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

Einführung in die Theoretische Informatik

Wintersemester 2016/17

— Lösungsskizze zur Aufgabe 9.4 —

Aufgabe 9.4 (10 Punkte) Zeigen Sie, dass das Problem

$$\mathrm{CVP} = \{\langle B, x, \mu\rangle : B \in \mathbb{Q}^{n\times n}, x \in \mathbb{Q}^n, \exists v \in \mathbb{Z}^n : \|x - Bv\| \leq \mu\}$$

NP-schwer ist.

Lösung
Wir zeigen, dass das Problem

$$\mathrm{SUBSETSUM} = \{\langle n, a_1, \ldots, a_n, A\rangle : n \in \mathbb{N}, a_i, A \in \mathbb{Q}, \exists I \subseteq [n] \text{ mit } \sum_{i\in I} a_i = A\}$$

polynomiell reduzierbar auf CVP ist. Dazu bilde eine Instanz $\langle n, a_1, \ldots, a_n, A\rangle$ ab auf:

$$B = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n & 0 \\ 2 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & 2 & 0 & \ldots & 0 & 0 \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & \ldots & 0 & 2 & 0 & 0 \\ 0 & \ldots & \ldots & 0 & 2 & 0 \end{pmatrix} \in \mathbb{Q}^{(n+1)\times(n+1)},\ x = \begin{pmatrix} A \\ 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix} \in \mathbb{Q}^{n+1} \text{ und } \mu = r,$$

wobei r eine rationale Zahl im Interval $[\sqrt{n}, \sqrt{n+1})$ ist. B und x sind offensichtlich in polynomieller Zeit konstruierbar. Zur Konstruierbarkeit von r kommen wir später.
Zunächst zeigen wir, dass dies die versprochene Reduktion ist, d.h., dass:

$$\langle n, a_1, \ldots, a_n, A\rangle \in \mathrm{SUBSETSUM} \iff \langle B, x, \mu\rangle \in \mathrm{CVP}.$$

$\Longrightarrow$**:** Sei $\langle n, a_1, \ldots, a_n, A\rangle \in \mathrm{SUBSETSUM}$, d.h. es gibt $I \subseteq [n]$ mit $\sum_{i\in I} a_i = A$. Dann wähle v als den charakteristischen Vektor von I, erweitert um eine 0 im letzten Eintrag. Dann ist $\|Bv - x\| = \sqrt{(A-A)^2 + \sum_{i=1}^n (2v_i - 1)^2} = \sqrt{n} \leq \mu$.

$\Longleftarrow$**:** Sei $\langle B, x, \mu\rangle \in \mathrm{CVP}$. Dann gibt es also ein $v \in \mathbb{Z}^{n+1}$ mit:

$$\|Bv - x\| = \sqrt{(\sum_{i=1}^n a_i v_i - A)^2 + \sum_{i=1}^n (2v_i - 1)^2} \leq \mu < \sqrt{n+1}.$$

Es gilt aber $(2v_i - 1)^2 \geq 1$ für alle i, da $v_i \in \mathbb{Z}$, und damit $\|Bv - x\| \geq \sqrt{n}$. Wir haben also $n \leq \|Bv - x\|^2 < n + 1$. Da auch $\|Bv - x\|^2 \in \mathbb{Z}$, folgt damit $\|Bv - x\|^2 = n$.

Daraus folgt aber wiederum, dass $\sum_{i=1}^n a_i v_i - A = 0$ und dass $(2v_i - 1)^2 = 1$ für alle i, also $v_i \in 0, 1$. Die Menge $I = \{i \in \{1, \ldots, n\} : v_i = 1\}$ ist also die gewünschte Indexmenge.

Es bleibt zu zeigen, dass wir in polynomieller Zeit eine rationale Zahl im Interval $[\sqrt{n}, \sqrt{n+1})$ konstruieren können. Alternativ könnten wir künstlich die Instanz $\langle n, a_1, \ldots, a_n, A\rangle$ erweitern zur Instanz $\langle n^2, a_1, \ldots, a_n, 0, \ldots, 0, A\rangle$ der Größe n^2 , ohne die Zugehörigkeit zu SUBSETSUM zu beeinflussen. Wenden wir die Reduktion nun auf diese Instanz an, können wir $\mu = n$ wählen.

Zur Konstruktion einer rationalen Zahl im Interval $[\sqrt{n}, \sqrt{n+1})$:
Eine Möglichkeit wäre, ein Verfahren zur Approximation von Quadratwurzeln bis zum Erreichen einer bestimmten Approximationsgenauigkeit laufen zu lassen. Es gibt z.B. ein Verfahren, das eine Stelle nach der anderen berechnet („Schriftliches Wurzelziehen"). Jeder Schritt liefert eine neue Stelle und läuft in logarithmischer Zeit.
Hiermit können wir eine rationale (endlich viele Nachkommastellen!) Zahl x_r bestimmen, die bis zur r-ten Nachkommastelle mit $\sqrt{n}$ übereinstimmt. Setzen wir $y_r := x_r + 10^{-r}$, so gilt

$$x_r \leq \sqrt{n} \leq y_r.$$

Nun muss r ausreichend klein gewählt werden, damit $y_r < \sqrt{n+1}$ gilt. Wählen wir r so, dass $10^{-r} \leq \sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1}+\sqrt{n}}$ gilt, haben wir:

$$y_r \leq x_r + \sqrt{n+1} - \sqrt{n} = \sqrt{n+1} - (\sqrt{n} - x_r) \leq \sqrt{n+1}.$$

Also können wir $r = \lceil \log_{10}(n+1) \rceil \geq \log_{10}(\sqrt{n+1} + \sqrt{n})$ wählen. (Der Einfachheit halber wurde im Dezimalsystem argumentiert, für das Binärsystem geht es analog.)
Wir benötigen also logarithmisch viele Schritte zur Bestimmung der Nachkommastellen. Dazu kommen logarithmisch viele Schritte für die Stellen vor dem Komma. Insgesamt haben wir also logarithmisch viele logarithmische Schritte.