ETH Zürich
Institute of Theoretical Computer Science
Prof. Rasmus Kyng
Prof. Angelika Steger

FS 2024

Algorithmen und Wahrscheinlichkeit
Peer-Aufgaben 4

Abgabe in Moodle (https://moodle-app2.let.ethz.ch/course/view.php?id=22385)
bis zum 02.05.2024 um 10:00 Uhr.

Das Peergrading findet in diesem Semester über Moodle statt. Bitte lösen Sie die Aufgabe selbstständig und laden Sie Ihre Lösung in Moodle hoch. Ihnen wird dann eine Lösung zum korrigieren zugewiesen. Die Korrektur erfolgt Donnerstag nach der Übung bis spätestens um Mitternacht am folgenden Sonntag. Sie erhalten die Bonuspuknte für einen ehrlichen Versuch die Aufgabe bestmöglich zu lösen und die Ihnen zugeteilte Abgabe bestmöglich zu korrigieren.

Aufgabe 1 – *Verifizierer*

Nehmen Sie an, dass die folgenden zwei Algorithmen gegeben sind:

- Ein Monte-Carlo-Algorithmus[1] A, der als Input eine Zahl $N \in \mathbb{N}$ nimmt, und der eine Zahl X im Intervall $[N, 2N]$ ausgibt, sodass X mit Wahrscheinlichkeit $p_N \geq 1/\log N$ eine Primzahl ist. Die Laufzeit von A sei $\mathcal{O}(\log N)$.
- Ein deterministischer Algorithmus V ("Verifizierer"), der als Input ein $x \in \mathbb{N}$ nimmt, und der in Zeit $\mathcal{O}((\log n)^{6.1})$ entscheidet, ob x eine Primzahl ist.

Konstruieren Sie einen Las-Vegas-Algorithmus, der als Input ein $N \in \mathbb{N}$ nimmt, und der eine Primzahl im Intervall $[N, 2N]$ ausgibt. Was ist die Laufzeit Ihres Algorithmus, wenn Sie eine Erfolgswahrscheinlichkeit von mindestens $1/2$ erreichen wollen?

Hinweis: Die Algorithmen A und V gibt es tatsächlich. Der Algorithmus V wurde 2002 von Agrawal, Kayal, und Saxena vorgestellt. Er wird nicht in der Praxis benutzt, zeigt aber, dass das Aufspüren von Primzahlen effizient möglich ist.

[1] Dies erweitert die Bezeichnung aus der Vorlesung. In der Vorlesung haben wir nur Entscheidungsalgorithmen betrachtet, also Algorithmen, die nur die Antworten "JA" oder "NEIN" ausgeben. Allgemeiner ist ein Monte-Carlo-Algorithmen ein randomisierter Algorithmus, der eine feste obere Schranke für die Laufzeit hat, der aber manchmal (oder oft) ein falsches Ergebnis ausgibt, in diesem Fall ein Nicht-Primzahl. Wenn nicht anders angegeben, meinen wir in dieser Vorlesung mit einem Monte-Carlo-Algorithmus jedoch immer einen Entscheidungsalgorithmus.