Mathematische Logik

Universität Freiburg

WS 2004/2005

Was ist ein mathematischer Beweis?

Was ist ein mathematischer Beweis?

Analyse des Beweisbegriffes, der Beweise,
wie wir sie in der Mathematik antreffen.

Was ist ein mathematischer Beweis?

Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

Was ist ein mathematischer Beweis?

Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte

Was ist ein mathematischer Beweis?

> Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte
- experimentelle Mathematik

Was ist ein mathematischer Beweis?

Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte
- experimentelle Mathematik
- das Aufspüren wichtiger Zusammenhänge und Behauptungen

Was ist ein mathematischer Beweis?

> Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte
- experimentelle Mathematik
- das Aufspüren wichtiger Zusammenhänge und Behauptungen
- das Herauskristallisieren des mathematischen Kerns eines Problems;

Was ist ein mathematischer Beweis?

> Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte
- experimentelle Mathematik
- das Aufspüren wichtiger Zusammenhänge und Behauptungen
- das Herauskristallisieren des mathematischen Kerns eines Problems;
- das geeignete Modellieren;

Was ist ein mathematischer Beweis?

> Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte
- experimentelle Mathematik
- das Aufspüren wichtiger Zusammenhänge und Behauptungen
- das Herauskristallisieren des mathematischen Kerns eines Problems;
- das geeignete Modellieren;
- die geschickte Einführung von Begriffen.

Was ist ein mathematischer Beweis?

Was ist ein mathematischer Beweis?

• Welches Interesse haben wir an der Behandlung dieser Frage?

• Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

• Welches Interesse haben wir an der Behandlung dieser Frage?

• Welches Interesse haben wir an der Behandlung dieser Frage?

Erkenntnistheoretisches Anliegen

• Welches Interesse haben wir an der Behandlung dieser Frage?

Erkenntnistheoretisches Anliegen

Aristoteles (384 - 322 v. Chr.)

• Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

• Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

1. Ist jede mathematische Aussage beweisbar?

• Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

1. Ist jede mathematische Aussage beweisbar?

   Goldbachsche Vermutung: Jede gerade Zahl ≥ 4 ist die Summe von zwei Primzahlen.

• Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

1. Ist jede mathematische Aussage beweisbar?

   Goldbachsche Vermutung: Jede gerade Zahl ≥ 4 ist die Summe von zwei Primzahlen.

   Kontinuumshypothese (CH): Für jede nichtleere Teilmenge $X \subseteq \mathbb{R}$ gilt: Es gibt $f : \mathbb{N} \to X$ surjektiv oder es gibt $f : X \to \mathbb{R}$ surjektiv.

• Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

1. Ist jede mathematische Aussage beweisbar?

   Goldbachsche Vermutung: Jede gerade Zahl ≥ 4 ist die Summe von zwei Primzahlen.

   Kontinuumshypothese (CH): Für jede nichtleere Teilmenge $X \subseteq \mathbb{R}$ gilt: Es gibt $f : \mathbb{N} \to X$ surjektiv oder es gibt $f : X \to \mathbb{R}$ surjektiv.

3. Ist die Mathematik widerspruchsfrei?

Gibt es also ein Programm, das folgendes leistet:

INPUT: Axiome einer mathematischen Theorie und
eine Behauptung (Vermutug)
OUTPUT: Behauptung richtig (Beweis) oder
Behauptung ist falsch (Gegenbeispiel).

4. Kann man das Beweisen Computern überlassen?

Gibt es also ein Programm, das folgendes leistet:

INPUT: Axiome einer mathematischen Theorie und eine Behauptung (Vermutug)

OUTPUT: Behauptung richtig (Beweis) oder Behauptung ist falsch (Gegenbeispiel).

Aristoteles (384 - 322 v. Chr.)

Schule der Sophisten

Achilles und die Schildkröte

> *Achilles und die Schildkröte laufen ein Wettrennen. Achilles gewährt der Schildkröte einen Vorsprung. Dann kann Achilles die Schildkröte niemals einholen.*

Zenon von Elea (490 - 425 v. Chr.) gibt folgende Begründung: Zu dem Zeitpunkt, an dem Achilles den Startpunkt der Schildkröte erreicht, ist die Schildkröte schon ein Stück weiter. Etwas später erreicht Achilles diesen Punkt, aber die Schildkröte ist schon etwas weiter. Wenn Achilles diesen Punkte erreicht, ist die Schildkröte wieder etwas weiter. So kann Achilles zwar immer näher an die Schildkröte herankommen, sie aber nie erreichen.

Der Barbier

In einem Städtchen wohnt ein Barbier, der genau diejenigen männlichen Einwohner rasiert, die sich nicht selbst rasieren.

Rasiert nun der Barbier sich selbst?

