Einführung in die Theoretische Informatik

Christian Dalvit   Manuel Eberl
Samuel Frontull   **Cezary Kaliszyk**   Daniel Ranalter

Wintersemester 2022/23

Zusammenfassung

Wintersemester 2022/23

Zusammenfassung der letzten LVA

	Einführung	*Elimination*
$\wedge$	$\dfrac{A \quad B}{A \wedge B}\ \wedge\!: \mathrm{i}$	$\dfrac{A \wedge B}{A}\ \wedge\!: \mathrm{e} \qquad \dfrac{A \wedge B}{B}\ \wedge\!: \mathrm{e}$
$\vee$	$\dfrac{A}{A \vee B}\ \vee\!: \mathrm{i} \qquad \dfrac{B}{A \vee B}\ \vee\!: \mathrm{i}$	$\dfrac{A \vee B \quad \boxed{\begin{array}{c} A \\ \vdots \\ C \end{array}} \quad \boxed{\begin{array}{c} B \\ \vdots \\ C \end{array}}}{C}\ \vee\!: \mathrm{e}$
$\rightarrow$	$\dfrac{\boxed{\begin{array}{c} A \\ \vdots \\ B \end{array}}}{A \rightarrow B}\ \rightarrow\!: \mathrm{i}$	$\dfrac{A \quad A \rightarrow B}{B}\ \rightarrow\!: \mathrm{e}$

	Einführung	*Elimination*
$\neg$	$\dfrac{\boxed{\begin{array}{l} A \\ \vdots \\ \mathsf{False} \end{array}}}{\neg A}\ \neg : \mathrm{i}$	$\dfrac{A \quad \neg A}{\mathsf{False}}\ \neg : \mathrm{e}$
False		$\dfrac{\mathsf{False}}{A}\ \mathsf{False} : \mathrm{e}$
$\neg\neg$		$\dfrac{\neg\neg A}{A}\ \neg\neg : \mathrm{e}$

Definition

Der Kalkül NK des natürlichen Schließens besteht aus den gerade betrachteten Beweisregeln.

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Kalkül des natürlichen Schließens, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

algebraische Strukturen, Boolesche Algebra

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen, Chomsky-Hierarchie, Anwendungen von formalen Sprachen

Einführung in die Berechenbarkeitstheorie und Komplexitätstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen, Komplexitätstheorie

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Kalkül des natürlichen Schließens, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

algebraische Strukturen, Boolesche Algebra

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen, Chomsky-Hierarchie, Anwendungen von formalen Sprachen

Einführung in die Berechenbarkeitstheorie und Komplexitätstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen, Komplexitätstheorie

Beispiel (Wiederholung)

Wir betrachten die Ableitung der Formel $\neg\neg p \to p$

1	$\boxed{\neg\neg p}$	Prämisse
2	$\boxed{p}$	$\neg\neg$: e
3	$\neg\neg p \to p$	1, 2, $\to$: i

Beispiel (Wiederholung)

Wir betrachten die Ableitung der Formel $\neg\neg p \to p$

$$
\begin{array}{lll}
1 & \neg\neg p & \text{Prämisse} \\
2 & p & \neg\neg\text{: e} \\
3 & \neg\neg p \to p & 1, 2, \to\text{: i}
\end{array}
$$

Beispiel

Wir betrachten die Ableitung der Umkehrung

$$p \to \neg\neg p$$

$$
\begin{array}{lll}
1 & p & \text{Prämisse} \\
2 & \neg p & \text{Prämisse} \\
3 & \text{False} & 1, 2, \neg\text{: e} \\
4 & \neg\neg p & 2{,}3, \neg\text{: i}
\end{array}
$$

Beispiel (Wiederholung)

