max planck institut
informatik

P versus NP

Kurt Mehlhorn und Adrian Neumann

Max Planck Institute for Informatics and Saarland University

1. Dezember 2013

Gliederung

- Informelle Formulierung des P = NP Problems
- Das Erfüllbarkeitsproblem der Aussagenlogik (SATisfiability Problem)
- Ausdruckskraft von SAT
- P und NP
- NP-Vollständigkeit
- Was wäre wenn P $\neq$ NP?
- Was wäre wenn P $=$ NP?
- Wie geht man mit NP-Vollständigkeit um?
- Beweis des Satzes von Cook-Levine (falls noch Zeit)

Das P = NP Problem (informelle Formulierung)

Gibt es Probleme, für die es schwieriger ist, eine Lösung zu finden als eine Lösung zu überprüfen?

Antwort: natürlich,

- meine Analysisübungsblätter
- Sudoku und Kreuzworträtsel
- Problem des Handlungsreisenden: gibt es eine Tour durch die alle Orte Deutschlands mit mehr als 5 Tausend Einwohnern, die höchstens 4000 Kilometer lang ist?
- Facility Location
- Rucksackproblem
- ...

Das P = NP Problem (informelle Formulierung)

Gibt es Probleme, für die es schwieriger ist, eine Lösung zu finden als eine Lösung zu überprüfen?

Antwort: natürlich,

- meine Analysisübungsblätter
- Sudoku und Kreuzworträtsel
- Problem des Handlungsreisenden: gibt es eine Tour durch die alle Orte Deutschlands mit mehr als 5 Tausend Einwohnern, die höchstens 4000 Kilometer lang ist?
- Facility Location
- Rucksackproblem
- ...

Das Erfüllbarkeitsproblem (SATisfiability-Problem)

Eingabe: Eine Formel der Aussagenlogik

Frage: Ist die Formel erfüllbar, d.h., gibt es eine Belegung der Variablen mit Wahrheitswerten, die die Formel erfüllt?

Beispiel

Formel: $(x \vee y) \wedge \neg x$

Belegung 1: $x \to T$, $y \to F$, dann $(T \vee F) \wedge \neg T = T \wedge F = F$

Belegung 2: $x \to F$, $y \to T$, dann $(F \vee T) \wedge \neg F = T \wedge T = T$

Das Erfüllbarkeitsproblem (SATisfiability-Problem)

Eingabe: Eine Formel der Aussagenlogik

Frage: Ist die Formel erfüllbar, d.h., gibt es eine Belegung der Variablen mit Wahrheitswerten, die die Formel erfüllt?

Das P versus NP Problem

Gibt es einen Polynomzeitalgorithmus für das Erfüllbarkeitsproblem?

Die Clay Stiftung hat für die Lösung dieses Problems einen Preis von 1 Million Dollar ausgesetzt.

Formeln der Aussagenlogik

(1) T (true, wahr), F (falsch, false) und Variablen sind Formeln.
(2) Wenn F und G Formeln sind, dann auch $(F \wedge G)$, $(F \vee G)$, und $\neg F$. Bei Variablen schreiben wir statt $\neg x$ auch $\overline{x}$.
(3) Das ist alles.

Belegung, Wert einer Formel, erfüllbar

Eine Belegung weist jeder Variablen einen Wahrheitswert zu.

Der Wert der Formel ergibt sich nach den Berechnungsregeln der Aussagenlogik: $F \vee F = F$, $F \vee T = T \vee F = T \vee T = T$, $F \wedge F = F \wedge T = T \wedge F = F$, $T \wedge T = T$, $\neg F = T$ und $\neg T = F$.

Eine Formel ist erfüllbar, wenn es eine Belegung gibt, unter der sie den Wert wahr erhält.

Das P versus NP Problem

Gibt es Polynomzeitalgorithmus für das Erfüllbarkeitsproblem?

Polynomzeitalgorithmus, polynomzeitbeschränkte Turingmaschine

Eine Turingmaschine M, die an jeder Eingabe in einer polynomiellen Anzahl von Schritten anhält.

Genauer: Es gibt ein Polynom p, so dass M an einer beliebigen Eingabe x in höchstens $p(|x|)$ Schritten anhält.

Dabei ist $|x|$ die Länge von x (Anzahl der Zeichen).

Das P versus NP Problem

Gibt es Polynomzeitalgorithmus für das Erfüllbarkeitsproblem?

Polynomzeitalgorithmus für das Erfüllbarkeitsproblem

Eine polynomzeitbeschränkte Turingmaschine M, die das Erfüllbarkeitsproblem entscheidet,

d.h. die für jede Eingabe φ (beliebige aussagenlogische Formel) in höchstens $p(|\varphi|)$ Schritten anhält und den Status von φ ausgibt: erfüllbar oder nicht erfüllbar.

