Tutorium Theoretische Informatik II 16. Juni 2010

Note Title 5/3/2010

A) Diagonalisierung ohne Tabelle (Aufgabe 7.4c)

2) Reduktionsfunktionen, Notation $g^{-1}(M)$ und Injektivität

3) Beweis für PCP $\leq$ MPCP

---

1 Diagonalbeweise:
- Die Tabelle ist nur eine Motivation für das Vorgehen, diagonal durch alle (berechenbaren) Funktionen und ihre Argumente durchzugehen
- In eigentlichen Beweis ist diese Tabelle nicht nötig sondern wird bestenfalls zur Illustration verwendet
- In manchen Aufgabenstellungen steckt die Diagonale bereits in der Formulierung der betrachteten Menge

z.B. $S = \{ i \mid \varphi_i(i) \text{ ist definiert} \}$

oder $V = \{ i \mid \varphi_i(1) = i \}$

Aufgabe 7.4c: $V = \{ i \mid \varphi_i(1) = i \}$ ist nicht entscheidbar (1)

aber aufzählbar (2)

(1a) Der Satz von Rice ist $\boxed{\text{nicht anwendbar}}$, da die Eigenschaft "$\varphi_i(1) = i$" von der konkreten Programmnummer abhängt

Für den Satz von Rice müsste V sich schreiben lassen als $V = \{ i \mid \varphi_i \in P \}$ für eine Menge P von berechenbaren Funktionen.

Es müsste gelten $P = \{ f \in \mathfrak{F} \mid f(i) = i \}$, aber in dieser Beschreibung ist nicht fest gelegt, was i sein soll d.h. P ist nicht sauber definierbar.

Die Eigenschaft '$\varphi_i(i) = i$' ist also nicht extensional, also nicht beschreibbar als eine Eigenschaft, die nur von der berechneten Funktion abhängt, und nicht vom Programm selbst.

Bleibt noch Diagonalisierung oder Reduktion

(1b) Diagonalisierung:

Wir nehmen an V wäre entscheidbar. Dann ist

$$\chi_V \text{ mit } \chi_V(i) = \begin{cases} 1 & \text{wenn } i \in V \text{ (also } \varphi_i(i) = i) \\ 0 & \text{sonst} \end{cases}$$

berechenbar. (das ist unsere Definition für 'entscheidbar')

Wir konstruieren eine Funktion g (mit dem Ziel einen widersprüchlichen Effekt zu erzielen – und verwenden dabei χ_V) durch

$$g(i) = \begin{cases} i+1 & \text{falls } \chi_V(i) = 1 \\ i & \text{sonst} \end{cases}$$

dann ist g berechenbar und total (weil $g(i) = i + \chi_V(i)$)
und damit gibt es eine Zahl j mit $g = \varphi_j$
(das ist die Definition für 'berechenbar')
Für dieses j gilt

$$\chi_V(j) = 1 \underset{\substack{\text{Definition}\\ \text{von } \chi_V}}{\iff} j \in V \underset{\substack{\text{Definition}\\ V = \{j \mid \varphi_j(j) = j\}}}{\iff} \varphi_j(j) = j \underset{g = \varphi_j}{\iff} g(j) = j \underset{\substack{\text{Definition}\\ \text{von } g}}{\iff} \chi_V(j) = 0$$

Dies ist ein Widerspruch, also kann χ_V nicht berechenbar sein,
und damit ist V nicht entscheidbar.

