19. 1. 2011

Vollständigkeitssatz:

$\Gamma \vDash \varphi$ gdw $\underbrace{\Gamma \vdash \varphi}$ es gibt einen formalen Beweis $\underline{\langle a_0, \dots, a_{n-1}, \varphi \rangle}$ von φ aus der Voraussetzung Γ.

korrekt

härtere Richtung

Folge, Implikation.
Wahrheitsbegriff

Korollare aus dem Vollständigkeitssatz

Aufzählbarkeitssatz: Sei Γ eine entscheidbare Formelmenge in einer effektiven Sprache. Dann ist $\{\varphi \mid \Gamma \vDash \varphi\}$ rekursiv aufzählbar.

$P = NP$

genügend viel Beschränkung von der Def.

P, NP, Berechnungen

Beweis: $\{\varphi \mid \Gamma \models \varphi\} = \{\varphi \mid \Gamma \vdash \varphi\}$

Gebe einen Algorithmus, der alle endl. ~~Fo~~ Folgen $\langle a_0, \dots, a_{n-1}, a_n \rangle$ von $\mathcal{L}(\Gamma)$-Formeln aufzählt.

$\mathcal{L}(\Gamma) = \mathcal{L}(\tau)$ ist abz., hat kleine Mächtigkeit

höchstens abz.

$\mathcal{L}(\tau)$ ist rekursiv aufzählbar

τ ist rek. aufz. nach Voraussetzung des Satzes.

M ~~Zur~~ sei ein Algorithmus, der alle endl. Folgen aufzählt.

Wir bauen nach M eine Beweisprüfungsmaschine N ein.

N arbeitet wie folgt: M übergibt $\langle a_0, \dots, a_n \rangle$ an N als Eingabe. N prüft ob $\langle a_0, \dots, a_n \rangle$ ein Beweis von a_n aus Γ ist. Wenn ja dann gibt N a_n aus. Danach stellt M die nächste Zeichenreihe $\langle a_0', \dots, a_{n'}' \rangle$ her. $\square$

Def: τ Symbolmenge.

Eine **Theorie** ist eine $\mathcal{L}(\tau)$-Satzmenge Γ.

Beispiele: Axiomensysteme, z.B. die Beschreibung von Turingberechnung

$\vdash \;\hat{=}\;$ Nachfolgekonfiguration.

Def $\Gamma \subseteq \mathcal{L}(\tau)$ sei eine Theorie.

Γ heißt **vollständig** $:\Leftrightarrow$ f.a. $\mathcal{L}(\tau)$-Sätze φ gilt

$\Gamma \models \varphi$ oder $\Gamma \models \neg\varphi$. $\mathfrak{A} \models \varphi$ oder $\mathfrak{A} \models \neg\varphi$

$\vdash$ $\vdash$

$\Gamma \models (\varphi \vee \neg\varphi)$.

$\Gamma \models (P = NP \;\vee\; P \neq NP)$

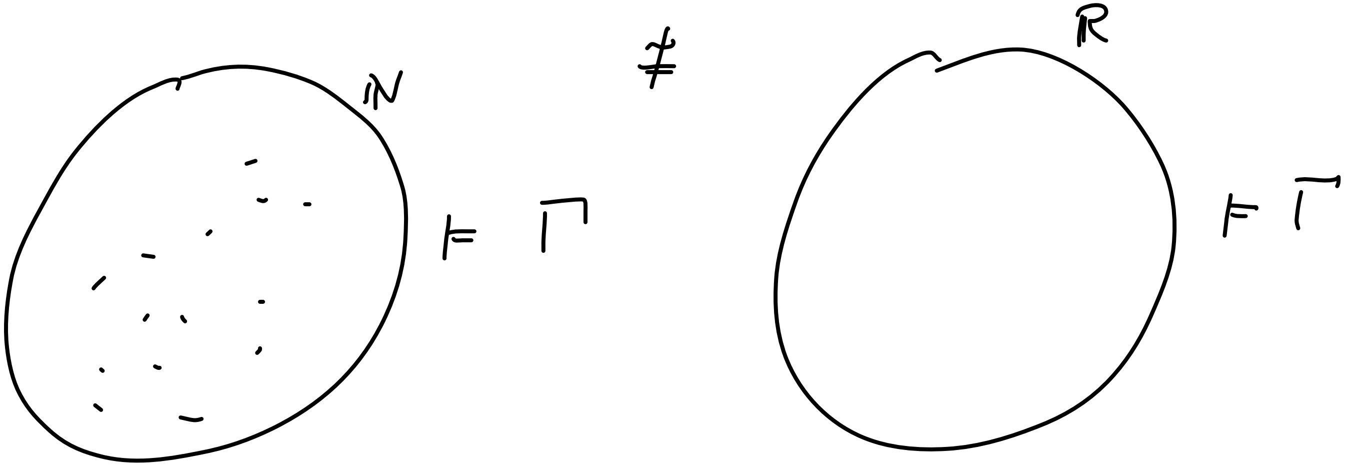
Warnung: Die „meisten" Theorie sind unvollständig.

