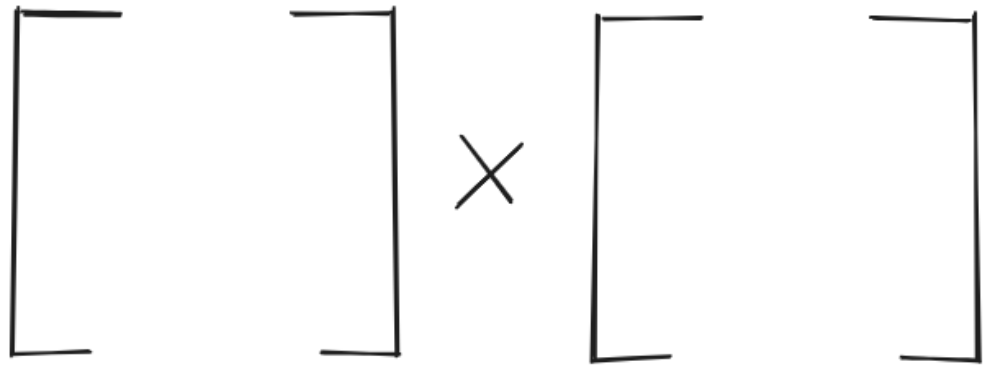
Naključnostni algoritmi II

Uroš Čibej



Pregled snovi

1. Freivaldsov algoritem
2. Kargerjev algoritem
3. Praštevilskost
    - Fermatov mali izrek
    - Solovay-Strassen
    - Rabin-Miller

Matrično množenje - verifikacija

vhod: matrike A, B, C dimenzij $n \times n$
vprašanje: $A \times B = C$?

Naivni pristop zmnožimo matriki A, B, primerjamo rezultat s C

Freivaldsov algoritem

- Rūsiņš Freivalds (Latvijski matematik)
- Monte Carlo algoritem
- $O(n^2)$
- ne poznamo deterministočnega algoritma s tako dobrim časom izvajanja

Postopek

vhod: A, B, C

1. Izberemo naključni vektor $w \in [0,1]^n$
2. $x = Bw$
3. $y = Ax$ torej (y=(AB)w)
4. $z = Cw$
5. Če $z = y$ vrni True, sicer False

1. $AB = C$ - odgovor True z verjetnostjo 1
2. $AB \neq C$, koliko je

$$P[\text{ algoritem odgovori } \mathrm{True}]?$$

Verjetnost napake

$$AB - C = 0?$$

$D = AB - C$ in $D \neq 0$

za naključni w:

$$P[Dw = 0] \leq \frac{1}{2}$$

Dokaz

Izrek: Naj bo D poljubna neničelna matrika in w naključni 0-1 vektor, potem

$$P[Dw = 0] \leq \frac{1}{2}$$

Vsaj polovica vektorjev w da rezultat $Dw \neq 0$.

1. naj bo x vektor pri katerem je $Dx = 0$
2. naj bo x' vektor, kjer je samo j ta komponenta negirana
3. Potem $Dx' \neq 0$, ker

$$Dx' = D(x \pm e_j) = Dx \pm De_j = \pm De_j \neq 0$$

Najmanjši prerez

vhod: Neusmerjen graf $G = \langle V, E \rangle$
problem: S_1, S_2 razbitje V.

Prerez:

$$C = \{(u, v) \mid u \in S_1, v \in S_2\}$$

Min:
$|C|$

Klasični pristop

- s-t pretoki in izrek "max-flow, min-cut"
- $\forall s, t$: poženemo nek algoritem za največji pretok

Kargerjev algoritem

- enostaven, hiter, presenetljiv
- veliko upanje za naključnostne algoritme
- uporabljan za
  - analizo omrežij
  - gručenje
  - segmentacijo slik

