# Das deduktive System $\mathcal{F}$

**Ziel:** Konstruiere ein geeignetes deduktives System $\mathcal{F} = (Ax, R)$ für die Prädikatenlogik erster Stufe.

**Geeignet:** Korrektheit $(\Rightarrow)$ und **Vollständigkeit** $(\Leftarrow)$

$$\begin{array}{rcl} \vdash_{\mathcal{F}} A & \text{gdw.} & \models A \\ \Sigma \vdash_{\mathcal{F}} A & \text{gdw.} & \Sigma \models A \end{array}$$

Die Definition von System $\mathcal{F}$ zusammen mit dem Beweis der Vollständigkeit ist ein großer Beitrag von Kurt Gödel (1906 — 1978).

# Aussagenlogische Tautologien in *FO* und Generalisierung

## Definition 5.1

Seien $A \in F$ eine aussagenlogische Tautologie, $\{p_1, \ldots, p_n\} = V(A)$, $A_1, \ldots, A_n \in FO(S)$ und $\theta = \{p_1/A_1, \ldots, p_n/A_n\}$. Dann heißt $A\theta \in FO(S)$ eine aussagenlogische Tautologien in $FO(S)$.

## Definition 5.2

Seien $A \in FO(S)$ und $\{x_1, \ldots, x_n\} \subseteq V$. Die Formel $\forall x_1 \ldots \forall x_n.A$ ist eine Generalisierung von $A$.

Sei $FO_0(S)$ die Teilmenge der Formeln aus $FO(S)$ über $\neg, \rightarrow, \forall, =$.

## Definition 5.3 (Deduktive Systeme )

Das **deduktive System** $\mathcal{F} = (Ax, R)$ für $FO_0(S)$ besteht aus den Axiomen, die als Generalisierungen der durch folgende Schemata beschriebenen Formeln gewonnen werden können:

**Ax1:** Aussagenlogische Tautologien in $FO_0(S)$

**Ax2:** $(\forall x.\ A) \rightarrow A\{x/t\}$

**Ax3:** $(\forall x.\ A \rightarrow B) \rightarrow ((\forall x.\ A) \rightarrow (\forall x.\ B))$

**Ax4:** $A \rightarrow \forall x.\ A$, falls $x \notin FV(A)$

**Ax5:** $x = x$

**Ax6:** $x = y \rightarrow (A \rightarrow A')$, wobei $A'$ aus $A$ durch Ersetzen einiger freier Vorkommen von $x$ durch $y$ entsteht (sofern erlaubt).

Das einzige Regelschema ist **Modus Ponens**: $\dfrac{A, A \rightarrow B}{B}$

# Deduktionstheorem und Generalisierungstheorem

## Satz 5.4

*Seien* $\Gamma \subseteq FO(S)$ *und* $A, B \in FO(S)$.

a) **Deduktionstheorem**

$$\Gamma \underset{\mathcal{F}}{\vdash} A \to B \qquad \textit{gdw.} \qquad \Gamma, A \underset{\mathcal{F}}{\vdash} B$$

b) **Generalisierungstheorem:**

$$\textit{Falls } \Gamma \underset{\mathcal{F}}{\vdash} A \textit{ und } x \textit{ nicht frei in } \Gamma \textit{ vorkommt, so } \Gamma \underset{\mathcal{F}}{\vdash} \forall x\ A$$

c) **Kontrapositionstheorem:**

$$\Gamma, A \vdash \neg B \qquad \textit{gdw.} \qquad \Gamma, B \vdash \neg A.$$

Es gelten also für System $\mathcal{F}$ die für das deduktive System $\mathcal{F}_0$ der Aussagenlogik bekannten Sätze.

# Konsistenz

## Definition 5.5

Eine Formelmenge $\Gamma \subseteq FO(S)$ heißt **konsistent**, falls es kein $A \in FO(S)$ gibt mit $\Gamma \underset{\mathcal{F}}{\vdash} A$ und $\Gamma \underset{\mathcal{F}}{\vdash} \neg A$.

