Einführung in die Theoretische Informatik

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

Wintersemester 2022/23

universität innsbruck

Zusammenfassung

Wintersemester 2022/23

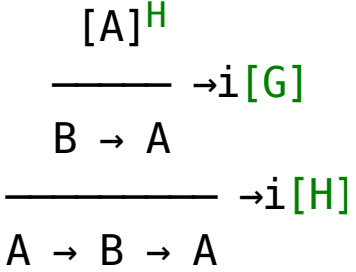
Erinnerung: Natürliches Schließen

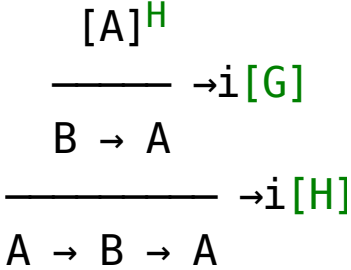
	Einführung	*Elimination*
$\neg$	$\dfrac{\boxed{\begin{array}{c}A\\\vdots\\\text{False}\end{array}}}{\neg A}\ \neg\text{: i}$	$\dfrac{A \quad \neg A}{\text{False}}\ \neg\text{: e}$
False		$\dfrac{\text{False}}{A}\ \text{False: e}$
$\neg\neg$		$\dfrac{\neg\neg A}{A}\ \neg\neg\text{: e}$

Satz

Der Kalkül NK *ist korrekt und vollständig für die Aussagenlogik:*

$$A_1, \ldots, A_n \models B \quad \textit{gdw.} \quad A_1, \ldots, A_n \vdash B$$


[A]H
→i[G]
B → A
→i[H]
A → B → A



1	H: A		assumption
2	G: B		assumption
3	A		copy 1
4	B → A		→i 2-3
5	A → B → A		→i 1-4

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

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

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 Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

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 Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Beweis.

Wir müssen zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind
2. seien $A, B, C \subseteq M$, dann gilt
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
3. für alle $A \subseteq M$ gilt
$$A \cup \sim(A) = M \quad A \cap \sim(A) = \varnothing$$

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Beweis.

Wir müssen zeigen, dass

3. für alle $A \subseteq M$ gilt

$$A \cup {\sim}(A) = M \quad A \cap {\sim}(A) = \varnothing$$

Wir beginnen mit den Gesetzen zum Komplement

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Beweis.

Wir müssen zeigen, dass

3. für alle $A \subseteq M$ gilt

$$A \cup {\sim}(A) = M \quad A \cap {\sim}(A) = \varnothing$$

Wir beginnen mit den Gesetzen zum Komplement; dazu beschränken wir uns auf $A \cap {\sim}(A) = \varnothing$, der Beweis für $A \cup {\sim}(A) = M$ ist ganz ähnlich

$$A \cap {\sim}(A) = A \cap \{x \in M \mid x \notin A\} = \{x \in M \mid x \in A \text{ und } x \notin A\} = \varnothing$$

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Beweis.

Wir müssen zeigen, dass

3. für alle $A \subseteq M$ gilt

$$A \cup {\sim}(A) = M \quad A \cap {\sim}(A) = \varnothing$$

Wir beginnen mit den Gesetzen zum Komplement; dazu beschränken wir uns auf $A \cap {\sim}(A) = \varnothing$, der Beweis für $A \cup {\sim}(A) = M$ ist ganz ähnlich

$$A \cap {\sim}(A) = A \cap \{x \in M \mid x \notin A\} = \{x \in M \mid x \in A \text{ und } x \notin A\} = \varnothing$$

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind
2. seien $A, B, C \subseteq M$, dann gilt

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind
2. seien $A, B, C \subseteq M$, dann gilt

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Die Korrektheit der Distributivgesetze folgt leicht aus den Definitionen der Mengenoperationen (nachrechnen!)

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind

Die Korrektheit der Distributivgesetze folgt leicht aus den Definitionen der Mengenoperationen (nachrechnen!)

Zeigen wir nun also, dass $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ ein kommunitative Monoid ist;

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind

Die Korrektheit der Distributivgesetze folgt leicht aus den Definitionen der Mengenoperationen (nachrechnen!)

Zeigen wir nun also, dass $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ ein kommunitative Monoid ist; dazu zeigen wir

- $\cup$ ist assoziativ
- $\varnothing$ ist das neutrale Element für $\cup$ auf $\mathcal{P}(M)$

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind

Die Korrektheit der Distributivgesetze folgt leicht aus den Definitionen der Mengenoperationen (nachrechnen!)

Zeigen wir nun also, dass $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ ein kommunitative Monoid ist; dazu zeigen wir

- $\cup$ ist assoziativ : $A \cup (B \cup C) = (A \cup B) \cup C$
- $\varnothing$ ist das neutrale Element für $\cup$ auf $\mathcal{P}(M)$: $A \cup \varnothing = \varnothing \cup A = A$

Beide Gleichungen folgen aus der Definition der Vereinigung.

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind

Die Korrektheit der Distributivgesetze folgt leicht aus den Definitionen der Mengenoperationen (nachrechnen!)

