Diskrete Optimierung: Fallstudien aus der Praxis

Barbara Wilhelm | Michael Ritter

Station 3: Zertifikate

Diskutieren Sie folgende Fragen in der Gruppe und tragen Sie Ihre Antworten auf dem Arbeitsblatt ein. Das ausgefüllte Blatt heften Sie anschließend in Ihre Gruppenmappe.

Problem 1: Graph Coloring

Input: Zahlen $n, m \in \mathbb{N}$, ein Graph $G = (V, E)$ mit n Knoten und m Kanten, eine natürliche Zahl $K \leq n$.

Frage: Gibt es eine Färbung von G mit höchstens K Farben? Eine *Färbung* (*Graph Coloring*) von G mit K Farben ist eine Funktion $\chi : V \to \{1, \ldots, K\}$ mit $\chi(u) \neq \chi(v)$ für alle Kanten $\{u, v\} \in E$.

Problem 2: LP-Optimality

Input: Zahlen $n, m \in \mathbb{N}$, eine Matrix $A \in \mathbb{Z}^{m \times n}$, Vektoren $b, c \in \mathbb{Z}^m$ und ein Punkt $x^* \in \mathbb{Q}^n$.

Frage: Ist x^* Optimallösung des linearen Programms max $c^T x$, $Ax \leq b$?

Problem 3: ILP-Feasibility

Input: Zahlen $n, m \in \mathbb{N}$, eine Matrix $A \in \mathbb{Z}^{m \times n}$, ein Vektor $b \in \mathbb{Z}^m$.

Frage: Gibt es einen ganzzahligen Punkt $x \in \mathbb{Z}^n$, der das Ungleichungssystem

$$Ax = b \ \wedge \ x \geq 0$$

erfüllt?

---

1. Beweisen Sie, dass Graph Coloring in $\mathcal{NP}$ ist. Beschreiben Sie dazu genau, wie ein Zertifikat für das Problem beschaffen sein soll und wie der Algorithmus aussieht, der das Zertifikat in polynomieller Zeit prüft.

Als Zertifikat kann man natürlich eine Färbung angeben, die mit K Farben auskommt, also einen Vektor $X \in \{1, \ldots, K\}^n$ der Länge n, der für jeden Knoten eine Farbe angibt. Der Algorithmus, der dieses Zertifikat überprüft, erhält als Input den Vektor X und eine Instanz von Graph Colorability. Der Algorithmus prüft dann für jede Kante des Graphen, ob die beiden Endknoten verschiedene Farben haben. Außerdem prüft er, ob alle Komponenten des Vektors X wirklich zwischen 1 und K liegen. Ist beides erfüllt, liefert der Algorithmus „Ja“ zurück, sonst „Nein“. Dazu benötigt er $\mathcal{O}(n + m)$ Operationen, das ist polynomiell in der Größe des Inputs. Ebenso ist die Länge des Zertifikats polynomiell in der Inputlänge.

Für jede Ja-Instanz des Problems gibt es natürlich ein Zertifikat, das zu einer Ja-Antwort führt (nämlich eine zulässige K-Färbung). Umgekehrt gibt es für Nein-Instanzen keine zulässige K-Färbung, einer der Tests des Algorithmus muss also in jedem Fall scheitern und die Antwort lautet korrekterweise „Nein“ (ganz egal, welche Färbung als Zertifikat benutzt wird). Damit ist Graph Colorability in $\mathcal{NP}$.

2. Überlegen Sie sich ein mögliches Zertifikat für das Problem LP-OPTIMALITY! Zeigen Sie, dass das Problem in $\mathcal{NP}$ ist.

Das Problem besteht hier darin, dass ein optimaler Punkt allein ja noch kein Beweis dafür ist, dass es keinen besseren Punkt gibt. Man muss deshalb ein bisschen tiefer in die Trickkiste greifen. Ein mögliches Zertifikat besteht aus einer primal zulässigen und optimalen Lösung x^* und einer für das duale Problem zulässigen und optimalen Lösung y^*. Der Algorithmus, der das Zertifikat prüft, erhält also ein Paar $(x^*, y^*) \in \mathbb{Q}^{n+m}$ als Zertifikat (und natürlich die Instanz selbst). Diese Eingabe prüft er dann auf Zulässigkeit (x^* und y^* ins primale bzw. duale Problem einsetzen, das geht polynomiell), außerdem wird $c^T x^* = b^T y^*$ überprüft. Nach dem Dualitätssatz gilt diese Gleichung für zulässige primale und duale Lösungen genau dann, wenn sowohl x^* als auch y^* optimal sind, das ist also der gesuchte Optimalitätsbeweis.

Der Algorithmus ist offenbar polynomiell, es gibt allerdings ein etwas fieses Problem: Das Zertifikat müsste ja auch in polynomiell vielen Bits codierbar sein. Das wirft die Frage auf, ob es immer eine Lösung gibt, die „ausreichend klein" ist, deren Komponenten also in der Inputlänge beschränkt bleiben (und ebenso für die duale Lösung). Da der zulässige Bereich ja auch ein unbeschränktes Polyeder sein könnte, ist das nicht ganz selbstverständlich. Man kann aber (mit etwas Arbeit, das wollen wir hier nicht ausführen) zeigen, dass sich dieses Problem lösen lässt. Allerdings eignet sich damit nicht mehr jedes beliebige primal-duale Paar als Zertifikat einer Ja-Instanz.

3. Zeigen Sie, dass ILP-FEASIBILITY in $\mathcal{NP}$ ist. Welche Schwierigkeit könnte beim Zertifikat auftreten?

Ein geeignetes Zertifikat für eine Ja-Instanz ist natürlich eine ganzzahlige, zulässige Lösung. Sowohl Ganzzahligkeit als auch Zulässigkeit lassen sich leicht nachprüfen. Wie oben tritt aber auch hier die Frage auf, ob es immer eine *ganzzahlige* Lösung gibt, deren Zahlen in der Inputlänge polynomiell beschränkt bleiben. Auch das kann man (mit noch etwas mehr Aufwand) zeigen. Hier sollte es aber nur darum gehen, Ihren Blick für solche etwas subtilen Details zu schärfen, den Beweis können Sie bei Interesse in der Literatur finden.