Antinomie des Lügners

Epimenides (Kreter, 600 v. Chr.)

Brief des Paulus an Titus 1:12-13:

> *Einer von ihren eigenen Landsleuten war ein Prophet, als er sagte: "Die Kreter lügen immer. Sie sind Raubtiere, liegen auf der faulen Haut und denken nur ans Fressen".* Er hat die Wahrheit gesagt.

Aus Don Quijote de la Mancha von Miguel de Cervantes (1517–1616)

> *Um eine gewisse Brücke zu überqueren, müssen alle Reisenden zunächst angeben,*

was ihr Ziel ist. Antworten sie wahrheitsgemäß, so dürfen sie die Brücke überqueren. Sonst werden sie gnadenlos an einem Galgen am Fuß der Brücke erhängt.

Eines Tages kommt ein Reisender, der angibt, sein Ziel sei es, am Galgen am Fuß der Brücke erhängt zu werden.

was ihr Ziel ist. Antworten sie wahrheitsgemäß, so dürfen sie die Brücke überqueren. Sonst werden sie gnadenlos an einem Galgen am Fuß der Brücke erhängt.

Eines Tages kommt ein Reisender, der angibt, sein Ziel sei es, am Galgen am Fuß der Brücke erhängt zu werden.

Aristoteles: Bemühen Überblick über die Rgeln des Schließens (Syllogismen).

Prämisse:	Alle *Menschen* sind *sterblich.*
Prämisse:	*Sokrates* ist ein *Mensch.*
Konklusion:	*Sokrates* ist *sterblich.*

Prämisse:	Alle *Sura* sind *derung.*
Prämisse:	*Plarq* ist ein *Sura.*
Konklusion:	*Plarq* ist *derung.*

Prämisse:	Alle p sind q.
Prämisse:	a ist ein p.
Konklusion:	a ist q.

Ziel: Alle Schlußregeln.

- R. Llullus (1235–1315), G. W. Leibniz (1646–1716)
- G. Boole (1815–1864), G. Frege (1848–1943)

- D. Hilbert (1862–1925), B. Russell (1872–1970), K. Gödel (1906–1978)

- D. Hilbert (1862–1925), B. Russell (1872–1970), K. Gödel (1906–1978)

Literatur:

Ebbinghaus, Flum, Thomas: Einführung in die mathematische Logik. Spektrum
Enderton: A mathematical introduction to logic. Academic Press
Prestel: Einführung in die mathematische Logik und Modelltheorie. Vieweg Rautenberg: Einführung in die mathematische Logik. Viewg

Σ Alphabet: Σ nichtleere Menge von
Zeichen (Buchstaben, Symbolen);

$\Sigma_1 = \{0, 1, \ldots, 9\}$; $\Sigma_2 = \{0, 1\}$;

$\Sigma_3 = \{a, b, \ldots, x, y, z\}$; $\Sigma_4 = \{a, d, f, x, \int,), (\}$.

konkrete Zeichen;

häufig auch unendliche Alphabete:

$\Sigma_5 = \{c_0, c_1, \ldots\}$; $\Sigma_6 = \{c_r \mid r \in \mathbb{R}\}$.

Alphabete: Σ, Π,...

Wort (Zeichenreihe) über Σ:
endliche Aneinanderreihung von Buchstaben aus Σ

Wörter: $u, v, w, \ldots$ leere Wort: λ;

Σ^* Menge der Wörter über dem Alphabet Σ;

$|w|$ Länge von w;

$\int f(x)dx$, $a \int \int dxd \in \Sigma_4^*$;

$|a \int \int dxd| = 6$, $|\lambda| = 0$.

$\Sigma_5 = \{c_0, c_1, \ldots\}$ ersetzen durch endliches Alphabet, etwa durch

$$\Sigma_7 := \{c, \, 0, \, 1, \ldots, \, 9\}.$$

Bei Identifikation von c_{25} mit $c_{\,2\,5}$:

$$\Sigma_5 \subseteq \Sigma_7^* \quad \text{und} \quad \Sigma_5^* \subseteq \Sigma_7^*.$$

$\Sigma = \{a_0, \ldots, a_n\}$ mit paarweise verschiedenen (p.v.) $a_0, \ldots, a_n$. Die lexikographische Ordnung von Σ^* (bzgl. $a_0, \ldots, a_n$):

$$\begin{aligned} u <_{\text{lex}} v \quad \Longleftrightarrow \quad & (|u| < |v| \text{ oder} \\ & (|u| = |v| \text{ und ex. } \leq i < j \leq n, \, x, y, z \in \Sigma^*: \\ & u = x a_i y \text{ und } v = x a_j z. \end{aligned}$$