Zeigen wir nun also, dass $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ ein kommunitative Monoid ist; dazu zeigen wir

- $\cup$ ist assoziativ : $A \cup (B \cup C) = (A \cup B) \cup C$
- $\varnothing$ ist das neutrale Element für $\cup$ auf $\mathcal{P}(M)$: $A \cup \varnothing = \varnothing \cup A = A$

Beide Gleichungen folgen aus der Definition der Vereinigung.

Ebenso zeigt man, dass $\langle \mathcal{P}(M); \cap, M \rangle$ ein kommunitative Monoid ist. ■

Gesetze Boolescher Algebren

die noch nicht in Rechnerarchitektur behandelt wurden

Lemma ①

Für alle $a, b \in B$ gilt die Eindeutigkeit des Komplements:

$$\textit{Wenn } a + b = 1 \textit{ und } ab = 0\textit{, dann } b = \sim(a)$$

Gesetze Boolescher Algebren

die noch nicht in Rechnerarchitektur behandelt wurden

Lemma ①

Für alle $a, b \in B$ gilt die Eindeutigkeit des Komplements:

$$\textit{Wenn } a + b = 1 \textit{ und } ab = 0, \textit{ dann } b = \sim(a)$$

Beweis.

Gelte $a + b = 1$ und $ab = 0$

$$\begin{aligned} b &= b1 = b(a + \sim(a)) \\ &= ba + b \cdot \sim(a) = 0 + b \cdot \sim(a) && \text{da } ba = ab = 0 \\ &= a \cdot \sim(a) + b \cdot \sim(a) = (a + b) \cdot \sim(a) \\ &= 1 \cdot \sim(a) && \text{da } a + b = 1 \\ &= \sim(a) \end{aligned}$$

Gesetze Boolescher Algebren

die noch nicht in Rechnerarchitektur behandelt wurden

Lemma ①

Für alle $a, b \in B$ gilt die Eindeutigkeit des Komplements:

$$\text{Wenn } a + b = 1 \text{ und } ab = 0, \text{ dann } b = \sim(a)$$

Beweis.

Gelte $a + b = 1$ und $ab = 0$

$$\begin{aligned} b &= b1 = b(a + \sim(a)) \\ &= ba + b \cdot \sim(a) = 0 + b \cdot \sim(a) && \text{da } ba = ab = 0 \\ &= a \cdot \sim(a) + b \cdot \sim(a) = (a + b) \cdot \sim(a) \\ &= 1 \cdot \sim(a) && \text{da } a + b = 1 \\ &= \sim(a) \end{aligned}$$

Lemma

Für alle $a \in B$ gilt das Involutionsgesetz:

$$\sim(\sim(a)) = a$$

Lemma

Für alle $a \in B$ gilt das Involutionsgesetz:

$$\sim(\sim(a)) = a$$

Beweis.

Nach Definition einer Booleschen Algebra und Kommutativität von $+$ beziehungsweise $\cdot$ gilt:

1. $\sim(a) + a = 1$
2. $\sim(a) \cdot a = 0$

Mit Lemma ① folgt, dass a das Komplement von $\sim(a)$ ist ■

Lemma

Für alle $a \in B$ gilt das Involutionsgesetz:

$$\sim(\sim(a)) = a$$

Beweis.

Nach Definition einer Booleschen Algebra und Kommutativität von $+$ beziehungsweise $\cdot$ gilt:

1. $\sim(a) + a = 1$
2. $\sim(a) \cdot a = 0$

Mit Lemma ① folgt, dass a das Komplement von $\sim(a)$ ist ■

Lemma

Für alle $a, b \in B$ gelten die Gesetze von de Morgan:

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

Idempotenz und Absorption

bereits in Rechnerarchitektur behandelt

Lemma

Für alle $a \in B$ gelten die Idempotenzgesetze:

$$a \cdot a = a \qquad a + a = a$$

und die folgenden Gesetze für 0 und 1 (Substitution):

$$0 \cdot a = 0 \qquad 1 + a = 1$$

Idempotenz und Absorption

bereits in Rechnerarchitektur behandelt

Lemma

Für alle $a \in B$ gelten die Idempotenzgesetze:

$$a \cdot a = a \qquad a + a = a$$

und die folgenden Gesetze für 0 und 1 (Substitution):

$$0 \cdot a = 0 \qquad 1 + a = 1$$

Lemma

Für alle $a, b \in B$ gelten die Absorptionsgesetze:

$$a + ab = a \qquad a(a + b) = a$$

$$a + {\sim}(a) \cdot b = a + b \qquad a({\sim}(a) + b) = ab$$

Erstes Gesetz von de Morgan.

- Wir zeigen $(a + b) + (\sim(a) \cdot \sim(b)) = 1$:

$$\begin{aligned}(a + b) + (\sim(a) \cdot \sim(b)) &= (a + b + \sim(a))(a + b + \sim(b)) \\ &= (a + \sim(a) + b)(a + b + \sim(b)) \\ &= (1 + b)(a + 1) \\ &= 1 \cdot 1 = 1\end{aligned}$$

Erstes Gesetz von de Morgan.