## Bemerkung 5.6

a) *$\Gamma$ ist konsistent gdw. jede endliche Teilmenge von $\Gamma$ konsistent ist.*

b) *Ist $\Gamma$ inkonsistent, dann gilt $\Gamma \underset{\mathcal{F}}{\vdash} A$ für jede Formel $A$.*

c) *Gilt $\Gamma \vdash A$, dann ist $\Gamma \cup \{\neg A\}$ inkonsistent.*

d) *Ist $\Gamma$ inkonsistent, so ist $\Gamma$ nicht erfüllbar.*

e) *Die Menge der allgemeingültigen Formeln ist konsistent.*

f) *Die Menge der Theoreme von $\mathcal{F}$ ist konsistent.*

# Das deduktive System $\mathcal{F}$ (Fort.)

## Satz 5.7 (Korrektheit und Vollständigkeit von $\mathcal{F}$, Gödel)

*Seien $A \in FO(S)$ und $\Sigma \subseteq FO(S)$, dann gilt:*

a) $\underset{\mathcal{F}}{\vdash} A$ *gdw.* $\models A$.

b) $\Sigma \underset{\mathcal{F}}{\vdash} A$ *gdw.* $\Sigma \models A$.

c) $\Sigma$ *konsistent* *gdw.* $\Sigma$ *erfüllbar.*

**Der Satz der Prädikatenlogik!**

## Beweis:

Korrektheit: *Ax* enthält nur allgemeingültige Formeln und (MP) führt nicht aus der Menge der allgemeingültigen Formeln hinaus.

Vollständigkeit: Siehe Enderton. ∎

# Theorien erster Stufe

Betrachte abgeschlossene Formeln, kurz Formeln in $FO_{abg}(S)$.

## Definition 5.8

Sei $S$ eine Signatur. Eine Formelmenge $\Gamma \subseteq FO_{abg}(S)$ heißt **Theorie erster Stufe**, falls $\Gamma$ abgeschlossen gegenüber logischer Folgerung ist:

$$A \in FO_{abg}(S) \quad \text{und} \quad \Gamma \models A \quad \text{impliziert} \quad A \in \Gamma.$$

Nutze $T$ als Bezeichner für Theorien.

Alternative Definitionen in der Literatur:

- $\Gamma$ Menge an Formeln aus $FO(S)$ anstatt $FO_{abg}(S)$, abgeschlossen gegen logische Folgerung.
- $\Gamma$ Theorie, falls $\Gamma$ abgeschlossen gegen MP und Generalisierung.

# Theorien erster Stufe (Forts.)

## Bemerkung 5.9 (und Definition)

*Sei $S$ eine Signatur.*

a) $T_S = \{A \in FO_{abg}(S) \mid A \text{ allgemeingültig}\}$ *ist eine Theorie.*

b) *Sei* $\Sigma \subseteq FO_{abg}(S)$. *Dann ist* $T_\Sigma = \{A \in FO_{abg}(S) \mid \Sigma \models A\}$ *die* **von $\Sigma$ erzeugte Theorie** *oder durch die Axiome $\Sigma$ definierte Theorie.*

c) *Sei $\mathcal{M}$ eine Struktur der Signatur $S$. Dann ist*

$$T_\mathcal{M} = \{A \in FO_{abg}(S) \mid \mathcal{M} \models A\}$$

*die* **Theorie von $\mathcal{M}$**. *Es ist auch $Th(\mathcal{M})$ als Symbol üblich.*

# Theorien erster Stufe (Forts.)

## Lemma 5.10 (und Definition)

(i) *Ist $T$ eine Theorie und $A \in FO_{abg}(S)$, dann gilt*

$$T \underset{\mathcal{F}}{\vdash} A \quad gdw. \quad A \in T.$$

(ii) *Theorie $T$ heißt* **inkonsistent***, falls es eine Formel $A \in FO_{abg}(S)$ gibt mit $T \underset{\mathcal{F}}{\vdash} A$ und $T \underset{\mathcal{F}}{\vdash} \neg A$. In dem Fall gilt $T = FO_{abg}(S)$.*

(iii) *$T_{\mathcal{M}}$ ist* **konsistent** *für jede Struktur $\mathcal{M}$.*

(iv) *$T_S$ ist in jeder Theorie über $S$ enthalten.*

# Theorien erster Stufe (Forts.)

## Definition 5.11

Sei $T$ eine Theorie erster Stufe über Signatur $S$.

a) $T$ heißt **vollständig**, falls für jede Formel $A \in FO_{abg}(S)$ gilt: $A \in T$ oder $\neg A \in T$.

b) $T$ heißt **(endlich, aufzählbar) axiomatisierbar**, falls es eine (endliche, aufzählbare) Teilmenge $\Sigma \subseteq FO_{abg}(S)$ gibt mit

$$T_\Sigma = T.$$

c) $T$ heißt **entscheidbar**, falls $T$ eine entscheidbare Teilmenge von $FO_{abg}(S)$ ist.