„ Beweistheorie

Beispiele vollständiger Theorien:

1. $\tau = \emptyset$. $\quad \Gamma = \{ \exists^{\geq n} x \; x = x \mid n \in \mathbb{N} \setminus \{0\} \}$,

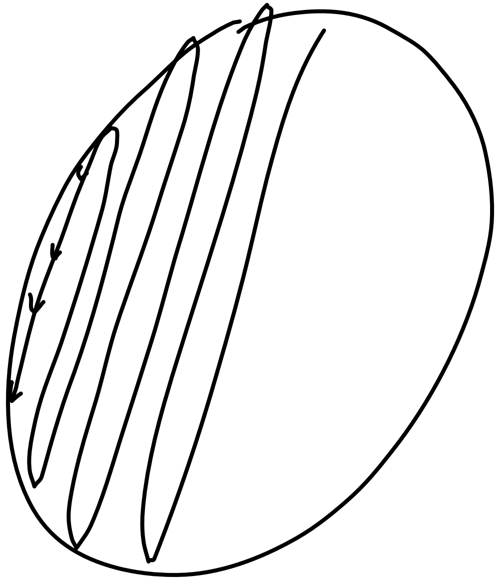
die Theorie der unendlichen Mengen.

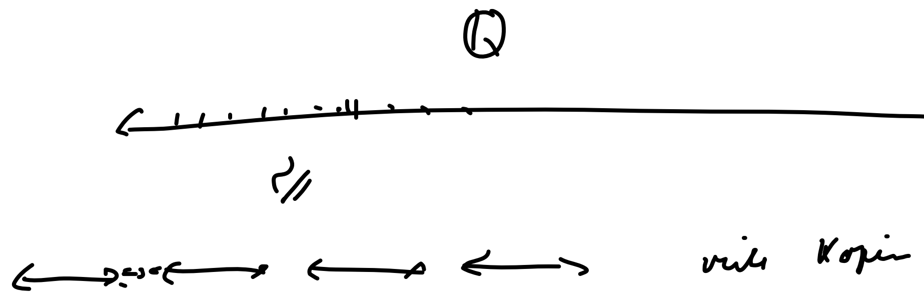


2. $\tau = \{ < \}$ $\quad <$ zweistellige Relation.

Theorie der dichten offenen Ordnungen ohne Enden.

$$\Gamma = \{ < \text{ ist eine lineare Ordnung}, \; \forall x \, \forall y \, (x < y \to \exists z \, (x < z \wedge z < y)), \; \forall x \, \exists y \; y > x, \; \forall x \, \exists y \; y < x \}$$

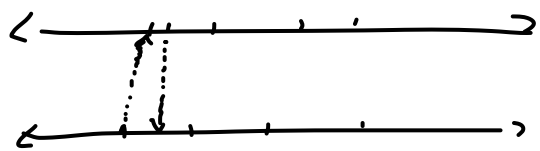




Beh: Γ ist vollständig.

φ geg. Zeige: $\Gamma \models \varphi$ oder $\Gamma \models \neg\varphi$.

Cantor: Je zwei abzählbare dichte lineare Ordn. ohne Enden sind isomorph.