- Wir zeigen $(a + b) + (\sim(a) \cdot \sim(b)) = 1$:

$$\begin{aligned}(a + b) + (\sim(a) \cdot \sim(b)) &= (a + b + \sim(a))(a + b + \sim(b)) \\ &= (a + \sim(a) + b)(a + b + \sim(b)) \\ &= (1 + b)(a + 1) \\ &= 1 \cdot 1 = 1\end{aligned}$$

- Wir zeigen $(a + b) \cdot (\sim(a) \cdot \sim(b)) = 0$:

$$\begin{aligned}(a + b) \cdot \sim(a) \cdot \sim(b) &= a \cdot \sim(a) \cdot \sim(b) + b \cdot \sim(a) \cdot \sim(b) \\ &= a \cdot \sim(a) \cdot \sim(b) + \sim(a) \cdot b \cdot \sim(b) \\ &= 0 \cdot \sim(b) + \sim(a) \cdot 0 \\ &= 0 + 0 = 0\end{aligned}$$

Erstes Gesetz von de Morgan.

- Wir zeigen $(a+b)+(\sim(a)\cdot\sim(b))=1$:

$$\begin{aligned}(a+b)+(\sim(a)\cdot\sim(b)) &= (a+b+\sim(a))(a+b+\sim(b))\\ &= (a+\sim(a)+b)(a+b+\sim(b))\\ &= (1+b)(a+1)\\ &= 1\cdot 1 = 1\end{aligned}$$

- Wir zeigen $(a+b)\cdot(\sim(a)\cdot\sim(b))=0$:

$$\begin{aligned}(a+b)\cdot\sim(a)\cdot\sim(b) &= a\cdot\sim(a)\cdot\sim(b)+b\cdot\sim(a)\cdot\sim(b)\\ &= a\cdot\sim(a)\cdot\sim(b)+\sim(a)\cdot b\cdot\sim(b)\\ &= 0\cdot\sim(b)+\sim(a)\cdot 0\\ &= 0+0=0\end{aligned}$$

- Die Voraussetzungen von Lemma ① sind gezeigt

Erstes Gesetz von de Morgan.

- Wir zeigen $(a+b)+(\sim(a)\cdot\sim(b))=1$:

$$\begin{aligned}(a+b)+(\sim(a)\cdot\sim(b)) &= (a+b+\sim(a))(a+b+\sim(b))\\ &= (a+\sim(a)+b)(a+b+\sim(b))\\ &= (1+b)(a+1)\\ &= 1\cdot 1 = 1\end{aligned}$$

- Wir zeigen $(a+b)\cdot(\sim(a)\cdot\sim(b))=0$:

$$\begin{aligned}(a+b)\cdot\sim(a)\cdot\sim(b) &= a\cdot\sim(a)\cdot\sim(b)+b\cdot\sim(a)\cdot\sim(b)\\ &= a\cdot\sim(a)\cdot\sim(b)+\sim(a)\cdot b\cdot\sim(b)\\ &= 0\cdot\sim(b)+\sim(a)\cdot 0\\ &= 0+0=0\end{aligned}$$

- Die Voraussetzungen von Lemma ① sind gezeigt
- Somit ist $\sim(a)\cdot\sim(b)$ das Komplement von $a+b$, wzzw.

Erstes Gesetz von de Morgan.

- Wir zeigen $(a+b)+(\sim(a)\cdot\sim(b))=1$:

$$\begin{aligned}(a+b)+(\sim(a)\cdot\sim(b)) &= (a+b+\sim(a))(a+b+\sim(b))\\ &= (a+\sim(a)+b)(a+b+\sim(b))\\ &= (1+b)(a+1)\\ &= 1\cdot 1 = 1\end{aligned}$$

- Wir zeigen $(a+b)\cdot(\sim(a)\cdot\sim(b))=0$:

$$\begin{aligned}(a+b)\cdot\sim(a)\cdot\sim(b) &= a\cdot\sim(a)\cdot\sim(b)+b\cdot\sim(a)\cdot\sim(b)\\ &= a\cdot\sim(a)\cdot\sim(b)+\sim(a)\cdot b\cdot\sim(b)\\ &= 0\cdot\sim(b)+\sim(a)\cdot 0\\ &= 0+0=0\end{aligned}$$

- Die Voraussetzungen von Lemma ① sind gezeigt
- Somit ist $\sim(a)\cdot\sim(b)$ das Komplement von $a+b$, wzzw.

