

Übungen zur Vorlesung
Berechenbarkeit und Formale Sprachen

WS 2009/2010

Blatt 7

Je mehr Plus-Zeichen +, desto wichtiger, je mehr Sterne *, desto schwieriger.

AUFGABE 37:

[Präsenzaufgabe, + + +, **]

- (a) Sei $k \in \mathbb{N}$. Ein ungerichteter Graph $G = (V, E)$ heißt k -färbbar, wenn es eine Abbildung $c : V \rightarrow \{1, \dots, k\}$ mit $\forall \{u, v\} \in E : c(u) \neq c(v)$.

Zeigen Sie:

$$\text{COL} := \{ \langle G, k \rangle \mid G \text{ ist ein } k\text{-färbbarer Graph} \} \in \text{NP}$$

- (b) Sei $p(x_1, x_2, \dots, x_k)$ ein Polynom mit ganzzahligen Koeffizienten (d. h. Koeffizienten aus \mathbb{Z}). Z. B. ist $p(x_1, x_2, x_3) = 5 \cdot x_1^4 \cdot x_3^2 - 12 \cdot x_2^2 \cdot x_3^5 - x_1 \cdot x_2 + x_1 + 19$ ein solches Polynom.

Bei einer *Diophantischen Gleichung* wird gefragt, ob es ganzzahlige Nullstellen von p gibt, also danach, ob es einen Vektor $\vec{x} = (x_1, x_2, \dots, x_k) \in \mathbb{Z}^k$ mit $p(x_1, x_2, \dots, x_k) = 0$.

Die Sprache $\text{DIOGL} := \{ \langle p \rangle \mid p \text{ ist Polynom mit ganzzahligen Koeffizienten und ganzzahligen Nullstellen} \}$ ist dann das Problem der Diophantischen Gleichungen.

Betrachten Sie nun folgende nichtdeterministische Turingmaschine: Rate Binärdarstellungen für x_1, x_2, \dots, x_k , werte das Polynom an den Stellen x_1, x_2, \dots, x_k aus und akzeptiere, wenn der Wert 0 ist.

Beweist dieser Algorithmus, daß $\text{DIOGL} \in \text{NP}$ ist?

AUFGABE 38 (4 Punkte):

[+ + +, **] Eine nichtdeterministische 2-Phasen-2-Band-Turingmaschine M_2 Phasen, arbeitet wie folgt: Zu Beginn einer Rechnung (in der Phase 1) darf die Eingabe x , die auf Band 1 steht, nicht gelesen werden, sondern es darf nur auf Band 2 nichtdeterministisch etwas berechnet werden. Die Phase 1 wird beendet durch eine „nichtdeterministische“ Entscheidung, die Phase 1 zu beenden. Ab nun, in Phase 2, darf M_2 Phasen auf die Eingabe x (und den Inhalt von Band 2) zugreifen, aber es darf keine nichtdeterministischen Schritte mehr geben, sie ist in der Phase 2 deterministisch.

Zeigen Sie: Jede beliebige nichtdeterministische 1-Band-Turingmaschine M mit Laufzeit $t(n)$ kann durch eine nichtdeterministische 2-Phasen-2-Band-Turingmaschine M_2 Phasen mit Laufzeit $O(t(n))$ simuliert werden.

AUFGABE 39 (4 Punkte):

[+ +, **] Sei $G = (V, E)$ ein ungerichteter Graph. Eine Teilmenge $C \subseteq V$ der Knotenmenge heißt (wie bereits in der Vorlesung definiert) *Clique*, wenn gilt: $\forall \{u, v\} \subseteq C, u \neq v : \{u, v\} \in E$.

Das *Cliquenproblem* ist die Sprache

$$\text{CLIQUE} = \{ \langle G, k \rangle \mid \text{der Graph } G \text{ enthält eine Clique } C \text{ mit } |C| = k \} .$$

- (a) Zeigen Sie: C ist genau dann eine Clique von G , wenn C eine unabhängige Menge (vgl. Aufgabe 32 auf Blatt 6) des Komplementgraphen \bar{G} von G ist.

Der Komplementgraph entsteht aus G , indem man alle in G vorhandenen Kanten löscht und die in G fehlenden Kanten hinzufügt. Formal können wir \bar{G} so beschreiben: $\bar{G} = (V, \bar{E})$ mit $\bar{E} = \{ \{u, v\} \mid u, v \in V, u \neq v, \{u, v\} \notin E \}$.

Machen Sie sich die Begriffe Clique und Komplementgraph an dem Graphen G aus Aufgabe 32 klar.

- (b) Beschreiben Sie einen Algorithmus, der CLIQUE entscheidet und der den Algorithmus $M_{\text{ent-IS}}$ aus Aufgabe 30(b) aufrufen darf. Was ist seine Laufzeit?

Hinweis: Als Ergebnis dieser Aufgabe haben Sie CLIQUE in (hoffentlich) Polynomzeit auf IS reduziert, also $\text{CLIQUE} \leq_p \text{IS}$ bewiesen ...

