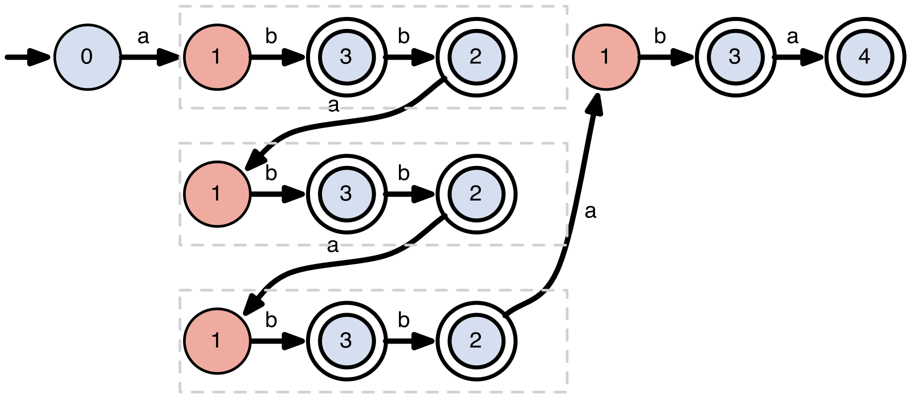
Berechenbarkeitstheorie

18. Vorlesung



Dr. Franziska Jahnke
Institut für Mathematische Logik und Grundlagenforschung
WWU Münster

Entscheidbarkeit Logischer Theorien

- Was ist eine mathematische Aussage?

Bsp. $\forall q \exists p \forall x, y\, [p > q \wedge (x, y > 1 \rightarrow xy \neq p)]$
(Es gibt unendlich viele Primzahlen)

Bsp. $\forall q \exists p \forall x, y\, [p > q \wedge (x, y > 1 \rightarrow (xy \neq p \wedge xy \neq p + 2))]$
(*twin prime conjecture*)

- Aussagen sind Wörter über folgendem Alphabet
  - $\wedge, \vee, \neg$ (boolsche Operatoren)
  - (,),[,] (Klammern)
  - x (für Variablen), $x_3 = \mathrm{xxx}$ etc.
  - $\exists, \forall$ (Quantoren)
  - $R_1, R_2, \ldots, R_k$ (Relationen)
  - , (Komma)
- atomare Formeln sind Wörter der Form $R_i(x_{\ell_1}, x_{\ell_2}, \ldots, x_{\ell_j})$, wobei j die Stelligkeit des Symbols R_i heißt
- zu jedem Symbol R_i ist eine Stelligkeit angegeben

- Formeln sind Wörter über über dem Alphabet $\{\mathtt{x}, (,), [,], \forall, \exists, R_1, \ldots, R_k, , \}$ für die gilt:
  1.) es sind atomare Formeln, oder
  2.) es sind Wörter der Form $(\phi_1 \wedge \phi_2)$, $(\phi_1 \vee \phi_2)$, (ϕ_1) oder $\neg\phi_1$, wobei ϕ_1, ϕ_2 kürzere Formeln sind, oder
  3.) es sind Wörter der Form $\exists x_i[\phi]$, oder $\forall x_i[\phi]$, wobei ϕ eine kürzere Formel ist.
- wir nehmen an, dass alle Formeln in Pränex-Form gegeben sind, d.h. alle Quantoren stehen vorne
- eine Variable heißt freie Variable, wenn sie nicht quantifiziert ist
- eine Aussage auch Satz ist eine Formel ohne freie Variablen

Bsp.1: $\exists x_1[\forall x_2[(R_1(x_2) \wedge R_2(x_2, x_1, x_3))]]$
(Formel mit einer freien Variable x_3)

Bsp.2: $\exists x_1[\forall x_2[(\neg R_1(x_1) \wedge (\neg R_2(x_2) \vee R_3(x_1, x_2)))]]$
(Formel ohne freie Variable = Aussage)