Definition (Boolesche Funktion)

1. Sei F ein Boolescher Ausdruck in den Variablen $x_1, \ldots, x_n$
2. $F(s_1, \ldots, s_n)$ die Instanz von F
3. Wir definieren die Funktion $f\colon \mathbb{B}^n \to \mathbb{B}$ wie folgt:

$$f(s_1, \ldots, s_n) := F(s_1, \ldots, s_n)\ .$$

Dann heißt f die Boolesche Funktion zum Ausdruck F

Definition (Boolesche Funktion)

1. Sei F ein Boolescher Ausdruck in den Variablen $x_1, \ldots, x_n$
2. $F(s_1, \ldots, s_n)$ die Instanz von F
3. Wir definieren die Funktion $f\colon \mathbb{B}^n \to \mathbb{B}$ wie folgt:

$$f(s_1, \ldots, s_n) := F(s_1, \ldots, s_n)\,.$$

Dann heißt f die Boolesche Funktion zum Ausdruck F

Beispiel (Boolesche Algebra $\mathcal{F}rm = \langle \mathrm{Frm}; \vee, \wedge, \neg, \mathrm{False}, \mathrm{True}\rangle$)

Sei $F = x_1 \wedge \neg(x_2 \vee x_1)$, dann ist $f\colon \mathbb{B}^2 \to \mathbb{B}$ die Boolesche Funktion zu F

Sei $G = x_1 \wedge x_2 \wedge \neg x_2$, dann ist $g\colon \mathbb{B}^2 \to \mathbb{B}$ die Boolesche Funktion zu G

s_1	s_2	$f(s_1, s_2)$	$g(s_1, s_2)$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	0	0

Definition

1. Sei $f : \mathbb{B}^n \to \mathbb{B}$ eine Boolesche Funktion
2. Sei F ein Boolescher Ausdruck, dessen Boolesche Funktion gleich f

Dann nennen wir F den Booleschen Ausdruck von f

Definition

1. Sei $f : \mathbb{B}^n \to \mathbb{B}$ eine Boolesche Funktion
2. Sei F ein Boolescher Ausdruck, dessen Boolesche Funktion gleich f

Dann nennen wir F den Booleschen Ausdruck von f

Satz (Darstellungssatz von Stone)

Jede Boolesche Algebra ist isomorph zu einer Mengenalgebra

Definition

1. Sei $f\colon \mathbb{B}^n \to \mathbb{B}$ eine Boolesche Funktion
2. Sei F ein Boolescher Ausdruck, dessen Boolesche Funktion gleich f

Dann nennen wir F den Booleschen Ausdruck von f

Satz (Darstellungssatz von Stone)

Jede Boolesche Algebra ist isomorph zu einer Mengenalgebra

Bemerkung

- Isomorphie bedeutet, dass die Operationen auf den Algebren ident sind.
- Der Darstellungssatz von Stone bedeutet also, dass jede Gleichheit in einer Mengenalgebra eine Gleichheit für alle Booleschen Algebren ist.
- Anders ausgedrückt stellen Mengenalgebren die eindeutige Darstellung von Booleschen Algebren dar.

Folgerung aus dem Darstellungssatz von Stone

Folgerung

1. *Seien A, B Boolesche Ausdrücke*
2. *Seien f, g ihre Booleschen Funktionen*

Dann sind A und B äquivalent ($A \approx B$), wenn $f = g$ in der Algebra der Booleschen Funktionen gilt

Folgerung aus dem Darstellungssatz von Stone

Folgerung

1. *Seien A, B Boolesche Ausdrücke*
2. *Seien f, g ihre Booleschen Funktionen*

Dann sind A und B äquivalent ($A \approx B$), wenn $f = g$ in der Algebra der Booleschen Funktionen gilt

Beweisskizze

- Äquivalenzen von Boolesche Ausdrücke gelten (per Definition) für alle Booleschen Algebren.
- Um diese Äquivalenzen zu überprüfen genügt (nach der Definition) die Verifikation in einer bestimmten Algebra, nämlich der Algebra der Booleschen Funktionen; das folgt aus dem Darstellungssatz von Stone

universität innsbruck

Boolesche Algebren

Wintersemester 2022/23

Isomorphie

vgl. Lineare Algebra

Definition

Seien $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$, $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$ Algebren, dann heißt eine Abbildung $\varphi\colon A \to B$ ein Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$, wenn gilt

Isomorphie

vgl. Lineare Algebra

Definition

Seien $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$, $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$ Algebren, dann heißt eine Abbildung $\varphi\colon A \to B$ ein Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$, wenn gilt

- φ ist bijektiv

Isomorphie

vgl. Lineare Algebra

Definition

Seien $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$, $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$ Algebren, dann heißt eine Abbildung $\varphi\colon A \to B$ ein Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$, wenn gilt

- φ ist bijektiv
- für alle Operationen $\circ_i$ von $\mathcal{A}$ ($\circ_i$ n-stellig) gilt:

$$\varphi(\circ_i(a_1, \ldots, a_n)) = \odot_i(\varphi(a_1), \ldots, \varphi(a_n)) \,,$$

für alle $a_1, \ldots, a_n \in A$.

Isomorphie

vgl. Lineare Algebra

Definition

Seien $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$, $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$ Algebren, dann heißt eine Abbildung $\varphi\colon A \to B$ ein Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$, wenn gilt

- φ ist bijektiv
- für alle Operationen $\circ_i$ von $\mathcal{A}$ ($\circ_i$ n-stellig) gilt:

$$\varphi(\circ_i(a_1, \ldots, a_n)) = \odot_i(\varphi(a_1), \ldots, \varphi(a_n)) \,,$$

für alle $a_1, \ldots, a_n \in A$.

