MATHEMATIQ

Der Newsletter der MathSIG
(Interessensgruppe innerhalb der Mensa Österreich)

Ausgabe 11

http://www.hugi.scene.org/adok/mensa/mathsig/

Editorial

Liebe Leserinnen und Leser!

Dies ist die elfte Ausgabe von MATHEMATIQ, dem Newsletter der MathSIG. Die MathSIG wurde gegründet, um die spezifischen Interessen mathematisch hochbegabter Menschen zu fördern. In erster Linie soll sie sich also den Themengebieten Mathematik, Informatik, Physik und Philosophie widmen. Beiträge von Lesern sind herzlich willkommen. Wenn in ihnen mathematische Sonderzeichen vorkommen, bitte ich aber, sie zwecks möglichst einfacher und fehlerfreier Formatierung im TEX-Format einzusenden. Als Vorlage ist eine Fassung des jeweils aktuellen Newsletters im TEX-Format auf Anfrage bei mir erhältlich. Außer Artikeln sind natürlich auch Illustrationen für das Titelblatt willkommen. Die Rechte an diesen müssen aber eindeutig bei euch selbst liegen, Kopieren von Bildern aus dem Internet ist nicht erlaubt.

Hinweis: Autoren sind für den Inhalt ihrer Artikel oder Werke selbst verantwortlich. Die in MATHEMATIQ veröffentlichten Beiträge widerspiegeln ausschließlich die Meinung ihrer Autoren und nicht jene des Vereins Mensa. Die Zusendung von Beiträgen gilt auch als Einverständnis zu deren Veröffentlichung in MATHEMATIQ.

Diese Ausgabe setzt den Themenschwerpunkt "Theoretische Informatik" fort.

In diesem Sinne: Viel Spaß beim Lesen und Lernen!

Claus D. Volko, cdvolko@gmail.com

Das Erfüllbarkeitsproblem der Aussagenlogik

Ein *NP*-vollständiges Problem ist das Erfüllbarkeitsproblem der Aussagenlogik, auch *Satisfiability* oder kurz *SAT* genannt. Dabei geht es darum, eine Belegung der Variablen einer gegebenen aussagenlogischen Formel zu finden, die beweist, dass diese Formel erfüllbar ist. Sollte es eine solche Belegung nicht geben, soll das Programm ausgeben, dass die Formel nicht erfüllbar ist. Das Problem bei der Sache ist, dass es unter Umständen zwar genügt, eine einzige Belegung zu überprüfen, um zur Konklusion zu kommen, dass die Formel erfüllbar ist. Aber um das Gegenteil zu beweisen, muss man alle möglichen Belegungen probieren - und das sind 2^n, also eine exponentielle Zahl (wobei n für die Anzahl der Variablen steht). Deswegen ist *SAT* in *NP*, aber wahrscheinlich nicht in *P*.

Sollte es aber einen Algorithmus mit polynomieller Laufzeit in Bezug auf die Anzahl der Variablen geben, der in der Lage ist, *SAT* zu lösen, dann liegt *SAT* und damit auch jedes andere Problem, das in der Menge *NP* enthalten ist, auch in *P* - damit wäre das *P*-*NP*-Problem in Sinne von $P = NP$ gelöst. Das ist jedoch eher unwahrscheinlich, weil gemeinhin angenommen wird, dass $P \neq NP$ gilt. Denn das Gegenteil wäre so leicht zu beweisen (es würde genügen, einen einzigen polynomiellen Algorithmus für ein beliebiges *NP*-vollständiges Problem zu finden), dass die Tatsache, dass dies im Laufe all der Jahrzehnte, in denen sich Forscher mit diesem Problem schon beschäftigt haben, noch niemanden gelungen ist, es sehr unwahrscheinlich erscheinen lässt, dass es zutreffen könnte.

