Mitschrieb: Randomisierte Algorithmen
SS 18

tensor.produkt@gmx.de

16. April 2018

Vorwort

Dies ist ein Mitschrieb der Vorlesungen vom 16.04.18 bis zum ... des Kurses Randomisierte Algorithmen an der Universität Heidelberg.
Dieses Dokument wurde „live“ in der Vorlesung getext. Sämtliche Verantwortung für Fehler übernimmt alleine der Autor dieses Dokumentes.
Auf Fehler kann gerne hingewiesen werden bei folgende E-Mail-Adresse

tensor.produkt@gmx.de

Ferner kann bei dieser E-Mail-Adresse auch der Tex-Code für dieses Dokument erfragt werden.

Inhaltsverzeichnis

Vorlesung vom 16.04.18

1 Einführung

1.1 Beispiel: Halb-Duplex-Kanal

Es seien A, B zwei Knoten, die durch einen Halb-Duplex-Kanal verbunden sind, d. h., es kann in beide Richtungen gesendet werden, aber nur in eine Richtung zu einem bestimmten Zeitpunkt. Senden A und B gleichzeitig, so erfahren sie weder was noch, ob die andere Seite sendet.
Dieses Problem lässt sich durch folgendes Protokoll lösen:

- Sendet eine Seite bereits, so schweigt die andere Seite.
- Senden beide Seiten gleichzeitig, so warten beide ein jeweils zufälliges Zeitintervall und fangen danach an zu senden; wobei diejenige Seite Priorität erhält, die als erste sendet.

1.2 Beispiel: Randomisiertes Quicksort

Bei Quicksort wird in jeder Iteration ein Element der Liste als Pivot-Element gewählt. Betrachte zwei Herangehensweisen:

- Im deterministischen Quicksort wird das Pivotelement entsprechend einem deterministischen Verfahren gewählt, z. Bsp. das erste Element oder der mittlere.
- Im randomisierten Quicksort wird das Pivotelement zufällig gleich verteilt aus allen Elementen der Liste gewählt.

Die randomisierte Variante hat für jede Liste eine Worst-Case Laufzeit von $O(n^2)$. Allerdings kann man zeigen, dass man eine erwartete Laufzeit von $O(n \log n)$ erhält. Die deterministische Variante realisiert für einige wenige Listen ihre Worst-Case Laufzeit und performt für viele Listen in $O(n \log n)$.

1.3 Beispiel: Das Copy Game

Zu Beginn jeder Runde wählen zwei Spieler A, B zufällig und geheim einen Wert $x_A, x_B \in \{0, 1\}$ und committen sich auf den.
Spieler A gewinnt, falls $x_A \neq x_b$. Ansonsten gewinnt B.

Hier ist es essentiell, dass A einer randomisierten Strategie folgt. Denn ist die Strategie von A deterministisch, so kann B diese erfahren oder lernen und sie in Zukunft simulieren (und dadurch immer gewinnen).
Folgt aber A einer zufälligen Strategie mit echten Zufall, so gewinnen beide Spieler mit einer Chance von 50%. Dies ist unabhängig von den Rechenkraft, die B zur Verfügung steht.

1.4 Definition

Für $a, b \in \{0,1\}$ definieren wir die **Paritätssumme** durch

$$a \oplus b := \begin{cases} 1 & a \neq b \\ 0 & a = b \end{cases}$$

Die Menge $\{0,1\}$ zusammen mit der Operation $\oplus$ ist eine abelsche Gruppe.

1.5 Beispiel: One-Time Pad

A will B eine Nachricht $w = w_1 \dots w_n \in \{0,1\}^n$ senden, wobei kein Dritter in der Lage sein soll diese Nachricht w durch Abhören des Kommunikationskanals zu lernen. Kennen A und B beide ein gemeinsames Geheimnis

$$r = r_1 \dots r_n \in \{0,1\}^n$$

das zufällig gewählt wurde, so kann A die bitweise Paritätssumme übermitteln. D. h., A sendet

$$w \oplus r := (w_1 \oplus r_1) \dots (w_n \oplus r_n) \in \{0,1\}^n$$

B erhält $w \oplus r$ und kann durch Addieren von r die Nachricht $w = (w \oplus r) \oplus r$ erlernen. Ein Dritter, der $w \oplus r$ abhört, hat keine Chance w zu erraten, weil r zufällig gleichverteilt gewählt wurde.
Beachte, die Sicherheit des One-Time Pads ist kompromittiert, wenn derselbe Zufall r für die Verschlüsselung verschiedener Nachrichten $w, v, x, \dots$ benutzt wird.

