B9

Friday, May 14, 2010
17:21

Rekursionstheorie beantwortet die Frage:
Was ist ein Algorithmus?
Die Antwort ist das kanonische, universelle Computer-Modell. Als Cor. lässt sich zeigen: Bestimmte Funktionen sind unentscheidbar etc.

Wir behandeln im Rest der Vorlesung eine andere Frage: Was ist wahr? Was ist ein Beweis?
Es stellt sich heraus dass die Antworten auf diese Fragen nicht ganz so einfach bzw kanonisch sind wie bei der Rekursionstheorie.

Ein grober Überblick:

(1) Es stellt sich heraus, dass wir eine (formale) <u>Sprache</u> fixieren müssen ("Objektsprache"), die wir dann "von außen" (in der "Metasprache") untersuchen. In dieser Hinsicht kann es keine universelle Sprache geben (siehe Richard Paradoxon).

(2) Ein wichtiges Konzept ist die Trennung von "mathematischen Inhalt" und der reinen "Form" (Logik). Z.B: $(A \wedge B) \to A$ ist rein logisch wahr, unabhängig davon welchen math. Inhalt die Aussagen A und B haben.
Insbesondere: Trennung vom Beweissystem in
(·) mathematische Axiome
(·) rein logische Ableitungsregeln (bzw "logische Axiome")
Idealerweise sind beide einfach und unmittelbar einsichtig, ergeben aber starke Folgerungen (idealerweise: alle wahren Sätze)

B9 (Forts.)

Friday, May 14, 2010
17:32

Die Frage "was ist ein Beweis" spaltet sich also in:
(Ax?) Was sind die (richtigen/vollständigen/...) Axiome?
(Log?) — " — logischen Ableitungsregeln?

(3) Konkreter: Mögliche Sprachen (oder: Frameworks)
(a) Aussagenlogik: Als Grundlage für Mathematik zu primitiv. Die Logik selbst ist auf triviale Weise entscheidbar (Wahrheitstabellen etc).
Für das oben skizzierte Programm (Trennung von math. Axiomen und log. Ableitungen) bringt Aussagenlogik nichts: Die Axiome und die Folgerungen sind ja fast identisch;
(b) Prädikatenlogik (erster Stufe): gerade mächtig genug, um Teile der Mathematik zu beschreiben (in Verbindung mit Mengenlehre sogar die gesamte Mathematik); die Logik ist zwar nicht "entscheidbar", aber trotzdem einigermaßen "handhabbar": Es gibt einen "maschinellen" Ableitungskalkül. "$\Sigma \vdash \varphi$" heißt: φ lässt sich aus Axiomenmenge Σ ableiten. Wenn Σ rekursiv ist, dann ist $\{\varphi : \Sigma \vdash \varphi\}$ r.e. (aber i.A. nicht rek.). Der Gödelsche Vollständigkeitssatz besagt dass dieser Ableitungskalkül auch vollständig ist, d.h., jeder Satz φ der "aus Σ folgt" lässt sich auch formal im Kalkül ableiten. Damit ist Frage (Log?) beantwortet, nicht aber Frage (Ax?).

B9 (Forts.)

Friday, May 14, 2010
18:27

(C) Prädikatenlogik höherer Stufen: Eigentlich natürlicher für Mathematik; das Problem ist daß es dafür <u>keinen</u> (maschinellen) Ableitungskalkül geben kann; in Hinblick auf obiges Programm: Man kann zB sehr leicht in der Logik 2. Stufe eine endliche Menge PA_2 von Axiomen angeben, die die natürlichen Zahlen bis auf Isomorphie charakterisiert (das ist in der Logik erster Stufe <u>nicht</u> möglich); d.h.

die Frage (Ax?) lässt sich in vielen Fällen viel "besser" (befriedigender) beantworten als in der Logik 1. Stufe; aber davon hat man nichts, weil ein Ableitungskalkül der Logik 2. Stufe, dh. die Antwort auf (Lg?) genauso kompliziert bzw unklar ist wie die zu untersuchenden mathematischen Objekte selbst.

Im weiteren Folge beschäftigen wir uns nur mit Prädikatenlog. erster Stufe (first order predicate calculus; f.o.) Genauer gibt es verschiedene f.o. sprachen; zu jeder Signatur (Mg von Funktions-, Relations- und Konstantensymbolen) eine.

(b) Für bestimmte mathematische Gebiete gibt es "verschieden gute" Antworten auf die Frage (Ax?):

(a) Auf dem Gebiet der Gruppen kann man zB einfach die Gruppenaxiome (in der "f.o. Sprache der Gruppen" $L=\{e, \circ, ^{-1}\}$) verwenden.
Nach Def. ist das eine vollständige Axiomatisierung.
Problem: Die first order Sprache der Gruppen ist zu primitiv, um Konzepte auszudrücken die in der Gruppenth. eigentlich interessant sind:
"es gibt einen Normalteiler H so daß ..."
ist zum Beispiel ein second order Quantor

B9 (Forts.)