Wie könnte man mit Hilfe von *SAT* aber $P \neq NP$ beweisen? Hierzu folgender Gedankengang: Die Größe des Lösungsraums beträgt bekanntlich 2^n. Entscheidend ist aber nicht die Größe des Lösungsraums, sondern die Größe des Suchraums. Gibt es einen Algorithmus, der, auch wenn der Lösungsraum exponentiell ist, nur eine polynomielle Anzahl von Lösungsmöglichkeiten durchsuchen muss? Wenn ja, dann ist $P = NP$; wenn nein, dann ist $P \neq NP$.

Dass der Suchraum grundsätzlich polynomiell oder sogar noch kleiner sein kann, auch wenn der Lösungsraum exponentiell ist, zeigt das Problem *2-COL*, also ob man einen Graphen mit nur zwei Farben färben kann, so dass es kein Paar miteinander durch eine Kante verbundener Knoten gibt, die die gleiche Farbe zugewiesen bekommen. Hier kann jedem Knoten eine von zwei verschiedenen Farben zugewiesen werden, der Lösungsraum hat daher wieder die Größe 2^n. Aber de facto muss nur eine einzige Lösung betrachtet werden, der Suchraum hat also die Größe 1, ist ergo konstant. Denn es genügt, bei einem beliebigen Knoten zu beginnen und dann jeweils die Nachbarknoten anzufärben; jeder Knoten muss höchstens einmal gefärbt werden, und zur Ermittlung seiner Farbe muss nur jeder seiner Nachbarknoten einmal betrachtet werden, womit sich eine Obergrenze von n^2 ergibt. Können auf diese Weise alle Knoten gefärbt werden, so ist der Graph mit zwei Farben färbbar; entsteht hingegen die Situation, dass einem Knoten keine der beiden Farben zugewiesen werden kann, weil er bereits mit Knoten beider Farben benachbart ist, so ist bewiesen, dass der Graph nicht mit zwei Farben färbbar ist.

Theoretisch ist es also sehr wohl möglich, dass ein Problem, das einen exponentiellen Lösungsraum hat, in polynomieller Zeit gelöst werden kann. Die Frage ist nur, ob das auch für *SAT* gilt - und vor allem: wie man beweisen sollte, dass es für *SAT* **nicht** gilt, wie es wahrscheinlich der Fall ist? Zu beweisen, dass etwas nicht gilt, ist unendlich viel schwieriger, als das Gegenteil zu beweisen!

Als **Übungsaufgabe** überlasse ich euch zu beweisen, dass *2-COL* nicht *NP*-vollständig ist, also man *SAT* nicht auf *2-COL* reduzieren kann (sehr wohl aber umgekehrt!).

Claus D. Volko, cdvolko@gmail.com

Zum Beweis der Nichtexistenz

Wie ich bereits mehrmals geschrieben habe, halte ich das *P*-*NP*-Problem deswegen für besonders schwierig, weil wahrscheinlich $P \neq NP$ gilt und es aber sehr viel schwieriger ist zu beweisen, dass etwas nicht gilt, als das Gegenteil zu beweisen. Denn dass etwas nicht gilt, ist gleichbedeutend damit, dass etwas nicht existiert, und wie soll man beweisen, dass etwas nicht existiert?

Nehmen wir das bekannte Raben-Beispiel: Die Aussage "Alle Raben sind schwarz" ist logisch äquivalent zur Aussage "Es existiert nichts, das ein Rabe und zugleich nicht schwarz ist". Das kann man in der Sprache der Aussagenlogik so ausdrücken:

$\neg\exists x R(x) \wedge \neg s(x)$.

Diese Aussage ist logisch äquivalent zur Aussage

$\forall x \neg s(x) \rightarrow \neg R(x)$.

Zum Beweis formen wir die Aussage Schritt für Schritt um:

$\neg\exists x R(x) \wedge \neg s(x)$
$\equiv \forall x \neg(R(x) \wedge \neg s(x))$
$\equiv \forall x \neg R(x) \vee s(x)$
$\equiv \forall x R(x) \rightarrow s(x)$ (das ist die direkte Übersetzung von "Alle Raben sind schwarz")
$\equiv \forall x \neg s(x) \rightarrow \neg R(x)$.