Dabei ist $|\varphi|$ die Länge von φ (Anzahl der Zeichen), etwa $|((x_{100} \wedge x_{20}) \vee x_{25})| = 16$, und p ein Polynom.

Das P versus NP Problem

Gibt es Polynomzeitalgorithmus für das Erfüllbarkeitsproblem?

Warum ist das Erfüllbarkeitsproblem so wichtig?

Wofür stehen P und NP?

Bedeutung des Erfüllbarkeitproblems

Wenn man einen Polynomzeitalgorithmus für das Erfüllbarkeitsproblem kennt, dann kennt man auch Polynomzeitalgorithmen für

1. Graphenfärbung
2. Hamiltonscher Kreis
3. Problem des Handlungsreisenden
4. Rucksackproblem
5. Partition
6. Sudoku
7. ....
8. jedes Problem in NP

Graphenfärbung (mit drei Farben)

Eingabe: Ein ungerichteter Graph $G = (V, E)$

Frage: Gibt es eine Dreifärbung der Knoten von G, d.h. eine Abbildung $f : V \to \{R, B, G\}$, so dass für jede Kante $\{u, v\} \in E$ gilt: $f(u) \neq f(v)$.

Reduktion: Färbung $\leq$ SAT

Variable $x_{u,c}$ für Knoten $u \in V$ und Farbe $c \in \{R, B, G\}$.

Intendierte Bedeutung: $x_{u,c} = T$ bedeutet u hat die Farbe c.

Formel:

$$\bigwedge_{u \in V} GE(x_{u,R}, x_{u,B}, x_{u,G}) \wedge \bigwedge_{\{u,v\} \in E} \bigwedge_{c \in \{R,B,G\}} \neg(x_{u,c} \wedge x_{v,c})$$

Dabei ist $GE(x_1, \ldots, x_n) = (\bigvee_i x_i) \wedge \neg(\bigvee_{i \neq j}(x_i \wedge x_j))$. GenauEine

Korrektheit der Reduktion

Reduktion: Färbung $\leq$ SAT

Variable $x_{u,c}$ für Knoten $u \in V$ und Farbe $c \in \{R, B, G\}$.

Intendierte Bedeutung: $x_{u,c} = T$ bedeutet u hat die Farbe c.

$$\bigwedge_{u \in V} GE(x_{u,R}, x_{u,B}, x_{u,G}) \wedge \bigwedge_{\{u,v\} \in E} \bigwedge_{c \in \{R,B,G\}} \neg(x_{u,c} \wedge x_{v,c})$$

Korrektheit der Reduktion

Sei $f : V \to \{R, B, G\}$ eine legale Färbung. Setze $x_{u,c} = T$ genau wenn $f(u) = c$. Diese Belegung erfüllt die Formel.

Reduktion: Färbung $\leq$ SAT

Variable $x_{u,c}$ für Knoten $u \in V$ und Farbe $c \in \{R, B, G\}$.

Intendierte Bedeutung: $x_{u,c} = T$ bedeutet u hat die Farbe c.

$$\bigwedge_{u \in V} GE(x_{u,R}, x_{u,B}, x_{u,G}) \wedge \bigwedge_{\{u,v\} \in E} \bigwedge_{c \in \{R,B,G\}} \neg(x_{u,c} \wedge x_{v,c})$$

Korrektheit der Reduktion

Sei b eine erfüllende Belegung. Definiere $f(u) = c$ genau wenn $b(x_{u,c}) = T$.

Da die Belegung $GE(x_{u,R}, x_{u,B}, x_{u,G})$ erfüllt, ist f wohldefiniert.

Betrachte eine beliebige Kante $\{u, v\}$: Da die Belegung $\bigwedge_{c \in \{R,B,G\}} \neg(x_{u,c} \wedge x_{v,c})$ erfüllt, haben u und v nicht die gleiche Farbe.

Reduktion: Färbung $\leq$ SAT

Variable $x_{u,c}$ für Knoten $u \in V$ und Farbe $c \in \{R, B, G\}$.

Intendierte Bedeutung: $x_{u,c} = T$ bedeutet u hat die Farbe c.

$$\bigwedge_{u \in V} GE(x_{u,R}, x_{u,B}, x_{u,G}) \wedge \bigwedge_{\{u,v\} \in E} \bigwedge_{c \in \{R,B,G\}} \neg(x_{u,c} \wedge x_{v,c})$$

Korrektheit der Reduktion

Die Formel hat Länge $O((n+m)\log n)$, da

es für jeden Knoten und jede Kante eine Teilformel konstanter Größe gibt.

das $\log n$ trägt der Tatsache Rechnung, dass die Variablennamen logarithmische Länge haben.

