Randomisierte Algorithmen

Ein sehr weites Gebiet.

- Las Vegas– und Monte Carlo–Algorithmen
- Universales Hashing, Bloom-Filter
- Symmetry Breaking
- Routing-Algorithmen
- Derandomisierung
- ...

Einfaches Beispiel

Eingabe: Zwei Polynome

Frage: Sind sie gleich?

$$
\begin{aligned}
& (x-13)(x-5)(x-3)(x+7)(x^2+12) \\
\stackrel{?}{=} \quad & x^6 - 14x^5 - 16x^4 + 472x^3 - 1701x^2 + 7656x - 16380
\end{aligned}
$$

Ausmultiplizieren: $\Theta(d^2)$ Multiplikationen

Geht es schneller?

Bloom-Filter

Wir wollen einmal ein Wörterbuch erstellen.

Dann schlagen wir sehr oft darin nach, ob es gegebene Wörter enthält.

Das Wörterbuch enthalte $w_1, \ldots, w_n$.

Wieviel Platz benötigen wir dafür?

Universelles Hashing

Definition

Es sei $\mathcal{H}$ eine nicht-leere Menge von Funktionen $U \to \{1, \ldots, m\}$.

Wir sagen, daß $\mathcal{H}$ eine universelle Familie von Hashfunktionen ist, wenn für jedes $x, y \in U$, $x \neq y$ folgendes gilt:

$$\frac{|\{\, h \in \mathcal{H} \mid h(x) = h(y) \,\}|}{|\mathcal{H}|} \leq \frac{1}{m}$$

Theorem

Es sei $\mathcal{H}$ eine universelle Familie von Hashfunktionen $U \to \{1, \ldots, m\}$ für das Universum U und $S \subseteq U$ eine beliebige Untermenge.

Wenn $x \in U$, $x \notin S$ und $h \in \mathcal{H}$ eine zufällig gewählte Hashfunktion ist, dann gilt

$$E\Big(|\{\, y \in S \mid h(x) = h(y) \,\}|\Big) \leq \frac{|S|}{m}.$$

Beweis

$$E\Big(|\{\, y \in S \mid h(x) = h(y) \,\}|\Big) = \sum_{y \in S} \Pr[h(x) = h(y)] = \sum_{y \in S} \frac{|\{\, h \in \mathcal{H} \mid h(x) = h(y) \,\}|}{|\mathcal{H}|} \leq \frac{|S|}{m}$$

Eine universelle Hashfamilie

Sei $U = \{0, \ldots, p-1\}$, wobei p eine Primzahl ist.

Es sei $h_{a,b}(x) = ((ax + b) \bmod p) \bmod m$.

Wir definieren

$$\mathcal{H} = \{\, h_{a,b} \mid 1 \leq a < p,\ 0 \leq b < p\}$$

Theorem

$\mathcal{H}$ ist eine universelle Familie von Hashfunktionen.

Es seien $x, y \in \{0, \ldots, p-1\}$, $x \neq y$.

Wir wollen zunächst zeigen, daß die Funktion

$$f\colon (a,b) \mapsto (ax + b \bmod p, ay + b \bmod p)$$

für $a, b \in \{0, \ldots, p-1\}$ injektiv und somit auch bijektiv ist.

$$\begin{aligned}
&(ax + b \bmod p, ay + b \bmod p) = (a'x + b' \bmod p, a'y + b' \bmod p)\\
\Leftrightarrow&(ax + b - b' \bmod p, ay + b - b' \bmod p) = (a'x \bmod p, a'y \bmod p)\\
\Leftrightarrow&(b - b' \bmod p, b - b' \bmod p) = ((a' - a)x \bmod p, (a' - a)y \bmod p)\\
\Leftrightarrow&(a' - a)x \bmod p = (a' - a)y \bmod p \Leftrightarrow a' = a \wedge b' = b
\end{aligned}$$

Nach wie vor gelte $x, y \in \{0, \ldots, p-1\}$, $x \neq y$.

Für wieviele Paare (a, b) haben $c_x := ax + b \bmod p$ und $c_y := ay + b \bmod p$ den gleichen Rest modulo m?