# Theorien erster Stufe (Forts.)

## Bemerkung 5.12

(a) *$T_{\mathcal{M}}$ ist* **vollständig** *für jede Struktur $\mathcal{M}$.*
*Mit Lemma 5.10 ist $T_{\mathcal{M}}$ also konsistent und vollständig.*

(b) *$T$ ist erfüllbar gdw. $T$ ist konsistent.*

(c) *Ist $T$ aufzählbar axiomatisierbar, dann ist $T$ aufzählbar.*

(d) *Ist $T$ vollständig und aufzählbar axiomatisierbar, dann ist $T$* **entscheidbar***.*

(e) *Ist $T$ vollständig und konsistent, dann $T = T_{\mathcal{M}}$ für eine Struktur $\mathcal{M}$.*

# Axiomatisierung

**Ziel**: Finde Axiomatisierungen wichtiger Theorien.

Insbesondere: Wann gilt $T_{\mathcal{M}} = T_\Sigma$ für $\Sigma$ **aufzählbar**.

**Motivation:** Entscheidbarkeit!

**Problem:** Wann ist $T_\Sigma$ vollständig für aufzählbare $\Sigma$?

# Axiomatisierung (Presburger)

Betrachte die Signatur der Arithmetik **ohne Multiplikation**:

$$S_{PA} = (\{0/_0, 1/_0, +/_2\}, \{\}).$$

Die zugehörige Struktur $\mathcal{M}_{PA} = (\mathbb{N}, I_{PA})$ mit der erwarteten Interpretation wird **Presburger-Arithmetik** genannt.

Sei $\Sigma_{PA}$ die Menge aus folgenden Axiomen und Instantierungen des gegebenen Axiomenschemas (Induktion):

$$\forall x.\ \neg(x + 1 = 0) \qquad \text{(Null)}$$

$$\forall x.\ x + 0 = x \qquad \text{(Plus Null)}$$

$$\forall x.\forall y.\ x + 1 = y + 1 \rightarrow x = y \qquad \text{(Nachfolger)}$$

$$\forall x.\forall y.\ x + (y + 1) = (x + y) + 1 \qquad \text{(Plus Nachfolger)}$$

$$A\{z/0\} \wedge (\forall x.\ A\{z/x\} \rightarrow A\{z/x+1\}) \rightarrow \forall x.\ A\{z/x\}, \qquad \text{(Induktion)}$$

wobei $A \in FO(S_{PA})$ eine Formel mit $x \notin FV(A)$ ist.

# Axiomatisierung (Presburger)

**Satz 5.13 (Vollständige Axiomatisierung der Presburger-Arithmetik)**

*Es gilt* $T_{\mathcal{M}_{PA}} = T_{\Sigma_{PA}}$. *Da* $\Sigma_{PA}$ *aufzählbar ist, ist* $T_{\mathcal{M}_{PA}}$ **entscheidbar**.

Vollständigkeit der Axiomatisierung ist anspruchsvoll.
Entscheidbarkeit folgt mit Bemerkung 5.12(d).

Es lassen sich also geschlossene Formeln aus $FO(S_{PA})$ **automatisch** auf Gültigkeit in Presburger-Arithmetik prüfen.

Zum Beispiel:

$$\forall w. \forall x. \exists y. \exists z.\ x + 2y + 3w = z + 13 \quad ?$$

Man beachte die Quantoren und vergleiche mit Gauß-Elimination.

# Axiomatisierung (Gödel und Peano)

Betrachte die Signatur der vollen Arithmetik:

$$S_{Arith} = (\{0/_0, 1/_0, +/_2, \cdot/_2\}, \{\}).$$

Die zugehörige Struktur $\mathcal{M}_{Arith} = (\mathbb{N}, I_{Arith})$ mit der erwarteten Interpretation wird **(First-Order-)Arithmetik** genannt.