Wir betrachten die Ableitung der Formel $\neg\neg p \to p$

1	$\neg\neg p$	Prämisse
2	p	$\neg\neg$: e
3	$\neg\neg p \to p$	1, 2, $\to$: i

Beispiel

Wir betrachten die Ableitung der Umkehrung

$$A \to \neg\neg A$$

1	A	Prämisse
2	$\neg A$	Prämisse
3	False	1, 2, $\neg$: e
4	$\neg\neg A$	2,3, $\neg$: i

Beispiel (Abgeleitete Regel $\neg\neg$: i)

Mit der selben Ableitung erhalten wir die folgende (abgeleitete) Inferenzregel:

$$\frac{A}{\neg\neg A}\ \neg\neg\colon \mathrm{i}$$

NB: Wir schreiben Inferenzregeln immer mit den Metavariablen für Formeln A, B, C ...

Beispiel (Abgeleitete Regel $\neg\neg$: i)

Mit der selben Ableitung erhalten wir die folgende (abgeleitete) Inferenzregel:

$$\frac{A}{\neg\neg A}\ \neg\neg\text{: i}$$

NB: Wir schreiben Inferenzregeln immer mit den Metavariablen für Formeln A, B, C ...

Beispiel

Wir betrachten noch eine weitere abgeleitete Inferenzregel, nämlich den Widerspruchsbeweis (WB):

$$\frac{\boxed{\begin{array}{l}\neg A\\ \vdots\\ \text{False}\end{array}}}{A}\ \text{WB}$$

Beispiel (Abgeleitete Regel WB)

Die Ableitung der Regel WB gelingt wie folgt:

1	$\neg A \rightarrow \text{False}$	Prämisse, $\rightarrow$: i
2	$\neg A$	Prämisse
3	False	1, 2, $\rightarrow$: e
4	$\neg\neg A$	2,3,$\neg$: i
5	A	4,$\neg\neg$: e

Beispiel (Abgeleitete Regel WB)

Die Ableitung der Regel WB gelingt wie folgt:

1	$\neg A \to \mathrm{False}$	Prämisse, $\to$: i
2	$\neg A$	Prämisse
3	False	1, 2, $\to$: e
4	$\neg\neg A$	2,3,$\neg$: i
5	A	4,$\neg\neg$: e

Beispiel

Nun wollen wir noch $p \vee q \vdash q \vee p$ zeigen:

1	$p \vee q$	Prämisse
2	p	Prämisse
3	$q \vee p$	2, $\vee$: i
4	q	Prämisse
5	$q \vee p$	4, $\vee$: i
6	$q \vee p$	1,2-3,4-5, $\vee$: e

Beispiel (Abgeleitete Regel WB)

Die Ableitung der Regel WB gelingt wie folgt:

1	$\neg A \rightarrow \mathrm{False}$	Prämisse, $\rightarrow$: i
2	$\neg A$	Prämisse
3	False	1, 2, $\rightarrow$: e
4	$\neg\neg A$	2,3,$\neg$: i
5	A	4,$\neg\neg$: e

Beispiel

Nun wollen wir noch $p \lor q \vdash q \lor p$ zeigen:

1	$p \lor q$	Prämisse
2	p	Prämisse
3	$q \lor p$	2, $\lor$: i
4	q	Prämisse
5	$q \lor p$	4, $\lor$: i
6	$q \lor p$	1,2-3,4-5, $\lor$: e

Beispiel (Abgeleitete Regel WB)

Die Ableitung der Regel WB gelingt wie folgt:

1	$\neg A \rightarrow \mathrm{False}$	Prämisse, $\rightarrow$: i
2	$\neg A$	Prämisse
3	False	1, 2, $\rightarrow$: e
4	$\neg\neg A$	2,3,$\neg$: i
5	A	4,$\neg\neg$: e

Beispiel

Nun wollen wir noch $p \vee q \vdash q \vee p$ zeigen:

1	$p \vee q$	Prämisse
2	p	Prämisse
3	$q \vee p$	2, $\vee$: i
4	q	Prämisse
5	$q \vee p$	4, $\vee$: i
6	$q \vee p$	1,2-3,4-5, $\vee$: e

Diskurs: Axiome für die Aussagenlogik nach Frege und Łukasiewicz

- Der Kalkül NK des natürlichen Schließens ist (beileibe) nicht der einzige korrekte und vollständige Kalkül für die Aussagenlogik.