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$ heißt isomorph zur Algebra $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$, wenn ein Isomorphismus $\varphi\colon A \to B$ existiert. Wir schreiben $\mathcal{A} \cong \mathcal{B}$.

Beispiel

- Betrachte die Monoide $\langle \{a, b\}, + \rangle$ und $\langle \{0, 1\}, \cdot \rangle$, wobei die Operationen $+$ bzw. $\cdot$ durch die folgenden Operationstafeln definiert sind:

$+$	a	b
a	a	b
b	b	a

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

Beispiel

- Betrachte die Monoide $\langle \{a, b\}, + \rangle$ und $\langle \{0, 1\}, \cdot \rangle$, wobei die Operationen $+$ bzw. $\cdot$ durch die folgenden Operationstafeln definiert sind:

$+$	a	b
a	a	b
b	b	a

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

- Dann ist die Abbildung $\varphi \colon \{a, b\} \to \{0, 1\}$ mit

$$\varphi(a) := 0 \qquad \varphi(b) := 1 \,,$$

ein Isomorphismus

Beispiel

- Betrachte die Monoide $\langle \{a, b\}, + \rangle$ und $\langle \{0, 1\}, \cdot \rangle$, wobei die Operationen $+$ bzw. $\cdot$ durch die folgenden Operationstafeln definiert sind:

$+$	a	b
a	a	b
b	b	a

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

- Dann ist die Abbildung $\varphi \colon \{a, b\} \to \{0, 1\}$ mit

$$\varphi(a) := 0 \qquad \varphi(b) := 1 \,,$$

ein Isomorphismus

Bemerkung

Wir interessieren uns besonders für Isomorphismen zwischen Booleschen Algebren und können damit den Darstellungsatz von Stone exakt definieren.

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$.

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

- Sei $\varphi \colon \mathbb{B} \to \{\varnothing, \{a\}\}$ wie folgt definiert

$$\varphi(0) := \varnothing \qquad \varphi(1) := \{a\}$$

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

- Sei $\varphi \colon \mathbb{B} \to \{\varnothing, \{a\}\}$ wie folgt definiert

$$\varphi(0) := \varnothing \qquad \varphi(1) := \{a\}$$

- Dann ist φ eine bijektive Funktion und außerdem sogar ein Isomorphismus:

$+$	1	0
1	1	1
0	1	0

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

$\sim$	
1	0
0	1

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

- Sei $\varphi \colon \mathbb{B} \to \{\varnothing, \{a\}\}$ wie folgt definiert

$$\varphi(0) := \varnothing \qquad \varphi(1) := \{a\}$$

- Dann ist φ eine bijektive Funktion und außerdem sogar ein Isomorphismus:

$\cup$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\{a\}$
$\varnothing$	$\{a\}$	$\varnothing$

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

$\sim$	
1	0
0	1

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

- Sei $\varphi \colon \mathbb{B} \to \{\varnothing, \{a\}\}$ wie folgt definiert

$$\varphi(0) := \varnothing \qquad \varphi(1) := \{a\}$$

- Dann ist φ eine bijektive Funktion und außerdem sogar ein Isomorphismus:

$\cup$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\{a\}$
$\varnothing$	$\{a\}$	$\varnothing$

$\cap$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\varnothing$
$\varnothing$	$\varnothing$	$\varnothing$

$\sim$	
1	0
0	1

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

- Sei $\varphi \colon \mathbb{B} \to \{\varnothing, \{a\}\}$ wie folgt definiert

$$\varphi(0) := \varnothing \qquad \varphi(1) := \{a\}$$

- Dann ist φ eine bijektive Funktion und außerdem sogar ein Isomorphismus:

$\cup$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\{a\}$
$\varnothing$	$\{a\}$	$\varnothing$

$\cap$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\varnothing$
$\varnothing$	$\varnothing$	$\varnothing$

$\sim$	
$\{a\}$	$\varnothing$
$\varnothing$	$\{a\}$

Partielle Ordnungen und Boolesche Algebren

Definition

Eine partielle Ordnung auf einer Menge $M \neq \varnothing$ ist eine Menge von geordneten Paaren $(a, b) \in M \times M$, geschrieben $a \leq b$, sodass gilt

- $a \leq a$, für alle $a \in M$ — Reflexivität
- $a \leq b$ und $b \leq c$ impliziert $a \leq c$, für alle $a, b, c \in M$ — Transitivität
- $a \leq b$ und $b \leq a$ impliziert $a = b$, für alle $a, b \in M$ — Antisymmetrie

Partielle Ordnungen und Boolesche Algebren

Definition

Eine partielle Ordnung auf einer Menge $M \neq \varnothing$ ist eine Menge von geordneten Paaren $(a, b) \in M \times M$, geschrieben $a \leq b$, sodass gilt

- $a \leq a$, für alle $a \in M$ — Reflexivität
- $a \leq b$ und $b \leq c$ impliziert $a \leq c$, für alle $a, b, c \in M$ — Transitivität
- $a \leq b$ und $b \leq a$ impliziert $a = b$, für alle $a, b \in M$ — Antisymmetrie

Fakt

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine Boolesche Algebra und definiere Relation $\leq$ auf B:

$$a \leq b \Leftrightarrow a \cdot b = a$$

- $\leq$ ist eine partielle Ordnung

Beweis des Darstellungsatz von Stone (I)

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine (endliche) Boolesche Algebra;
- sei $\leq$, die von $\mathcal{B}$ induzierte partielle Ordnung.

