ETH Zürich FS 2023
Institute of Theoretical Computer Science
Prof. Rasmus Kyng, Prof. Angelika Steger, Prof. Emo Welzl
Marc Kaufmann, Ulysse Schaller

Algorithmen und Wahrscheinlichkeit
Peer-Aufgaben 4

Lösung zu Aufgabe 1

Wir konstruieren einen Las-Vegas Algorithms A', der als Input ein $N \in \mathbb{N}$ nimmt und dann eine Primzahl im Intervall $[N, 2N]$ ausgibt: im ersten Schritt führt A' den Monte-Carlo Algorithmus A auf N aus und erhält die Ausgabe X. Im zweiten Schritt überprüft A' mit Hilfe von V ob X eine Primzahl ist. Ist dies der Fall, gibt A' die Primzahl X aus, ansonsten kehrt er zum ersten Schritt zurück.

Per Konstruktion gibt A' immer eine Primzahl zurück, ist also korrekt. Seine Laufzeit ist eine Zufallsvariable. Im folgenden berechnen wir zunächst die erwartete Laufzeit T. Der Algorithmus wiederholt zwei Schritte, solange bis ein Erfolg eintritt. Da die Wiederholungen unabhängig sind und ein Erfolg mit Wahrscheinlichkeit p_N auftritt ist die Anzahl Wiederholungen geometrisch verteilt mit Parameter p_N. Die erwartete Anzahl Wiederholungen ist somit $1/p_n \leq \log N$. Die Laufzeit einer Wiederholung besteht aus zwei Schritten mit Laufzeiten von $\mathcal{O}(\log N)$ und $\mathcal{O}(\log^{6.1} N)$, insgesamt hat eine Wiederholung von A' folglich Laufzeit $\mathcal{O}(\log^{6.1} N)$. Daher ergibt sich als erwartete Gesamtlaufzeit $T = \mathcal{O}(\log^{7.1} N)$.

Wenn wir erreichen wollen, dass der Algorithmus Erfolgswahrscheinlichkeit mindestens $1/2$ hat, genügt es, ihn für Zeit $2T$ laufen zu lassen. Markovs Ungleichung ($T \geq 0$) impliziert nämlich, dass

$$\Pr[\text{Laufzeit} \geq 2T] \leq \frac{\text{erwartete Laufzeit}}{2T} = \frac{1}{2}.$$

Bemerkung: Der Monte-Carlo Algorithmus A, der gegeben $N \in \mathcal{N}$ eine Zahl X im Interval $[N, 2N]$ ausgibt, sodass X mit Wahrscheinlichkeit $p_N \geq 1/\log N$ eine Primzahl ist, ist erstaunlich simpel: A gibt einfach eine zufällige ungerade Zahl im Interval $[N, 2N]$ aus. Dies funktioniert jedenfalls für $N \geq 100$, da ein Satz aus der Zahlentheorie besagt, dass es für $N \geq 100$ mindestens $\frac{N}{2 \log N}$ Primzahlen im Intervall $[N, 2N]$ gibt. (Asymptotisch gilt sogar, dass es $(1 + o(1))\frac{N}{\log N}$ Primzahlen im Intervall $[N, 2N]$ gibt.)