- Was bedeutet eine Aussage? Dazu muss man spezifizieren:
  1.) Was sagen die Relationen aus?
  2.) Aus welchem Universum werden die Variablen gewählt?
  3.) Was bedeuten die boolschen Operationen und Quantoren?
  (Allgemein klar, Boolsche Algebra, siehe Wiki)
- Das Universum und die Bedeutung der Relationen werden durch das Modell beschrieben.

  formal: $\mathcal{M} = (U, \underbrace{P_1, P_2, \ldots, P_k}_{})$ heißt Modell

  Menge (Universum) Bedeutung Relationen (P_i beschreibt R_i)
- Eine Aussage ϕ ist entweder wahr oder falsch in einem Modell
- Wenn ϕ wahr im Modell $\mathcal{M}$, sagen wir $\mathcal{M}$ ist ein Modell für ϕ

Bsp.: $\phi = \forall y[\exists x[R_1(x, x, y)]]$

- $\mathcal{M}_1 = (\mathbf{R}, \text{PLUS})$ ist Modell für ϕ

  $\text{PLUS} = \{(a, b, c) \mid a + b = c\}$
- $\mathcal{M}_2 = (\mathbf{N}, \text{PLUS})$ ist kein Modell für ϕ

- Sprache aller wahren Aussagen für ein Modell $\mathcal{M}$ heißt Theorie von $\mathcal{M}$ - Schreibweise $\mathrm{Th}(\mathcal{M})$.

Satz 29

Sei $(\mathbf{N}, \mathrm{PLUS})$ das Modell der natürlichen Zahlen mit der Addition. Dann gilt, dass $\mathrm{Th}((\mathbf{N}, \mathrm{PLUS}))$ ist entscheidbar.

Beweis

- Ziel ist Entscheider für Aussagen ϕ

$$\phi = \phi_0 \quad = \exists\!\!\!\forall x_1 \underbrace{\exists\!\!\!\forall x_2 \exists\!\!\!\forall x_3 \ldots \exists\!\!\!\forall x_k [\psi]}_{\phi_1} \longleftarrow \text{Aussage}$$

$$i = 1..k \quad \phi_i \quad = \exists\!\!\!\forall x_{i+1} \exists\!\!\!\forall x_{i+2} \ldots \exists\!\!\!\forall x_k [\psi] \longleftarrow \text{Formeln mit freien Variablen}$$

$$\phi_k \quad = \psi \longleftarrow \text{Formel ohne Quantoren}$$

Plan: Konstruiere für jedes ϕ_i einen DEA, der alle freien Variablenbelegungen akzeptiert, die ϕ_i erfüllen.

- Induktive Konstruktion: Zuerst DEA für ψ, dann für ϕ_{k-1}, usw. bis ϕ.

Repräsentation freier Variablen

- Variablenbelegung = Wort
- Zeichen kodieren die Bits (Binärdarstellung) an einer festen Stelle
- Bei ℓ Variablen, kodiert 1 Zeichen also ℓ Bits. $\rightarrow \Sigma = \{0,1\}^{\ell}$
- Reihenfolge der Bits: Vom niederwertigem zum höherwertigem

Bsp.

Variablenbelegung: $x_1 = 3, x_2 = 10, x_3 = 5$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \qquad \begin{aligned} \mathrm{bin}(3) &= 0011 \\ \mathrm{bin}(10) &= 1010 \\ \mathrm{bin}(5) &= 0101 \end{aligned}$$

