universität
innsbruck

Einführung in die Theoretische Informatik

David Drexel
Julian Fodor
Alexander Lochmann
Georg Moser
Alexander Maringele
David Obwaller
Jonas Schöpf

cbr.uibk.ac.at

universität
innsbruck

Zusammenfassung

Modus Ponens

$$\frac{A \to B \quad A}{B}\ MP$$

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

$$(1) \qquad A \to (B \to A)$$

$$(2) \qquad (A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

$$(3) \qquad (\neg A \to \neg B) \to (B \to A)$$

Satz

Das Axiomensystem mit Inferenzregel MP ist korrekt und vollständig für die Aussagenlogik: $A_1, \ldots, A_n \models B \quad$ *gdw.* $\quad A_1, \ldots, A_n \vdash B$

Deduktionstheorem

Satz (Deduktionstheorem)

Sei B mit Hilfe der Prämisse A beweisbar, dann existiert ein Beweis von $A \to B$, der A nicht als Prämisse hat

Beweis.

Mit Hilfe von Induktion über die Beweislänge ■

Bemerkung

- Wenn wir einen „wenn, dann“ Satz analysieren, dann prüfen wir die Gültigkeit indem wir die Hyphothese H annehmen und dann die Konklusion K prüfen
- So prüfen wir mathematische Aussagen, bzw. Aussagen in der Informatik
- Informell bedeutet das Deduktionstheorem, dass wir genau so auch formal schließen können

Feedback

Ich habe eine Frage zur vollständigen Induktion: Wie kann die Induktionsannahme beim Beweis des Deduktionstheorems von letzter Woche sich auf ALLE $l < k$ beziehen (und dann auf k schließen), wenn Induktion doch ein Prinzip ist, das von $k - 1$ auf k schließen müsste? Meiner Meinung nach ist die Induktionsannahme „zu stark“.

Beispiel (Deduktionstheorem)

Wir betrachten die folgende Tautologie

$$a \to (b \to (c \to (d \to (e \to c)))))$$

1	a	Prämisse
2	b	Prämisse
3	c	Prämisse
4	d	Prämisse
5	e	Prämisse
6	c	3
7	$e \to c$	5, 6, DT
8	$d \to e \to c$	4, 7, DT
9	$c \to d \to e \to c$	3, 8, DT
10	$b \to c \to d \to e \to c$	2, 9, DT
11	$a \to b \to c \to d \to e \to c$	1, 10, DT

Beispiel

- Die Formel $\neg\neg p \to p$ ist eine Tautologie.

Beispiel

- Die Formel $\neg\neg p \to p$ ist eine Tautologie.
- Die Formel $\neg\neg p \to p$ is formal beweisbar.

Beispiel

- Die Formel $\neg\neg p \to p$ ist eine Tautologie.
- Die Formel $\neg\neg p \to p$ is formal beweisbar.
- Insbesonders gilt die folgende Äquivalenz:

$$\neg\neg p \models p \quad \text{gdw.} \quad \neg\neg p \vdash p$$

Beispiel

- Die Formel $\neg\neg p \to p$ ist eine Tautologie.
- Die Formel $\neg\neg p \to p$ is formal beweisbar.
- Insbesonders gilt die folgende Äquivalenz:

$$\neg\neg p \models p \quad \text{gdw.} \quad \neg\neg p \vdash p$$

Beispiel

Wir betrachten die formale Ableitung der Formel

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

Beispiel

- Die Formel $\neg\neg p \to p$ ist eine Tautologie.
- Die Formel $\neg\neg p \to p$ is formal beweisbar.
- Insbesonders gilt die folgende Äquivalenz:

$$\neg\neg p \models p \quad \text{gdw.} \quad \neg\neg p \vdash p$$

Beispiel

Wir betrachten die formale Ableitung der Formel

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

1	$\neg\neg\neg p \to \neg p$	voriges Beispiel
2	$(\neg\neg\neg p \to \neg p) \to (p \to \neg\neg p)$	Axiom (3)
3	$p \to \neg\neg p$	1, 2, MP

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

universität
innsbruck

Algebraische Strukturen

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

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 $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ 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.

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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 der Träger von $\mathcal{A}$ endlich ist, 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 $b = c$:

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

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. $\cdot$ distribuiert 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. $\cdot$ distribuiert 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. Wenn $\mathcal{A}$ ein Ring ist
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 $x_1, x_2, \ldots$ 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

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

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

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

Boolesche Ausdrücke

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:

$\cdot$	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 Boolsche 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 Boolsche 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 Boolschen 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 Boolschen 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 $\mathbb{B}$:
$\mathbb{B}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{B}\}$; wir betrachten

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

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

Algebra des Kartesischen Produkts und der Schaltfunktionen

Definition

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

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

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

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

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

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

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

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

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

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

Lemma

Die Algebra der Schaltfunktionen ist eine Boolesche Algebra