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

Einführung in die Theoretische Informatik

Wintersemester 2016/17

— Aufgabenblatt 12 —

Aufgabe 12.1 Zeigen Sie: $\mathrm{BPP} = \mathrm{BP}(\mathrm{P})$.

Aufgabe 12.2 Sei $R \in \{0,1\}^{k \times p}$ eine zufällige Matrix und sei $X \subseteq \{0,1\}^p$ mit $X \neq \emptyset$, $0 \notin X$. Zeigen Sie

$$\mathrm{Var}[S] = \frac{(1 - \frac{1}{2^k})|X|}{2^k}$$

für die Zufallsvariable $S = |\{x \in X : Rx = 0 \pmod 2\}|$. (Beweisen Sie also Lemma 2 (ii) auf S. 129 des Skripts.)

Aufgabe 12.3 Eine Menge $C \subseteq \mathbb{F}_3^n$ heißt *linearer Code*, falls C ein Untervektorraum von $\mathbb{F}_3^n$ ist. Für eine Matrix $B \in \mathbb{F}_3^{n \times k}$ vollen Rangs sei $C(B)$ der Code mit (Vektorraum-)Dimension k, der von den Spalten von B aufgespannt wird.
Zwei lineare Codes $C = C(B)$ und $C' = C(B')$ heißen *isomorph*, falls es eine Matrix $T \in \mathbb{F}_3^{n \times n}$ gibt, so dass gilt: TB erzeugt den Code C', d.h. $C' = C(TB)$, und $T = DP$, wobei P eine Permutationsmatrix und D eine invertierbare Diagonalmatrix ist.

Zeigen Sie für das Problem

$$\mathrm{CI} = \{\langle B_1, B_2 \rangle : B_1, B_2 \in \mathbb{F}_3^{n \times k}, C(B_1) \text{ und } C(B_2) \text{ sind isomorphe lineare Codes der Dimension } k\},$$

dass sein Komplement $\overline{\mathrm{CI}}$ in $\mathrm{IP}(2)$ liegt.

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

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

Abgabe: Bis Mittwoch, 1. Februar 2017 um 12 Uhr im Schließfach im Studierendenarbeitsraum im MI (Raum 3.01). Bitte Namen und Matrikelnummer auf die Abgabe schreiben.

New Short Cut Found For Long Math Proofs

In a discovery that overturns centuries of mathematical tradition, a group of graduate students and young researchers has discovered a way to check even the longest and most complicated proof by scrutinizing it in just a few spots.

The finding, which some mathematicians say seems almost magical, depends upon transforming the set of logical statements that constitute a proof into a special mathematical form in which any error is so amplified as to be easily detectable.

Using this new result, the researchers have already made a landmark discovery in computer science. They showed that it is impossible to compute even approximate solutions for a large group of practical problems that have long foiled researchers. Even that negative finding is very significant, experts say, because in mathematics, a negative result, showing something is impossible, can be just as important and open just as many new areas of research as a positive one.

The discovery was made by Sanjeev Arora and Madhu Sudan, graduate students at the University of California at Berkeley, Dr. Rajeev Motwani, an assistant professor at Stanford University, and Dr. Carsten Lund and Dr. Mario Szegedy, young computer scientists at A.T.&T. Bell Laboratories. Dr. Motwani, who is the senior member of the group, just turned 30 on March 26.

“With the conventional notion of a proof, you had to check it line by line,” said Dr. Michael Sipser, a theoretical computer scientist at the Massachusetts Institute of Technology. “An error might be buried on page 475, line 6. A ‘less than or equal to’ should have been a ‘less than.’ That would totally trash the whole proof. But you’d have to dig through the whole thing to find it,” Dr. Sipser said. Now, he added, “the new idea is that there is a way to transform any proof so that if there is an error, it appears almost everywhere. I’d say, ‘You have a proof? Show me a page.’ If there is an error, it will be there.”

The finding, which is built on two and a one half years work by leading researchers, is expected to have a profound impact. But because it is so new and unexpected, mathematicians and computer scientists cannot yet predict its scope of application.

“This is philosophically important,” said Dr. Mihalis Yannakakis, a theoretical computer scientist at A.T.&T. Bell Laboratories.

[...]

The New York Times, April 7, 1992
`http://www.nytimes.com/1992/04/07/science/new-short-cut-found-for-long-math-proofs.html`