Wir haben auf der letzten Folie bewiesen, daß sich für jedes Paar (a, b) ein eindeutiges Paar (c_x, c_y) ergibt. Für ein festes c_x gibt es nur

$$\lceil p/m \rceil - 1 = \left\lfloor \frac{p+m-1}{m} \right\rfloor - 1 \leq \frac{p-1}{m}$$

viele mögliche Werte von c_y mit $c_x \equiv c_y \mod m$ und $c_x \neq c_y$.

Weil p verschiedene Werte für c_x existieren, gibt es insgesamt höchstens $p(p-1)/m$ Paare der gesuchten Art.

$$\frac{|\{\, h \in \mathcal{H} \mid h(x) = h(y) \,\}|}{|\mathcal{H}|} \leq \frac{p(p-1)/m}{p(p-1)} \leq \frac{1}{m}$$

Min-Cut

Einfacher Algorithmus:

Kontrahiere zufällige Kanten, bis nur zwei Knoten übrig.

Mit Wahrscheinlichkeit $\Omega(n^{-2})$ ein Min-Cut.

Verwende Amplifizierung.

(Verbesserung: Zwei Kontraktionssequenzen bis etwa $n/\sqrt{2}$ Knoten bleiben, dann rekursiv.)

Min-Cut: Analyse

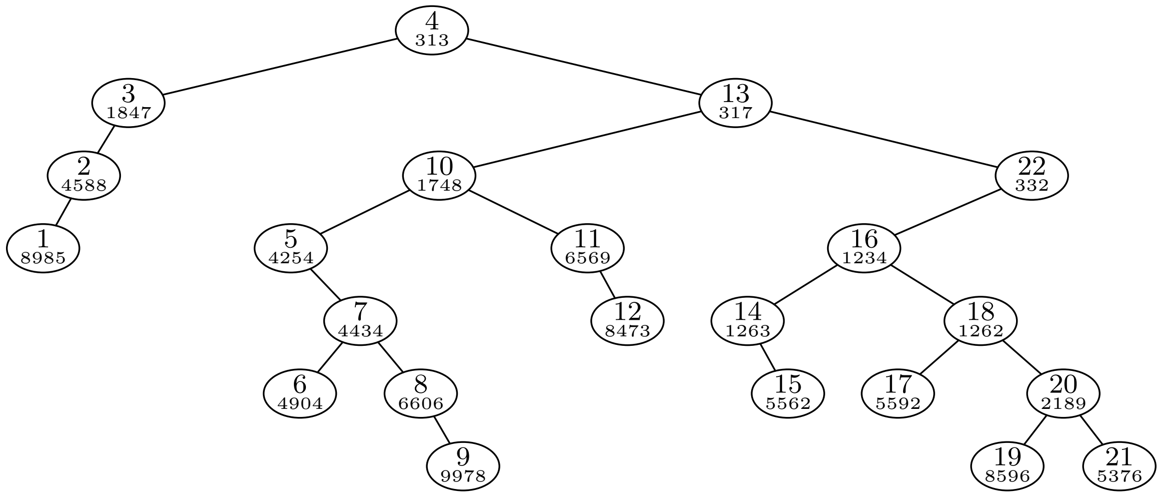
Nehmen wir an es gibt einen Min-Cut der Größe k und der Graph hat m Kanten und n Knoten.

Dann ist $2m \geq nk$ (weil $D(G) \geq k$).

Die Wahrscheinlichkeit keine Kante aus dem Min-Cut zu kontrahieren ist $1 - k/m$ und dafür daß alle Kanten richtig gewählt werden ist

$$\left(1 - \frac{k}{m}\right)\left(1 - \frac{k}{m-1}\right) \cdots \left(1 - \frac{k}{m-k-1}\right)$$
$$\geq \left(1 - \frac{2}{n}\right)\left(1 - \frac{2}{n-1}\right) \cdots \left(1 - \frac{2}{n-k-1}\right)$$
$$= \frac{n-2}{n}\frac{n-3}{n-1}\frac{n-4}{n-2} \cdots \frac{2}{4}\frac{1}{3} = \frac{2}{n(n-1)}$$

Treaps


4
313
3
1847
13
317
2
4588
10
1748
22
332
1
8985
5
4254
11
6569
16
1234
7
4434
12
8473
14
1263
18
1262
6
4904
8
6606
15
5562
17
5592
20
2189
9
9978
19
8596
21
5376