Beweis des Darstellungsatz von Stone (I)

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine (endliche) Boolesche Algebra;
- sei $\leq$, die von $\mathcal{B}$ induzierte partielle Ordnung.

Definition

- Sei $a \in B \setminus \{0\}$.
- Wenn $0 \leq a$ und kein $a' \in B \setminus \{0\}$, $a \neq a'$ existiert, sodass $0 \leq a' \leq a$, dann nennen wir a ein Atom.

Beweis des Darstellungsatz von Stone (I)

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine (endliche) Boolesche Algebra;
- sei $\leq$, die von $\mathcal{B}$ induzierte partielle Ordnung.

Definition

- Sei $a \in B \setminus \{0\}$.
- Wenn $0 \leq a$ und kein $a' \in B \setminus \{0\}$, $a \neq a'$ existiert, sodass $0 \leq a' \leq a$, dann nennen wir a ein Atom.

Kürzer: die Atome sind die oberen Nachbarn von 0 in B.

Beweis des Darstellungsatz von Stone (I)

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine (endliche) Boolesche Algebra;
- sei $\leq$, die von $\mathcal{B}$ induzierte partielle Ordnung.

Definition

- Sei $a \in B \setminus \{0\}$.
- Wenn $0 \leq a$ und kein $a' \in B \setminus \{0\}$, $a \neq a'$ existiert, sodass $0 \leq a' \leq a$, dann nennen wir a ein Atom.

Kürzer: die Atome sind die oberen Nachbarn von 0 in B.

Beispiel

Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra, dann ist $1 \in \mathbb{B}$ ein Atom. Es gibt kein Element $\neq 0$ in $\mathbb{B}$ gibt, das größer als 0 und (echt) kleiner als 1 ist.

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

1. Sei $M := \{a \in B \mid a \text{ ein Atom in } \mathcal{B}\}$.

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

1. Sei $M := \{a \in B \mid a \text{ ein Atom in } \mathcal{B}\}$.
2. Wir betrachten nun die Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$.

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

1. Sei $M := \{a \in B \mid a \text{ ein Atom in } \mathcal{B}\}$.
2. Wir betrachten nun die Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$.
3. Für jedes $b \in B$, definiere $A(b) := \{a \in B \mid a \text{ ein Atom in } \mathcal{B} \text{ und } a \leq b\}$.

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

1. Sei $M := \{a \in B \mid a \text{ ein Atom in } \mathcal{B}\}$.
2. Wir betrachten nun die Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$.
3. Für jedes $b \in B$, definiere $A(b) := \{a \in B \mid a \text{ ein Atom in } \mathcal{B} \text{ und } a \leq b\}$.
4. Schließlich definieren wir die Abbildung $\varphi \colon B \to \mathcal{P}(M)$, sodass $\varphi(b) := A(b)$.

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

1. Sei $M := \{a \in B \mid a \text{ ein Atom in } \mathcal{B}\}$.
2. Wir betrachten nun die Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$.
3. Für jedes $b \in B$, definiere $A(b) := \{a \in B \mid a \text{ ein Atom in } \mathcal{B} \text{ und } a \leq b\}$.
4. Schließlich definieren wir die Abbildung $\varphi \colon B \to \mathcal{P}(M)$, sodass $\varphi(b) := A(b)$.

Lemma

Die Abbildung φ ist ein Isomorphismus von $\langle B; +, \cdot, \sim, 0, 1 \rangle$ auf $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$. ■

universität innsbruck

Formale Sprachen

Wintersemester 2022/23

Definition (Alphabet)

Ein Alphabet Σ ist eine endliche, nicht leere Menge von Symbolen

Definition (Alphabet)

Ein Alphabet Σ ist eine endliche, nicht leere Menge von Symbolen

Beispiel

- $\Sigma = \{0, 1\}$ ist das binäre Alphabet

Definition (Alphabet)

Ein Alphabet Σ ist eine endliche, nicht leere Menge von Symbolen

Beispiel

- $\Sigma = \{0, 1\}$ ist das binäre Alphabet
- $\Sigma = \{a, b, \ldots, z\}$, die Menge aller Kleinbuchstaben

Definition (Alphabet)

Ein Alphabet Σ ist eine endliche, nicht leere Menge von Symbolen

Beispiel

- $\Sigma = \{0, 1\}$ ist das binäre Alphabet
- $\Sigma = \{a, b, \ldots, z\}$, die Menge aller Kleinbuchstaben
- die Menge der (druckbaren) ASCII-Zeichen

Definition (Alphabet)

