Algorithmen und Wahrscheinlichkeit

Woche 9

Ilya Maier

Abschätzen von Wahrscheinlichkeiten

Markovs Ungleichung:

$$\Pr[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$$

$\forall X \geq 0$

$\forall t > 0,\ t \in \mathbb{R}$

Chebyshevs Ungleichung:

$$\Pr[\,|X - \mathbb{E}[X]\,| \geq t] \leq \frac{\mathsf{Var}[X]}{t^2}$$

$\forall X$

$\forall t > 0,\ t \in \mathbb{R}$

Ist nun Markov oder Chebyshev besser?

$$\Pr[X \geq t] \quad = \quad \Pr[X - \mathbb{E}[X] \geq t - \mathbb{E}[X]] \quad \leq \quad \Pr[\,|X - \mathbb{E}[X]\,| \geq t - \mathbb{E}[X]] \quad \leq \quad \frac{\mathsf{Var}[X]}{(t - \mathbb{E}[X])^2}$$

d.h. $t > \mathbb{E}[X]$, also WLOG sei $t = \mathbb{E}[X] + k \cdot \sqrt{\mathsf{Var}[X]}$ für $k > 0$

dann $\dfrac{\mathsf{Var}[X]}{(t - \mathbb{E}[X])^2} = \dfrac{\mathsf{Var}[X]}{k^2 \mathsf{Var}[X]} = \dfrac{1}{k^2}$, wenn also $k^2\mathbb{E}[X] > \mathbb{E}[X] + k\sqrt{\mathsf{Var}[X]}$ ist, dann ist Chebyshev besser

Abschätzen von Wahrscheinlichkeiten

Chernoffs Ungleichung:

1. $\Pr[X \geq (1+\delta)\mathbb{E}[X]] \leq e^{-\frac{1}{3}\delta^2\mathbb{E}[X]}$ $\quad\forall X \sim$ Bin(n, p)
2. $\Pr[X \leq (1-\delta)\mathbb{E}[X]] \leq e^{-\frac{1}{2}\delta^2\mathbb{E}[X]}$ $\quad\forall 0 < \delta \leq 1$

Korollar:

1. $\Pr[X - \mathbb{E}[X] \geq \delta\mathbb{E}[X]] \leq e^{-\frac{1}{3}\delta^2\mathbb{E}[X]}$
2. $\Pr[X - \mathbb{E}[X] \leq -\delta\mathbb{E}[X]] \leq e^{-\frac{1}{2}\delta^2\mathbb{E}[X]}$
3. $\Pr[\,|X - \mathbb{E}[X]| \geq \delta\mathbb{E}[X]] \leq e^{-\frac{1}{3}\delta^2\mathbb{E}[X]} + e^{-\frac{1}{2}\delta^2\mathbb{E}[X]} \leq 2e^{-\frac{1}{3}\delta^2\mathbb{E}[X]}$

Target Shooting

Gegeben: endliche Mengen S, U s.d. $S \subseteq U$,

$$I_S : U \to \{0,1\} : I_S(u) = 1 \iff u \in S$$

Gesucht: $|S|/|U|$

Algorithmus

1) wähle $u_1, \ldots, u_N$ aus U zufällig unabhängig und gleichverteilt

2) **return** $Y := \frac{1}{N} \sum_{i=1}^{N} I_S(u_i) \qquad \Longrightarrow \qquad \mathbb{E}[Y] = \frac{|S|}{|U|}$

Satz: (geeignetes N finden)
Für $\delta, \epsilon > 0$:

$$N \geq 3 \frac{|U|}{|S|} \epsilon^{-2} \ln\left(\frac{2}{\delta}\right) \qquad \Longrightarrow \qquad \Pr\left[\left|Y - \mathbb{E}[Y]\right| \geq \epsilon \cdot \mathbb{E}[Y]\right] \leq \delta$$

(Kann man mit Chernoffs Ungleichungen i) und ii) zeigen)

Primzahltest

A. GGT

$\gcd(a, n) > 1$ für $1 \leq a \leq n - 1$

$\implies n$ nicht prim

i) “nicht prim” immer richtig

ii) $\Pr[\text{"prim"} \mid \text{nicht prim}] = \dfrac{|Z_n^*|}{n-1}$

$\implies$ Verbesserung durch (viel) Wiederholung

iii) cost$(\gcd(m, n)) = \mathcal{O}((\log nm)^3)$

B. Fermat’s little theorem

n ist prim

$\implies \forall a \in [n-1] : a^{n-1} \equiv 1 \mod n$

i) “nicht prim” immer richtig

ii) $\Pr[\text{"prim"} \mid \text{nicht prim}] = \dfrac{|PB_n|}{n-1}$

iii) $PB_n := \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \text{ mod } n\}$

iv) Carmichael-Zahl n:

1) n ist nicht prim

2) $PB_n = \mathbb{Z}_n^*$

v) $\Pr[\text{"prim"} \mid \text{nicht prim}] < 0.5,$

falls n nicht Carmichael

$\implies$ Verbesserung durch Wiederholung

vi) cost$(a^{n-1} \mod n) = \mathcal{O}((\log n)^3)$

C. Miller-Rabin

Miller-Rabin-PrimeTest(n)

1) Wähle $1 \leq a \leq n-1$ gleichverteilt zufällig

2) $d, k \in \mathbb{N}$ s.d. $n - 1 = 2^k d$, wobei d ungerade

3) **if** $a^d \mod n \neq 1$ **&&**

$\nexists i < k : a^{2^i d} \mod n = n - 1$ **then**

return “nicht prim"

4) **else return** "prim"

i) “nicht prim” immer richtig

ii) $\Pr[\text{"prim"} \mid \text{nicht prim}] \leq \dfrac{1}{4}$

$\implies$ Verbesserung durch Wiederholung

iii) Laufzeit: $\mathcal{O}(\text{poly}(\log n))$

Kahoot

Fehlerreduktion

Monte-Carlo - Einseitiger Fehler:

$\Pr[A(I) = \text{Ja}] = 1$ für alle Ja-Instanzen I $\Longrightarrow$ Wenn $A(I) = \text{Ja}$, dann könnte die Ausgabe falsch sein

$\Pr[A(I) = \text{Nein}] \geq \epsilon$ für alle Nein-Instanzen I Wenn $A(I) = \text{Nein}$, dann ist die Ausgabe immer korrekt

Sei A_δ für $\delta > 0$ ein Algorithmus, der entweder Nein ausgibt, sobald das erste Mal Nein vorkommt,

oder der nach $N = \lceil \epsilon^{-1} \cdot \ln(\delta^{-1}) \rceil$ Versuchen Ja ausgibt

dann gilt:

$\Pr[A_\delta(I) = \text{Ja}] = 1$ für alle Ja-Instanzen I

$\Pr[A_\delta(I) = \text{Nein}] \geq 1 - \delta$ für alle Nein-Instanzen I

Aufgaben

Aufgabe 1: NEERC'15, Problem J

Sie spielen das neue Spiel Jump. Es ist eine gerade Zahl n gegeben und Sie müssen einen Bit-String der Länge n

erraten. Dabei können Sie die Funktion $\mathrm{Jump}(Q) = \begin{cases} n & S = Q \\ \frac{n}{2} & Q \text{ hat } \frac{n}{2} \text{ viele korrekte Bits} \\ 0 & \text{sonst} \end{cases}$

aufrufen. Beschreiben Sie einen Las-Vegas Algorithmus, der S in $\mathcal{O}\left(2^n \cdot \frac{\frac{n}{2}! \cdot \frac{n}{2}!}{n!}\right) + (n+1)$ vielen Aufrufen von

Jump findet.

Hint: Sei Q ein Bit-String mit $\mathrm{Jump}(Q) = \dfrac{n}{2}$ und seien $i, j \in [n]$, sodass das i-te Bit von Q korrekt und das j-te Bit von Q inkorrekt ist. Dann ist $\mathrm{Jump}(Q') = \dfrac{n}{2}$, wobei Q' ein Bit-String ist, wo wir nur die Bits i und j geflipped haben.

Aufgabe 2: Abschätzungen (FS2020, Aufg. 3)

1. Wir werfen eine faire Münze $n \geq 1$ mal. Sei X die Anzahl der Würfe bei denen die Münze 'Kopf' zeigt. Geben Sie möglichst gute obere Schranken für $\Pr[X \geq 0.75n]$ an.

i) Mithilfe der Ungleichung von Markov. (1 Punkt)

ii) Mithilfe der Ungleichung von Chebychev. (2 Punkte)

iii) Mithilfe der Chernoff Schranken. (2 Punkte)

Altogether: 5/44 Punkten ≈ 11%