Bei dieser Umformung haben wir zuerst davon Gebrauch gemacht, dass jede Existenzaussage über einen Term A eine negierte Allaussage über Nicht-A darstellt, dann davon, dass eine negierte Konjunktion äquivalent ist zu einer Disjunktion der Negationen der Einzelaussagen, dann von der Möglichkeit, Implikationen als Disjunktionen auszudrücken und zum Schluss von der Tatsache, dass die so genannte Kontraposition einer Implikation zu dieser logisch äquivalent ist.

Daraus ergibt sich, dass wir die Aussage "Alle Raben sind schwarz" beweisen könnten, wenn wir alle nicht-schwarzen Objekte kennten und zeigen könnten, dass es sich bei keinem von ihnen um einen Raben handelt.

Im Fall des *P*-*NP*-Problems lautet die zu beweisende Aussage: "Es gibt kein *NP*-vollständiges Problem, das Element der Menge *P* ist." Diese Aussage könnte also bewiesen werden, wenn es möglich wäre, alle Probleme, die Elemente der Menge *P* sind, aufzuzählen und für jedes dieser Probleme zu zeigen, dass es nicht *NP*-vollständig ist. Die Aussage $P \neq NP$ könnte auch bewiesen werden, wenn man eine Eigenschaft fände, die allen Problemen in *P* inhärent ist, aber die kein *NP*-vollständiges Problem aufweist.

Darüber hinaus sollte man aber nicht vergessen, dass es gar nicht notwendig ist,

eine zu $P \neq NP$ logisch äquivalente Aussage zu beweisen, um $P \neq NP$ zu beweisen. Es ist auch möglich, $P \neq NP$ zu beweisen, indem man eine Aussage beweist, die $P \neq NP$ impliziert. Eine solche Aussage zu finden, erfordert freilich ein wenig Kreativität.

Wenn wir uns die Aussage

$$\forall x \neg s(x) \rightarrow \neg R(x)$$

ansehen, dann ist jedenfalls klar, dass gilt:

$$(\forall x \neg R(x)) \rightarrow (\forall x \neg s(x) \rightarrow \neg R(x)).$$

Im Kontext des *P*-*NP*-Problems würde dies bedeuten: Wenn es gar keine *NP*-vollständige Probleme gäbe, dann wäre bewiesen, dass kein Problem, das in *P* liegt, *NP*-vollständig sein kann. Das ist trivial und bringt uns nichts, denn wir wissen ja, dass es *NP*-vollständige Probleme gibt.

Wir müssten also eine wahre Aussage finden, die die zu beweisende Aussage impliziert. Wenn man das Problem aber nur aussagenlogisch betrachtet und nicht die Eigenschaften von Problemen in *P* und von *NP*-vollständigen Problemen berücksichtigt, wird man meines Erachtens keine finden. Wir müssen also auf jeden Fall untersuchen, was Elemente der Menge *P* sonst noch auszeichnet außer der trivialen Eigenschaft, dass sie in polynomieller Zeit in Bezug auf die Größe der Eingabedaten gelöst werden können.

Claus D. Volko, cdvolko@gmail.com

Erratum

In MATHEMATIQ Ausgabe 2 wurde ein Beispiel für eine kontextfreie Sprache gebracht, die nicht zugleich regulär ist. Dieses Beispiel ist ungültig, die Sprache lässt sich nämlich durch den regulären Ausdruck *(a* b*)** ausdrücken, ist also sehr wohl regulär. Dieser Fehler ist mir beim Übersetzen des Artikels ins Englische aufgefallen. In der englischen Fassung in MATHEMATIQ Ausgabe 10 (Sonderausgabe) habe ich deswegen ein anderes Beispiel gebracht; dieses Beispiel stellt tatsächlich eine kontextfreie Sprache dar, die nicht zugleich regulär ist.

Claus D. Volko, cdvolko@gmail.com