Osnovna ideja

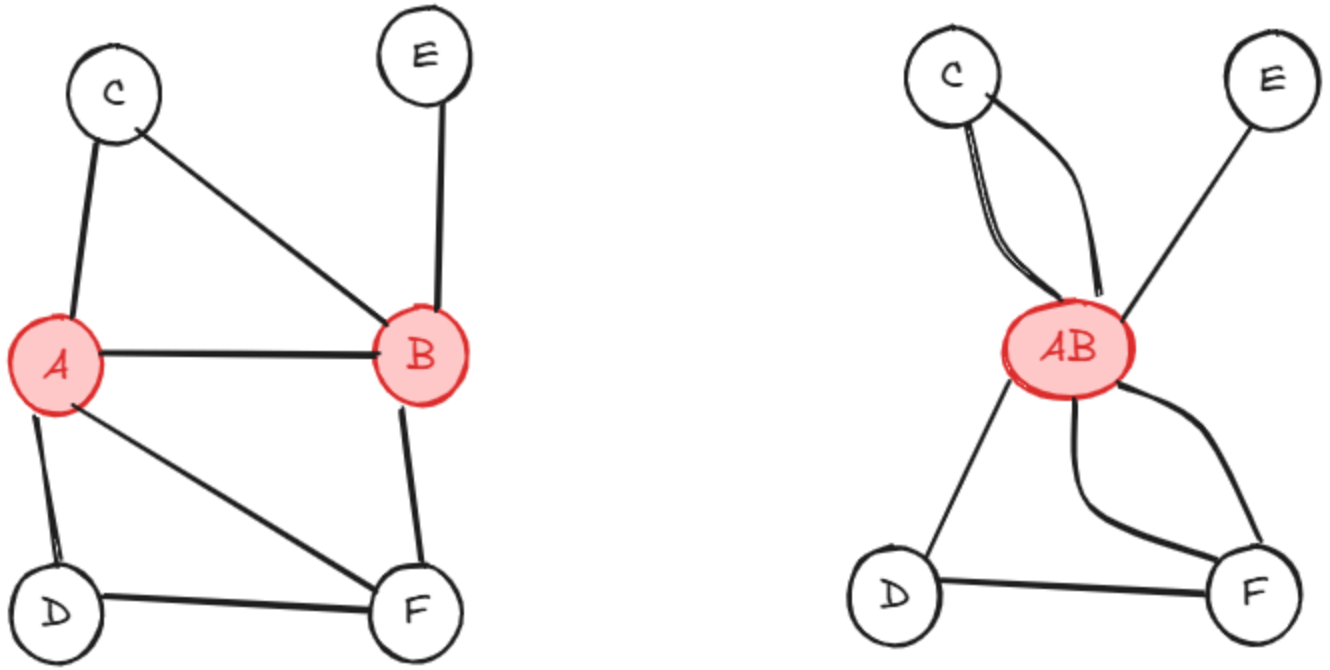
Deterministični algoritem: Nagamochi, Ibaraki (1992)

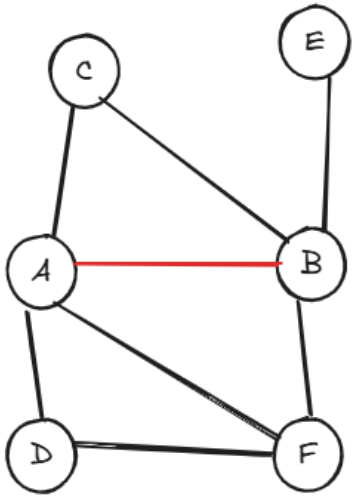
Ponavljaj (dokler nimamo zgolj dveh vozlišč):

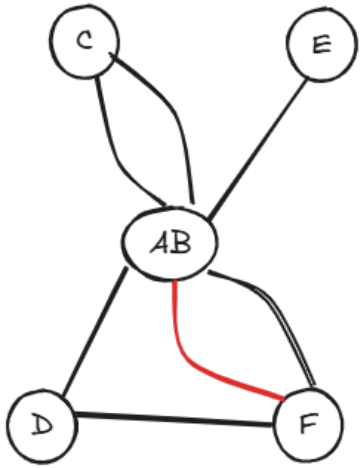
1. detekcija povezave, ki je gotovo ni v najmanjšem prerezu ($O(m)$)
2. združitev krajišč te povezave (skrčitev)

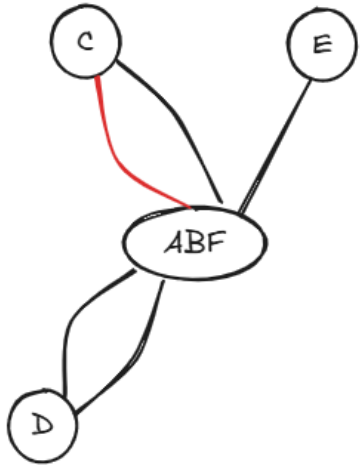
Izbirajmo povezavo povsem naključno?

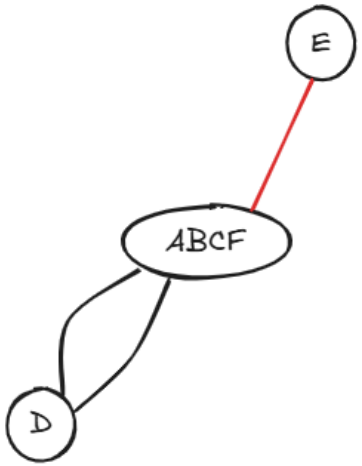
Skrčitev

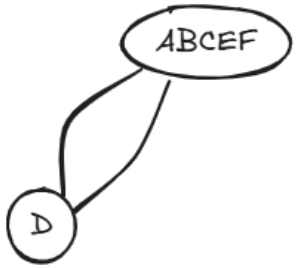



C
E
A
B
D
F


C
E
AB
D
F


C
E
ABF
D


E
ABCF
D


ABCEF
D

Algoritem

```
def min_cut(G=V,E):
  while |V|>2:
    u,v = naključna povezava iz E
    G = contract(G, u, v)
  return G # graf ima samo dve vozlišči, ki predstavljata particijo V
```

Intuicija

- Med izvajanjem imamo med vozlišči večkratne povezave
- Vozlišča predstavjajo že "delne prereze"
- Večji delni prerezi imajo večjo verjetnost, da bodo združeni
- Manjši prerezi imajo večjo verjetno, da preživijo skrčitve