$\Sigma_5 = \{c_0, c_1, \ldots\}$ ersetzen durch endliches Alphabet, etwa durch

$$\Sigma_7 := \{c, \, 0, \, 1, \ldots, \, 9\}.$$

Bei Identifikation von c_{25} mit $c_{\,2\,5}$:

$$\Sigma_5 \subseteq \Sigma_7^* \quad \text{und} \quad \Sigma_5^* \subseteq \Sigma_7^*.$$

$\Sigma = \{a_0, \ldots, a_n\}$ mit paarweise verschiedenen (p.v.) $a_0, \ldots, a_n$. Die lexikographische Ordnung von Σ^* (bzgl. $a_0, \ldots, a_n$):

$$\begin{aligned} u <_{\text{lex}} v \quad \Longleftrightarrow \quad & (|u| < |v| \text{ oder} \\ & (|u| = |v| \text{ und ex. } \leq i < j \leq n, \, x, y, z \in \Sigma^*: \\ & u = x a_i y \text{ und } v = x a_j z. \end{aligned}$$

$\lambda, a_0, \ldots, a_n, \qquad \ldots a_0 a_n, a_1 a_0, \ldots, a_1 a_n, \ldots, a_n a_n, a_0 a_0 a_0, \ldots$

$\Sigma_5 = \{c_0, c_1, \ldots\}$ ersetzen durch endliches Alphabet, etwa durch

$$\Sigma_7 := \{c, \, 0, \, 1, \ldots, \, 9\}.$$

Bei Identifikation von c_{25} mit $c_{\,2\,5}$:

$$\Sigma_5 \subseteq \Sigma_7^* \quad \text{und} \quad \Sigma_5^* \subseteq \Sigma_7^*.$$

$\Sigma = \{a_0, \ldots, a_n\}$ mit paarweise verschiedenen (p.v.) $a_0, \ldots, a_n$. Die lexikographische Ordnung von Σ^* (bzgl. $a_0, \ldots, a_n$):

$$\begin{aligned} u <_{\text{lex}} v \quad \Longleftrightarrow \quad & (|u| < |v| \text{ oder} \\ & (|u| = |v| \text{ und ex. } \leq i < j \leq n, \, x, y, z \in \Sigma^*: \\ & u = x a_i y \text{ und } v = x a_j z. \end{aligned}$$

$$\lambda, a_0, \ldots, a_n, a_0 a_0, \ldots a_0 a_n, a_1 a_0, \ldots, a_1 a_n, \ldots, a_n a_n, a_0 a_0 a_0, \ldots$$

Natürliche Zahlen als Wörter

$\Sigma := \{|\}$ $\qquad n \mapsto \underbrace{|\ldots|}_{n} \quad (:= [n]_1)$

$b \geq 2$, $\Sigma_b := \{0, \ldots, b-1\}$.

$$[\ ]_b : \mathbb{N} \to \Sigma^*$$

$n \mapsto [n]_b$ $\qquad$ b-adische Darstellung von n

$[25]_3 = 221$ da $25 = 2 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0$

$[81]_3 = 10000$ da
$81 = 1 \cdot 3^4 + 0 \cdot 3^3 + 0 \cdot 3^2 + 0 \cdot 3^1 + 0 \cdot 3^0$

$[0]_3 = 0$

- Für $n > 0$: $|[n]_b| = \lfloor \log_b n \rfloor + 1$

Seien $a, b \in \mathbb{N}$, $a, b \geq 2$, $n > 1$

$$\begin{aligned} |[n]_b| &= \log_b n + 1 = \log_b a \cdot \log_a n + 1 \\ &\leq \log_b a \cdot |[n]_a| + 1 \leq \underbrace{(\log_b a + 1)}_{c} \cdot |[n]_a| \end{aligned}$$

Dagegen

$$|[n]_1| = n \approx b^{|[n]_b|}$$

Beispiele von Verfahren (Algorithmus):

Verfahren

1. zur Addition von natürlichen Zahlen (in Dezimaldarstellung);
2. zur Prüfung, ob vorgegebene Zahl eine Primzahl ist;
3. zur Auflistung der Primzahlen.

Unterschiede:

- mehrere, ein oder kein Input;
- stoppt mit Output; mit rot/grünen Lämpchen; läuft unendlich lange und liefert unendlich viele Outputs.

Gemeinsamkeiten und Normierungen, die zu einem “mathematisch brauchbarem” intuitiven Begriff führen werden:

1. Ein Verfahren ist gegeben durch eine (endliche) **Vorschrift**. Ausführung, Verlauf und Ergebnis sind durch diese und die Inputs in allen Eizelheiten festgelegt (Reproduzierbarkeit).
2. Verfahren operiert schrittweise mit konkreten, handhabbaren Objekten; System hat diskrete Zustände.

2’. Verfahren operiert mit Zeichenreihen über einem (endlichen) Alphabet.