AUFGABE 40 (4 Punkte):

[+ + +, *] Zeigen Sie: Ist $P = \text{NP}$, dann ist jede Sprache $L \in P$ mit $\emptyset \neq L \neq \{0, 1\}^*$ sogar NP-vollständig.

Hinweis: Diesmal dürfen Sie in die Reduktionsfunktion die Lösung des Problems hineinpacken, was sonst ja strikt verboten ist.

Die Annahme $P = \text{NP}$ hat zur Folge, daß dann z. B. die Sprache $L = \{0, 1\}$ NP-vollständig ist, d. h. daß $\text{SAT} \leq_p L$ gilt. Vermuten Sie, daß das wirklich gilt? ☺

AUFGABE 41 (4 Punkte):

[+ +, **] Sei $K = \ell_1 \vee \dots \vee \ell_n$ eine Klausel aus n Literalen über den verschiedenen Variablen (x_1, \dots, x_n) .

Zur Erinnerung: Ein Literal ist entweder eine Boolesche Variable oder eine negierte Boolesche Variable. Ein Beispiel für eine Klausel ist $K = x_1 \vee \bar{x}_2 \vee \bar{x}_3 \vee x_4$. Eine Belegung c ist eine Zuordnung von Wahrheitswerten (dargestellt durch 0 für FALSE und 1 für TRUE) auf die Variablen, z. B. $c_1 = (0, 1, 1, 0)$ und $c_2 = (1, 0, 1, 0)$. $c(K)$ beschreibt den Wahrheitswert der Klausel, der sich durch Auswertung von K unter der Belegung c ergibt, also $c_1(K) = 0$ und $c_2(K) = 1$.

- Sei $k \in \mathbb{N}$. Konstruieren Sie zur Klausel K einen Booleschen Ausdruck Φ_K in Konjunktiver Normalform über den $n + k$ verschiedenen(!) Variablen $(x_1, \dots, x_n, y_1, \dots, y_k)$, so daß für jede Belegung c der Variablen gilt: $c(K) = c(\Phi_K)$. Man soll also sagen können, daß man das Ergebnis der Auswertung von Φ_K unter c schon bekommt, wenn man K unter c auswertet. Die Belegung der Variablen y_1, \dots, y_k ist gewissermaßen egal.
- Zu einer beliebigen KNF Ψ bezeichnet $\text{size}(\Psi)$ die Anzahl der in ihr vorkommenden Symbole \wedge und \vee . Es ist $\text{size}(K) = n - 1$. Bestimmen Sie $\text{size}(\Phi_K)$.

Ein Beispiel: Betrachten Sie mit der Klausel K von oben und $k = 1$ die KNF $\Phi_K = (K \vee y_1) \wedge (K \vee \bar{y}_1)$. Egal wie Sie y_1 in einer Belegung c wählen, nie ist $c(K) \neq c(\Phi_K)$. Mit anderen Worten, K wird um k Variablen künstlich verlängert, die nichts am Wahrheitswert einer Belegung der Variablen von K ändern können. Es ist $\text{size}(K) = 3$ und $\text{size}(\Phi_K) = 9$.

Auf den folgenden Seiten kommt eine vielleicht interessante Fußnote zur Geschichte des P-NP-Problems.

In der Vorlesung wurde erwähnt, daß Steven Cook von der University of Toronto 1971 das Konzept der NP-Vollständigkeit eingeführt hat.

Im Archiv der *Library of Congress* in Washington findet sich der hier wiedergegebene Brief, den Kurt Gödel im März 1956 an John v. Neumann schrieb. Beide waren zu der Zeit in Princeton, aber an unterschiedlichen Instituten, tätig. Damals schrieb man noch sorgfältig formulierte Briefe mit der Hand und verschickte sie per Post. © Die erste E-Mail wurde erst Ende 1971 verschickt . . .

Vor ihrer Auswanderung in die USA waren die beiden in Österreich-Ungarn geborenen Wissenschaftler an deutschsprachigen Universitäten tätig: der Österreicher Gödel an der Universität Wien und der Ungar v. Neumann an der Humboldt-Universität zu Berlin, der Universität Göttingen und der Universität Hamburg. Deswegen korrespondierten die beiden auch in den USA in deutscher Sprache. Eine Faksimile dieses Briefes finden Sie auf den Seiten 613/614 des Papers

M. Sipser. The history and status of the P versus NP question. Proc. 24th *ACM Symposium on Theory of Computing (STOC)*, pp. 603–618, 1992,

das Sie unter dem URL <http://www.win.tue.nl/~gwoegi/sipser.pdf> downloaden können.

Der längere Mittelabschnitt kommt der P-NP-Problematik und ausgerechnet dem Erfüllbarkeitsproblem verblüffend nah. Denken Sie auch an den Verifizierer der Vorlesung und die Formulierung „ob F einen Beweis der Länge n hat“ in Gödels Brief.

Die in der Vorlesung häufiger ☺ angesprochene Frage, ob es für die NP-vollständigen Probleme bessere Verfahren als das „dumme“ Ausprobieren gibt, findet sich in der Formulierung „wie stark im allgemeinen bei finiten kombinatorischen Problemen die Anzahl der Schritte gegenüber dem blossen Probieren verringert werden kann.“

Es ist leider nicht bekannt, ob v. Neumann auf diesen Brief geantwortet hat. Man vermutet, daß er es nicht hat, da er zu diesem Zeitpunkt bereits schwer erkrankt war. Am 8. Februar 1957 ist er gestorben.