Diskurs: Axiome für die Aussagenlogik nach Frege und Łukasiewicz

- Der Kalkül NK des natürlichen Schließens ist (beileibe) nicht der einzige korrekte und vollständige Kalkül für die Aussagenlogik.

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

$$
\begin{array}{ll}
(1) & A \to (B \to A) \\
(2) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\
(3) & (\neg A \to \neg B) \to (B \to A)
\end{array}
$$

Satz

Das Axiomensystem nach Frege und Łukasiewicz mit Inferenzregel Modus Ponens ist korrekt und vollständig für die Aussagenlogik. ∎

Konjunktive und Disjunktive Normalformen

Wintersemester 2022/23

Definition

Eine Wahrheitsfunktion $f\colon \{\mathsf{T}, \mathsf{F}\}^n \to \{\mathsf{T}, \mathsf{F}\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet (vgl. Rechnerarchitektur)

Definition

Eine Wahrheitsfunktion $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet (vgl. Rechnerarchitektur)

Definition

Sei $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ eine Wahrheitsfunktion; wir definieren:

$$\mathsf{TV}(f) := \{(s_1,\dots,s_n) \mid f(s_1,\dots,s_n) = \mathsf{T}\}$$

Definition

Eine Wahrheitsfunktion $f\colon \{\mathrm{T},\mathrm{F}\}^n \to \{\mathrm{T},\mathrm{F}\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet (vgl. Rechnerarchitektur)

Definition

Sei $f\colon \{\mathrm{T},\mathrm{F}\}^n \to \{\mathrm{T},\mathrm{F}\}$ eine Wahrheitsfunktion; wir definieren:

$$\mathrm{TV}(f) := \{(s_1,\dots,s_n) \mid f(s_1,\dots,s_n) = \mathrm{T}\}$$

Definition (Konjunktive und Disjunktive Normalform)

1. Ein Literal ist ein Atom p oder die Negation eines Atoms $\neg p$
2. Formel A ist in disjunktiver Normalform (DNF), wenn A eine Disjunktion von Konjunktionen von Literalen
3. Formel A ist in konjunktiver Normalform (KNF), wenn A eine Konjunktion von Disjunktionen von Literalen

Lemma

- $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ *eine Wahrheitsfunktion*
  $\mathsf{TV}(f) \neq \varnothing$, $\mathsf{TV}(f) \neq \{\mathsf{T},\mathsf{F}\}^n$

Lemma

- $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ *eine Wahrheitsfunktion*
  $\mathsf{TV}(f) \neq \varnothing$, $\mathsf{TV}(f) \neq \{\mathsf{T},\mathsf{F}\}^n$
- $p_1, \ldots, p_n$ *atomare Formeln*

Lemma

- $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ *eine Wahrheitsfunktion*
  $\mathsf{TV}(f) \neq \varnothing$, $\mathsf{TV}(f) \neq \{\mathsf{T},\mathsf{F}\}^n$
- $p_1,\dots,p_n$ *atomare Formeln*
- *Sei DNF* D *definiert als:*

$$D := \bigvee_{(s_1,\dots,s_n)\in\mathsf{TV}(f)} \ \bigwedge_{i=1}^{n} A_i$$

wobei $A_i = p_i$, *wenn* $s_i = \mathsf{T}$ *und* $A_i = \neg p_i$ *sonst*

Lemma

- $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ *eine Wahrheitsfunktion*
  $\mathsf{TV}(f) \neq \varnothing$, $\mathsf{TV}(f) \neq \{\mathsf{T},\mathsf{F}\}^n$
- $p_1, \dots, p_n$ *atomare Formeln*
- *Sei DNF D definiert als:*

