Alle oder einzelne

Lemma

Wahl von $r = (r_1, \ldots, r_n) \in_R \mathbb{F}_2^n$ ist äquivalent zur Wahl aller $r_i \in_R \mathbb{F}_2$.

Beweis:

- $\Rightarrow$: oBdA sei $i = 1$.
- Es existieren 2^{n-1} Vektoren der Form $0\{0,1\}^{n-1}$ bzw. $1\{0,1\}^{n-1}$.
- D.h. $\Pr(r_1 = 0) = \frac{2^{n-1}}{2^n} = \frac{1}{2} = \Pr(r_1 = 1)$.
- $\Leftarrow$: Wähle alle $r_i \in_R \mathbb{F}_2$ und setze $r = (r_1, \ldots, r_n)$.
- Dann gilt für alle $x \in \mathbb{F}_2^n$

$$\Pr(r = x) = \Pr(r_1 = x_1 \cap \ldots \cap r_n = x_n) = \prod_{i=1}^{n} \Pr(r_i = x_i) = \frac{1}{2^n}.$$

Analyse von ProbMatrix

Lemma

Sei $\mathbf{AB} \neq \mathbf{C}$. Dann gilt für alle $r \in_R \mathbb{F}_2^n$

$$\Pr(\mathbf{AB}r = \mathbf{C}r) \leq \tfrac{1}{2}.$$

Beweis:

- Sei $\mathbf{D} = \mathbf{AB} - \mathbf{C} \neq 0$. OBdA $d_{11} \neq 0$.
- Angenommen $\mathbf{AB}r = \mathbf{C}r$, d.h. $\mathbf{D}r = 0$ und insbesondere
$$\sum_{j=1}^{n} d_{1j} r_j = 0 \text{ bzw. } r_1 = -\frac{\sum_{j=2}^{n} d_{1j} r_j}{d_{11}}.$$
- Wir wählen in dieser Reihenfolge $r_n, \ldots, r_2, r_1 \in_R \mathbb{F}_2$.
- Die Wahl von $r_n, \ldots, r_2 \in_R \mathbb{F}_2$ determiniert $x := -\frac{\sum_{j=2}^{n} d_{1j} r_j}{d_{11}} \in \mathbb{F}_2$.
- Es folgt $\Pr(r_1 = x) = \frac{1}{2}$ und damit insgesamt
$$\Pr(\mathbf{D}r = 0) \leq \Pr(\textstyle\sum_{j=1}^{n} d_{1j} r_j = 0) = \frac{1}{2}.$$

Korollar

ProbMatrix liefert für $\mathbf{AB} = \mathbf{C}$ stets die korrekte Antwort und für $\mathbf{AB} \neq \mathbf{C}$ die korrekte Antwort mit Ws mindestens $1 - (\frac{1}{2})^k$.

Umdrehen der bedingten Ws

Problem:

- Haben bisher $\Pr(\text{Ausgabe "gleich"} | \mathbf{AB} \neq \mathbf{C})$ analysiert.
- Uns interessiert aber oft $\Pr(\mathbf{AB} \neq \mathbf{C} | \text{Ausgabe "gleich"})$.

Satz von der totalen Ws

Seien $E_1, \ldots, E_n \subset \Omega$ disjunkt mit $\bigcup_{i=1}^n E_i = \Omega$. Dann gilt

$$\Pr(B) = \sum_{i=1}^n \Pr(B \cap E_i) = \sum_{i=1}^n \Pr(B \mid E_i) \Pr(E_i).$$

Beweis: per Bild.

Satz von Bayes

Seien $E_1, \ldots, E_n \subset \Omega$ disjunkt mit $\bigcup_{i=1}^n E_i = \Omega$, $\Pr(B) > 0$. Dann gilt

$$\Pr(E_j \mid B) = \frac{\Pr(E_j \cap B)}{\Pr(B)} = \frac{\Pr(B|E_j) \Pr(E_j))}{\sum_{i=1}^n \Pr(B|E_i) \Pr(E_i)}.$$

Umdrehen der bedingten Ws

Berechnen von $\Pr(\mathbf{AB} \neq \mathbf{C} | \text{Ausgabe “gleich”})$:

- Sei E das Ereignis $\mathbf{AB} = \mathbf{C}$ und B das Ereignis $\mathbf{AB}r = \mathbf{C}r$.
- Starten mit *A priori Modell*, dass $\Pr(E) = \Pr(\bar{E}) = \frac{1}{2}$.
- Es gilt $\Pr(B \mid E) = 1$ und $\Pr(B \mid \bar{E}) \leq \frac{1}{2}$. Mit Satz von Bayes folgt

$$\Pr(E \mid B) = \frac{\Pr(B|E)\Pr(E)}{\Pr(B|E)\Pr(E)+\Pr(B|\bar{E})\Pr(\bar{E})} \geq \frac{\frac{1}{2}}{\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}} = \frac{2}{3}.$$

- Passen Modell nach 1. Iteration an: $\Pr(E) \geq = 23$ und $\Pr(\bar{E}) = \frac{1}{3}$.
- Bei erneutem Ereignis B liefert der Satz von Bayes

$$\Pr(E \mid B) \geq \frac{\frac{2}{3}}{\frac{2}{3}+\frac{1}{2}\cdot\frac{1}{3}} = \frac{4}{5}.$$

- Allgemein erhalten wir nach dem k-ten Auftreten von B induktiv

$$\Pr(E \mid B) \geq 1 - \frac{1}{2^k+1}.$$

- D.h. nach z. B. 100 Iterationen erhalten wir
  $\Pr(\text{Ausgabe “gleich”} \mid \mathbf{AB} \neq \mathbf{C}) \geq 1 - \frac{1}{2^{100}}$ und
  $\Pr(\mathbf{AB} \neq \mathbf{C} \mid \text{Ausgabe “gleich”}) \geq 1 - \frac{1}{2^{100}+1}$.

