Probabilistische Algorithmen

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Sommersemester 2016

Organisatorisches

- Vorlesung: **Di 10–12** (2+2 SWS, 6 CP)
- Übung: **tba**
- Assistent: **Robert Kübler**
- Übungsbetrieb: jeweils abwechselnd alle 2 Wochen
  - Präsenzübung, Start 19. April
  - Zentralübung, Start 26. April
- Übungsaufgaben werden korrigiert.
- Gruppenabgaben bis 3 Personen möglich.
- Mündliche Prüfungen: Fr. 29.07.2016 (?)

Ws-Funktion

Definition

Ein *Wsraum* besteht aus

1. *Ergebnismenge* Ω mit Ereignissen $E \subseteq \Omega$,
2. *Ereignismenge* $\mathcal{F} \subseteq 2^{\Omega}$,
3. *Wsfunktion* $\Pr : \mathcal{F} \to \mathbb{R}$.

Ein $e \in \Omega$ heißt *Elementarereignis*.

Definition Wsfunktion

Für eine *Wsfunktion* $\Pr : \mathcal{F} \to \mathbb{R}$ gilt:

1. $0 \leq \Pr(E) \leq 1$ für alle Ereignisse $E \subseteq \Omega$.
2. $\Pr(\Omega) = 1$.
3. Für alle (abzählbar un-)endlichen Sequenzen $E_1, E_2, \ldots$ paarweise disjunkter Ereignisse
$$\Pr(\bigcup_{i \geq 1} E_i) = \sum_{i \geq 1} \Pr(E_i).$$

Eintreten von mindestens einem Ereignis

Lemma

Für beliebige Ereignisse E_1, E_2 gilt:

$$\Pr(E_1 \cup E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \cap E_2).$$

Beweisidee: Schreibe $E_1 \cup E_2 = E_1 \cup (E_2 \setminus (E_1 \cap E_2))$.

Korollar 1 Union Bound

Für alle (abzählbar un-)endlichen $E_1, E_2, \ldots$ gilt

$$\Pr(\bigcup_{i\geq 1} E_i) \leq \sum_{i\geq 1} \Pr(E_i).$$

Korollar 2 Inklusion-Exklusion

Für alle Ereignisse $E_1, E_2, \ldots, E_n$ gilt

$$\Pr(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} \Pr(E_i) - \sum_{i<j} \Pr(E_i \cup E_j) + \sum_{i<j<k} \Pr(E_i \cap E_j \cap E_k) - \ldots$$

Unabhängigkeit und Bedingte Ws

Definition Unabhängigkeit

Zwei Ereignisse E_1, E_2 sind *unabhängig* gdw

$$\Pr(E_1 \cap E_2) = \Pr(E_1) \cdot \Pr(E_2).$$

Allgemein: $E_1, \ldots, E_k$ sind *unabhängig* gdw für alle $I \subseteq [1, \ldots, k]$ gilt

$$\Pr[\bigcap_{i \in I} E_i] = \prod_{i \in I} \Pr(E_i).$$

Definition Bedingte Ws

Die *bedingte Ws*, dass E_2 eintritt, falls E_1 eintritt, ist

$$\Pr[E_2 \mid E_1] = \frac{\Pr[E_1 \cap E_2]}{\Pr[E_1]} \text{ falls } \Pr[E_1] > 0.$$

Anmerkung: Für unabhängige E_1, E_2 gilt

$$\Pr(E_2 \mid E_1) = \frac{\Pr(E_1 \cap E_2)}{\Pr(E_1)} = \frac{\Pr(E_1)\Pr(E_2)}{\Pr(E_1)} = \Pr(E_2).$$

Polynomvergleich

Problem: Polynomvergleich.

- Überprüfe, ob $(x+1)(x+2)(x+3) \stackrel{?}{=} x^3 + 6x^2 + 10x + 6$.
- Sei d der Grad der zu vergleichenden Polynome.
- Deterministische Lösung: Multipliziere linke Seite in $\mathcal{O}(d^2)$ aus.
- Algorithmus liefert stets die korrekte Lösung.

Notation: $r \in_R A$ bedeutet, wir wählen $r \in A$ uniform gleichverteilt, d.h.

$$\Pr(r = a) = \frac{1}{|A|} \text{ für alle } a \in A.$$

Algorithmus Probabilistischer Polynomvergleich PROBPOLY

EINGABE: $F(x), G(x)$

1. FOR $i = 1$ to k
   1. Wähle $r \in_R \{1, \ldots, 100d\}$.
   2. Falls $F(r) \neq G(r)$ Ausgabe “verschieden”, EXIT.

   Ausgabe “gleich”.