$$D := \bigvee_{(s_1,\dots,s_n) \in \mathsf{TV}(f)} \bigwedge_{i=1}^{n} A_i$$

wobei $A_i = p_i$, *wenn* $s_i = \mathsf{T}$ *und* $A_i = \neg p_i$ *sonst*

- *Sei KNF K definiert als:*

$$K := \bigwedge_{(s_1,\dots,s_n) \notin \mathsf{TV}(f)} \bigvee_{j=1}^{n} B_j$$

wobei $B_j = \neg p_j$, *wenn* $s_j = \mathsf{T}$ *und* $B_j = p_j$ *sonst*

Lemma

- $f\colon \{\mathrm{T},\mathrm{F}\}^n \to \{\mathrm{T},\mathrm{F}\}$ *eine Wahrheitsfunktion*
  $\mathrm{TV}(f) \neq \varnothing$, $\mathrm{TV}(f) \neq \{\mathrm{T},\mathrm{F}\}^n$
- $p_1,\dots,p_n$ *atomare Formeln*
- *Sei DNF* D *definiert als:*

$$D := \bigvee_{(s_1,\dots,s_n)\in\mathrm{TV}(f)} \; \bigwedge_{i=1}^{n} A_i$$

  wobei $A_i = p_i$, *wenn* $s_i = \mathrm{T}$ *und* $A_i = \neg p_i$ *sonst*
- *Sei KNF* K *definiert als:*

$$K := \bigwedge_{(s_1,\dots,s_n)\notin\mathrm{TV}(f)} \; \bigvee_{j=1}^{n} B_j$$

  wobei $B_j = \neg p_j$, *wenn* $s_j = \mathrm{T}$ *und* $B_j = p_j$ *sonst*
- *Die Wahrheitstabellen von D und K entsprechen der Wahrheitsfunktion f*

Satz

1 *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*

Satz

1. *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
2. *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Satz

1. *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
2. *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Beweis.

1. Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
   - $\mathsf{TV}(f) = \varnothing$
   - $\mathsf{TV}(f) = \{\mathsf{T}, \mathsf{F}\}^n$

Satz

1. *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
2. *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Beweis.

1. Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
   - $\mathrm{TV}(f) = \varnothing$
   - $\mathrm{TV}(f) = \{\mathrm{T}, \mathrm{F}\}^n$
2. Setze $D = K := \bigwedge_{i=1}^{n} (p_i \wedge \neg p_i)$ im ersten Fall
3. Setze $D = K := \bigvee_{i=1}^{n} (p_i \vee \neg p_i)$ im zweiten Fall

Satz

1. *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
2. *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Beweis.

1. Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
   - $\mathrm{TV}(f) = \varnothing$
   - $\mathrm{TV}(f) = \{\mathrm{T}, \mathrm{F}\}^n$
2. Setze $D = K := \bigwedge_{i=1}^{n}(p_i \land \neg p_i)$ im ersten Fall
3. Setze $D = K := \bigvee_{i=1}^{n}(p_i \lor \neg p_i)$ im zweiten Fall ∎

Satz

1. *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
2. *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Beweis.

1. Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
   - $\mathrm{TV}(f) = \varnothing$
   - $\mathrm{TV}(f) = \{\mathrm{T}, \mathrm{F}\}^n$
2. Setze $D = K := \bigwedge_{i=1}^{n}(p_i \wedge \neg p_i)$ im ersten Fall
3. Setze $D = K := \bigvee_{i=1}^{n}(p_i \vee \neg p_i)$ im zweiten Fall ∎

Folgerung

Für jede Formel A existiert eine DNF D und eine KNF K, sodass $A \equiv D \equiv K$ gilt.

