Rev. 1, 28.06.2018
TU Ilmenau, Fakultät für Informatik und Automatisierung
FG Komplexitätstheorie und Effiziente Algorithmen
Univ.-Prof. Dr. M. Dietzfelbinger, M. Sc. P. Schlag
http://www.tu-ilmenau.de/iti/lehre/lehre-ss-2018/ra/

TECHNISCHE UNIVERSITÄT
ILMENAU

Randomisierte Algorithmen SS 2018 – Übung 7

Besprechung: Montag, 9. Juli 2018

Hinweis: Für das erfolgreiche Vorrechnen einer mit „*“ gekennzeichneten Aufgabe wird ein Bonuspunkt vergeben, es gibt maximal zwei Bonuspunkte pro Studierendem im Semester. Bitte geben Sie Ihren Lösungsvorschlag bis zum Vortag der Übung (Sonntag), 13:00 Uhr, per E-Mail an philipp.schlag@tu-ilmenau.de oder bis Freitag, 15:00 Uhr, direkt in meinem Büro (Z 1048) ab.

Aufgabe 1 (Parameterschätzung bei Bernoulli-Experimenten, z. B. Münzwurf) *

Seien $Z_1, Z_2, Z_3, \ldots$ unabhängige Zufallsvariable, die jeweils zum Parameter p, mit $0 < p < 1$, geometrisch verteilt sind. Diese Zufallsvariablen modellieren die Wartezeit auf den (Anzahl Versuche bis zum) ersten Erfolg bei unabhängigen Versuchen mit Erfolgswahrscheinlichkeit p. Weiter sei für $k \geq 1$ die Zufallsvariable Y_k definiert durch $Y_k = Z_1 + Z_2 + \cdots + Z_k$. Dann modelliert Y_k die Wartezeit auf k Erfolge bei unabhängigen Versuchen mit Erfolgswahrscheinlichkeit p. Wir wollen eine Art Hoeffding-Schranke für Y_k ermitteln, um damit den (unbekannten) Parameter p abzuschätzen.

(a) Zeigen Sie: $\mathbf{E}(Y_k) = k/p$.

Wenn $X_1, X_2, X_3, \ldots$ unabhängige $\{0,1\}$-wertige Zufallsvariable mit $\mathbf{Pr}(X_i = 1) = p$ sind, dann kann man sich vorstellen, dass Y_k wie folgt definiert ist:

$$Y_k = \min\{i \mid X_1 + X_2 + \cdots + X_i \geq k\}.$$

Damit gilt „$Y_k \leq t \iff X_1 + \cdots + X_t \geq k$“ und „$Y_k \geq t \implies X_1 + \cdots + X_t \leq k$“ für $t \in \mathbb{Z}$.

(b) Finden Sie eine obere Schranke für $\mathbf{Pr}\left(Y_k \geq (1+\delta)\frac{k}{p}\right)$, $\delta \geq 0$, indem Sie die Hoeffding-Ungleichung (Korollar 2.6.3) anwenden. **Hinweis:** Die Funktion $f(z) := z^k \cdot e^{-z}$, $k \geq 1$, ist für $0 < z < k$ streng monoton wachsend und für $z > k$ streng monoton fallend.

(c) Finden Sie eine obere Schranke für $\mathbf{Pr}\left(Y_k \leq (1-\delta)\frac{k}{p}\right)$, $0 \leq \delta \leq 1$.

(d) Benutzen Sie Ihre Ergebnisse von (b) und (c), um folgende Strategie zu analysieren:

Gegeben ist eine unfaire Münze, die mit Wahrscheinlichkeit p Kopf und mit Wahrscheinlichkeit $1-p$ Zahl zeigt. Der unbekannte Parameter p soll geschätzt werden. Man wirft die Münze mehrmals, bis genau k-mal Kopf erschienen ist (für ein $k \geq 1$). Die beobachtete Zahl der Versuche ist Y. Nun gibt man $\hat{p} = k/Y$ als Schätzwert für p aus.