[Im Tutorium habe ich einen anderen Widerspruch vergeführt

$$g(j) = \begin{cases} j+1 & \text{, falls } \chi_V(j) = 1 \text{, d.h. } j \in V \text{, d.h. } \varphi_j(j) = j \text{, d.h. } g(j) = j \\ j & \text{, } \chi_V(j) = 0 \text{ .... d.h. } g(j) \neq j \end{cases}$$

also immer $g(j) \neq g(j)$ ↯
Der obige Widerspruch ist leichter zu erkennen]

(1c) Reduktion: Um die nicht-Entscheidbarkeit von V zu zeigen müssen wir eine andere, nicht-entscheidbare Menge finden, die auf V reduziert werden kann. Wir wählen hierzu eine Menge, die eine gewisse Ähnlichkeit zu V besitzt:

$$S = \{ i \mid \varphi_i(i) \text{ ist definiert} \}$$

Für die Reduktion müssen wir eine berechenbare (totale!) Funktion f finden mit der Eigenschaft $S = f^{-1}(V)$, also $i \in S \Leftrightarrow f(i) \in V$, bzw

$$\varphi_i(i) \text{ definiert} \Leftrightarrow \varphi_{f(i)}(f(i)) = f(i)$$

Dies ist keineswegs so einfach, wie es auf den ersten Blick erscheint, da wir den Test '$\varphi_i(i)$ definiert' nicht durchführen können. Man müsste eine Konstruktion mit dem smn Theorem analog zum Beweis des Satzes von Rice ausführen.
Im Vergleich zum Diagonalbeweis ist dies deutlich komplizierter und daher nicht als Lösung zu empfehlen

(2) Noch zu zeigen ist, dass V aufzählbar ist. Hierzu könnte man versuchen $V \subseteq S$ zu beweisen. Dann würde aus der Aufzählbarkeit von S die von V folgen. Der Reduktionsbeweis ist allerdings

ähnlich aufwendig wie der von $S \leq V$ und daher nicht zu empfehlen.

Einfacher ist der direkte Beweis:

V ist aufzählbar $\Longleftrightarrow$ V semi-entscheidbar

$$\Longleftrightarrow \quad \psi_V \text{ mit } \psi_V(i) = \begin{cases} 1 & i \in V \text{, d.h. } \varphi_i(i) = i \\ \perp & \text{sonst} \end{cases}$$

ist berechenbar

Es ist
$$\psi_V(i) = \begin{cases} 1 & \text{wenn } u\langle i,i\rangle = i \\ \perp & \text{sonst} \end{cases}$$

und damit ist ψ_V berechenbar, weil u berechenbar ist.

[Wer es 'ausprogrammieren' will, könnte sagen

$$\psi_V(i) = \mu_z \left[\, |u\langle i,i\rangle - i| = 0 \right]$$

oder ein Programm schreiben, das $u\langle i,i\rangle = i$ testet und in eine Endlosschleife geht wenn dies nicht zutrifft oder $u\langle i,i\rangle$ nicht definiert ist.
Für den Beweis wäre dies also nicht erforderlich]

(2) Reduktionen und die Notation $g^{-1}(M)$

Eine Menge M' ist reduzierbar auf eine andere Menge M, wenn es eine berechenbare ~~und totale~~ Funktion g gibt mit $M' = g^{-1}(M)$.
Die Schreibweise hierfür ist $M' \leq M$ und bedeutet, daß M' nicht schwerer zu berechnen ist als M [oder 'leichter']

a) Die Notation $g^{-1}(M)$ hat nichts mit Umkehrfunktionen zu tun sondern beschreibt die Menge der Urbilder von M unter g, also die Menge der Elemente, die durch g auf Elemente von M abgebildet werden. ~~Genau~~ Genau besagt

$$g^{-1}(M) = \{ i \mid g(i) \in M \}, \quad \text{also} \quad i \in g^{-1}(M) \iff g(i) \in M$$

Dabei ist es irrelevant, ob g injektiv ist oder nicht. Rein hypothetisch ist es möglich, daß g alle Zahlen auf nur zwei Elemente abbildet ein $x \in M$ und ein $y \notin M$. Dann wäre $g^{-1}(M) = \{ i \mid g(i) = x \}$ d.h. es werden viele Elemente auf x abgebildet.

