Hintergrund und Bedeutung des $P \neq NP$ Problems

Franziska Rapp

Einführung in das wissenschaftliche Arbeiten

Leopold Franzens Universität Innsbruck, Fachbereich Informatik

1. Juni 2012

Inhaltsverzeichnis

1 Einleitung

Das $P \neq NP$ Problem (auch P versus NP Problem genannt) ist das neueste der sieben Millennium-Probleme, die vom Clay Mathematics Institute im Jahr 2000 als Liste von wichtigen ungelösten Problemen der Mathematik festgelegt wurde. Für die Lösung jedes dieser Probleme ist ein Preisgeld von einer Million US-Dollar ausgeschrieben worden. Es lohnt sich also durchaus, sich etwas näher mit diesem Problem zu beschäftigen, auch wenn es für einen Nichtmathematiker schwer sein dürfte, einen Beweis für $P = NP$ oder $P \neq NP$ zu finden. Zuerst werden die notwendigen Definitionen der verschiedenen Komplexitätsklassen angegeben und das Problem kurz erläutert. Darauffolgend wird der Umgang mit der Komplexität von NP Problemen und bisher verwendeten Beweisansätzen erläutert. Abschließend wird die Bedeutung des Problems für die Menschheit aufgezeigt.

2 Definitionen

Die Komplexitätsklasse P ist die Klasse aller Probleme, für die es einen Algorithmus gibt, der das Problem in polynomieller worst case Laufzeit löst. Hierbei ist polynomiell in Bezug auf die Länge der Eingabe gemeint. Diese Probleme sind immer auch auf einer deterministischen Turingmaschine (DTM) in polynomieller Zeit lösbar. Polynomialzeitalgorithmen werden oft auch als „effiziente Algorithmen“ bezeichnet. Demnach ist P auch die Klasse aller Probleme, die effizient gelöst werden können.

Die Komplexitätsklasse NP ist die Klasse aller Probleme, die von einer nichtdeterministischen Turingmaschine in polynomieller Zeit gelöst werden können. Dazu ist es notwendig, dass eine mögliche Lösung von einer deterministischen Turingmaschine in polynomieller Zeit verifiziert werden kann. NP steht für „nichtdeterministisch polynomielle Zeit“. Man sagt auch, NP ist die Klasse aller Probleme, die effizient verifiziert werden können.

Nun gibt es noch die Komplexitätsklasse der NP-vollständigen Probleme (NPC). Eingeführt wurde diese Klasse 1971 von Cook, der zeigte, dass das SAT Problem[1] ein Maximum seiner Klasse ist. Will man nun zeigen, dass ein Problem M in der Klasse NPC liegt, reicht es zu zeigen, dass es in der Klasse NP liegt und eine polynomielle Reduktion des SAT Problems auf M zu konstruieren.

Es ist recht einfach zu zeigen, dass $P \subseteq NP$. Die Frage ist nun, ob $P = NP$ oder $P \subset NP$, was so viel heißt wie $P \neq NP$. Wäre $P = NP$, würde das laut den obigen Definitionen heißen, dass jedes Problem, welches sich effizient verifizieren lässt, auch effizient gelöst werden kann. Noch vor der Definition der Klasse NP tauchte 1956 eine ähnliche Frage in Gödels Brief an von Neumann auf. Definiert wurde das Problem allerdings erst 1971 von Cook und Levin (unabhängig). Bis jetzt wurde weder die eine noch die andere mögliche Lösung bewiesen, obwohl es zahlreiche Beweisansätze und -versuche gab.