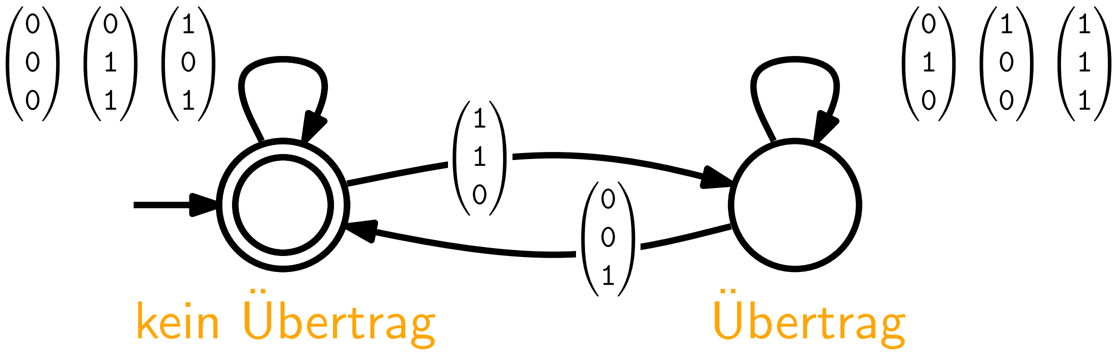
DEA für ϕ

1. Teil: Umsetzung von PLUS

- erst einmal: 3 Variablen: x_1, x_2, x_3 und DEA soll $\langle x_1, x_2, x_3 \rangle$ akzeptieren, gdw. wenn $x_1 + x_2 = x_3$

1. Teil: Umsetzung von PLUS

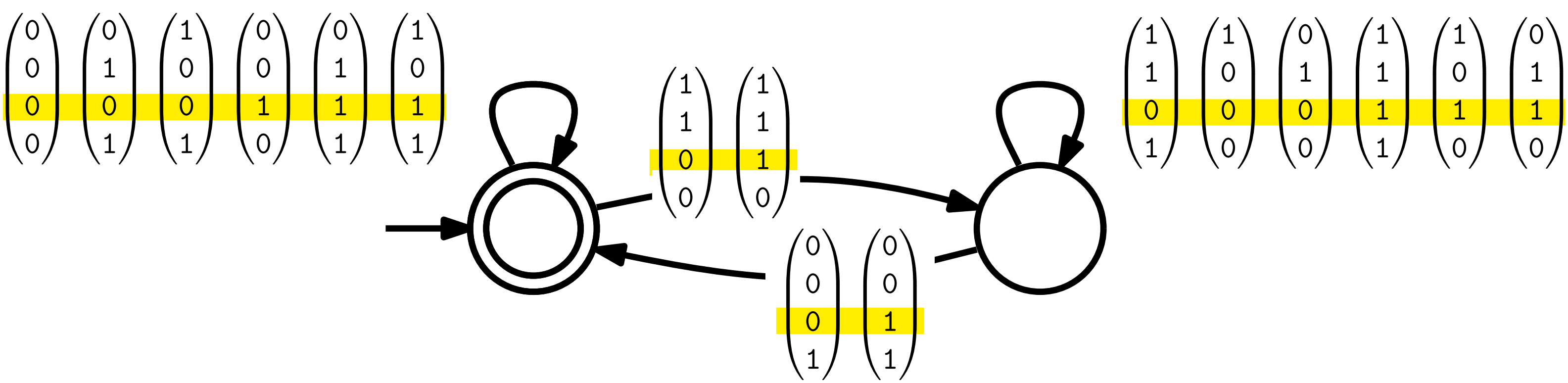
- Simulation des Bitweisen Addierens (Hausaufgabe)



Fehlende Übergänge führen zu einem nicht akzept. Zustand

- für jede PLUS Instanz kann so ein DEA gebaut werden
- nicht berücksichtigte Variablen werden in allen Kombinationen eingfügt

Bsp. DEA für PLUS(x_1, x_2, x_4) bei $\ell = 4$



2. **Teil:** Umsetzung der boolschen Operationen

- ψ ist boolscher Term über PLUS Ausdrücken
- Konstruktion des DEA zu ψ folgt der induktiven Definition von ψ
  - Sei $\psi = \psi_1 \wedge \psi_2$, dann gibt es DEA M_1 für ψ_1 und DEA M_2 für ψ_2