$(\mathbb{Q}, <^{\mathbb{Q}}) \models \varphi$? Wenn ja, dann $\Gamma \models \varphi$

wenn nein, dann $\Gamma \models \neg\varphi$.

3. Beispiel: $\tau = \{+, \cdot, 0, 1\}$ Sprache der Körper.

Theorie der $\underbrace{\text{algebraisch abgeschlossenen}}_{\mathbb{C}}$ Körper einer festen Charakteristik.

$$\underbrace{1 + 1 \dots + 1}_{\substack{\infty \\ p}} = 0$$

$$\forall / \exists x \; a_0 x^0 + a_1 x^1 \dots + a_n x^n = 0$$

$$\frac{1 + \dots + 1}{1 + \dots + 1}$$

Algebra.

<u>Def</u>: $\mathfrak{A}$ sei eine τ-Struktur.

$$Th(\mathfrak{A}) = \{ \varphi \in \mathcal{L}(\tau) \mid \varphi \text{ Satz und } \mathfrak{A} \models \varphi \}$$

heißt die <u>Theorie von $\mathfrak{A}$</u>.

4. Beispiel: F.a. $\mathfrak{A}$ ist $Th(\mathfrak{A})$ ~~ist~~ vollständig.

Def von $\models$. $\mathfrak{A} \models \varphi$ oder $\mathfrak{A} \models \neg\varphi$.

$\Gamma = Th(\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}})$?

$\varphi \in \Gamma$ ist ~~A~~ Thm - beweisbar

0 1 2

$\forall \varphi \quad \Gamma \models \varphi$ oder $\Gamma \models \neg\varphi$

Korollar: Sei Γ entscheidbar und vollständig.

Dann ist $\{\varphi \mid \Gamma \models \varphi\}$ entscheidbar.

Bew: Übung.

Satz Satz von Löwenheim und Skolem.

Spezialfall für abzählbare τ.

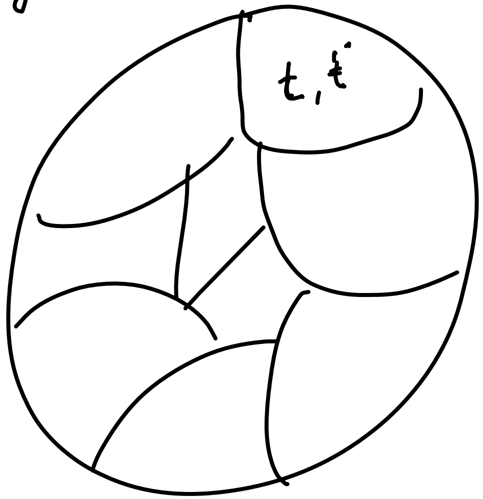
Sei Γ eine konsistente Formelmenge in $\mathcal{L}(\tau)$.

b) Wenn Γ ein unendliches Modell hat, dann hat Γ ein überabzählbares Modell. a) Γ hat ein abzählbares Modell.

endl. oder abz. unendl.

Beweis:

a) ~~Da~~ Jedes Henkin-Modell ist abzählbar. (oder endl.)



$t \in \mathcal{I}(\tau)$ - Term

$f v_0 \ldots v_n$

$\vdots$

$\in \tau$

b) Sei $(\mathfrak{A}, s) \models \Gamma$ und sei A unendl.

$\tau' = \tau \cup \{ c_r \mid r \in \mathbb{R} \}$

↑ neue, ~~ve~~ paarweise Konst.

$\Gamma' := \Gamma \cup \{ c_r \neq c_s \mid s \neq r, \ s, r \in \mathbb{R} \}$

Γ' ist überabz. , $\Gamma_0' \subseteq \Gamma \cup \{ c_{r_i} \neq c_{r_j} \mid 1 \leq i < j \leq n \}$

Zeige Γ' ist erfüllbar

Kompaktheitssatz: Jede endl. Teilmenge von Γ' ist erfüllbar

$\Longrightarrow$ Γ' ist erfüllbar.

Zeige: Jede endl. Tm. Γ_0' von Γ' ist erfüllbar.

