \dots 2^n = 2^{n+1} - 1)$

1. Induktionsanfang:  $\varphi(0)$  soll gelten  $2^0 = 2^{0+1} - 1 \Leftrightarrow 1 = 1\checkmark$
2. Induktionsschritt:

$$\begin{aligned}\varphi(n) &\Rightarrow \varphi(n^+) \\ 2^0 + 2^1 + \dots 2^n + 2^{n+1} &= 2^{(n+1)+1} - 1 \\ \Leftrightarrow 2^{n+1} - 1 + 2^{n+1} &= 2^{(n+1)+1} - 1 \\ \Leftrightarrow 2^1 \cdot 2^{n+1} - 1 &= 2^{(n+1)+1} - 1 \\ \Leftrightarrow 2^{(n+2)} - 1 &= 2^{(n+2)} - 1\checkmark\end{aligned}$$

3. Induktionsschluss:

# Kleiner Gauß

## Theorem

*Die Gaußsche Summenformel ist eine Formel für die Summe der ersten  $n$  aufeinanderfolgenden natürlichen Zahlen:*

$$0 + 1 + 2 + \dots + n = \sum_{i=1}^n i = \frac{n(n+1)}{2} = \frac{n^2 + n}{2}$$

# Kleiner Gauß.

1. Induktionsanfang:  $\varphi(1)$  soll gelten  $\frac{1(1+1)}{2} = 1 \quad \checkmark$   
 Voraussetzung, z.z.:  $\sum_i^{i+1} = \frac{(n+1)(n+1+1)}{2} = \frac{(n+1)(n+2)}{2}$
2. Induktionsschritt:

$$\begin{aligned}
 \sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + (n+1) \\
 &= \frac{n(n+1)}{2} + (n+1) \\
 &= \frac{n(n+1) + 2 \cdot (n+1)}{2} \\
 &= \frac{(n+1)(n+2)}{2} \quad \checkmark
 \end{aligned}$$

3. Induktionsschluss: nach IA und IS  $\Rightarrow \varphi(n)(\forall n(\varphi(n)))$



# Strukturelle Induktion

- ▶ Vollständige Induktion ist eine Spezialfall der strukturellen Induktion
- ▶ Wie in der vollständigen Induktion: Beweis für Basisfälle (Atome)
- ▶ Anschließend via Induktionsschritt zeigen, dass sich die Gültigkeit der Behauptung auf nächste Ebene überträgt
- ▶ Basisfälle (bool'sche Algebra): Alle nicht zusammengesetzten Elemente
  - ▶ Wahrheitswerte 0 und 1,
  - ▶ bool'schen Ausdrücke mit einer Variablen
  - ▶ D.h. Rückführung auf  $x \wedge \neg x$  bzw.  $x \vee \neg x$
  - ▶ Induktionsanfang den Ausdruck  $f = x$
- ▶ Induktionsschritt: Zeigt, dass Behauptung für beliebig zusammengesetzte Ausdrücke gilt
  - ▶ Induktionsschritt nur Elementaroperatoren:  $\neg, \wedge, \vee$

# Beispiel Strukturelle Induktion

## Theorem

*Sei  $\varphi$  ein beliebiger boolescher Ausdruck, in dem neben den Variablen  $x_1, \dots, x_n$  ausschließlich der Implikationsoperator vorkommt.  
Dann ist  $\varphi$  stets erfüllbar.*

- Idee: Wir zeigen, dass  $\varphi(x_1, \dots, x_n)$  stets gleich 1 ist, wenn wir alle Variablen 1 sind

# Beispiel Strukturelle Induktion

## Beweis.

**Induktionsanfang (IA):**  $\varphi$  sei ein nicht zusammengesetzter boolescher Term.  $\varphi$  hat die Form  $x_i$ , da keine Konstanten erlaubt sind. Es gilt  $\varphi(1) = 1$ .

**Induktionsvoraussetzung (IV):**  $\varphi$  sei ein zusammengesetzter boolescher Ausdruck, in dem neben den Variablen  $x_1, \dots, x_n$  ausschließlich der Implikationsoperator vorkommt. Wir nehmen an, die Behauptung sei für alle Unterterme von  $\varphi$  bereits bewiesen.