Es soll etwas über die Wahrscheinlichkeit gesagt werden, dass man mit dieser Schätzung nah am echten p liegt. Geben Sie dazu für $\delta \geq 0$ und $0 \leq \delta' \leq 1$ eine untere Schranke für

$$\mathbf{Pr}\left(\frac{p}{1+\delta} \leq \hat{p} \leq \frac{p}{1-\delta'}\right)$$

an.

Jacobi-Symbol

Sei $n \geq 3$ ungerade mit Primzahlzerlegung $n = p_1 \cdot \ldots \cdot p_r$. Für $a \in \mathbb{Z}$ ist

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right) \in \{1, -1, 0\}$$

$$\text{mit } \left(\frac{a}{p_i}\right) := \left\{ \begin{array}{ll} 1 & \text{, falls } a \text{ ein quadratischer Rest modulo } p_i \text{ ist} \\ -1 & \text{, falls } a \text{ ein quadratischer Nicht-Rest modulo } p_i \text{ ist} \\ 0 & \text{, falls } a \text{ durch } p_i \text{ teilbar ist} \end{array} \right\} \text{ für } 1 \leq i \leq r$$

das *Jacobi-Symbol von a und n*. Dann gilt für ungerade $n \geq 3$ und ganze Zahlen a, b:
(i) $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$ **(ii)** $\left(\frac{0}{n}\right) = 0$ **(iii)** $\left(\frac{1}{n}\right) = 1$ **(iv)** $\left(\frac{2}{n}\right) = (-1)^{(n+1)(n-1)/8}$ **(v)** $\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$
Fakt (Quadratisches Reziprozitätsgesetz): Für ungerade Zahlen $a, n \geq 3$ gilt:

$$\left(\frac{a}{n}\right) = (-1)^{(a-1)(n-1)/4} \cdot \left(\frac{n}{a}\right)$$

Aufgabe 2 (Solovay-Strassen-Test) *

(a) Zeigen Sie:

Wenn p eine ungerade Primzahl ist, dann gilt $a^{(p-1)/2} \cdot \left(\frac{a}{p}\right) \bmod p = 1$ für alle $1 \leq a < p$.[1]

Sei $n \geq 3$ eine ungerade zusammengesetzte Zahl.
Eine Zahl a, $1 \leq a < n$, heißt *E-Zeuge für n*, wenn $a^{(n-1)/2} \cdot \left(\frac{a}{n}\right) \bmod n \neq 1$ ist.[2]
Andernfalls heißt sie *E-Lügner für n*. Die Menge der E-Lügner nennen wir L_n^{E}.
Beweisen Sie die folgenden Behauptungen:

(b) $L_n^{\mathrm{E}} \subseteq L_n^{\mathrm{F}} \subseteq \mathbb{Z}_n^*$. (Jeder E-Lügner ist auch F-Lügner und jeder F-Zeuge ist auch E-Zeuge für n.)

(c) $|L_n^{\mathrm{E}}| \leq \frac{1}{2} \cdot |\mathbb{Z}_n^*|$.

Hinweis: Orientieren Sie sich am Beweis von Satz 5.31. Sie dürfen außerdem die Tatsache verwenden, dass es mindestens einen E-Zeugen in $\mathbb{Z}_n^*$ gibt.

Betrachten Sie nun den folgenden randomisierten Primzahltest (Algorithmus 1):

Algorithmus 1 : Solovay-Strassen-Test

Eingabe : Ungerade Zahl $n \geq 3$

1 Wähle a zufällig aus $\{1, \ldots, n-1\}$;
2 **if** $a^{(n-1)/2} \cdot \left(\frac{a}{n}\right) \bmod n \neq 1$ **then return** 1 **else return** 0;

Beweisen Sie die nachstehenden Behauptungen bzgl. Korrektheit und Laufzeit:

(d) **(i)** Wenn n eine Primzahl ist, ist die Ausgabe stets 0.

(ii) Wenn n zusammengesetzt ist, gilt $\mathbf{Pr}(\text{Ausgabe } 0) < \frac{1}{2}$.

(e) Der Algorithmus benötigt $O((\log n)^3)$ Bitoperationen.

[1] Dabei bezeichnet $\left(\frac{a}{p}\right)$ das oben eingeführte Jacobi-Symbol von a und p.

[2] *E* steht für Euler in Bezug auf das Eulersche Kriterium (Proposition 5.45).