Monday, May 17, 2010
14:37

(H ist ja Teilmenge der Grundmenge, nicht Element)
"x hat endl. Ordnung", dh. $\exists n \geq 1$ sd $x^n = e$
ist nicht formulierbar, weil in der f.o. Sprache
keine unendlichen Disjunktionen
$x = e \vee x \cdot x = e \vee x \cdot x \cdot x = e \vee \ldots$
möglich ist etc.

(b) Elementare Zahlentheorie, $L = \{0, 1, S, +, \cdot, <\}$
Wir hätten gerne Axiome Σ, aus denen genau die
L-Sätze folgen die in $\mathbb{N}$ gelten. Aber:
(Gödelscher Unvollständigkeitssatz): So ein Σ kann
nicht rekursiv sein.
Es gibt aber interessante "unvollständige" Axiomen-
mengen, zB PA (Peano Arithmetik)
Jedenfalls lassen sich in L viele wichtige
Zahlentheo. Fragen formulieren (Ü: Goldbachsche
Vermutung)

(c) Mengenlehre: ermöglicht es, die
Einschränkungen von f.o. Sprachen teilweise zu
umgehen. (Nächste Stunden)

Richard Paradox:
Sei n die kleinste natürliche Zahl, die sich nicht
mit einem Satz mit weniger als tausend Buchstaben
definieren lässt.

Zeigt: Notwendigkeit von Trennung in Objekt-
und Metasprache (es gibt in dieser Hinsicht
keine universelle Sprache)

B9 (Forts.)

Thursday, June 10, 2010

Weiterführende Bem.:

Wir werden später die Sprache $L_\in = \{\in\}$ der Mengenlehre kennenlernen, die eine de-facto universelle Sprache für die "normale" Mathematik ist. Es lassen sich also alle "normalen" mathematischen Sätze in ZFC formulieren; aber man kann eben auch sinnvolle mathematische Eigenschaften konstruieren, die in ZFC nicht formulierbar sind:

Bsp1: In Anlehnung an das Richard Paradoxon

$\varphi(n,m) \equiv$ die natürliche Zahl n lässt sich mit einem formalen $L_\in$-Satz der Länge m definieren.

Bsp2: (in der Mengenlehre von größerer technischen Bedeutung) das Wahrheitsprädikat T:

$T(n) \equiv$ der Satz mit Gödelnummer n ist wahr.

D.h., wir hätten gerne eine Formel $T(x)$ sd. für alle Sätze φ gilt: $T(\ulcorner\varphi\urcorner) \leftrightarrow \varphi$.

Das ist aber nicht möglich: Es gilt allgemein:

(*) Für jede Formel $\psi(x)$ gibt es Satz φ sd $ZFC \vdash \varphi \leftrightarrow \psi(\ulcorner\varphi\urcorner)$

(Dann setze $\psi \equiv \neg T$, Widerspruch)

(Das ist 10.3 im Ziegler Skriptum)

Bem (Von noch größerer technischer Bedeutung:)

Im Unterschied zu T lässt sich "φ ist beweisbar aus ZFC" sehr wohl durch Formel $Pr(\ulcorner\varphi\urcorner)$ in $L_\in$ formulieren

Wichtige Eig.: (1) $ZFC \vdash \varphi \Leftrightarrow ZFC \vdash Pr(\ulcorner\varphi\urcorner)$ und

(2) $ZFC \vdash \varphi \to \psi \longrightarrow ZFC \vdash Pr(\ulcorner\varphi\urcorner) \to Pr(\ulcorner\psi\urcorner)$

(3) $ZFC \vdash Pr(\ulcorner\varphi\urcorner) \to Pr(\ulcorner Pr(\ulcorner\varphi\urcorner)\urcorner)$

(4) $ZFC \vdash Pr(\ulcorner\varphi_1\urcorner) \wedge Pr(\ulcorner\varphi_2\urcorner) \to Pr(\ulcorner\varphi_1 \wedge \varphi_2\urcorner)$

Setze $Con(ZFC) \equiv \neg Pr(\perp)$ für $\perp \equiv \forall x\ x \neq x$ oder dergl.

B9 (Forts.)

Thursday, June 10, 2010
10:56

Dann gibt (*) den Gödelschen Unvollständigkeitssatz:

Sei $\psi(x) \equiv \neg Pr(x)$. Wir bekommen also φ sd

$ZFC \vdash \varphi \leftrightarrow \neg Pr(\ulcorner\varphi\urcorner)$. Es folgt aus (2) $ZFC \vdash Pr(\varphi) \to Pr(\neg Pr(\varphi))$

und aus (3) $ZFC \vdash Pr(\varphi) \to Pr(Pr(\varphi))$, d.h. mit (4)

$ZFC \vdash \neg\varphi \leftrightarrow Pr(\ulcorner\varphi\urcorner) \to \neg Con(ZFC)$

<u>Wenn</u> $ZFC \vdash Con(ZFC)$, dann $ZFC \vdash \varphi$, dann $ZFC \vdash \neg Pr(\varphi)$, dann $ZFC \nvdash \varphi$

(Siehe Ziegler Kapitel 10)

Das alles funktioniert analog für andere Theorien, siehe Kap 19