**Induktionsschritt (IS):** Da die Implikation der einzige Operator ist, der in  $\varphi$  vorkommen darf, hat  $\varphi$  die Form  $\varphi_1 \Rightarrow \varphi_2$ . Dann ist

$$\varphi(1, \dots, 1) = \varphi_1(1, \dots, 1) \Rightarrow \varphi_2(1, \dots, 1) = 1 \Rightarrow 1 = 1$$

somit ist  $\varphi$  bewiesen. □

# Negationstheorem

## Theorem (Negationstheorem)

*Sei  $f(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)$  ein boolescher Ausdruck, in dem neben den Konstanten 1 und 0 und den Variablen  $x_1, \dots, x_n$  die booleschen Operatoren  $\wedge, \vee$  und  $\neg$  vorkommen. Dann gilt:*

$$\overline{f(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} = f(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg)$$

# Beweis: Negationstheorem

## Negationstheorem.

**Induktionsanfang (IA):** Sei  $\varphi$  ein nicht zusammengesetzter Ausdruck. Wir betrachten alle Ausdrücke  $f$  der Länge 1:

Fall 1  $\varphi = 0$

$$\overline{\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} = \overline{0} = 1 = \varphi(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg)$$

Fall 2  $\varphi = 1$

$$\overline{\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} = \overline{1} = 0 = \varphi(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg)$$

Fall 3  $\varphi = x_i$

$$\overline{\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} = \overline{(x_i)} = (\overline{(x_i)}) = \varphi(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg)$$





# Beweis: Negationstheorem

Beweis.

**Induktionsvoraussetzung (IV):** Wir nehmen an, die Behauptung sei für alle Unterterme von  $f$  bereits bewiesen.



# Beweis: Negationstheorem

Beweis.

**Induktionsschritt (IS):** Wir unterscheiden drei Fälle:

Fall 1:  $\varphi = \overline{\varphi_1}$

$$\begin{aligned} & \overline{\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &= \overline{\varphi_1(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &\stackrel{IV}{=} \overline{\varphi_1(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg)} \\ &= \varphi(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \end{aligned}$$



# Beweis: Negationstheorem

Beweis.

**Induktionsschritt (IS):** Wir unterscheiden drei Fälle:

Fall 2:  $\varphi = \varphi_1 \wedge \varphi_2$

$$\begin{aligned} & \overline{\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &= \overline{\varphi_1(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg) \wedge \varphi_2(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &= \overline{\varphi_1(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \vee \overline{\varphi_2(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &\stackrel{IV}{=} \varphi_1(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \vee \varphi_2(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \\ &= \varphi(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \end{aligned}$$



# Beweis: Negationstheorem

Beweis.

**Induktionsschritt (IS):** Wir unterscheiden drei Fälle:

Fall 3:  $\varphi = \varphi_1 \vee \varphi_2$

$$\begin{aligned} & \overline{\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &= \overline{\varphi_1(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg) \vee \varphi_2(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &= \overline{\varphi_1(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \wedge \overline{\varphi_2(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)} \\ &\stackrel{IV}{=} \varphi_1(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \wedge \varphi_2(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \\ &= \varphi(1, 0, \overline{x_1}, \dots, \overline{x_n}, \vee, \wedge, \neg) \end{aligned}$$



# Negationstheorem & De Morgan'sche Regel

- ▶ Mithilfe des Negationstheorem haben wir die De Morgansche Regel bewiesen:
  - ▶ (M1)  $\overline{x \vee y} = \bar{x} \wedge \bar{y}$
  - ▶ (M2)  $\overline{x \wedge y} = \bar{x} \vee \bar{y}$
- ▶ Noch besser: Wir erhalten das Dualitätsprinzip – Symmetrieeigenschaft!
- ▶ D.h. Gültigkeit der dualen Gleichung ableitbar
- ▶ Durch Vertauschen der Wahrheitswerte und der Operatoren  $\wedge$  und  $\vee$  entsteht

# Dualitätsprinzip

## Theorem

*Sei*

$$\varphi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg) = \psi(0, 1, x_1, \dots, x_n, \wedge, \vee, \neg)$$

*ein Gesetz der booleschen Algebra, in der neben Variablen und den Konstanten 0 und 1 ausschließlich die Elementarverknüpfungen  $\neg$ ,  $\wedge$  und  $\vee$  vorkommen. Dann ist auch die duale Gleichung*

$$\varphi(1, 0, x_1, \dots, x_n, \vee, \wedge, \neg) = \psi(1, 0, x_1, \dots, x_n, \vee, \wedge, \neg)$$

*ein Gesetz der booleschen Algebra.*

# Vollständige Operatorensysteme

## Definition (Vollständige Operatorensystem)

$\mathcal{M}$  sei eine beliebige Menge von Operatoren.  $\mathcal{M}$  ist ein vollständiges Operatorensystem, wenn sich jede boolesche Funktion durch einen Ausdruck beschreiben lässt, in dem neben den Variablen  $x_1, \dots, x_n$  ausschließlich Operatoren aus  $\mathcal{M}$  vorkommen.