Randomisierter Min-Cut Algorithmus

Problem Min-Cut

Gegeben: Zusammenhängender ungerichteter Graph $G = (V, E)$
Gesucht: $C \subseteq E$ mit min. $|C|$ und $G = (V, E \setminus C)$ nicht zusammenh.

Algorithmus KANTEN-KONTRAKTION (Karger 1993)

EINGABE: $G = (V, E)$

1. REPEAT UNTIL $|V| = 2$
   1. Wähle $e = \{u, v\} \in_R E$.
   2. Verschmelze u, v zu einem Knoten mit Label u, v.
      Entferne dabei alle Kanten zwischen u und v.

AUSGABE: $C = E$, d.h. alle verbliebenen Kanten

- **Laufzeit:** $\mathcal{O}(|V| + |E|) = \mathcal{O}(n + m)$ für $|V| = n, |E| = m$.
- Bei Terminierung: Zwei Knoten mit Label $S \subset V$ und $V \setminus S$.
- Damit ist C ein Cut, der die Partitionen S und $V \setminus S$ trennt.
- C besitzt aber nicht notwendigerweise minimale Größe.

Analyse KANTEN-KONTRAKTION

Satz

KANTEN-KONTRAKTION berechnet minimalen Cut mit Ws $\geq \frac{2}{n(n-1)}$.

Beweis:

- Sei C_{min} ein minimaler Cut in G mit $|C| = k$.
- Falls nie eine Kante in C_{min} kontrahiert wird, erfolgt Ausgabe C_{min}.
- E_i: Ereignis Kante $\{u, v\} \notin C$ in i-ter Iteration.
- Sei $F_i = \bigcap_{j=1}^{i} E_j$. Wir berechnen zunächst $\Pr(F_1) = \Pr(E_1)$.
- Jedes $v \in V$ besitzt $\deg(v) \geq k$. (Warum?)
- Damit gilt $|V| \geq \frac{kn}{2}$. D.h. $\Pr(\bar{E}_1) \leq \frac{k}{\frac{kn}{2}} = \frac{2}{n}$ bzw. $\Pr(E_1) \geq 1 - \frac{2}{n}$.
- Nach E_1 verbleibt G mit $n-1$ Knoten und minimalem Cut C_{min}.
- D.h. $\Pr(E_2 \mid F_1) \geq 1 - \frac{2}{n-1}$ und allg. $\Pr(E_i \mid F_{i-1}) \geq 1 - \frac{2}{n-(i-1)}$.
- KANTEN-KONTRAKTION liefert nach $n-2$ Kontraktionen C_{min} mit

$$\begin{aligned} \Pr(F_{n-2}) &= \Pr(E_{n-2} \cap F_{n-3}) = \Pr(E_{n-2} \mid F_{n-3}) \cdot \Pr(F_{n-3}) \\ &= \Pr(E_{n-2} \mid F_{n-3}) \cdot \Pr(E_{n-3} \mid F_{n-4}) \cdot \ldots \cdot \Pr(E_2 \mid F_1) \cdot \Pr(F_1) \end{aligned}$$

- Es folgt $\Pr(F_{n-2}) \geq \prod_{i=1}^{n-2} \left(1 - \frac{2}{n-(i-1)}\right) = \frac{2}{n(n-1)}$.

Amplification

Lemma Amplification

$n(n-1)\ln n$-maliges Wiederholen von KANTEN-KONTRAKTION und Ausgabe des kleinsten Cuts liefert minimalen Cut mit Ws $\geq 1 - \frac{1}{n^2}$.

Beweis:

- Ereignis E_i: kein minimaler Cut in i-ter Wiederholung
- Damit liefert KANTEN-KONTRAKTION keinen minimalen Cut mit $\Pr(E_1 \cap \ldots \cap E_{n(n-1)\ln n}) = \prod_{i=1}^{n(n-1)\ln n} \Pr(E_i) \leq \left(1 - \frac{2}{n(n-1)}\right)^{n(n-1)\ln n}$.
- Mittels $1 - x \leq e^{-x}$ erhalten wir

$$\Pr(E_1 \cap \ldots \cap E_{n(n-1)\ln n}) \leq e^{-2\ln n} = \frac{1}{n^2}.$$

Diskrete Zufallsvariablen

Definition Zufallsvariable

Eine *Zufallsvariable (ZV)* X ist eine Abbildung $X : \Omega \to \mathbb{R}$. Eine *diskrete Zufallsvariable* nimmt nur (abzählbar un-)endlich viele Werte an.

Bsp:

- Sei $\Omega = \{(1,1),(1,2),\ldots\}$ ein 2-maliger Münzwürf.
- ZV X: Summe der beiden Würfe. X nimmt Werte in $\{2,\ldots,12\}$ an.
- $\Pr(X=4) = \Pr((1,3)) + \Pr((2,2)) + \Pr((3,1)) = \frac{3}{36} = \frac{1}{12}$

Definition Unabhängigkeit von Zufallsvariablen

Zwei ZV X, Y sind *unabhängig* gdw

$$\Pr((X=x)\cap(Y=y)) = \Pr(X=x)\cdot\Pr(Y=y) \text{ für alle } x,y.$$

Allgemein: $X_1,\ldots,X_k$ sind *unabhängig* gdw für alle $I \subseteq \{1,\ldots,k\}$ gilt

$$\Pr\left(\bigcap_{i\in I} X_i = x_i\right) = \prod_{i\in I}\Pr(X_i=x_i) \text{ für alle } x_i \text{ mit } i\in I.$$