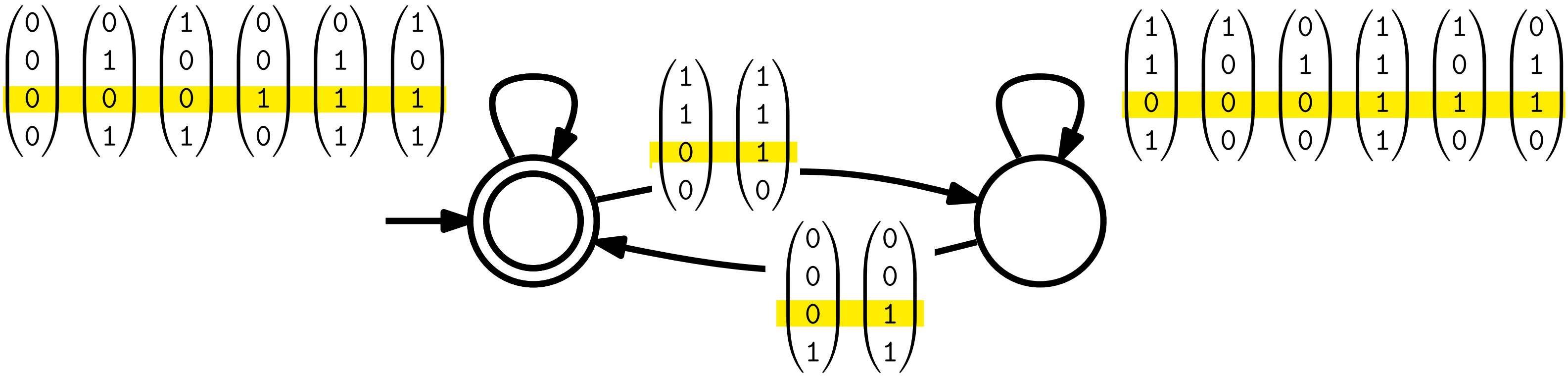
  $\rightarrow$ DEA für ψ muss $L(M_1) \cap L(M_2)$ erkennen

  $\rightarrow$ einen solchen DEA kann man konstruieren (Abschlusseigenschaften)
  - Sei $\psi = \psi_1 \vee \psi_2$, dann gibt es DEA M_1 für ψ_1 und DEA M_2. Konstruiere für ψ einen DEA der $L(M_1) \cup L(M_2)$ erkennt.
  - Sei $\psi = \neg\psi_1$, dann gibt es DEA M_1 für ψ_1. Konstruiere für ψ einen DEA der $\overline{L(M_1)}$ erkennt.
- Mit diesen Konstruktionen kann ich einen DEA für ψ konstruieren, der alle Variablenbelegungen akzeptiert, welche ψ erfüllbar machen.
- Ausgangspunkt der induktiven Konstruktion der DEAs für ϕ_i

Zusammenfassung: DEA für ψ

1. Teil: Umsetzung von PLUS

Bsp. DEA für PLUS(x_1, x_2, x_4) bei $\ell = 4$



Verwerfender Dummy-Zustand muss noch ergänzt werden

2. Teil: Umsetzung der boolschen Operationen

- ψ ist boolscher Term über PLUS Ausdrücke, konstruiere ψ aus den DEAs zu PLUS über Abschlusseigenschaften

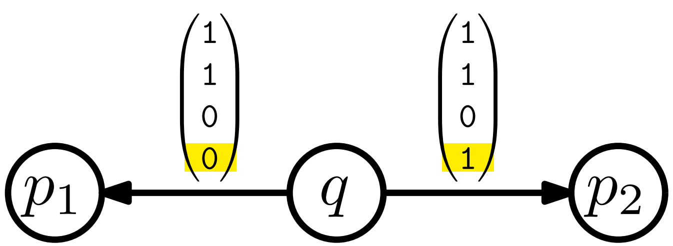
DEA für ϕ_i

1.Fall: ϕ_i beginnt mit Existenzquantor $\exists$

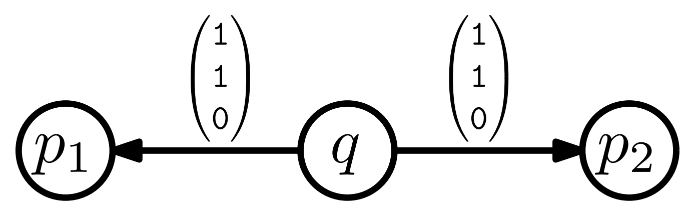
- wie gehabt sollen alle Variablen akzeptiert werden, die ϕ_i erfüllen
- Ziel ist es den DEA für ϕ_i aus dem DEA für ϕ_{i+1} zu gewinnen