Princeton, 20./III. 1956

Lieber Herr v. Neumann!

Ich habe mit grösstem Bedauern von Ihrer Erkrankung gehört. Die Nachricht kam mir ganz unerwartet. Morgenstern hatte mir zwar schon im Sommer von einem Schwächeanfall erzählt, den Sie einmal hatten, aber er meinte damals, dass dem keine grössere Bedeutung beizumessen sei. Wie ich höre, haben Sie sich in den letzten Monaten einer radikalen Behandlung unterzogen u. ich freue mich, dass diese den gewünschten Erfolg hatte u. es Ihnen jetzt besser geht. Ich hoffe u. wünsche Ihnen, dass Ihr Zustand sich bald noch weiter bessert u. dass die neuesten Errungenschaften der Medizin, wenn möglich, zu einer vollständigen Heilung führen mögen.

Da Sie sich, wie ich höre, jetzt kräftiger fühlen, möchte ich mir erlauben, Ihnen über ein mathematisches Problem zu schreiben, über das mich Ihre Ansicht sehr interessieren würde: Man kann offenbar leicht eine Turingmaschine konstruieren, welche von jeder Formel F des engeren Funktionenkalküls u. jeder natürl. Zahl n zu entscheiden gestattet, ob F einen Beweis der Länge n hat [Länge = Anzahl der Symbole]. Sei $\psi(F, n)$ die Anzahl der Schritte, die die Maschine dazu benötigt u. sei $\varphi(n) = \max_F \psi(F, n)$. Die Frage ist, wie rasch $\varphi(n)$ für eine optimale Maschine wächst. Man kann zeigen $\varphi(n) \geq K \cdot n$. Wenn es wirklich eine Maschine mit $\varphi(n) \sim K \cdot n$ (oder auch nur $\sim K \cdot n^2$) gäbe, hätte das Folgerungen von der grössten Tragweite. Es würde nämlich offenbar bedeuten, dass man trotz der Unlösbarkeit des Entscheidungsproblems die Denkarbeit des Mathematikers bei ja-oder-nein Fragen vollständig durch Maschinen ersetzen könnte. Man müsste ja bloss das n so gross wählen, dass, wenn die Maschine kein Resultat liefert, es auch keinen Sinn hat über das Problem nachzudenken. Nun scheint es mir aber durchaus im Bereich der Möglichkeit zu liegen, dass $\varphi(n)$ so langsam wächst. Denn 1.) scheint $\varphi(n) \geq K \cdot n$ die einzige Abschätzung zu sein, die man durch eine Verallgemeinerung des Beweises für die Unlösbarkeit des Entscheidungsproblems erhalten kann; 2.) bedeutet ja $\varphi(n) \sim K \cdot n$ (oder $\sim K \cdot n^2$) bloss, dass die Anzahl der Schritte gegenüber dem blossen Probieren von N auf $\log N$ (oder $(\log N)^2$) verringert werden kann. So starke Verringerungen kommen aber bei anderen finiten Problemen durchaus vor, z. B. bei der Berechnung eines quadratischen Restsymbols durch wiederholte Anwendung des Reziprozitätsgesetzes. Es wäre interessant zu wissen, wie es damit z. B. bei der Feststellung, ob eine Zahl Primzahl ist, steht u. wie stark im allgemeinen bei finiten kombinatorischen Problemen die Anzahl der Schritte gegenüber dem blossen Probieren verringert werden kann.

Ich weiss nicht, ob Sie gehört haben, dass “Post’s problem” (ob es unter den Problemen $(\exists y)\varphi(y, x)$ mit rekursivem φ Grade der Unlösbarkeit gibt) von einem ganz jungen Mann namens Richard Friedberg in positivem Sinn gelöst wurde. Die Lösung ist sehr elegant. Leider will Friedberg nicht Mathematik, sondern Medizin studieren (scheinbar unter dem Einfluss seines Vaters).

Was halten Sie übrigens von den Bestrebungen, die Analysis auf die verzweigte Typentheorie zu begründen, die neuerdings wieder in Schwung gekommen sind? Es ist Ihnen wahrscheinlich bekannt, dass Paul Lorenzen dabei bis zur Theorie des Lebesgueschen Masses vorgedrungen ist. Aber ich glaube, dass in wichtigen Teilen der Analysis nicht eliminierbare imprädikative Schlussweisen vorkommen.

Ich würde mich sehr freuen, von Ihnen persönlich etwas zu hören; u. bitte lassen Sie es mich wissen, wenn ich irgend etwas für Sie tun kann.

Mit besten Grüßen u. Wünschen, auch an Ihre Frau Gemahlin.

Ihr sehr ergebener

Kurt Gödel

PS. Ich gratuliere Ihnen bestens zu der Auszeichnung, die Ihnen von der amerik. Regierung verliehen wurde.

^aabgesehen von der Aufstellung der Axiome