1.6 Beispiel: Das Dining Cryptographers Problem

Drei Kryptographen A, B, C essen in einem Restaurant und erfahren am Ende, dass ihre Rechnung bereits bezahlt wurde.
Sie wollen ein Protokoll etablieren, durch das sie am Ende wissen, ob einer von ihnen für die Rechnung bezahlt hat:

- Jedes Paar von Kryptographen wirft eine faire Münze, dessen Ergebnis gegenüber dem Dritten verborgen wird. Dadurch erhalten wir Zufallbits $r_{A,B}, r_{B,C}$ und $r_{C,A}$.
- Setze dann

$$u_A := r_{A,B} \oplus r_{C,A} \qquad u_B := r_{A,B} \oplus r_{B,C} \qquad u_C := r_{C,A} \oplus r_{B,C}$$

- Danach macht jeder Kryptograph X sein Bit $v_X := u_X$ öffentlich, falls er nicht die Rechnung bezahlt hat. Hat er bezahlt, so veröffentlicht er $v_X := 1 \oplus u_X$.
- Es gilt nun

$$v_A \oplus v_B \oplus v_C = r_{A,B} \oplus \ldots \oplus r_{C,A} = 0$$

  falls keiner der Kryptographen die Rechnung bezahlt hat (oder falls zwei der Kryptographen die Rechnung bezahlt haben), und

$$v_A \oplus v_B \oplus v_C = 1 \oplus r_{A,B} \oplus \ldots \oplus r_{C,A} = 1$$

  falls genau einer (oder drei) der Kryptographen die Rechnung bezahlt hat.
- Keiner der Kryptographen kann erfahren, wer bezahlt von den anderen bezahlt hat, da er eine der Zufallsvariablen $r_{A,B}, r_{B,C}, r_{C,A}$ nicht kennen kann.

2 Diskrete Wahrscheinlichkeitsmaße

Betrachte ein Zufallsexperiment mit Ergebnissen aus einer Menge Ω, die entweder endlich oder abzählbar unendlich ist.
Die Wahrscheinlichkeiten werden durch ein **diskretes Wahrscheinlichkeitsmaß**

$$\mathrm{Prob} : \Omega \longrightarrow [0,1]$$

so dass gilt

$$\sum_{\omega \in \Omega} \mathrm{Prob}(\omega) = 1$$

Bei (Ω, Prob) handelt es sich um einen **diskreten Wahrscheinlichkeitsraum**.
Eine Teilmenge von $E \subset \Omega$ heißt **Ereignis**. Ereignisse erhalten eine Wahrscheinlichkeit durch

$$\mathrm{Prob}(E) := \sum_{\omega \in E} \mathrm{Prob}(\omega)$$

Auf einer endlichen Menge Ω ist das gleich verteilte Wahrscheinlichkeitsmaß definiert durch

$$\mathrm{Prob}(\omega) := \frac{1}{|\Omega|}$$

2.1 Definition

Eine **Zufallsvariable** ist eine Abbildung

$$X : \Omega \longrightarrow \mathbb{R}$$

Jede Zufallsvariable definiert ein Wahrscheinlichkeitsmaß Prob_X auf $\mathbb{R}$ durch

$$\text{Prob}_X(x) := \sum_{\omega \in X^{-1}(x)} \text{Prob}(\omega)$$

Prob_X heißt die **Verteilung** von X.
Wir legen folgende Notationen fest

$$\text{Prob}(X = x) := \text{Prob}_X(x)$$
$$\text{Prob}(X \geq x) := \sum_{t \geq x} \text{Prob}_X(t)$$

etc.