- Sei A_{i+1} der DEA für ϕ_{i+1}, wir suchen einen DEA A_i für ϕ_i
- DEA A_{i+1} arbeitet auf Wörtern über $\{0,1\}^{i+1}$ – der DEA A_i arbeit auf Wörtern über $\{0,1\}^i$
- Zuerst konstruieren wir einen NEA B_i (Grundlage für A_i)
  - B_i hat die Zustände von A_{i+1}, Startzustand, akzeptiernede Zustände auch gleich
  - B_i *ignoriert* die Bits von x_{i+1} (x_{i+1} ist keine freie Variable in ϕ_i)

Bsp.



Situation in A_{i+1}



Situation in B_i

- Führe diese Modifikation für jeden Übergang aus.
- A_i ist der DEA zu B_i

2.Fall: ϕ_i beginnt mit Allquantor $\forall$

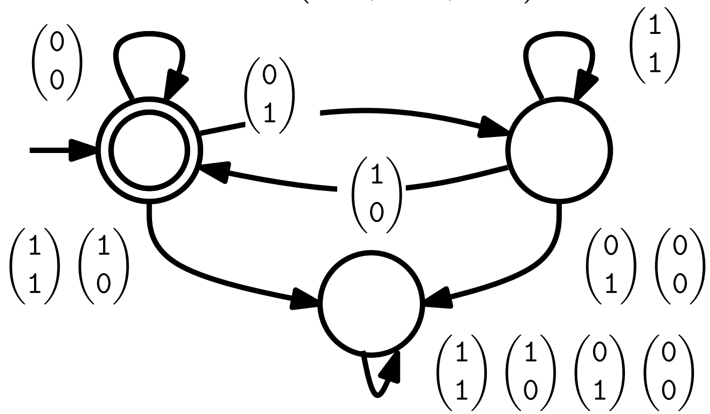
- Wie im ersten Fall: Konstruiere sei A_{i+1} der DEA für ϕ_{i+1}, wir suchen einen DEA A_i für ϕ_i
- Es gilt $\phi_i = \forall x_{i+1}\phi_{i+1} = \neg\exists x_{i+1}\neg\phi_{i+1}$
- Vorgehensweise:
  1. Bestimme DEA für $\neg\phi_{i+1}$ an Hand von A_{i+1}
  2. Konstruiere DEA $\bar{A}_i$ für $\exists x_{i+1}\neg\phi_{i+1}$ wie im 1. Fall
  3. Bilde A_i als komplementären DEA zu $\bar{A}_i$

Ende der Konstruktion

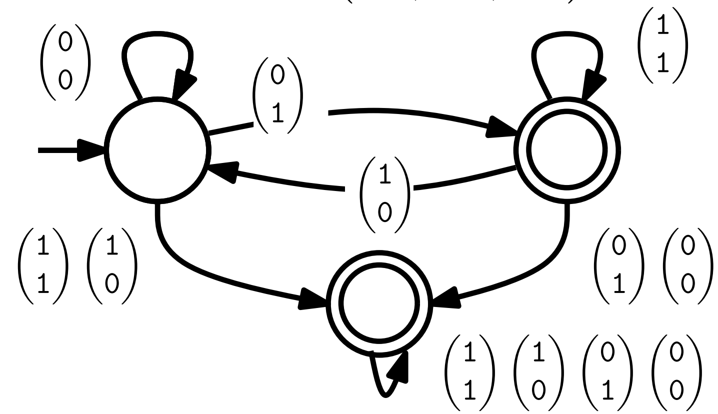
- DEA A_i arbeitet auf $\Sigma = \{0, 1\}^i$
- Wir stoppen bei A_1
- Ist der Quantor für x_1 ein Allquantor, akzeptieren wir, wenn alle mit $w \in \Sigma^+$ erreichbaren Zustände in A_1 akzeptierend sind
- Ist der Quantor für x_1 ein Existenzquantor, akzeptieren wir, wenn es einen durch $w \in \Sigma^+$ erreichbaren akz. Zustand in A_1 gibt
- Th$((\mathbf{N}, \text{PLUS}))$ entscheidbar $\square$