- ▶ Die Elementaroperatoren  $\wedge, \vee$  und  $\neg$  bilden zusammen ein vollständiges Operatorensystem
- ▶ Die Operatoren NAND und NOR bilden jeder für sich bereits ein vollständiges Operatorensystem
- ▶ Die Implikation und die 0 bilden zusammen ebenfalls ein vollständiges Operatorensystem

# Universelle Operatoren

- Reduktion von  $\wedge$ ,  $\vee$  und  $\neg$  auf NAND

$$\bar{x} = \overline{x \wedge x}$$

$$\begin{aligned} x \wedge y &= \overline{\overline{x \wedge y}} && \text{Idee: Doppelte Negation hebt sich auf} \\ &= \overline{\overline{x} \wedge \overline{y}} \end{aligned}$$

$$\begin{aligned} x \vee y &= \overline{\overline{x \vee y}} && \text{Idee: OR ist A und K} \\ &= \overline{\bar{x} \wedge \bar{y}} \\ &= \overline{\overline{x \wedge x} \wedge \overline{y \wedge y}} \end{aligned}$$



# Normalformdarstellungen

- ▶ Normalform beschreibt eine eindeutige Darstellung
- ▶ Vollform: Ausdruck, in dem jede Variable genau einmal vorkommt
- ▶ Literal: Teilausdruck, der entweder negierte oder unnegierte Variable darstellt
- ▶ Wahrheitstafeldarstellung ist eine Art der Normalformdarstellungen
- ▶ Bool'sche Ausdrücke hingegen sind keine Normalformdarstellung
  - ▶ Jede bool'sche Funktion durch unendlich viele Ausdrücke beschrieben werden

# Normalformdarstellungen

- ▶ Vollform: Ausdruck, in dem jede Variable genau einmal vorkommt
- ▶ Vollkonjunktion (**Minterm**): Ausdruck, in dem sämtliche vereinbarten Variablen (bzw. deren Negate) konjunktiv verbunden sind
  - ▶ Beispiel:  $A, B, C : A \wedge \neg B \wedge C$
- ▶ Volldisjunktion (**Maxterm**): Ausdruck, in dem sämtliche vereinbarten Variablen (bzw. deren Negate) disjunktiv verbunden sind
  - ▶ Beispiel:  $A, B, C : A \vee \neg B \vee \neg C$
- ▶ Negationen nur in atomarer Form
  - ▶  $\neg(A \wedge B)$ : nicht atomar
  - ▶  $(\neg A \vee \neg B)$ : atomar

# Formale Definition

## Definition (Minterm, Maxterm, Literal)

Sei  $f(x_1, \dots, x_n)$  eine beliebige  $n$ -stellige boolesche Funktion. Jeder Ausdruck der Form

$$\hat{x}_1 \wedge \dots \wedge \hat{x}_n \quad \text{mit } \hat{x}_i \in \{\overline{x_i}, x_i\}$$

heißt **Minterm**, jeder Ausdruck der Form

$$\hat{x}_1 \vee \dots \vee \hat{x}_n \quad \text{mit } \hat{x}_i \in \{\overline{x_i}, x_i\}$$

wird **Maxterm** genannt.

Der Teilausdruck  $\hat{x}_i$ , der entweder aus einer negierten oder einer unnegierten Variablen besteht, heißt **Literal**.