3 Behandlung von NP Problemen

Deshalb muss man sich für Probleme, die in der Klasse NP liegen andere Methoden einfallen lassen, um trotzdem zu einer Lösung zu kommen. Ist die Größe der Eingabe klein genug, gibt es keine großen Schwierigkeiten, eine optimale Lösung des Problems in annehmbarer Zeit zu finden. Da reicht sogar manchmal noch die „Brute Force“ Methode, die alle Möglichkeiten durchprobiert. Die Schwierigkeiten wachsen aber mit zunehmender Eingabegröße und sie wachsen so schnell, dass auch zukünftige Generationen nicht auf einen Supercomputer hoffen können, der ihnen eine Lösung für eine etwas größere Eingabegröße mit der „Brute Force“ Methode liefert. Deshalb muss man Algorithmen suchen, die eine Lösung nahe der optimalen liefern. Genauso arbeitet auch ein GPS-System, das versucht, den kürzesten oder schnellsten Weg von A nach B zu finden. Würde es solche Algorithmen nicht geben, müssten wir uns heute immer noch auf der Landkarte unseren

[1] Beim SAT Problem muss herausgefunden werden, ob es eine Variablenbelegung für eine gegebene aussagenlogische Formel gibt, die die Formel wahr werden lässt.

Weg selbst überlegen. Das Traveling Salesman Problem ist NP vollständig.[2] Arora [1] konnte aber effiziente Algorithmen für dieses und eine Menge weiterer NP Probleme finden, die jeweils eine sehr gute Näherung der optimalen Lösung liefern.

4 Beweisansätze

Über die letzten Jahrzehnte wurden die unterschiedlichsten Herangehensweisen an den Beweis von $P \neq NP$ gewählt. Leider wurde für die meisten bisher verwendeten Beweistechniken gezeigt, dass sie allein nicht ausreichen, eine Lösung des Problems zu beweisen. Baker, Gill und Solovay [2] zeigten, dass relativierende Beweistechniken, wie z.B. die Diagonalisierung[3] nicht für einen solchen Beweis geeignet sind.

Um zu zeigen, dass $P \neq NP$, würde es auch genügen zu zeigen, dass es NP vollständige Probleme gibt, die nicht von relativ kleinen Schaltkreisen bestehend aus AND, OR und NOT Gattern gelöst werden können. Mit „relativ klein“ ist hier gemeint, dass die Anzahl der Gatter polynomiell von der Länge der Eingabe abhängen muss. Razborov[4] zeigte 1985, dass das Cliquenproblem, welches NP vollständig ist, solch einen kleinen Schaltkreis nicht hat, wenn man nur AND und OR Gatter verwendet. Das Problem an dem durchaus vielversprechenden Ansatz ist, dass der Beweis scheitert, sobald man auch NOT Gatter zulässt, die aber für einen Beweis (wie oben beschrieben) notwendig wären. Razborov selbst hat den Beweis dazu geliefert.[6]

Mulmuley und Sohoni [5] wählten den Weg der geometrischen Komplexitätstheorie. Dafür haben sie eine Familie hoch-dimensionaler Polygone P_n definiert. Wenn man nun zeigen kann, dass P_n für alle n einen Integralpunkt besitzt, würde das $P \neq NP$ implizieren. Da der direkte Beweis dafür sehr schwierig ist, haben Mulmuley und Sohoni einen Beweisansatz entwickelt, der drei Schritte beinhaltet. Sie haben dabei die Frage nach der Existenz eines Polynomialzeit-Algorithmus für alle NP vollständigen Probleme auf die Frage nach der Existenz eines Polynomialzeit-Algorithmus (mit bestimmten Eigenschaften) für ein spezielles Problem reduziert. Trotz dieses vielversprechenden Ansatzes glaubt Mulmuley, dass es durchaus 100 Jahre dauern könnte, einen solchen Beweis zu liefern, falls es überhaupt funktioniert.

Der aktuellste, erstzunehmende Versuch eines Beweises stammt von dem HP Labs Mitarbeiter Vinay Deolalikar, der 2010 eine erste vorläufige 100-seitige Version seines Beweises veröffentlichte, um ihn von anderen Wissenschaftlern bewerten und korrigieren zu lassen. Die verbesserte Version wird er bald auf seine Website stellen.[5] Es könnte trotzdem noch ein paar Jahre dauern, bis der Beweis angenommen oder abgelehnt wird. Dennoch haben schon einige Journalisten geschrieben, dass das P versus NP Problem möglicherweise gelöst sei. Zumindest wurde bisher noch kein Fehler in der Beweisführung gefunden.