Bsp. $\phi = \forall x_1 \exists x_2 \neg \mathrm{PLUS}(x_2, x_2, x_1)$

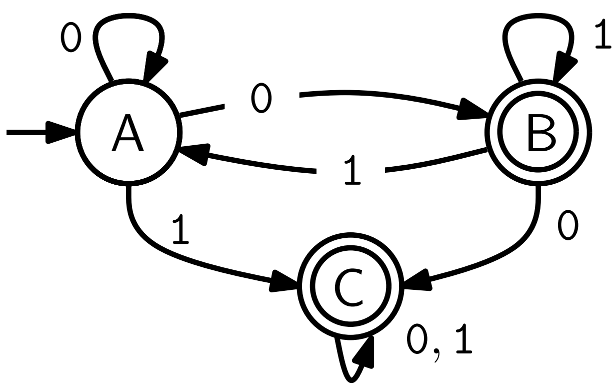
DEA zu PLUS(x_2, x_2, x_1)



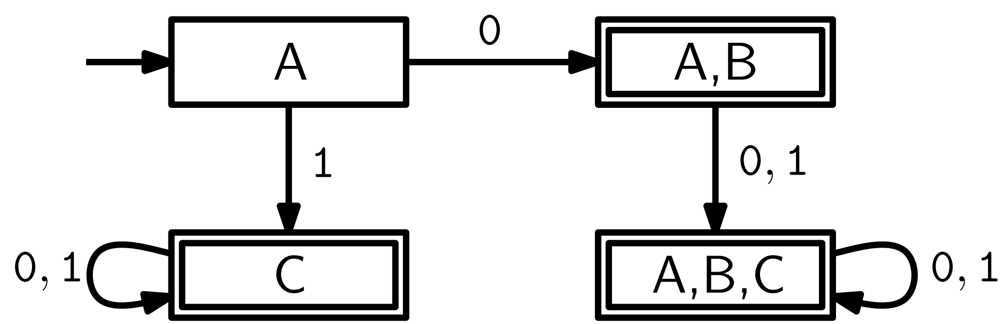
DEA zu $\neg$PLUS(x_2, x_2, x_1)



NEA zu $\exists x_2 \neg$PLUS(x_2, x_2, x_1)



DEA zu $\exists x_2 \neg$PLUS(x_2, x_2, x_1)



- x_1 ist mit $\forall$ quantifiziert, also testen wir ob alle mit $w \in \Sigma^+$ erreichbaren Zustände akzeptierend sind
- das stimmt, also ist ϕ wahr

Satz 30

Sei $(\mathbf{N}, +, \cdot)$ das Modell der natürlichen Zahlen mit Addition und Multiplikation. Dann gilt, dass $\mathrm{Th}((\mathbf{N}, +, \cdot))$ ist **nicht entscheidbar.**

Beweisidee

- kodiere Berechnungspfad als (sehr große) natürliche Zahl
- ob eine Zahl y einen akzeptierenden Berechnungspfad für $M(x)$ kodiert, kann ich mit einer Formel ausdrücken
- diese Formel sei $\phi_{\langle M,x \rangle}$
  - $\phi_{\langle M,x \rangle}$ prüft ob Anfangsteil Startkonfiguration
  - $\phi_{\langle M,x \rangle}$ prüft auf korrekte Folgekonfigurationen
  - $\phi_{\langle M,x \rangle}$ prüft ob Ende akzept. Konfiguration
- Wir zeigen $A_{\mathrm{TM}} \leq_m \mathrm{Th}((\mathbf{N}, +, \cdot))$
- Reduktion f: $f(\langle M, w \rangle) = \exists y[\phi_{\langle M,w \rangle}]$
- Formel $\phi_{\langle M,w \rangle}$ kann durch TM konstruiert werden
  $\rightarrow \mathrm{Th}((\mathbf{N}, +, \cdot)) \notin \mathbb{E}$