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$\mathsf{TV}(\oplus) = \{(\mathsf{F}, \mathsf{T}), (\mathsf{T}, \mathsf{F})\}$$

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$\mathrm{TV}(\oplus) = \{(F, T), (T, F)\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion
F	F	F	
T	T	F	

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	p $\oplus$ q
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$\mathsf{TV}(\oplus) = \{(\mathsf{F},\mathsf{T}),(\mathsf{T},\mathsf{F})\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion
F	F	F	$p_1 \vee p_2$
T	T	F	

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$\mathrm{TV}(\oplus) = \{(\mathrm{F}, \mathrm{T}), (\mathrm{T}, \mathrm{F})\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion
F	F	F	$p_1 \vee p_2$
T	T	F	$\neg p_1 \vee \neg p_2$

Beispiel

Die folgende Operation ($\oplus$) wird XOR genannt:

p	q	p $\oplus$ q
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$TV(\oplus) = \{(F,T),(T,F)\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion	KNF
F	F	F	$p_1 \vee p_2$	
T	T	F	$\neg p_1 \vee \neg p_2$	$(p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2)$

universität
innsbruck

Algebraische Strukturen

Wintersemester 2022/23

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \dots, A_n; \circ_1, \dots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \dots, A_n$
2. Operationen $\circ_1, \dots, \circ_m$ auf den Trägern

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Nullstellige Operationen werden auch Konstanten genannt; wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und für jede Operation $\circ_i$ der Algebra $\mathcal{A}$ ein Symbol $\circ_i$ der gleichen Stelligkeit

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Nullstellige Operationen werden auch Konstanten genannt; wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und für jede Operation $\circ_i$ der Algebra $\mathcal{A}$ ein Symbol $\circ_i$ der gleichen Stelligkeit

Definition (Algebraische Ausdrücke)

Wir definieren die algebraischen Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \dots, A_n; \circ_1, \dots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \dots, A_n$
2. Operationen $\circ_1, \dots, \circ_m$ auf den Trägern

Nullstellige Operationen werden auch Konstanten genannt; wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \dots$ und für jede Operation $\circ_i$ der Algebra $\mathcal{A}$ ein Symbol $\circ_i$ der gleichen Stelligkeit

Definition (Algebraische Ausdrücke)

Wir definieren die algebraischen Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Nullstellige Operationen werden auch Konstanten genannt; wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und für jede Operation $\circ_i$ der Algebra $\mathcal{A}$ ein Symbol $\circ_i$ der gleichen Stelligkeit

Definition (Algebraische Ausdrücke)

Wir definieren die algebraischen Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $A_1, \ldots, A_n$ algebraische Ausdrücke, $\circ$ eine Operation, dann ist $\circ(A_1, \ldots, A_n)$ ein algebraischer Ausdruck

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- Wenn $0 \in A$ existiert, sodass für alle $a \in A$

  $$a \circ 0 = 0 \circ a = 0$$

  dann heißt 0 Nullelement für $\circ$

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- Wenn $0 \in A$ existiert, sodass für alle $a \in A$

  $$a \circ 0 = 0 \circ a = 0$$

  dann heißt 0 Nullelement für $\circ$

- Wenn $1 \in A$ existiert, sodass für alle $a \in A$

  $$a \circ 1 = 1 \circ a = a$$

  dann heißt 1 Einselement (neutrales Element) für $\circ$

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- Wenn $0 \in A$ existiert, sodass für alle $a \in A$
$$a \circ 0 = 0 \circ a = 0$$
dann heißt 0 Nullelement für $\circ$
- Wenn $1 \in A$ existiert, sodass für alle $a \in A$
$$a \circ 1 = 1 \circ a = a$$
dann heißt 1 Einselement (neutrales Element) für $\circ$
- Sei 1 das neutrale Element für $\circ$ und für $a \in A$, existiert $b \in A$, sodass
$$a \circ b = b \circ a = 1$$
Dann heißt b das Inverse (Komplement) von a