# Disjunktive Normalform

- ▶ Die disjunktive Normalform (DNF) ist jene Darstellungsart, bei der eine Reihe von Vollkonjunktionen disjunktiv verknüpft wird. Negationen treten nur in atomarer Form auf.
  - ▶  $(A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C) \vee (\neg A \wedge \neg B \wedge C)$
- ▶ Andere Bezeichnungen:
  - ▶ Kanonische disjunktive/konjunktive Normalform (KDNF/KKNF)
  - ▶ Vollständige disjunktive/konjunktive Normalform

## Beispiel: Disjunktive Normalform

$$f(x_1, x_2, x_3) = (x_1 \Rightarrow x_2) \wedge (\neg x_1 \Leftrightarrow x_3)$$

	$x_1$	$x_2$	$x_3$	$x_1 \Rightarrow x_2$	$\neg x_1 \Leftrightarrow x_3$	$(x_1 \Rightarrow x_2) \wedge (\neg x_1 \Leftrightarrow x_3)$
1	0	0	0	1	0	0
2	0	0	1	1	1	1
3	0	1	0	1	0	0
4	0	1	1	1	1	1
5	1	0	0	0	1	0
6	1	0	1	0	0	0
7	1	1	0	1	1	1
8	1	1	1	1	0	0

Vollkonjunktion/Minterm: 2:  $(\neg x_1 \wedge \neg x_2 \wedge x_3)$ , 4:  $(\neg x_1 \wedge x_2 \wedge x_3)$ , 7:  $(x_1 \wedge x_2 \wedge \neg x_3)$

DNF:  $(\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)$

# Konjunktive Normalform

- ▶ Die konjunktive Normalform (KNF) ist jene Darstellungsart, bei der eine Reihe von Volldisjunktionen konjunktiv verknüpft wird. Negationen treten nur in atomarer Form auf.
  - ▶  $(\neg A \vee \neg B \vee \neg C) \wedge (A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C)$
- ▶ Andere Bezeichnungen:
  - ▶ Kanonische disjunktive/konjunktive Normalform (KDNF/KKNF)
  - ▶ Vollständige disjunktive/konjunktive Normalform

## Beispiel: Konjunktive Normalform

$$f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee x_3$$

	$x_1$	$x_2$	$x_3$	$x_1 \wedge x_2$	$(x_1 \wedge x_2) \vee x_3$
1	0	0	0	0	0
2	0	0	1	0	1
3	0	1	0	0	0
4	0	1	1	1	1
5	1	0	0	0	0
6	1	0	1	0	1
7	1	1	0	1	1
8	1	1	1	1	1

Vollkonjunktion/Minterm: 1:  $\neg(\neg x_1 \wedge \neg x_2 \wedge \neg x_3)$ , 3:  $\neg(\neg x_1 \wedge x_2 \wedge \neg x_3)$ , 5:  $\neg(x_1 \wedge \neg x_2 \wedge \neg x_3)$

Volldisjunktion/Maxterm: 1:  $(x_1 \vee x_2 \vee x_3)$ , 3:  $(x_1 \vee \neg x_2 \vee x_3)$ , 5:  $(\neg x_1 \vee x_2 \vee x_3)$

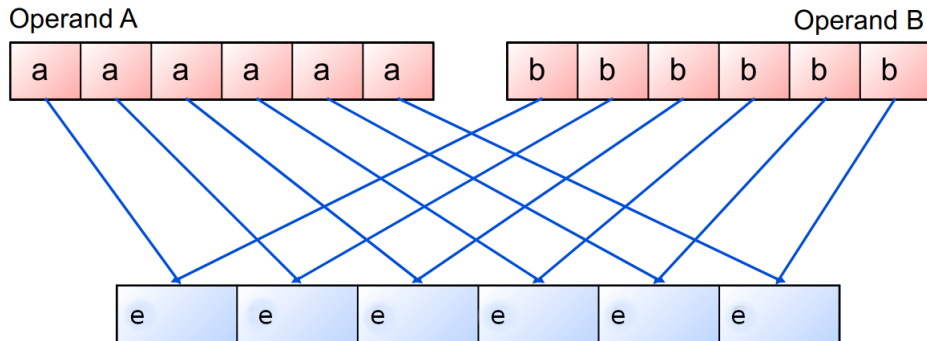
KNF:  $(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3)$

- ▶ Eigenschaft eines Minterms bzw. Maxterms ermöglicht Konstruktion aller  $n$ -stelligen bool'schen Funktionen
- ▶ D.h. durch KNF und DNF können wir eindeutige Darstellungen für beliebige Funktionen angeben
- ▶ Diese Darstellung hat ein Problem: Sie ist nicht minimal
  - ▶ Es gibt eine kürzere Darstellung
  - ▶ KNF für jedes Element der Nullmenge einen Maxterm
  - ▶ DNF für jedes Element der Einsmenge einen Minterm
  - ▶ Dünn bzw. dicht besetzte Funktionen kompakte Darstellung
  - ▶ Andere Formelklassen: Länge steigt der KNDF/DNF exponentiell mit Anzahl freien Variablen der Funktion
- ▶ Bsp.: Antivalenz (XOR)  $A_n(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n$
- ▶ Lösung: Reed-Muller-Normalform