Beweisbare Aussagen

- Sei $\pi = (S_1, S_2, \ldots, S_n)$ eine Folge von Aussagen für die gilt:
  - S_1 ist aximomatisch definierte wahre Aussage
  - S_{i+1} folgt aus S_i durch axiomatisch beschriebene Ableitungsregeln
- Sei π heißt **Beweis von S_n**.
- Anforderungen an ein *Beweissystem*:

① $\{\langle \phi, \pi \rangle \mid \pi \text{ ist Beweis von } \phi\}$ ist entscheidbar

② $\forall \phi \, [\exists \text{ Beweis } \pi \text{ für } \phi] \longrightarrow \phi \in \mathrm{Th}(\cdot)$
(wenn es einen Beweis gibt, ist ϕ in der betrachteten Theorie wahr)

- Ein Beweissystem, welches ② erfüllt heißt korrekt.
- Notation: **Pr(Th(X))** bezeichnet die Menge aller beweisbaren Aussagen von $\mathrm{Th}(X)$ im betrachteten Beweissystem

Satz 31

$$\text{Pr}(\text{Th}(\mathbf{N}, +, \cdot)) \in \mathbb{A}$$

Beweis

- wir geben eine TM B an, die die Sprache der beweisbaren Aussagen erkennt

  $B(\langle \phi \rangle)$
  - Zähle alle potentiellen Beweise $\langle \pi \rangle$ für ϕ auf
    1. Prüfe, ob π Beweis für ϕ
    2. Wenn ja akzeptiere, wenn nein, wähle nächstes π aus

- Schritt 1. kann ausgeführt werden, da wegen ① $\{\langle \phi, \pi \rangle \mid \pi \text{ ist Beweis von } \phi\}$ entscheidbar
- es werden nach ② nur wahre Aussagen bewiesen
- existiert ein Beweis, wird er durch B gefunden
- B erkennt $\text{Pr}(\text{Th}(\mathbf{N}, +, \cdot))$ □

Satz 32

$$\mathsf{Pr}(\mathsf{Th}(\mathbf{N},+,\cdot)) \subsetneq \mathsf{Th}(\mathbf{N},+,\cdot)$$

Beweis durch Widerspruch

- wir nehmen an, dass $\mathsf{Pr}(\mathsf{Th}(\mathbf{N},+,\cdot)) = \mathsf{Th}(\mathbf{N},+,\cdot)$
- wir konstruieren die Turingmaschine D wie folgt:

> $D(\langle\phi\rangle)$
> - Konstruiere $\neg\phi$
> - Simuliere $B(\phi)$ und $B(\neg\phi)$ parallel
> - sobald eine der Simulationen stoppt, akzeptiere oder verwerfe nach deren Ergebnis

- $D(\phi)$ erkennt ob ϕ wahre Aussage in $\mathsf{Th}(\mathbf{N},+,\cdot)$
- D ist ein Entscheider, denn entweder stoppt $B(\phi)$ oder $B(\neg\phi)$
- demnach wäre $\mathsf{Th}(\mathbf{N},+,\cdot)$ also entscheidbar, was aber nicht stimmt
  $\rightarrow$ Widerspruch zur Annahme

Ein nicht beweisbarer wahrer Satz

- Sei die Turingmaschine M wie folgt konstruiert

> $S(z)$
> 1. Konstruiere $\langle S \rangle$
> 2. $\psi = \neg\exists y[\phi_{\langle S,\varepsilon\rangle}]$
> 3. Simuliere $B(\psi)$ und akzeptiere, gdw, Simulation akzeptiert

- $\phi_{\langle S,\varepsilon\rangle}$ wie im Satz 30 definiert
  (Formel die prüft, ob y Berechnungspfad für $S(\varepsilon)$)
- B ist die TM, die alle beweisbaren Aussagen erkennt
- Das heißt ψ ist wahr $\iff$ $S(\varepsilon)$ akzeptiert nicht

Satz 33

Die Aussage $\psi = \neg\exists y[\phi_{\langle S,\varepsilon\rangle}]$ ist wahr aber nicht beweisbar in der Erweiterung von Th$(\mathbf{N}, +, \cdot)$.