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

- Halbgruppe, wenn $\circ$ assoziativ

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

- Halbgruppe, wenn $\circ$ assoziativ
- Monoid, wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ eine Halbgruppe mit Einselement 1 für $\circ$

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

- Halbgruppe, wenn $\circ$ assoziativ
- Monoid, wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ eine Halbgruppe mit Einselement 1 für $\circ$
- Gruppe, wenn $\mathcal{A}$ ein Monoid ist und jedes Element ein Inverses hat

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

- Halbgruppe, wenn $\circ$ assoziativ
- Monoid, wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ eine Halbgruppe mit Einselement 1 für $\circ$
- Gruppe, wenn $\mathcal{A}$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid oder eine Gruppe heißt kommutativ, wenn $\circ$ kommutativ

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

- Halbgruppe, wenn $\circ$ assoziativ
- Monoid, wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ eine Halbgruppe mit Einselement 1 für $\circ$
- Gruppe, wenn $\mathcal{A}$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid oder eine Gruppe heißt kommutativ, wenn $\circ$ kommutativ

Beispiel

Die im vorigen Beispiel definierte Algebra $\mathcal{A}$ hat folgende Eigenschaften:

1. a ist das neutrale Element von $\circ$
2. Jedes Element besitzt ein Inverses
3. $\circ$ ist nicht kommutativ

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$
3. Wir zeigen, dass $e = u$

$$\begin{aligned} e &= e \circ u && \text{da } u \text{ Einselement} \\ &= u && \text{da } e \text{ Einselement} \end{aligned}$$

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$
3. Wir zeigen, dass $e = u$

$$\begin{aligned} e &= e \circ u && \text{da } u \text{ Einselement} \\ &= u && \text{da } e \text{ Einselement} \end{aligned}$$

∎

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$b = b \circ 1 \qquad \text{1 ist neutrales Element}$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Komplement von } a
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Komplement von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Komplement von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ \\
&= 1 \circ c && b \text{ ist Komplement von } a
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Komplement von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ \\
&= 1 \circ c && b \text{ ist Komplement von } a \\
&= c && \text{1 ist neutrales Element}
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Komplement von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ \\
&= 1 \circ c && b \text{ ist Komplement von } a \\
&= c && \text{1 ist neutrales Element}
\end{aligned}
$$

$\blacksquare$

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1\rangle$ heißt Ring, wenn

1. $\langle A; +, 0\rangle$ eine kommutative Gruppe

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid
3. $\cdot$ distributiert über $+$ (von links und von rechts), das heißt für alle $a, b, c \in A$ gilt:

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

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid
3. $\cdot$ distributiert über $+$ (von links und von rechts), das heißt für alle $a, b, c \in A$ gilt:

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

Definition (Körper)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Körper, wenn

1. $\mathcal{A}$ ein Ring
2. $\langle A \setminus \{0\}; \cdot, 1 \rangle$ eine kommutative Gruppe

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ heißt Boolesche Algebra wenn gilt:

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$
3. Für alle $a \in B$ gilt
$$a + \sim(a) = 1 \qquad a \cdot \sim(a) = 0$$

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$
3. Für alle $a \in B$ gilt
$$a + \sim(a) = 1 \qquad a \cdot \sim(a) = 0$$

Das Element $\sim(a)$ heißt das Komplement oder die Negation von a

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1\rangle$ heißt Boolesche Algebra wenn gilt:

1. $\langle B; +, 0\rangle$ und $\langle B; \cdot, 1\rangle$ sind kommutative Monoide
2. Die Operationen $+$ und $\cdot$ distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$
3. Für alle $a \in B$ gilt
$$a + \sim(a) = 1 \qquad a \cdot \sim(a) = 0$$