[2] Bei diesem Problem muss eine Reihenfolge für den Besuch einer Menge von Orten so gewählt werden, dass die gesamte Reisestrecke nach der Rückkehr zum Ausgangsort möglichst kurz ist.

[3] Mit Hilfe der Diagonalisierung lässt sich z.B. beweisen, dass die reellen Zahlen überabzählbar sind.

[4] Razborov, Alexander A.: URL: http://www.springerlink.com/content/k0074362858167p8/fulltext.pdf. Stand: 01.06.2012.

[5] Deolalikar, Vinay: URL: http://www.hpl.hp.com/personal/Vinay_Deolalikar. Stand: 30.05.2012.

5 Auswirkungen einer Lösung des Problems

Die meisten theoretischen Informatiker gehen davon aus, dass $P \neq NP$. Das liegt hauptsächlich daran, dass es die näherliegende Variante ist und selbst nach jahrzehntelanger Suche niemand auch nur für eines der vielen Probleme in NP einen Polynomialzeit-Algorithmus finden konnte. Es ist fast unvorstellbar, was sich alles ändern würde, wenn sich herausstellen sollte, dass $P = NP$ gilt. Auch in der Kryptographie wurde davon ausgegangen, dass $P \neq NP$ bzw. dass die Faktorisierung extrem vieler, großer Werte nicht in polynomieller Zeit möglich ist. Das nutzen viele Methoden der Kryptographie. Diese Art der Verschlüsselung wäre mit $P = NP$ allerdings nicht mehr sicher und das könnte sowohl finanziell als auch militärisch katastrophale Konsequenzen haben. Allerdings wären die meisten Folgen positiver Natur. Es gäbe dann effiziente Algorithmen für alle Probleme aus NP. Dadurch könnte man sowohl Menschen als auch Waren einfacher und schneller transportieren. Die Produktion von Unternehmen wäre optimal an die Nachfrage angepasst. Für jedes Theorem, das einen Beweis annehmbarer Länge hat, könnte ein solcher Beweis effizient gefunden werden.[4] Falls jemand $P = NP$ beweisen kann, würde er nicht nur eine Million Dollar, sondern gleich sechs vom Clay Institute erhalten.[3]

6 Schlussfolgerung

Diese Arbeit hat das $P \neq NP$ Problem, seine Bedeutung und die Versuche $P \neq NP$ zu beweisen, erläutert. Die Komplexität der Beweise macht eine kurze Darstellung schwierig. Dennoch hat das $P \neq NP$ Problem nicht nur für die Mathematik, sondern auch für die Allgemeinheit eine große Bedeutung. Eine seriöse Prognose, wann das Problem gelöst werden wird, kann nicht abgegeben werden.

Literatur

[1] S. Arora, *Polynomial time approximation schemes for Euclidean traveling salesman and other geometric problems*, J. ACM, 45 (1998), pp. 753–782.

[2] T. P. Baker, J. Gill, and R. Solovay, *Relativizatons of the P =? NP Question*, SIAM J. Comput., 4 (1975), pp. 431–442.

[3] L. Fortnow, *The status of the P versus NP problem*, Commun. ACM, 52 (2009), pp. 78–86.

[4] E. Mayordomo, *P vs NP*, Monografías de la Real Academia de Ciencias de Zaragoza, 26 (2004), pp. 57–68.

[5] K. Mulmuley and M. A. Sohoni, *Geometric Complexity Theory I: An Approach to the P vs. NP and Related Problems*, SIAM J. Comput., 31 (2001), pp. 496–526.

[6] A. A. Razborov, *On the Method of Approximations*, in STOC, 1989, pp. 167–176.