Beweis Satz 33

- Zur Erinnerung:
  $\psi = \neg\exists y[\phi_{\langle S,\varepsilon\rangle}]$ ist wahr $\iff$ $S(\varepsilon)$ akzeptiert nicht

> $S(z)$
> 1. Konstruiere $\langle S\rangle$
> 2. $\psi = \neg\exists y[\phi_{\langle S,\varepsilon\rangle}]$
> 3. Simuliere $B(\psi)$ und akzeptiere, gdw, Simulation akzeptiert

- Angenommen B findet Beweis für ψ:
  $\Rightarrow$ S akzeptiert alles, also auch ε
  $\Rightarrow$ ψ ist nicht wahr
  $\Rightarrow$ es gibt keinen Beweis für ψ $\rightarrow$ Widerspruch
- Demnach findet B keinen Beweis:
  $\Rightarrow$ S stoppt nie, daraus folgt $S(\varepsilon)\uparrow$
  $\Rightarrow$ $S(\varepsilon)$ akzeptiert nicht, und demnach ist ψ eine wahre Aussage $\square$

Nachbetrachtung zum Satz 33

- Ist es nicht widersprüchlich, das wir beweisen konnten, dass eine Aussage "wahr aber nicht beweisbar" ist?

$\rightarrow$ Beweis der Nichtbeweisbarkeit innerhalb der Erweiterung von Th$(\mathbf{N}, +, \cdot)$ wurde innerhalb eines anderen Systems erbracht

Formulierung als Unvollständigkeitssatz

- System X heißt **konsistent**, gdw. $\neg\exists\phi[\phi \in X \wedge \neg\phi \in X]$
- System X heißt **vollständig**, gdw. $\forall\phi[\phi \in X \vee \neg\phi \in X]$
- **vollständig und konsistent**:
  $\forall\phi[(\phi \in X \vee \neg\phi \in X) \wedge (\phi \notin X \vee \neg\phi \notin X)]$

widerspricht

Gödels 1. Unvollständigkeitssatz

Jedes axiomatische Beweissytem X, in welchem sich der Begriff des Beweis für Aussagen aus Th$(\mathbf{N}, +, \cdot)$ formaliseren lässt, ist entweder konsistent oder vollständig.

- Satz 32: Es gibt wahre Aussagen in X, die nicht beweisbar sind. Unter Annahme $\forall\phi[\phi \in X \vee \phi \notin X]$ gilt $\exists\phi[\phi \notin X \wedge \neg\phi \notin X]$

- Satz 33: Die Aussage $\psi = \neg\exists y[\phi_{\langle S,\varepsilon\rangle}]$ ist wahr aber nicht beweisbar in $\text{Th}(\mathbf{N}, +, \cdot)$

Gödels 2. Unvollständigkeitssatz

Sei X ein Beweissystem welches die Vorraussetzungen des ersten Unvollständigkeitsatzes erfüllt und in welchem sich der Satz 32 beweisen lässt. Dann ist die Konsistenz von X in X selbst nicht beweisbar.

- Angenommen wir könnten die Konsistenz von X in X beweisen
- Satz 33 liefert uns (wenn X konsistent) einen wahren Satz ψ, der in X nicht zu beweisen ist.
- Da die Konsistenz von X bewiesen wurde, erhalten wir also einen Beweis, dass ψ nicht beweisbar in X.
- Der Beweis, dass ψ wahr ist, wurde (als Beweis zu Satz 33) jedoch auch in X geführt. Also ist ψ beweisbar in X.
- Widerspruch zur Annahme $\rightarrow$ Konsistenz von X kann nicht in X bewiesen werden!