

Theoretische Informatik III

6. Serie

Abgabe bis 13:00 Uhr am 13. Juli

Aufgabe 1 [2 Punkte]

Beweisen Sie, dass im Gale-Shapley-Algorithmus höchstens ein Mann mit der Frau verheiratet wird, die er am wenigsten mag.

Aufgabe 2 [2 Punkte]

Gibt es eine Wahl für die Parameter a , b und $x_0 \in \mathbb{N}$, so dass $x_{i+1} = (ax_i + b) \bmod 2$ eine „gute“ Zufallsfolge von 0-1-Zahlen erzeugt? Begründen Sie Ihre Antwort.

Aufgabe 3 [4 Punkte]

Sei $m \in \mathbb{N}$ und $f: \{0, \dots, m-1\} \rightarrow \{0, \dots, m-1\}$ eine beliebige Funktion. Für gegebenes $x_0 \in \{0, \dots, m-1\}$ betrachten wir die Folge $(x_n)_{n \in \mathbb{N}}$ definiert durch $x_{i+1} = f(x_i)$. (Zufallsgeneratoren basierend auf der linearen Kongruenzmethode erzeugen z.B. solche Folgen.)

- (i) Beweisen Sie, dass jede so generierte Folge *periodisch* ist, d.h. es existieren μ und $\lambda \in \mathbb{N}$, so dass $x_0, \dots, x_\mu, \dots, x_{\mu+\lambda-1}$ paarweise verschieden sind, aber $x_{n+\lambda} = x_n$ für alle $n \geq \mu$. Was können Sie über die größtmögliche Periodenlänge λ sagen?
- (ii) Beweisen Sie, dass ein $n > 0$ existiert, so dass $x_n = x_{2n}$ und dass das kleinste solche n in der Menge $\{\mu, \dots, \mu + \lambda\}$ enthalten ist.
- (iii) Entwickeln Sie einen Algorithmus, der für gegebenes x_0 und f die Werte von μ und λ in $O(\mu + \lambda)$ unter der Annahme, dass f sich in $\Theta(1)$ auswerten lässt, berechnet. Beweisen Sie die Korrektheit und analysieren Sie die Laufzeit Ihres Algorithmus’.
- (iv) Was können Sie über die Periodenlänge aussagen, wenn man an Stelle von einwertigen Funktionen f allgemeiner k -wertige Funktionen f mit $k \in \mathbb{N}$ verwendet. Genauer sei $f: \{0, \dots, m-1\}^k \rightarrow \{0, \dots, m-1\}$ für ein $k \in \mathbb{N}$ und

$$x_{i+k} = f(x_i, \dots, x_{i+k-1}),$$

wobei x_0, \dots, x_{k-1} beliebig gewählt werden.

Aufgabe 4 [4 Punkte]

Gegeben seien zwei Teilmengen A und B von $\{0, \dots, n\}$. Wir betrachten die Multimenge $C = \{a + b \mid a \in A \text{ und } b \in B\}$. Geben Sie einen effizienten Algorithmus an, der die Elemente von C und deren Häufigkeit berechnet. Der Algorithmus soll, unter der Annahme, dass zwei Zahlen in $\Theta(1)$ multipliziert werden können, eine Laufzeit von $O(n \log n)$ haben. Beweisen Sie die Korrektheit und analysieren Sie die Laufzeit von Ihrem Algorithmus.

Aufgabe 5

[4 Punkte]

- (i) Zeigen Sie, wie zwei lineare Polynome $a_1x + a_0$ und $b_1x + b_0$ unter Verwendung von *nur* 3 Multiplikationen miteinander multipliziert werden können.
- (ii) Generalisieren Sie die Idee von Teil (i) und entwickeln Sie einen rekursiven *divide-and-conquer* Algorithmus, der zwei Polynome vom Grad n (gegeben in Koeffizientendarstellung) mit Hilfe von $O(n^{\log_2(3)})$ Multiplikationen ausmultipliziert.
- (iii) Zeigen Sie, wie zwei n -Bit-Integerzahlen in $O(n^{\log_2(3)})$ Schritten miteinander multipliziert werden können, wobei jeder Schritt auf einer höchstens konstanten (unabhängig von n) Anzahl von 1-Bit-Werten arbeitet.