Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Aussagen

Die mathematische Logik verwendet mathematische Methoden, um das logische Denken formal zu beschreiben.

- Populäre Definition: Eine Aussage ist ein Satz, der entweder falsch oder wahr ist.
- Problem: Wie definiert man *wahr* und *falsch*?
- Ein Beweis stellt sicher, daß eine Aussage wahr ist.
- DEFINITION: Eine Aussage ist eine Konstruktion, durch welche festgelegt wird, wie ihre Beweise zu konstruieren sind.
- Eine Aussage, die wir nicht beweisen können, muß nicht unbedingt falsch sein.

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Definition der Implikation, $\Rightarrow$

Formation

Sind P und Q Aussagen, dann bezeichnet $P \Rightarrow Q$ ebenfalls eine Aussage, die Implikation von P und Q.

Introduktion

Um $P \Rightarrow Q$ zu beweisen, muß man Q beweisen, wobei man einen Beweis von P voraussetzen darf.

Elimination

Hat man einen Beweis von $P \Rightarrow Q$, so reicht ein Beweis von P, um auch Q zu beweisen.

Schlussregeln

$$\dfrac{\begin{array}{c}P\\ \vdots\\ Q\end{array}}{P \Rightarrow Q}\Rightarrow\mathcal{I} \qquad \dfrac{P \Rightarrow Q \quad P}{Q}\Rightarrow\mathcal{E}$$

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Definition der Konjuktion, $\wedge$

Formation

Sind P und Q Aussagen, dann bezeichnet $P \wedge Q$ ebenfalls eine Aussage, die Konjunktion von P und Q.

Introduktion

Um $P \wedge Q$ zu beweisen, muß man sowohl P als auch Q beweisen.

Elimination

Hat man einen Beweis von $P \wedge Q$ so auch einen Beweis von P, und auch einen Beweis von Q.

Schlussregeln

$$\frac{P \quad Q}{P \wedge Q}\wedge\mathcal{I} \qquad \frac{P \wedge Q}{P}\wedge\mathcal{E}_0 \qquad \frac{P \wedge Q}{Q}\wedge\mathcal{E}_1$$

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Kommutativität der Konjunktion

Satz

Die logische Konjunktion ist kommutativ, d.h. die Aussage

$$A \wedge B \Rightarrow B \wedge A$$

ist allgemeingültig.

Beweis.

$$\dfrac{\dfrac{\boxed{\dfrac{\dfrac{A \wedge B}{B}\wedge\mathcal{E}_1 \qquad \dfrac{A \wedge B}{A}\wedge\mathcal{E}_0}{B \wedge A}\wedge\mathcal{I}}}{A \wedge B \Rightarrow B \wedge A}\Rightarrow\mathcal{I}}{A \wedge B}$$

□

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Definition der Äquivalenz, $\Longleftrightarrow$

Notation

Die logische Äquivalenz wird mit $P \iff Q$ bezeichnet und ist lediglich eine Abkürzung für $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Bemerkung

Zwei Aussagen sind äquivalent wenn sie vom logischen Standpunkt aus betrachtet gleichwertig sind.

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Definition der Disjunktion, $\vee$

Formation

Sind P und Q Aussagen, dann bezeichnet $P \vee Q$ ebenfalls eine Aussage, die Disjunktion von P und Q.

Introduktion

Um $P \vee Q$ zu beweisen, genügt es, P zu beweisen, oder Q zu beweisen.

Elimination

Folgt irgendeine Aussage R sowohl aus P als auch aus Q, dann folgt sie auch aus $P \vee Q$ (Beweis durch Fallunterscheidung).

Schlussregeln

$$\frac{P}{P \vee Q}\vee\mathcal{I}_0 \qquad \frac{Q}{P \vee Q}\vee\mathcal{I}_1 \qquad \frac{P \Rightarrow R \quad Q \Rightarrow R}{P \vee Q}\vee\mathcal{E} \; R$$

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Allquantor, $\forall$

- Sei X ein Datentyp, und $P[x]$ für jedes $x \epsilon X$ eine Aussage. Dann bezeichnet $\forall_{x \epsilon X} P[x]$ eine All-Aussage.
- Die All-Aussage drückt eine universelle Quantifizierung aus.
- Ein Beweis von $\forall_{x \epsilon X} P[x]$ konstruiert für jedes beliebige $x \epsilon X$ einen Beweis von $P[x]$.
- Praktisch: Es sei $\forall_{x \epsilon X} P[x]$ zu beweisen.
  Vorgangsweise: Annahme $x \epsilon X$; beweise $P[x]$.
- Hängt $P[x]$ nicht von x ab, dann liegt eine normale Implikation vor: $\forall_{x \epsilon X} P$ ist dasselbe wie $X \rightarrow P$.