Weitere Probleme $\leq$ SAT

Hamiltonscher Kreis

Eingabe: Ein ungerichteter Graph $G = (V, E)$

Frage: Gibt es eine Anordnung $v_1, \ldots, v_n$ der Knoten, so dass $\{ v_i, v_{i+1} \} \in E$ für $1 \leq i \leq n$? Dabei sei $v_{n+1} = v_1$.

Rucksackproblem

Eingabe: n Objekte, je mit einem ganzzahligen Gewicht g_i und einem ganzahligen Wert w_i. Zielwert W und Gewichtsbeschränkung G.
Frage: Gibt es eine Teilmenge $I \subseteq \{1, \ldots, n\}$, so dass $\sum_{i \in I} g_i \leq G$ und $\sum_{i \in I} w_i \geq W$?

Tausend Weitere

siehe Compendium of NP-complete Problems

Weitere Probleme $\leq$ SAT

Hamiltonscher Kreis

Eingabe: Ein ungerichteter Graph $G = (V, E)$

Frage: Gibt es eine Anordnung $v_1, \ldots, v_n$ der Knoten, so dass $\{ v_i, v_{i+1} \} \in E$ für $1 \leq i \leq n$? Dabei sei $v_{n+1} = v_1$.

Rucksackproblem

Eingabe: n Objekte, je mit einem ganzzahligen Gewicht g_i und einem ganzahligen Wert w_i. Zielwert W und Gewichtsbeschränkung G.
Frage: Gibt es eine Teilmenge $I \subseteq \{ 1, \ldots, n \}$, so dass $\sum_{i \in I} g_i \leq G$ und $\sum_{i \in I} w_i \geq W$?

Tausend Weitere

siehe Compendium of NP-complete Problems

Weitere Probleme $\leq$ SAT

Hamiltonscher Kreis

Eingabe: Ein ungerichteter Graph $G = (V, E)$

Frage: Gibt es eine Anordnung $v_1, \ldots, v_n$ der Knoten, so dass $\{ v_i, v_{i+1} \} \in E$ für $1 \leq i \leq n$? Dabei sei $v_{n+1} = v_1$.

Rucksackproblem

Eingabe: n Objekte, je mit einem ganzzahligen Gewicht g_i und einem ganzahligen Wert w_i. Zielwert W und Gewichtsbeschränkung G.
Frage: Gibt es eine Teilmenge $I \subseteq \{ 1, \ldots, n \}$, so dass $\sum_{i \in I} g_i \leq G$ und $\sum_{i \in I} w_i \geq W$?

Tausend Weitere

siehe Compendium of NP-complete Problems

Problem

Sei Σ ein festes Alphabet. Eine Teilmenge von Σ^* heißt Problem.

P (Polynomzeitentscheidbar)

Ein Problem L gehört zu P, wenn es eine polynomzeitbeschränkte Turingmaschine M gibt, die L einscheidet, d.h.
an einer beliebigen Eingabe x gibt M entweder JA oder NEIN aus und es gilt $x \in L$ genau wenn die Ausgabe JA ist.

Beispiele für Probleme in P

1. $L = \{ x_1 \# \ldots \# x_n \# w;\ w = x_i \text{ für ein } i \}$
2. $L = \{ G = (V, E);\ G \text{ is zweifärbbarer Graph} \}$, d.h. es gibt $f : V \to \{ R, B \}$, so dass $f(u) \neq f(v)$ für alle $\{ u, v \} \in E$.
3. Lineare Gleichungssysteme, Kürzeste Wege, maximale Flüsse, ...

P (Polynomzeitentscheidbar)

Ein Problem L gehört zu P, wenn es eine polynomzeitbeschränkte Turingmaschine M gibt, die L einscheidet,

NP (Polynomzeitentscheidbar mit Raten)

Ein Problem L gehört zu NP, wenn es ein Problem L' in P und ein Polynom q gibt, so dass gilt:

$$x \in L \text{ genau wenn es ein } w \in (\Sigma \setminus \#)^* \text{ gibt, so dass } |w| \leq q(|x|) \text{ und } x\#w \in L'.$$

wir sagen: w bezeugt (beweist) die Mitgliedschaft von x.

man erhält L aus L' wie folgt: Betrachte ein beliebiges Wort in L'. Falls es kein # enthält, trägt es nicht zu L bei. Anderfalls schreibe das Wort als $x\#w$, wobei w kein # enthält. Falls $|w| \leq q(|x|)$, dann $x \in L$.