Das Element $\sim(a)$ heißt das Komplement oder die Negation von a

Konventionen

- Wir lassen $\cdot$ oft weg und schreiben ab statt $a{\cdot}b$
- Wir verwenden die folgende Präzedenz: $\sim$ bindet stärker als $+$ und $\cdot$
- Die Definition ist eine Verallgemeinerung der Definition in Rechnerarchitektur

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \dots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Variablen sind Boolesche Ausdrücke

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Variablen sind Boolesche Ausdrücke
2. Wenn E und F Boolesche Ausdrücke sind, dann sind

$$\sim(E) \qquad (E \cdot F) \qquad (E + F)$$

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Variablen sind Boolesche Ausdrücke
2. Wenn E und F Boolesche Ausdrücke sind, dann sind

$$\sim(E) \qquad (E \cdot F) \qquad (E + F)$$

Boolesche Ausdrücke A und B heißen äquivalent ($A \approx B$), wenn für alle Booleschen Algebren, in allen Instanzen A' und B' gilt: $A' = B'$.

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Variablen sind Boolesche Ausdrücke
2. Wenn E und F Boolesche Ausdrücke sind, dann sind

$$\sim(E) \qquad (E \cdot F) \qquad (E + F)$$

Boolesche Ausdrücke A und B heißen äquivalent ($A \approx B$), wenn für alle Booleschen Algebren, in allen Instanzen A' und B' gilt: $A' = B'$.

Beispiel (vgl Rechnerarchitektur)

Die folgenden Ausdrücke sind Boolesche Ausdrücke:

$$x_1 \quad x_2 \quad x_1 + x_2 \quad x_1 \cdot x_2 \quad x_1 \cdot (x_1 + x_2) \quad x_1(x_1 + x_2) \quad x_1 \sim(x_1 + x_2)$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\sim$ die Komplementärmenge

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\sim$ die Komplementärmenge

Diese Algebra nennt man Mengenalgebra.

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die Potenzmenge von M, also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\sim$ die Komplementärmenge

Diese Algebra nennt man Mengenalgebra.

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Binäre Algebra

Definition

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$. Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \sim$ wie folgt definiert:

Binäre Algebra

Definition

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$. Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \sim$ wie folgt definiert:

$\cdot$	1	0
1	1	0
0	0	0

$+$	1	0
1	1	1
0	1	0

$\sim$	
1	0
0	1

Binäre Algebra

Definition

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$. Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \sim$ wie folgt definiert:

$$\begin{array}{c|cc} \cdot & 1 & 0 \\ \hline 1 & 1 & 0 \\ 0 & 0 & 0 \end{array} \qquad \begin{array}{c|cc} + & 1 & 0 \\ \hline 1 & 1 & 1 \\ 0 & 1 & 0 \end{array} \qquad \begin{array}{c|c} \sim & \\ \hline 1 & 0 \\ 0 & 1 \end{array}$$

Diese Algebra nennt man binäre Algebra oder Boolesche Algebra im engeren Sinn (Rechnerarchitektur)

Binäre Algebra

Definition

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$. Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$$

wobei die Operationen $+, \cdot, \sim$ wie folgt definiert:

$\cdot$	1	0
1	1	0
0	0	0

$+$	1	0
1	1	1
0	1	0

$\sim$	
1	0
0	1

Diese Algebra nennt man binäre Algebra oder Boolesche Algebra im engeren Sinn (Rechnerarchitektur)

Lemma

Die binäre Algebra ist eine Boolesche Algebra

Algebra der Aussagenlogik

Sei Frm die Menge der aussagenlogischen Formeln

Definition

Wir betrachten die Algebra $\mathcal{F}rm$

$$\langle \mathsf{Frm}; \vee, \wedge, \neg, \mathsf{False}, \mathsf{True} \rangle$$

Wobei die Zeichen wie in der Aussagenlogik interpretiert werden und Gleichheit von Booleschen Ausdrücken logische Äquivalenz bedeutet