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Allquantor, Introduktion und Elimination

- Um $\forall_{x \epsilon X} P[x]$ zu beweisen, muß man $P[x]$ für ein beliebiges $x \epsilon X$ beweisen.
- $\forall$-Introduktion:

$$\dfrac{\begin{array}{c}[x \epsilon X] \\ \vdots \\ P[x]\end{array}}{\forall_{x \epsilon X} P[x]} \forall \mathcal{I}$$

- Wurde $\forall_{x \epsilon X} P[x]$ bewiesen, und ist $a \epsilon X$, dann hat man einen Beweis von $P[a]$.
- $\forall$-Elimination:

$$\dfrac{\forall_{x \epsilon X} P[x] \quad a \epsilon X}{P[a]} \forall \mathcal{E}$$

Allquantor, Beispiel

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall_{x \epsilon X}\, A[x] \;\vee\; \forall_{y \epsilon Y}\, B[y]}}{x \;\epsilon\; X}}{y \;\epsilon\; Y}}{\vdots}}{\dfrac{A[x] \;\vee\; B[y]}{\forall_{y \epsilon Y}\,(A[x] \;\vee\; B[y])}\forall\mathcal{I}}}{\dfrac{}{\forall_{x \epsilon X}\,\forall_{y \epsilon Y}\,(A[x] \;\vee\; B[y])}\forall\mathcal{I}}$$

$$\dfrac{}{\forall_{x \epsilon X}\, A[x] \;\vee\; \forall_{y \epsilon Y}\, B[y] \Rightarrow \forall_{x \epsilon X}\,\forall_{y \epsilon Y}\,(A[x] \;\vee\; B[y])}\Rightarrow\mathcal{I}$$

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Allquantor: Beispiel (Fortsetzung)

Annahmen: $\forall_{x \epsilon X}\, A[x] \ \vee\ \forall_{y \epsilon Y}\, B[y], \qquad x \,\epsilon\, X, \quad y \,\epsilon\, Y$

Zu beweisen:

$$\dfrac{\begin{array}{cc}\overset{\forall_{x\epsilon X}\, A[x]}{\boxed{\begin{array}{c}\vdots\\ A[x] \ \vee\ B[y]\end{array}}} & \overset{\forall_{y\epsilon Y}\, B[y]}{\boxed{\begin{array}{c}\vdots\\ A[x] \ \vee\ B[y]\end{array}}}\end{array}}{\forall_{x\epsilon X}\, A[x] \ \vee\ \forall_{y\epsilon Y}\, B[y] \Rightarrow A[x] \ \vee\ B[y]}\vee\mathcal{E}$$

Die beiden Fälle:

$$\dfrac{\dfrac{\forall_{x\epsilon X}\, A[x] \quad x \,\epsilon\, X}{A[x]}\forall\mathcal{E}}{A[x] \ \vee\ B[y]}\vee\mathcal{I}_0 \qquad \dfrac{\dfrac{\forall_{y\epsilon Y}\, B[y] \quad y \,\epsilon\, Y}{B[y]}\forall\mathcal{E}}{A[x] \ \vee\ B[y]}\vee\mathcal{I}_1$$

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Existenzquantor, $\exists$

- Sei X ein Datentyp, und $P[x]$ für jedes $x \epsilon X$ eine Aussage. Dann bezeichnet $\exists_{x \epsilon X} P[x]$ eine Existenz-Aussage.
- Die Existenzaussage drückt eine existenzielle Quantifizierung aus.
- Ein Beweis von $\exists_{x \epsilon X} P[x]$ konstruiert ein $a \epsilon X$ und einen Beweis von $P[a]$.
- Praktisch: Es sei $\exists_{x \epsilon X} P[x]$ zu beweisen.
  Vorgangsweise: Man wählt ein passendes $a \epsilon X$, und versucht damit $P[a]$ zu beweisen.
- Hängt $P[x]$ nicht von x ab, dann liegt eine normale Konjunktion vor: $\exists_{x \epsilon X} P$ ist dasselbe wie $X \wedge P$.

Mathematik und Logik

2011W

Was ist Logik?

Elementare Zahlentheorie

Natürliche Zahlen

Teilbarkeit

Gemeinsame Teiler

Diophantische Gleichungen

Teilerfremde Zahlen

Modulare Arithmetik

Primzahlen

RSA-Verschlüsselung

Logik

Aussagenlogik

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Äquivalenz, $\Longleftrightarrow$

Logische Disjunktion, $\vee$

Prädikatenlogik

Allquantor, $\forall$

Existenzquantor, $\exists$

Datentypen

Logische Implikation, $\Rightarrow$

Logische Konjunktion, $\wedge$

Logische Disjunktion, $\vee$

Curry-Howard-Isomorphismus

Listen

Lineare Algebra

Existenzquantor: Introduktion und Elimination

- Um $\exists_{x \epsilon X}\, P[x]$ zu beweisen, muß man ein $a \epsilon X$ finden und damit $P[a]$ beweisen.
- $\exists$-Introduktion:
$$\frac{a \epsilon X \quad P[a]}{\exists_{x \epsilon X}\, P[x]} \exists\mathcal{I}$$
- Wurde $\exists_{x \epsilon X}\, P[x]$ bewiesen, so kann man für's weitere annehmen, daß es ein soches Objekt gibt.
- $\exists$-Elimination:

$$\frac{\exists_{x \epsilon X}\, P[x] \qquad \begin{array}{|c|}\hline y \epsilon X \quad P[y] \\ \vdots \\ Q \\ \hline \end{array}}{Q} \exists\mathcal{E}$$