# Bitweise logische Operationen

$A, B$  seien Bitvektoren,  $\circ$  eine beliebige Verknüpfung



Dann erhalten wir als Ergebnis:  $E = A \circ B$

# Bitmaskierung

UND, ODER und XOR als spezielle Bit-Masken

$$\begin{array}{r} \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 0 & 1 & 0 & 0 \\ \hline \end{array} \\ \wedge \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 1 & 1 & 0 & 0 \\ \hline \end{array} \\ \hline = \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 1 & 0 & 0 \\ \hline \end{array} \end{array}$$

$$\begin{array}{r} \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 0 & 1 & 0 & 0 \\ \hline \end{array} \\ \vee \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 1 & 1 & 0 & 0 \\ \hline \end{array} \\ \hline = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 1 & 1 & 0 & 0 \\ \hline \end{array} \end{array}$$

$$\begin{array}{r} \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 0 & 1 & 0 & 0 \\ \hline \end{array} \\ \oplus \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 1 & 1 & 0 & 0 \\ \hline \end{array} \\ \hline = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 0 & 0 & 0 \\ \hline \end{array} \end{array}$$

# UND Maskierung

Maskierung von IP-Adressen:

	IPv4-Adresse	11000000 10101000 00000001 10000001	192.168.1.129
UND	Netzmaske	11111111 11111111 11111111 00000000	255.255.255.0
=	Netzwerkteil	11000000 10101000 00000001 00000000	192.168.1.0

	IPv4-Adresse	11000000 10101000 00000001 10000001	192.168.1.129
UND	NOT Netzmaske	00000000 00000000 00000000 11111111	0.0.0.255
=	Geräteteil	00000000 00000000 00000000 10000001	0.0.0.129

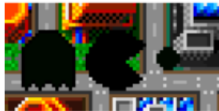
# OR Maskierung

## Image Mask

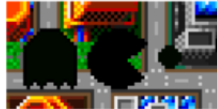
First step:



AND



Second step:



OR








# XOR Encryption

- ▶ Zufällig gleichverteilter Schlüssel der Länge  $n$ :  $k \in \mathcal{K}, \mathcal{K} := \{0, 1\}^n, n \in \mathbb{N}$ , Schlüsselraum  $\mathcal{K}$  ist die Permutationen aller Bitstrings
- ▶ Nachricht  $m \in \mathcal{M}$  binär kodiert, sodass  $\min\{0, 1\}^n$
- ▶ Nachricht und Schlüssel sind gleich lang
- ▶ Verschlüsselung:  $Enc_k(m) = m \oplus k = c$
- ▶ Entschlüsselung:  $Dec_k(c) = c \oplus k = m$
- ▶ Korrektheit:  $m = Dec_k(Enc_k(m)) = m$ , da  $m = k \oplus m \oplus k = m$  und  $k \oplus k = 0$  den Bitvektor  $\vec{0}$  ergibt


msg:	0	1	1	1	0	0	1	1
key:	1	1	0	0	1	0	0	1
<hr/>								
CT:								

$\oplus$

# Quellen I

-  Barnett, Janet Heine (2013). "Boolean algebra as an abstract structure: Edward V. Huntington and axiomatization". In: *Convergence*.
-  Bewersdorff, Jörg (2007). "Algebra für Einsteiger: Von der Gleichungsauflösung zur Galois-Theorie, 3". In: *Aufl. Vieweg+ Teubner, Wiesbaden (2007, Juli)*.
-  Hoffmann, Dirk W (2020). *Grundlagen der technischen Informatik*. Carl Hanser Verlag GmbH Co KG.
-  Rautenberg, Wolfgang (2008). *Einführung in die mathematische Logik*. Springer.
-  Sasao, Tsutomu (1999). "Lattice and Boolean Algebra". In: *Switching Theory for Logic Synthesis*. Springer, S. 17–34.

## Quellen II

 Teschl, Gerald und Susanne Teschl (2013). *Mathematik für Informatiker: Band 1: Diskrete Mathematik und Lineare Algebra*. Springer-Verlag.