Ein Alphabet Σ ist eine endliche, nicht leere Menge von Symbolen

Beispiel

- $\Sigma = \{0, 1\}$ ist das binäre Alphabet
- $\Sigma = \{a, b, \ldots, z\}$, die Menge aller Kleinbuchstaben
- die Menge der (druckbaren) ASCII-Zeichen

Definition (Wort)

- Eine Zeichenreihe (ein Wort, ein String) ist eine endliche Folge von Symbolen über einem Alphabet Σ
- Die leere Zeichenreihe wird mit ϵ bezeichnet

Beispiel

Die Symbolkette 01101 ist eine Zeichenreihe über dem Alphabet $\{0, 1\}$

Beispiel

Die Symbolkette 01101 ist eine Zeichenreihe über dem Alphabet $\{0, 1\}$

Konvention

- Buchstaben werden mit a, b, c, ... bezeichnet
- Wörter werden mit x, y, z, ... bezeichnet
- $\epsilon \notin \Sigma$

Beispiel

Die Symbolkette 01101 ist eine Zeichenreihe über dem Alphabet $\{0, 1\}$

Konvention

- Buchstaben werden mit a, b, c, ... bezeichnet
- Wörter werden mit x, y, z, ... bezeichnet
- $\epsilon \notin \Sigma$

Definition (Wortlänge)

- Die Länge eines Wortes w ist die Anzahl der Positionen in w
- Die Länge von w wird auch mit $|w|$ bezeichnet
- Das Leerwort ϵ hat die Länge 0

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge
  der Wörter der Länge k, deren Symbole aus Σ stammen

Σ^k

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ Σ^+

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ Σ^+
- $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$ Σ^*

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ Σ^+
- $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$ Σ^*

Beispiel

Sei $\Sigma = \{0, 1\}$. Dann ist

- $\Sigma^0 = \{\epsilon\}$

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen — Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ — Σ^+
- $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$ — Σ^*

Beispiel

Sei $\Sigma = \{0, 1\}$. Dann ist

- $\Sigma^0 = \{\epsilon\}$
- $\Sigma^1 = \{0, 1\}$

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ Σ^+
- $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$ Σ^*

Beispiel

Sei $\Sigma = \{0, 1\}$. Dann ist

- $\Sigma^0 = \{\epsilon\}$
- $\Sigma^1 = \{0, 1\}$
- $\Sigma^2 = \{00, 01, 10, 11\}$

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen — Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ — Σ^+
- $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$ — Σ^*

Beispiel

Sei $\Sigma = \{0, 1\}$. Dann ist

- $\Sigma^0 = \{\epsilon\}$
- $\Sigma^1 = \{0, 1\}$
- $\Sigma^2 = \{00, 01, 10, 11\}$
- $\Sigma^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$

Definition

Seien x, y Wörter über Σ, wir schreiben $x \cdot y$ für die Konkatenation von x und y

$$\epsilon \cdot x = x$$
$$(ax) \cdot y = a(x \cdot y)$$

Hier gilt $a \in \Sigma$.

Definition

Seien x, y Wörter über Σ, wir schreiben $x \cdot y$ für die Konkatenation von x und y

$$\epsilon \cdot x = x$$
$$(ax) \cdot y = a(x \cdot y)$$

Hier gilt $a \in \Sigma$.

Beispiel

- Sei $x = 01101$, $y = 110$, $z = 10101$

Definition

Seien x, y Wörter über Σ, wir schreiben $x \cdot y$ für die Konkatenation von x und y

$$\epsilon \cdot x = x$$
$$(ax) \cdot y = a(x \cdot y)$$

Hier gilt $a \in \Sigma$.

Beispiel

- Sei $x = 01101$, $y = 110$, $z = 10101$
- Dann ist $x \cdot y = 01101110$ und $y \cdot x = 11001101$

Definition

Seien x, y Wörter über Σ, wir schreiben $x \cdot y$ für die Konkatenation von x und y

$$\epsilon \cdot x = x$$
$$(ax) \cdot y = a(x \cdot y)$$

Hier gilt $a \in \Sigma$.

Beispiel

- Sei $x = 01101$, $y = 110$, $z = 10101$
- Dann ist $x \cdot y = 01101110$ und $y \cdot x = 11001101$

Lemma

- *Konkatenation ist assoziativ und besitzt das Leerwort ϵ als neutrales Element*
- *Wir lassen $\cdot$ oft weg und schreiben xy statt $x \cdot y$*
- *Die Algebra $\langle \Sigma^*; \cdot, \epsilon \rangle$ ist ein Monoid; das Wortmonoid*