3. Kein Mangel an Zeit, Raum und Materie.

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsawsg.: Füge a an Wort in R_i.

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsawsg.: Füge a an Wort in R_i.

(2) $k\ R_i \leftarrow [R_i)$ $\qquad (k, i \in \mathbb{N})$

Verkürzungsawsg: Streiche letzten Buchstaben in R_i; falls λ in R_i, so bleibt λ in R_i.

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsawsg.: Füge a an Wort in R_i.

(2) $k\ R_i \leftarrow [R_i)$ $\qquad (k, i \in \mathbb{N})$

Verkürzungsawsg: Streiche letzten Buchstaben in R_i; falls λ in R_i, so bleibt λ in R_i.

(3) $k\ R_i = [R_i)a \Rightarrow \ell; m$ $\qquad (k, i, \ell, m \in \mathbb{N},\ a \in \Sigma)$

Sprungawsg.: Falls Wort in R_i mit a endet, gehe zu Zeile mit der Nummer ℓ sonst zur Zeile m.

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsawsg.: Füge a an Wort in R_i.

(2) $k\ R_i \leftarrow [R_i)$ $\qquad (k, i \in \mathbb{N})$

Verkürzungsawsg: Streiche letzten Buchstaben in R_i; falls λ in R_i, so bleibt λ in R_i.

(3) $k\ R_i = [R_i)a \Rightarrow \ell; m$ $\qquad (k, i, \ell, m \in \mathbb{N},\ a \in \Sigma)$

Sprungawsg.: Falls Wort in R_i mit a endet, gehe zu Zeile mit der Nummer ℓ sonst zur Zeile m.

(4) k PRINT R_i $\qquad (k, i \in \mathbb{N})$

Druckawsg: Drucke Wort in R_i.

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsawsg.: Füge a an Wort in R_i.

(2) $k\ R_i \leftarrow [R_i)$ $\qquad (k, i \in \mathbb{N})$

Verkürzungsawsg: Streiche letzten Buchstaben in R_i; falls λ in R_i, so bleibt λ in R_i.

(3) $k\ R_i = [R_i)a \Rightarrow \ell; m$ $\qquad (k, i, \ell, m \in \mathbb{N},\ a \in \Sigma)$

Sprungawsg.: Falls Wort in R_i mit a endet, gehe zu Zeile mit der Nummer ℓ sonst zur Zeile m.

(4) k PRINT R_i $\qquad (k, i \in \mathbb{N})$

Druckawsg: Drucke Wort in R_i.

(5) k HALT $\qquad (k \in \mathbb{N})$

Halteawsg: Halte.

Einem R-Programm P entspricht auf natürliche Weise ein Verfahren. Wir stellen uns dabei eine Rechenmaschine vor, die mit P programmiert ist und über die in P angesprochenen Register verfügt. Soll das Verfahren auf $(x_1, \ldots, x_r)$ angewendet werden, so sind zu Beginn der Berechnung alle Register leer, d.h. es steht in allen Registern das leere Wort, ausgenommen sind die Register $R_1, \ldots, R_r$, in denen sich $x_1, \ldots, x_r$ befinden. Die Berechnung erfolgt schrittweise; ein Schritt entspricht dabei der Ausführung einer Zeile. Beginnend mit der ersten Zeile wird dabei Zeile für Zeile abgearbeitet; es sei denn, dass durch eine Sprunganweisung eine andere Zeile aufgerufen wird. Ausgabewörter sind die evtl. bei Druckanweisungen ausgedruckten Wörter. Die Maschine hält, wenn die Halteanweisung erreicht wird.

P R-Programm, $r \geq 1$.

$f_{P,r}$ sei die Funktion mit

$$\mathrm{df}(f_{P,r}) \subseteq (\Sigma^*)^r \text{ und } \mathrm{bd}(f_{P,r}) \subseteq \Sigma^*$$

für die gilt:

$(x_1, \ldots, x_r) \in \mathrm{df}(f_{P,r})$ gdw $P : (x_1, \ldots, x_r) \rightarrow halt$

P R-Programm, $r \geq 1$.

$f_{P,r}$ sei die Funktion mit

$$\mathrm{df}(f_{P,r}) \subseteq (\Sigma^*)^r \text{ und } \mathrm{bd}(f_{P,r}) \subseteq \Sigma^*$$

für die gilt:

$(x_1, \ldots, x_r) \in \mathrm{df}(f_{P,r})$ gdw $P : (x_1, \ldots, x_r) \rightarrow \mathit{halt}$

und für $(x_1, \ldots, x_r) \in \mathrm{df}(f_{P,r})$:

$f_{P,r}(x_1, \ldots, x_r) = y$ gdw $P : (x_1, \ldots, x_r) \rightarrow y$.