## Satz 5.14 (Gödel)

*$T_{\mathcal{M}_{Arith}}$ ist nicht entscheidbar.*

*Konsequenz 1: $T_{\mathcal{M}_{Arith}}$ ist* **nicht** *aufzählbar axiomatisierbar.*

*Konsequenz 2: Jedes aufzählbare Axiomensystem für $T_{\mathcal{M}_{Arith}}$ ist* **unvollständig***.*

Die Konsequenzen ergeben sich aus Bemerkung 5.12(a) und (d).

# Axiomatisierung (Gödel und Peano)

Insbesondere sind die Peano-Axiome $\Sigma_{Peano}$ **keine** vollständige Axiomatisierung von $T_{\mathcal{M}_{Arith}}$ mit $A \in FO(S_{Arith})$ und $x \notin FV(A)$:

$$\begin{aligned}
&\forall x.\ \neg(x + 1 = 0) && \text{(Null)}\\
&\forall x.\ x + 0 = x && \text{(Plus Null)}\\
&\forall x.\forall y.\ x + 1 = y + 1 \to x = y && \text{(Nachfolger)}\\
&\forall x.\forall y.\ x + (y + 1) = (x + y) + 1 && \text{(Plus Nachfolger)}\\
&A\{z/0\} \wedge (\forall x.\ A\{z/x\} \to A\{z/x + 1\}) \to \forall x.\ A\{z/x\} && \text{(Induktion)}\\
&\forall x.\ x \cdot 0 = 0 && \text{(Mal Null)}\\
&\forall x.\forall y.\ x \cdot (y + 1) = x \cdot y + x && \text{(Mal Nachfolger)}
\end{aligned}$$

Es gibt also abgeschlossene Formeln $A \in FO(S_{Arith})$ mit $\mathcal{M}_{Arith} \models A$, für die $T_{\Sigma_{Peano}} \models A$ **nicht** gilt.

# Axiomatisierung zur Spezifikation von Strukturen

Beobachtungen:

- In allen Modellen einer vollständigen Theorie (beispielsweise $T_{\Sigma_{PA}}$) gelten die gleichen Formeln.
- Bei Modellen $\mathcal{M}$ einer unvollständigen Theorie $T_\Sigma$ (beispielsweise $T_{\Sigma_{Peano}}$) kann es $A \in FO(S)$ geben mit $\mathcal{M} \models A$, aber nicht $T_\Sigma \models A$.

Fragen:

- Gibt es Theorien mit genau einem Modell? Kann man eine gegebene Struktur durch eine Theorie eindeutig axiomatisieren?
- Haben $T_{\Sigma_{PA}}$ und $T_{\Sigma_{Peano}}$ mehrere Modelle?

**Satz 5.15**

*$T_{\Sigma_{PA}}$ und $T_{\Sigma_{Peano}}$ haben außer $\mathcal{M}_{PA}$ und $\mathcal{M}_{Arith}$ weitere Modelle, sogenannte Nicht-Standardmodelle.*

Beweis: siehe Vorlesung

# Axiomatisierung (Arrays)

Gegeben seien Funktionen für Lese- und Schreibzugriffe auf Arrays:

$$S_{McC} = (\{\text{read}/_2, \text{write}/_3\}, \{\}).$$

Betrachte **McCarthys Array-Axiome $\Sigma_{McC}$**:

$$\forall x.\ x = x \qquad \text{(Reflexivität)}$$

$$\forall x. \forall y.\ x = y \rightarrow y = x \qquad \text{(Symmetrie)}$$

$$\forall x. \forall y. \forall z.\ x = y \wedge y = z \rightarrow x = z \qquad \text{(Transitivität)}$$

$$\forall a. \forall i. \forall j.\ i = j \rightarrow \text{read}(a, i) = \text{read}(a, j) \qquad \text{(Array-Kongruenz)}$$

$$\forall a. \forall v. \forall i. \forall j.\ i = j \rightarrow \text{read}(\text{write}(a, i, v), j) = v \qquad \text{(Read-Write 1)}$$

$$\forall a. \forall v. \forall i. \forall j.\ i \neq j \rightarrow \text{read}(\text{write}(a, i, v), j) = \text{read}(a, j) \qquad \text{(Read-Write 2)}$$

**Satz 5.16**

*$T_{\Sigma_{McC}}$ ist* ***nicht entscheidbar****, insbesondere also* ***nicht vollständig****.*
*Entscheidbare Fragmente sind aktives Forschungsgebiet, Aaron Bradley'06.*