b) Wenn $M' \leq M$ und $M \leq M'$ gilt, dann sind M und M' nicht notwendigerweise gleich, sondern nur 'gleich schwer'. So kann man zB die Menge der geraden Zahlen auf die ungeraden reduzieren durch $g(i) = i+1$ und umgekehrt (ebenfalls mit $g(i) = i+1$), denn es gilt

i gerade $\Leftrightarrow$ $i+1$ ungerade und
i ungerade $\Leftrightarrow$ $i+1$ gerade

Daß im zweiten Fall die 0 nicht getroffen wird, ist ebenfalls irrelevant

c) Ein Reduktionsbeispiel liefert Aufgabe 7.4a

" $T = \{ i \mid \varphi_{i-100}(i-100)$ undefiniert $\}$ ist nicht aufzählbar

Wir reduzieren $\bar{S} = \{ i \mid \varphi_i(i)$ undefiniert $\}$ auf V durch

$g(i) = i+100$. Dann ist g berechenbar und total und es gilt

$i \in \bar{S} \Leftrightarrow \varphi_i(i)$ undefiniert $\Leftrightarrow \varphi_{(i+100)-100}(i+100-100)$ undef.

$\Leftrightarrow i+100 \in T$

damit folgt $\bar{S} \leq T$ und da $\bar{S}$ nicht aufzählbar ist, gilt dies auch für T.

d) Ein weiteres Beispiel liefert die Reduktion $PKP \leq MPKP$ aus Aufgabe 8.1a. Es ist

$$PKP = \{ (u_1,v_1)..(u_k,v_k) \mid \exists i_1..i_n .\ u_{i_1}..u_{i_n} = v_{i_1}..v_{i_n},\ n \geq 1 \}$$
$$MPKP = \{ (u_1,v_1)..(u_k,v_k) \mid \exists i_2..i_n .\ u_1 u_{i_2}..u_{i_n} = v_1 v_{i_2}..v_{i_n},\ n \geq 1 \}$$

der Unterschied besteht darin, daß bei MPKP die Korrespondenz mit dem ersten genannten Paar beginnen muß! Dies wird im Beweis der Unentscheidbarkeit von PKP als Zwischenschritt benötigt.

Um die Reduktion zu konstruieren, müssen wir jede Wortpaarfolge in eine Wortpaarfolge umwandeln, die eine Korrespondenz besitzt, wenn zuerst das erste Wortpaar verwendet wird und anschließend die ursprüngliche PKP Korrespondenz wieder verwendet, wenn es eine gibt. Es ist nicht erforderlich, daß jede Korrespondenz mit dem ersten Wortpaar beginnt, sondern nur, daß eine solche Korrespondenz möglich ist.
Der Trick ist, ein Wortpaar $(\#\#, \#)$ zu ergänzen, wobei $\#$ ein neues Symbol ist und dann die v_i entsprechend mit einem $\#$ am Anfang zu versehen, so daß die alte Korrespondenz wieder verwendet werden kann. Wir definieren also

$$g((u_1,v_1)\dots(u_k,v_k)) = (\#\#,\#)\,(u_1,\#v_1)\dots(u_k,\#v_k)\,(u_1,v_1)\dots(u_k,v_k)$$

dann ist g berechenbar (über Wörtern) und total und es gilt

$$(u_1,v_1)\dots(u_k,v_k) \in PKP \iff \exists_{n\geq 1}\, i_1..i_n \quad u_{i_1}..u_{i_n} = v_{i_1}..v_{i_n}$$

$$\iff \exists_{n\geq 1}\, i_1..i_n \quad \#\#\,u_{i_1}..u_{i_n} = \#\,\#v_{i_1}..v_{i_n}$$

$$\overset{(1)}{\iff} g((u_1,v_1)..(u_k,v_k)) \in MPKP$$

Man beachte daß die Umkehrung (1) nur gilt, weil das erste Paar nicht alleine eine Korrespondenz darstellt und damit mindestens ein $(u_j, \#v_j)$ verwendet werden muß. Damit bekommen wir eine nicht leere Korrespondenz für PKP aus der für MPKP.