Algebra der Aussagenlogik

Sei Frm die Menge der aussagenlogischen Formeln

Definition

Wir betrachten die Algebra $\mathcal{F}rm$

$$\langle \mathsf{Frm}; \vee, \wedge, \neg, \mathsf{False}, \mathsf{True} \rangle$$

Wobei die Zeichen wie in der Aussagenlogik interpretiert werden und Gleichheit von Booleschen Ausdrücken logische Äquivalenz bedeutet

Lemma

Die Algebra $\mathcal{F}rm$ ist eine Boolesche Algebra

Algebra des Kartesischen Produkts und der Schaltfunktionen

Definition

Sei $\mathbb{B} := \{0, 1\}$ und sei $\mathbb{B}^n$ das n-fache kartesische Produkt von $\mathbb{B}$:
$\mathbb{B}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{B}\}$; wir betrachten

$$\langle \mathbb{B}^n; +, \cdot, \sim, (0, \dots, 0), (1, \dots, 1) \rangle$$

1. $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$
2. $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 \cdot b_1, \dots, a_n \cdot b_n)$
3. $\sim((a_1, \dots, a_n)) = (\sim(a_1), \dots, \sim(a_n))$

Algebra des Kartesischen Produkts und der Schaltfunktionen

Definition

Sei $\mathbb{B} := \{0, 1\}$ und sei $\mathbb{B}^n$ das n-fache kartesische Produkt von $\mathbb{B}$:
$\mathbb{B}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{B}\}$; wir betrachten

$$\langle \mathbb{B}^n; +, \cdot, \sim, (0, \dots, 0), (1, \dots, 1) \rangle$$

1. $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$
2. $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 \cdot b_1, \dots, a_n \cdot b_n)$
3. $\sim((a_1, \dots, a_n)) = (\sim(a_1), \dots, \sim(a_n))$

Lemma

Die oben definierte Algebra ist eine Boolesche Algebra

Definition

Sei Abb die Menge der Abbildungen von $\mathbb{B}^n$ nach $\mathbb{B}^m$ wir betrachten

$$\langle \mathrm{Abb}; +, \cdot, \sim, (\mathbf{0}, \dots, \mathbf{0}), (\mathbf{1}, \dots, \mathbf{1}) \rangle$$

1. $(\mathbf{0}, \dots, \mathbf{0})\colon (a_1, \dots, a_n) \mapsto (0, \dots, 0)$
2. $(\mathbf{1}, \dots, \mathbf{1})\colon (a_1, \dots, a_n) \mapsto (1, \dots, 1)$
3. $(f + g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) + g(a_1, \dots, a_n)$
4. $(f \cdot g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) \cdot g(a_1, \dots, a_n)$
5. $\sim(f)(a_1, \dots, a_n) = \sim(f(a_1, \dots, a_n))$

Diese Algebra nennt man Algebra der Schaltfunktionen oder n-stelligen Booleschen Funktionen

Definition

Sei Abb die Menge der Abbildungen von $\mathbb{B}^n$ nach $\mathbb{B}^m$ wir betrachten

$$\langle \mathrm{Abb}; +, \cdot, \sim, (\mathbf{0}, \dots, \mathbf{0}), (\mathbf{1}, \dots, \mathbf{1}) \rangle$$

1. $(\mathbf{0}, \dots, \mathbf{0})\colon (a_1, \dots, a_n) \mapsto (0, \dots, 0)$
2. $(\mathbf{1}, \dots, \mathbf{1})\colon (a_1, \dots, a_n) \mapsto (1, \dots, 1)$
3. $(f + g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) + g(a_1, \dots, a_n)$
4. $(f \cdot g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) \cdot g(a_1, \dots, a_n)$
5. $\sim(f)(a_1, \dots, a_n) = \sim(f(a_1, \dots, a_n))$

Diese Algebra nennt man Algebra der Schaltfunktionen oder n-stelligen Booleschen Funktionen

Lemma

Die Algebra der Schaltfunktionen ist eine Boolesche Algebra