Formale Sprachen

Definition

Eine Teilmenge L von Σ^* heißt eine formale Sprache über Alphabet Σ

Formale Sprachen

Definition

Eine Teilmenge L von Σ^* heißt eine formale Sprache über Alphabet Σ

Beispiel

- Die Sprache aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$:

$$\{\epsilon, 01, 0011, 000111, \cdots\}$$

Formale Sprachen

Definition

Eine Teilmenge L von Σ^* heißt eine formale Sprache über Alphabet Σ

Beispiel

- Die Sprache aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$:

$$\{\epsilon, 01, 0011, 000111, \cdots\}$$

- Die Menge der Wörter, die jeweils die selbe Anzahl 0en und 1er enthalten:

$$\{\epsilon, 01, 10, 0011, 0101, \cdots\}$$

Formale Sprachen

Definition

Eine Teilmenge L von Σ^* heißt eine formale Sprache über Alphabet Σ

Beispiel

- Die Sprache aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$:
$$\{\epsilon, 01, 0011, 000111, \cdots\}$$
- Die Menge der Wörter, die jeweils die selbe Anzahl 0en und 1er enthalten:
$$\{\epsilon, 01, 10, 0011, 0101, \cdots\}$$
- Σ^* ist eine Sprache, $\varnothing$—die leere Sprache—ist eine Sprache, $\{\epsilon\}$ ist eine Sprache. Beachte $\{\epsilon\} \neq \varnothing$

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert

$$L \cup M = \{x \mid x \in L \text{ oder } x \in M\}$$

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert

$$L \cup M = \{x \mid x \in L \text{ oder } x \in M\}$$

- Wir definieren das Komplement von L:

$$\sim L = \Sigma^* \setminus L := \{x \in \Sigma^* \mid x \notin L\}$$

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert

$$L \cup M = \{x \mid x \in L \text{ oder } x \in M\}$$

- Wir definieren das Komplement von L:

$$\sim L = \Sigma^* \setminus L := \{x \in \Sigma^* \mid x \notin L\}$$

- Der Durchschnitt von L und M ist wie folgt definiert:

$$L \cap M = \{x \mid x \in L \text{ und } x \in M\}$$

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert

$$L \cup M = \{x \mid x \in L \text{ oder } x \in M\}$$

- Wir definieren das Komplement von L:

$$\sim L = \Sigma^* \setminus L := \{x \in \Sigma^* \mid x \notin L\}$$

- Der Durchschnitt von L und M ist wie folgt definiert:

$$L \cap M = \{x \mid x \in L \text{ und } x \in M\}$$

- Das Produkt (oder Verkettung) von L und M ist definiert als:

$$LM = \{xy \mid x \in L, y \in M\}$$

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert
$$L \cup M = \{x \mid x \in L \text{ oder } x \in M\}$$
- Wir definieren das Komplement von L:
$$\sim L = \Sigma^* \setminus L := \{x \in \Sigma^* \mid x \notin L\}$$
- Der Durchschnitt von L und M ist wie folgt definiert:
$$L \cap M = \{x \mid x \in L \text{ und } x \in M\}$$
- Das Produkt (oder Verkettung) von L und M ist definiert als:
$$LM = \{xy \mid x \in L, y \in M\}$$

Lemma

Seien L, L_1, L_2, L_3 formale Sprachen, dann gilt

$$(L_1L_2)L_3 = L_1(L_2L_3) \qquad L\{\epsilon\} = \{\epsilon\}L = L$$

Definition

Sei L eine formale Sprache und $k \in \mathbb{N}$

Die k-te Potenz von L definiert als:

$$L^k = \begin{cases} \{\epsilon\} & \text{falls } k = 0 \\ L & \text{falls } k = 1 \\ \underbrace{LL \cdots L}_{k\text{-mal}} & \text{falls } k > 1 \end{cases}$$

Definition

Sei L eine formale Sprache und $k \in \mathbb{N}$

Die k-te Potenz von L definiert als:

$$L^k = \begin{cases} \{\epsilon\} & \text{falls } k = 0 \\ L & \text{falls } k = 1 \\ \underbrace{LL \cdots L}_{k\text{-mal}} & \text{falls } k > 1 \end{cases}$$

Definition

Der Kleene-Stern * oder Abschluss von L ist wie folgt definiert:

$$L^* = \bigcup_{k \geqslant 0} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k \geqslant 0\}$$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k > 0\}$$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k > 0\}$$

Beispiel

- Sei $\Sigma = \{0, 1\}$ und betrachte die Sprache L aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k > 0\}$$

Beispiel

- Sei $\Sigma = \{0, 1\}$ und betrachte die Sprache L aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$
- Wir können L konzise in Mengennotation angeben:

$$L = \{0^n 1^n \mid n \geqslant 0\}$$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k > 0\}$$

Beispiel

- Sei $\Sigma = \{0, 1\}$ und betrachte die Sprache L aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$
- Wir können L konzise in Mengennotation angeben:

$$L = \{0^n 1^n \mid n \geqslant 0\}$$

- Es gilt $010101 \notin L$, aber $010011 \in L^2$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k > 0\}$$

Beispiel

- Sei $\Sigma = \{0, 1\}$ und betrachte die Sprache L aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$
- Wir können L konzise in Mengennotation angeben:

$$L = \{0^n 1^n \mid n \geqslant 0\}$$

- Es gilt $010101 \notin L$, aber $010011 \in L^2$
- Allgemein erhalten wir etwa:

$$L^2 = \{0^n 1^n 0^k 1^k \mid n, k \geqslant 0\}$$