Universität zu Köln
Mathematisches Institut
Prof. Dr. F. Vallentin
Dr. A. Gundert

Einführung in die Theoretische Informatik

Wintersemester 2016/17

— Lösungsskizze zur Aufgabe 12.4 —

Aufgabe 12.4 (10 Punkte)

1. Zeigen Sie, dass man für Matrizen $B_1, B_2 \in \mathbb{F}_3^{n\times k}$ vom Rang k in polynomieller Zeit entscheiden kann, ob $C(B_1) = C(B_2)$ gilt.

2. Zeigen Sie: $\overline{\mathrm{CI}} \in \mathrm{BP(NP)}$.

   Tipp: Passen Sie den Beweis von $\overline{\mathrm{GI}} \in \mathrm{BP(NP)}$ aus der Vorlesung an. Die Teile, die direkt übernommen werden können, müssen natürlich nicht nochmal bewiesen werden. Wo können Sie 1. verwenden?

Lösung

1. Hier für können z.B. beide Matrizen in reduzierte Stufenform gebracht werden. Da die reduzierte Stufenform eines linearen Gleichungssystems eindeutig ist, entspricht die Geichheit der Codes der Gleichheit der Matrizen in reduzierter Stufenform.

2. Seien $B_1, B_2 \in \mathbb{F}_3^{n\times k}$ Matrizen vom Rang k. Analog zum Beweis von $\overline{\mathrm{GI}} \in \mathrm{BP(NP)}$ in der Vorlesung wollen wir eine Menge $N(B_1, B_2)$ definieren, deren Kardinalität entscheidet, ob $C(B_1) \cong C(B_2)$ gilt. Dabei sollten sowohl die Elemente von $N(B_1, B_2)$ als auch $|N(B_1, B_2)|$ polynomielle Größe bezüglich der Eingabe $\langle B_1, B_2\rangle$ haben. Zudem sollte die Zugehörigkeit zu $N(B_1, B_2)$ mittels eines Zertifkats polynomieller Größe in polynomieller Zeit getestet werden können.

   Wir setzen

   $$\mathcal{T} := \{T \in \mathbb{F}_3^{n\times n} : T = DP, D \text{ invertierbare Diagonalmatrix und } P \text{ Permutationsmatrix}\}.$$

   Ein erster Ansatz, analog zum Vorgehen für $\overline{\mathrm{GI}}$, wäre die folgende Menge:

   $$\{(C, T) : C \cong C(B_1) \text{ oder } C \cong C(B_2), T \in \mathcal{T}, TC = C\}.$$

   Allerdings haben hier die einzelnen Elemente keine Kodierung in polynomieller Größe bezüglich der Eingabe $\langle B_1, B_2\rangle$. Wir setzen also stattdessen:

   $$N(B_1, B_2) := \{(B, T) : C \cong C(B_1) \text{ oder } C \cong C(B_2), T \in \mathcal{T}, TC = C \text{ für } C = C(B)\}.$$

   Wir zeigen gleich, dass dann gilt:

   $$|N(B_1, B_2)| = \begin{cases} N, \text{ falls } C(B_1) \cong C(B_2) \\ 2 \cdot N, \text{ sonst,} \end{cases}$$

   für $N = 2^n \cdot n! \cdot \prod_{i=0}^{k-1}(3^k - 3^i)$.

   Das weitere Vorgehen verläuft analog wie im Beweis aus der Vorlesung. Wir setzen $Y = N(B_1, B_2)^5$. Dann können Elemente von Y als binäre Vektoren ($\neq 0$) der Länge $p(n)$ für ein Polynom p geschrieben werden. Wir setzen $\ell := \log^4(N^5)$, was polynomielle Größe in n hat, und betrachten zufällige Matrizen aus $\{0, 1\}^{\ell\times p(n)}$.

Für $R \in \{0,1\}^{\ell \times p(n)}$ setzen wir $S(R) := |Y \cap \ker(R)|$ und können analog zur Vorlesung zeigen, dass $\Pr[S \geq 1] \leq \frac{1}{4}$, falls $C(B_1) \cong C(B_2)$, und $\Pr[S \geq 1] \geq \frac{3}{4}$ sonst.

Für (B, T) können wir die Zugehörigkeit zu $N(B_1, B_2)$ mit Hilfe von $T' \in \mathcal{T}$ bezeugen, für das $C(T'B) = C(B_i)$ gilt. Dies lässt sich nach Teil 1. in polynomieller Zeit testen.

Die Sprache

$$\begin{aligned} L' = \{\langle B_1, B_2, y', y'', R\rangle : {} & y' \in Y, y'' \in \mathcal{T}^5, \\ & y''_i \text{ bezeugt die Zugehörigkeit von } y'_i \text{ zu } N(B_1, B_2), \\ & R \in \{0,1\}^{\ell \times p(n)} \text{ mit } Ry' \neq 0\} \end{aligned}$$

liegt also in P und leistet das Gewünschte.

Zur Größe von $N(B_1, B_2)$:
Setze

$$N(C) = \{(C', T) : C \cong C', T \in \mathcal{T}, TC' = C'\}$$

und

$$N(B) := \{(B', T) : C(B) \cong C(B'), T \in \mathcal{T}, TC(B') = C(B')\}.$$

Analog zur Vorlesung lässt sich zeigen, dass $|N(C)| = |\mathcal{T}| = 2^n \cdot n!$, da $\mathcal{T}$ eine Gruppe ist. Zur Bestimmung von $|N(B)|$ ist nun noch zu beachten, dass wir für jedes Paar (C, T) aus $N(C)$ in $N(B)$ genau so viele Elemente erhalten, wie der Code C Basen hat und dass jeder k-dimensionale $\mathbb{F}_3$-Vektorraum $\prod_{i=0}^{k-1}(3^k - 3^i)$ viele Basen besitzt.