Nekaj oznak

n - število vozlišč, m - število povezav grafa

δ - najmanjša stopnja vozlišča v grafu

C - nek konkreten najmanjši prerez

c - velikost najmanjšega prereza v grafu

Lema o rokovanju

Za vsak neusmerjen graf $G = \langle V, E \rangle$

$$\sum_{v \in V} deg(v) = 2|E|$$

Spodnja meja za število povezav v grafu

Najmanjša stopnja je zgornja meja za minimalni prerez

$$c \leq \delta$$

Če poznamo minimalni prerez lahko ocenimo koliko je najmanj povezav v grafu:

$$m \geq \frac{n\delta}{2} \geq \frac{nc}{2}$$

Verjetnost uspeha

Naj bo S_i dogodek, da smo v i-ti iteraciji izbrali povezavo $e \notin C$.

$$P[\text{ C ostane}] = P[S_1]P[S_2|S_1]P[S_3|S_1S_2]\dots P[S_{n-1}|S_1S_2\dots S_{n-3}]$$

Verjetnost uspeha S_1, $S_2|S_1$

Verjetnost, da s prvo izbiro uničimo C je:

$$\frac{c}{m} \geq \frac{2c}{nc} = \frac{2}{n}$$

P[S_1**]** je torej ($\geq$):

$$1 - \frac{2}{n}$$

P[$S_2|S_1$**]** (presek je isti, vozlišče eno manj)

$$1 - \frac{2}{n-1}$$

Algoritem vrne C

$$P[\text{ C ostane}] = (1 - \frac{2}{n})(1 - \frac{2}{n-1})(1 - \frac{2}{n-2}) \dots (1 - \frac{2}{4})(1 - \frac{2}{3})$$

oklepaje na skupni imenovalec

$$P[\text{ C ostane}] = (\frac{n-2}{n})(\frac{n-3}{n-1})(\frac{n-4}{n-2}) \dots (\frac{2}{4})(\frac{1}{3})$$

okrajšamo:

$$P[\text{ C ostane}] = \frac{2}{n(n-1)}$$

Nekaj o implementaciji

Zgodovina praštevilskosti

- iskanje faktorjev do $\sqrt{n}$
- Eratostenovo rešeto
- **Fermatov mali izrek** (1640)
- **Solovay-Strassen** (1977)
- **Rabin-Miller** (1976)
- AKS (2002)

Skupno ogrodje

1. Izberemo število a na intervalu $1 < a < n - 1$ ($gcd(n, a) = 1$)
2. Izvedemo test (nek izračun v modularni aritmetiki)
3. Če je test negativen je a priča, da je n sestavljeno število
4. Če je test pozitiven je n praštevilo z dovolj veliko verjetnostjo

Ko je test pozitiven, n pa ni praštevilo, je a **lažniva priča**

Fermatov mali izrek

Izrek Če je n praštevilo in $a \in (1..n-1)$, potem

$$a^{n-1} \equiv 1 \pmod{n}$$

problem: Carmichaelova števila

Eulerjev test

Izrek Naj bo $n > 2$ liho število

$$n \text{ je praštevilo} \iff \forall a \in (1..n-1) : a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$$

$\left(\frac{a}{n}\right)$ je Jacobi-jev simbol

Rabin-Millerjev test

Izrek n liho praštevilo $\iff$

$$n - 1 = 2^s \cdot d$$

kjer je d liho število in $s \geq 1$, mora veljati vsaj eden od naslednjih dveh pogojev:

- $a^d \equiv 1 \pmod{n}$
- $\exists r \in \{0, 1, 2, \ldots, s-1\}$, da velja:$a^{2^r \cdot d} \equiv n - 1 \pmod{n}$

Algoritem

Razbijemo $n-1$ na

$$n-1=2^s d$$

in izračunamo:

$$a^d$$

Če je to 1, vrnemo **verjetno praštevilo**, sicer kvadriramo:

$$a^{2d}, a^{4d}, \ldots, a^{2^s d}$$

Sestavljeno število: $a^x \equiv 1$ za $x < n$

Verjetno praštevilo: $a^x \equiv -1$

Primer

89

$88 = 2^3 \cdot 11$ torej $s = 3$ in $d = 11$

Testiranje z $a = 2$

$$2^{11} = 1$$

$a = 7$

$$7^{11} = 37, 7^{2 \cdot 11} = 34, 7^{4 \cdot 11} = 88 = -1$$

Verjetnost napak

- **Fermatov mali izrek**: nezanesljiv zaradi Carmichaelovih števil ($561, 1105, \ldots$) večina a-jev je lažnivcev.
- **Euler-jev kriterij**. verjetnost napake je največ $1/2$
- **Miller-Rabin**: verjetnost napake je največ $1/4$.

Primer

561

Generiranje praštevil

k - bitno praštevilo

Ponavljamo:

- n = naključen niz 0 in 1 (začne in konča se z 1) dolžine k
- če n je verjetno praštevilo
  - vrnemo n

Praštevilski izrek

Število praštevil na intervalu $[1 \ldots n]$ je $\approx \frac{n}{\ln n}$