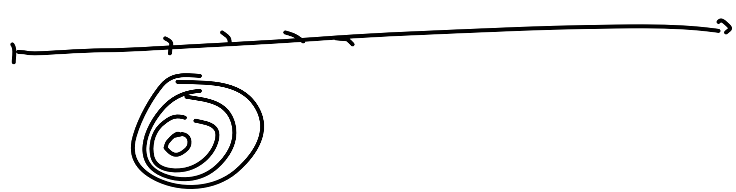
$(\mathfrak{A}', s) \models \Gamma_0'$ bei geeigneter Interpretation von c_{r_i}

$\mathfrak{A}' = \left(\mathfrak{A}, \left(c_{r_i}^{\mathfrak{A}'}\right)_{i \leq n}\right)$, $c_{r_i}^{\mathfrak{A}'} \neq c_{r_j}^{\mathfrak{A}'}$ für $1 \leq i < j \leq n$

alles in I int.

ist ~~trivial~~ einrichtbar, da A unendl. ist.

$(\mathfrak{A}', s) \models \Gamma \cup \Gamma_0'$.



Kap 5 Der polynomiale Primzahltest

von Agrawal, Kayal und Saxena. 2004 Annals of Mathematics

Turingmaschine mit deterministisch polynomialer Zeitkomplexität. p

Ist n prim? soll in ~~p(n)~~ Schritten beantwortet werden.

$$p(\log_2(n))$$

$$(\log_2(n))^{\frac{21}{2}}$$

Inputlänge $\log_2(n)$

Ja oder nein. Algorithmus gibt keine konkrete Zerlegung an.

Lemma Sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, und $(a, n) = 1$

$ggT(a,n)$

größte gemeinsame Teiler.

Dann ist n prim gdw

$$(X + a)^n = X^n + a \pmod n$$

Variable, läuft im praktisch Teile von $0, \dots, n-1$

Bewis:

$$(X+a)^n = \sum_{i=0}^{n} \binom{n}{i} X^i a^{n-i}$$

$$= a + \underbrace{\sum_{i=1}^{n-1} \binom{n}{i} X^i a^{n-1}}_{= 0 \pmod n} + X^n \pmod n$$

„$\Rightarrow$" n ist prim.

$1 \leq i \leq n$

$$\binom{n}{i} = \frac{n!}{(n-i)!\, i!} = \frac{(n-1)!\, n}{(n-i)!\, i!} = n \cdot \underbrace{\frac{(n-1)!}{(n-i)!\, i!}}_{\in \mathbb{Z},\ \text{da } n \text{ prim.}} = 0 \bmod n$$

„$\Longleftarrow$":

Sei n zusammengesetzt.

Sei q eine Primzahlzahl, die ~~q~~ n teilt.

Sei $k \geq 1$ maximal, so dass $q^k \mid n$

$$q^k \parallel n \qquad q \nmid \frac{n}{q^k} = n'$$

$$n = \prod_{i=0}^{r} q_i^{k_i} \qquad q_i \neq q_j$$

$$\binom{n}{q} = \frac{(n' \cdot q^k)!}{(n' \cdot q^k - q)! \; q!}$$

$$q \parallel q! = 1 \cdot 2 \cdot \ldots \cdot q$$

$$q^{q+1} \parallel q^2! = 1 \cdot \ldots \; q \ldots \cdot 2q \cdot \ldots \cdot 3q \ldots \cdot qq$$

Es gibt ein r s.d.

$$q^r \;\|\; (n' \cdot q^k)!$$

und

$$q^{r-k+1} \;\|\; \underbrace{(n' \cdot q^k - q)}_{} ! \; \underline{q}\,!$$

k ~~viele~~ weniger q-Faktoren als in $(n' q^k)!$

$$1 \cdot 2 \cdot \ldots \ldots$$

$$(n'-1) \cdot q^k \cdot \ldots \ldots \cdot n' \cdot q^k$$

$$\underbrace{(n'-1) \cdot q^k \cdot \ldots ((n'-1) q^k + q) \ldots}_{q^{?} \;\|}$$