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