Rev. 1, 31.05.2018
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 5

Besprechung: Montag, 11. Juni 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 (Vierfach unabhängige Suche) *

Wir betrachten das folgende aus der Vorlesung bekannte Problem (Kapitel 4.1): Gegeben ist ein endlicher Körper $A = \mathbb{Z}_p$ (für eine Primzahl p) sowie eine nicht-leere Teilmenge $B \subseteq A$. Die Dichte von B in A ist $0 < \rho := |B|/|A| \leq 1$. Gesucht ist (irgend)ein Element von B. Bei der Suche nach einem solchen Element können wir die Elemente von A nur systematisch aufzählen oder zufällig wählen und ein gegebenes Element auf das Enthaltensein in B testen.
Wir wollen nun eine weitere Strategie untersuchen: Wähle vier zufällige Elemente $a_1, a_2, a_3, a_4 \in A = \mathbb{Z}_p$ und untersuche die Folge

$$(a_1 + a_2 \cdot 0 + a_3 \cdot 0^2 + a_4 \cdot 0^3) \bmod p,$$
$$(a_1 + a_2 \cdot 1 + a_3 \cdot 1^2 + a_4 \cdot 1^3) \bmod p,$$
$$(a_1 + a_2 \cdot 2 + a_3 \cdot 2^2 + a_4 \cdot 2^3) \bmod p, \ \ldots$$

bis zum ersten gefundenen Element aus B.
Dazu definieren wir Zufallsvariablen X_i, $0 \leq i \leq p-1$, mit

$$X_i = (a_1 + a_2 \cdot i + a_3 \cdot i^2 + a_4 \cdot i^3) \bmod p,$$

die die untersuchten Elemente in passender Reihenfolge beschreiben. Man kann zeigen:

- Jede Zufallsvariable X_i, $0 \leq i \leq p-1$, ist in $A = \mathbb{Z}_p$ uniform verteilt.
- Für $0 \leq a < b < c < d \leq p-1$ sind X_a, X_b, X_c, X_d unabhängig.

Wie in der Vorlesung seien

$$Y_i := \begin{cases} 1 & \text{, falls } X_i \in B, \\ 0 & \text{, sonst,} \end{cases}$$

für $0 \leq i \leq p-1$ sowie $Z_k := Y_0 + \cdots + Y_{k-1}$ für $0 \leq k \leq p$.

(a) Zeigen Sie:

$$\mathbf{Pr}(Z_k = 0) \leq \frac{\mathbf{E}\left((Z_k - k\rho)^4\right)}{(k\rho)^4}$$

Hinweis: Verallgemeinerte Markov-Ungleichung (Proposition 2.3.4).

(b) Beweisen Sie:

$$\mathbf{E}\left((Z_k - k\rho)^4\right) \leq k\rho + 3(k\rho)^2$$

Hinweis: Für unabhängige Zufallsvariablen X, Y ist der Erwartungswert multiplikativ, d. h., es ist $\mathbf{E}(X \cdot Y) = \mathbf{E}(X) \cdot \mathbf{E}(Y)$. Man multipliziere $\mathbf{E}\left((\sum_{0 \leq i < k}(Y_i - \rho))^4\right)$ aus und vereinfache mit der Multiplikationsregel. Dabei fallen sehr viele Terme weg, weil $\mathbf{E}(Y_i - \rho) = 0$ ist.

(c) Zeigen Sie:

$$\mathbf{Pr}(Z_k = 0) \leq \frac{1}{(k\rho)^3} + \frac{3}{(k\rho)^2}$$

Falls $k\rho \geq 1$ gilt, ist dies nicht größer als $4/(k\rho)^2$.

(d) Zeigen Sie:

$$\mathbf{E}(\#\text{Tests}) \leq 2 + \frac{5}{\rho} = O\left(\frac{1}{\rho}\right)$$

Hinweis: Den Erwartungswert schätzt man mit der Formel $\mathbf{E}(\#\text{Tests}) = \sum_{k \geq 0} \mathbf{Pr}(\#\text{Tests} \geq k+1)$ und Teil (c) ab. Die entstehende Summe wird durch ein Integral abgeschätzt.

Aufgabe 2 (Münzwurf und Glückssträhnen) *

Wir betrachten n unabhängige Münzwürfe. In jedem Wurf tritt das Ereignis „Kopf“ (bzw. „Zahl“) mit Wahrscheinlichkeit $\frac{1}{2}$ ein. Sei L die Länge einer längsten Sequenz von (unmittelbar aufeinanderfolgenden) Würfen mit dem Ergebnis „Kopf“. Wir zeigen, dass $\mathbf{E}(L) = \Theta(\log n)$ gilt.

(a) Zeigen Sie, dass für beliebige Zufallsvariablen X mit Wertebereich $\{0, 1, 2, \ldots, n\}$ und beliebige ganze Zahlen $1 \leq a, b \leq n$ gilt:

$$a\mathbf{Pr}(X \geq a) \leq \mathbf{E}(X) \leq b - 1 + n\mathbf{Pr}(X \geq b).$$

(b) Zeigen Sie: $\mathbf{Pr}(L \geq b) \leq n/2^b$.
Hinweis: „Es gibt eine Sequenz von b (unmittelbar aufeinanderfolgenden) Würfen mit dem Ergebnis ‚Kopf‘“ folgt aus „$L \geq b$“.

(c) Zeigen Sie: $\mathbf{E}(L) \leq \lceil 2 \log n \rceil$.
Hinweis: Folgern Sie aus (a) und (b) eine obere Schranke für $\mathbf{E}(L)$ und wählen Sie b, sodass die Schranke möglichst genau wird.

(d) Wir teilen die beobachtete Sequenz von Münzwürfen in $B = \lfloor n/a \rfloor$ aufeinanderfolgende Blöcke der Länge $a \geq 1$. (Der letzte Block hat evtl. Länge $< a$, ist für die Analyse aber irrelevant.) Zeigen Sie:

$$\mathbf{Pr}(L \geq a) \geq 1 - \left(1 - \frac{1}{2^a}\right)^B \geq 1 - \left(1 - \frac{1}{2^a}\right)^{\frac{n}{a} - 1}.$$

Hinweis: Aus „Es gibt einen Block, der nur Ergebnisse ‚Kopf‘ aufweist“ folgt „$L \geq a$“.

(e) Wählen Sie eine Konstante c so, dass $\mathbf{Pr}(L \geq \lfloor c \cdot \log n \rfloor) \geq 1 - o(1)$ folgt.

(f) Folgern Sie aus (a), (c), (e): $\mathbf{E}(L) = \Theta(\log n)$.