NP (Polynomzeitentscheidbar mit Raten)

Ein Problem L gehört zu NP, wenn es ein Problem L' in P und ein Polynom q gibt, so dass gilt:

$$x \in L \text{ genau wenn es ein } w \in (\Sigma \setminus \#)^* \text{ gibt, so dass } |w| \leq q(|x|) \text{ und } x\#w \in L'.$$

wir sagen: w bezeugt (beweist) die Mitgliedschaft von x.

Beispiele für Probleme in NP

1. Erfüllbarkeitsproblem: $x =$ aussagenlogische Formel, $w =$ erfüllende Belegung
2. Knapsackproblem: $x =$ Problemstellung, $w =$ leichte Teilmenge mit hohem Wert
3. Nichtprimzahlen: $x =$ eine natürliche Zahl, $w =$ eine nicht-triviale Faktorisierung
4. Sudoku: $x =$ Spielplan, $w =$ Lösung

SAT ist ein schwerstes Problem in NP

Satz (Stephen Cook und Leonid Levin, 71)

Falls es einen Polynomzeitalgorithmus für das Erfüllbarkeitsproblem gibt, dann gibt es einen Polynomzeitalgorithmus für jedes Problem in NP.

The class NP was defined and the theorem above was proved independently by Stephen Cook (University of Toronto) and Leonid Levin (then Moscow, now Boston) in 1971.
Stephen Cook was denied tenure by the Berkeley Math department in 1970.
Cook is a recipient of the 1982 Turing Award. Levin is a recipient of the 2012 Knuth Prize.

P versus NP

$P \subseteq NP$

Sei L in P beliebig. Definiere $L' = \{ x\#; x \in L \}$. Dann ist sicher $L' \in P$. Also gilt $L \in NP$.

Das P = NP Problem (formal)

Ist P = NP?

Das P = NP Problem (informelle Formulierung)

Gibt es Probleme, für die es schwieriger ist, eine Lösung zu finden als eine Lösung zu überprüfen?

P versus NP

$P \subseteq NP$

Sei L in P beliebig. Definiere $L' = \{ x\#; x \in L \}$. Dann ist sicher $L' \in P$. Also gilt $L \in NP$.

Das P = NP Problem (formal)

$$\text{Ist } P = NP?$$

Das P = NP Problem (informelle Formulierung)

Gibt es Probleme, für die es schwieriger ist, eine Lösung zu finden als eine Lösung zu überprüfen?

NP-Vollständigkeit

Definition

Ein Problem L in NP ist NP-vollständig, wenn aus $L \in P$ folgt $\mathrm{P} = \mathrm{NP}$.

Cook-Levine bewiesen, dass das Erfüllbarkeitsproblem NP-vollständig ist.

Satz (Karp, 1972)

Das Graphenfärbungsproblem, das Hamiltonsche Kreisproblem, Knapsack, und 20 andere Probleme sind NP-vollständig.

Die Liste ist inzwischen auf mehrere Tausend angewachsen.

Richard Karp erhielt den Turing-Award in 1985.

War wäre, wenn P $\neq$ NP?

- es würde sich nicht viel ändern, denn da wir keinen Polynomzeitalgorithmus für das Erfüllbarkeitsproblem kennen, leben wir faktisch in einer Welt, in der P ungleich NP ist.
- die meisten Fachleute glauben, dass P $\neq$ NP?
- aber: im Augenblick gibt es keinen Ansatz, wie man P $\neq$ NP beweisen könnte. Man weiß nur, dass einige natürliche Ansätze NICHT funktionieren können. Wenn man einen Beweis findet, muss dieser eine neue Methode einführen. Diese Methode könnte weitere Anwendungen haben.
- alle paar Jahre wird ein (falscher) Beweis angekündigt.

War wäre, wenn P = NP?

- das wäre eine Revolution
- wir hätten Polynomzeitalgorithmen für Erfüllbarkeit, ...,
- Mathematiker würden arbeitslos:

  Input: ein mathematischer Satz S, eine Anzahl n unbeschriebener Blätter

  Frage: gibt es einen Beweis für S (in einem formalen System), der auf die n Blätter passt?

  Dieses Problem ist in NP. Falls P = NP, dann ist dieses Problem in P.
- alle paar Monate wird ein (falscher) Beweis angekündigt.

Wie geht man mit NP-Vollständigkeit um?

- Heuristiken
- Exakte Algorithmen für kleine n
- Speziallfälle
- Approximationsalgorithmen