Prof. Dr. Rolf Wanka
Bernd Bassimir, Alexander Raß, Jonas Schreiner,
Stefan Schwanecke, Jeanette Wohnig

Erlangen, 11. Dezember 2018

Abgabe bis Di., 18.12.18, 23:59 Uhr

Übungen zur Vorlesung

Berechenbarkeit und Formale Sprachen

WS 2018/2019

Blatt 7

Je mehr Plus-Zeichen $+$, desto wichtiger, je mehr Sterne $\star$, desto schwieriger.

AUFGABE 35:
[Präsenzaufgabe, $+++, \star\star$]

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

Zeigen Sie:

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

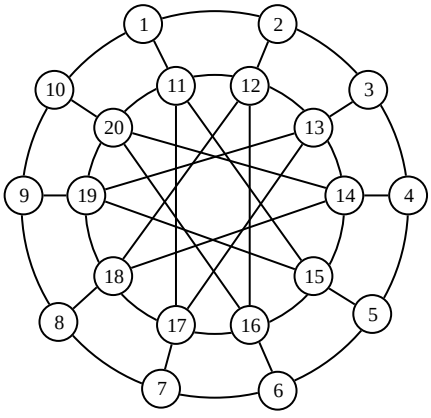
(b) Sei $p(x_1,x_2,\ldots,x_k)$ ein Polynom mit ganzzahligen Koeffizienten (d. h. Koeffizienen aus $\mathbb{Z}$). Z. B. ist $p(x_1,x_2,x_3) = 5\cdot x_1^4\cdot x_3^2 - 12\cdot x_2^2\cdot x_3^5 - x_1\cdot x_2 + x_1 + 19$ ein solches Polynom.

Bei einer *Diophantischen Gleichung* wird gefragt, ob es ganzzahlige Nullstellen von p gibt, also danach, ob es einen Vektor $\bar{x} = (x_1,x_2,\ldots,x_k) \in \mathbb{Z}^k$ mit $p(x_1,x_2,\ldots,x_k) = 0$ gibt. Das Polynom $p(x,y) = x^2 - 5y^2 + 1$ hat solche Nullstellen, z. B. $(x,y) = (2,1)$.

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

Betrachten Sie nun folgende nichtdeterministische Turingmaschine: Die Eingabe sei $\langle p\rangle$. Rate Binärdarstellungen für $x_1,x_2,\ldots,x_k$, werte das Polynom an den Stellen $x_1,x_2,\ldots,x_k$ aus und akzeptiere $\langle p\rangle$, wenn der Wert 0 ist. Beweist *dieser* Algorithmus, daß $\textsc{DioGL} \in$ NP ist? (Stichwort, falls Sie googlen möchten: 10. Hilbertsches Problem) Beweist dieser Algorithmus überhaupt etwas? (Hinweis: Korollar 2.4)

AUFGABE 36 (4 Punkte)**:**
$[+++, \star]$ Gegeben sei der rechts dargestellte Graph G:



(a) Hat G einen Hamiltonkreis, d. h. ist $\langle G\rangle \in \text{HC}$?

(b) Hat G eine Knotenüberdeckung der Größe 10, d. h. ist $\langle G,10\rangle \in \text{VC}$?

(c) Können die Knoten so mit zwei Farben gefärbt werden, daß benachbarte Knoten unterschiedliche Farben besitzen (vgl. Aufgabe 35(a)), d. h. ist $\langle G,2\rangle \in \textsc{Col}$?

(d) Bestimmen Sie eine möglichst große unabhängige Knotenmenge U (vgl. Aufgabe 30 auf Blatt 6) und begründen Sie, warum es keine größere unabhängige Knotenmenge gibt.

AUFGABE 37 (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: $\forall\{u,v\} \subseteq C, u \neq v : \{u,v\} \in E$. (Machen Sie sich hier auch mal wieder mit der Kompaktheit mathematischer Formulierungen vertraut. ☺)
Das *Cliquenproblem* ist die Sprache $\text{CLIQUE} = \{\langle G,k\rangle \mid \text{der Graph } G \text{ enhält eine Clique } C \text{ mit } |C| = k\}$.

(a) Zeigen Sie: C ist genau dann eine Clique von G, wenn C eine unabhängige Menge (vgl. Aufgabe 30 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 30 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 $\text{CLIQUE} \leq_\text{p} \text{IS}$ bewiesen … ✌

AUFGABE 38 (4 Punkte)**:**
[++++, ⋆⋆] Zeigen Sie: Ist P = NP, dann ist *jede* Sprache $L \in \text{P}$ 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 = NP hat zur Folge, daß dann z. B. die Sprache $L = \{0,1\}$ NP-vollständig ist, d. h. daß $\text{SAT} \leq_\text{p} L$ gilt. Vermuten Sie, daß das wirklich gilt? ☺

AUFGABE 39 (4 Punkte)**:**
[++++, ⋆] Sei H das Halteproblem.

(a) Zeigen Sie: $\text{SAT} \leq_\text{p} H$

(b) Warum folgt, daß H somit NP-schwer ist? Könnte sich H sogar als NP-vollständig erweisen?

Hinweis: Ja, der einzelne ⋆ ist richtig, und ja, es gibt wirklich eine *Polynomialzeit*reduktion.

AUFGABE 40 (4 **Bonus**- Punkte)**:**
[++, ⋆⋆⋆⋆] Bezeichne $\text{BB}(n)$ die Busy-Beaver-Funktion aus Aufgabe 24 auf Blatt 4. In Aufgabe 34 auf Blatt 6 wurde gezeigt, daß die Sprache $\mathcal{BB}_1 = \{\langle n, \text{BB}(n)\rangle \mid n \in \mathbb{N}\}$ nicht rekursiv aufzählbar ist. Nun betrachten wir die Sprache $\mathcal{BB}_2 = \{\langle \text{BB}(n)\rangle \mid n \in \mathbb{N}\}$.

Zeigen Sie, daß $\mathcal{BB}_2$ nicht rekursiv aufzählbar ist.

Hinweis: Sie benötigen vermutlich eine universelle Turing-Maschine mit fester Zustandszahl k, das initiale Halteproblem H_ε und die strenge Monotonie von $\text{BB}(n)$.

Auf den folgenden zwei 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 Brief-Post.☺ Die erste E-Mail überhaupt wurde erst Ende 1971 verschickt, und die erste E-Mail in Deutschland 1984 ...

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. doi:10.1145/129712.129771

das Sie unter dem URL `http://dx.doi.org/10.1145/129712.129771` downloaden können.

Der längere Mittelabschnitt kommt der P-NP-Problematik und ausgerechnet (oder naheliegenderweise) dem Erfüllbarkeitsproblem verblüffend nah. Sie sehen, daß 1956 der Begriff der Turing-Maschine bereits Standard war und auch gegenüber dem Wissenschaftler, der den von-Neumann-Rechner (also unsere RAM) einführte, benutzt wurde.
Denken Sie beim Lesen 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[a] 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 Reziprozitätsgesetztes. 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, das 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.

[a] abgesehen von der Aufstellung der Axiome