2.2 Definition

Die **Indikator-Variable** für eine Menge $A \subset \Omega$ ist die Zufallsvariable

$$1_A(\omega) := \begin{cases} 1 & \omega \in A \\ 0 & \text{sonst} \end{cases}$$

2.3 Definition: Multivariate Verteilungen

Seien $X_1, \ldots, X_m$ Zufallsvariablen auf Ω. Wir definieren die **Multivariate Verteilung** $\text{Prob}_{X_1,\ldots,X_m}$ durch

$$\text{Prob}_{X_1,\ldots,X_m}(r_1, \ldots, r_m) := \sum_{\omega \in \Omega : X_1(\omega) = r_1, \ldots, X_m(\omega) = r_m} \text{Prob}(\omega)$$

Wir schreiben in Zukunft:

$$\text{Prob}(X_1 = r_1, \ldots, X_m = r_m) := \text{Prob}_{X_1,\ldots,X_m}(r_1, \ldots, r_m)$$

2.4 Definition

$X_1, \ldots, X_m$ heißen **gemeinsam unabhängig**, falls für alle $r_1, \ldots, r_m$ gilt

$$\text{Prob}(X_1 = r_1, \ldots, X_m = r_m) = \text{Prob}(X_1 = r_1) \cdots \text{Prob}(X_m = r_m)$$

$X_1, \ldots, X_m$ heißen **paarweise (stochastisch) unabhängig**, falls für alle $r_1, \ldots, r_m$ und $i \neq j$ gilt

$$\text{Prob}(X_i = r_i, X_j = r_j) = \text{Prob}(X_i = r_i) \cdot \text{Prob}(X_j = r_j)$$

Sie heißen **k-weise unabhängig**, falls jedes k-Tupel von Zufallsvariablen gemeinsam unabhängig ist.

2.5 Bemerkung

Gemeinsame oder $k+1$-weise Unabhängigkeit impliziert immer k-weise Unabhängigkeit. Allerdings ist die Umkehrung im Allgemeinem falsch.

2.6 Beispiel

$X_1, X_2, X_3 \in \{0, 1\}$ seien zufällig gezogen. Setze

$$Z_1 := X_2 \oplus X_3 \qquad Z_2 := X_1 \oplus X_3 \qquad Z_3 := X_1 \oplus X_2$$

Dann sind die Z_i paarweise unabhängig, aber nicht gemeinsam unabhängig.

2.7 Definition

Für eine Zufallsvariable X ist der Erwartungswert definiert durch

$$\mathbb{E}(X) := \sum_{\omega \in \Omega} X(\omega) \cdot \text{Prob}(\omega)$$

Wir sagen, dass $\mathbb{E}(X)$ existiert, falls obige Reihe absolut konvergiert. D. h.

$$\sum_{\omega \in \{\omega_1, \ldots, \omega_n\}} |X(\omega) \cdot \text{Prob}(\omega)|$$

konvergiert für $n \to |\Omega|$.

2.8 Bemerkung

- $\mathbb{E}$ ist $\mathbb{R}$-linear.
- Sind $X_1, \ldots, X_m$ gemeinsam unabhängig, so gilt

$$\mathbb{E}(X_1 \cdots X_m) = \mathbb{E}(X_1) \cdots \mathbb{E}(X_m)$$

2.9 Definition

Die **bedingte Wahrscheinlichkeit** eines Ereignisses A unter B ist definiert durch

$$\mathrm{Prob}(A|B) := \frac{\mathrm{Prob}(A \cap B)}{\mathrm{Prob}(B)}$$

für $\mathrm{Prob}(B) > 0$.
Die **bedingte Verteilung** einer Zufallsvariable X unter B ist definiert durch

$$\mathrm{Prob}(X = x|B) := \frac{\sum_{\omega \in \Omega \cap B} \mathrm{Prob}(\omega)}{\mathrm{Prob}(B)}$$

Definiere den **bedingten Erwartungswert** durch

$$\mathbb{E}(X|B) := \sum_{r \in \mathbb{R}} r \cdot \mathrm{Prob}(X = r|B)$$