Laufzeit: $\mathcal{O}(kd) = \mathcal{O}(d)$ für konstantes k.

Korrektheit

Satz

PROBPOLY liefert für $F(x) = G(x)$ stets die korrekte Antwort und für $F(x) \neq G(x)$ die korrekte Antwort mit Ws $\geq 1 - (\frac{1}{100})^k$.

Beweis:

- Falls $F(x) = G(x)$, so gilt auch $F(r) = G(r)$ für alle r.
- Angenommen $F(x) \neq G(x)$. Damit gilt $P(x) = F(x) - G(x) \neq 0$.
- $P(x)$ besitzt $\text{grad}(P(x)) \leq d$ und damit höchstens d Nullstellen.
- Ereignis E_i: PROBPOLY liefert nicht "verschieden" in Iteration i.

$$\Pr[E_i] = \Pr[\text{r ist Nullstelle von } P(x)] \leq \frac{d}{100d} = \frac{1}{100} \text{ für alle } i.$$

- Definiere $E = E_1 \cap \ldots \cap E_k$. Aus der Unabhängigkeit der E_i folgt

$$\Pr(E) = \Pr(E_1 \cap \ldots \cap E_k) = \prod_{i=1}^{k} \Pr(E_i) \leq (\frac{1}{100})^k.$$

- E bedeutet, dass letztlich Ausgabe "gleich" erfolgt. D.h.

$$\Pr[\text{Ausgabe "verschieden"} | F(x) \neq G(x)] = \Pr[\bar{E}] \geq 1 - (\frac{1}{100})^k.$$

Verbesserter Algorithmus

Idee: Hätten gerne paarweise verschiedene r_i in Iteration i.

Algorithmus Probabilistischer Polynomvergleich PROBPOLY2

EINGABE: $F(x), G(x)$

1. FOR $i = 1$ to k
   1. Wähle $r_i \in_R \{1, \ldots, 100d\}$ mit $r_i \neq r_j$ für alle $j = 1, \ldots, k-1$.
   2. Falls $F(r) \neq G(r)$ Ausgabe “verschieden”, EXIT.

   Ausgabe “gleich”.

Analyse

Analyse der Irrtumsws.

- Angenommen $F(x) \neq G(x)$, d.h. $P(x) = F(x) - G(x) \neq 0$.
- Die Ereignisse E_i, dass $P(r_i) = 0$, sind nun abhängig. D.h.

$$\begin{aligned} \Pr(E_1 \cap \ldots \cap E_k) &= \Pr(E_k \mid E_1 \cap \ldots \cap E_{k-1}) \cdot \Pr(E_1 \cap \ldots \cap E_{k-1}) = \ldots \\ &= \Pr(E_1) \cdot \Pr(E_2 \mid E_1) \cdot \ldots \cdot \Pr(E_k \mid E_1 \cap \ldots \cap E_{k-1}). \end{aligned}$$

- Ziehen der r_i ohne Zurücklegen liefert

$$\Pr(E_j \mid E_1 \cap \ldots \cap E_{j-1}) \leq \frac{d-(j-1)}{100d-(j-1)}.$$

- Es folgt für die Fehlerws

$$\Pr(E) = \Pr(E_1 \cap \ldots \cap E_k) \leq \prod_{j=1}^{k} \frac{d-(j-1)}{100d-(j-1)}.$$

- Dies ist für $k \ll d$ nur unwesentlich kleiner als $(\frac{1}{100})^k$ zuvor.
- Wir ziehen daher häufig eine vereinfachte Analyse vor.
- D.h. wir verwenden oft unabhängig gleichverteilte r_i.

Matrixmultiplikation

Problem Matrixvergleich.

- Gegeben seien Matrizen $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{F}_2^{n \times n}$. Überprüfe $\mathbf{AB} \stackrel{?}{=} \mathbf{C}$.
- Produkt $\mathbf{A}b_i$ kann für $b_i \in \mathbb{F}_2^n$ in Zeit $\mathcal{O}(n^2)$ berechnet werden.
- Deterministisch: Multipliziere $\mathbf{AB}$ in Zeit $\mathcal{O}(n^3)$ (bzw. $\mathcal{O}(n^{2.37})$) aus.

Algorithmus ProbMatrix

EINGABE: $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{F}_2^{n \times n}$

1. For $i = 1$ to k
   1. Wähle $r_i \in_R \{0,1\}^n$.
   2. Falls $\mathbf{A}(\mathbf{B}r) \neq \mathbf{C}r$ Ausgabe “verschieden”, EXIT.

   Ausgabe “gleich”.

Laufzeit: $\mathcal{O}(kn^2) = \mathcal{O}(n^2)$ für $k \ll n$