

mriežka $\sqrt{n} \times \sqrt{n}$, prednosť má hocikto; ukážte, že v najhoršom prípade treba viac ako $2\sqrt{n}$ krokov, ale stačí $O(\sqrt{n})$

mriežka $\sqrt{n} \times \sqrt{n}$, v každom vrchole správa do náhodného. Ukážte, že w.h.p. do žiadneho vrchola nesmeruje viac ako $3 \log n / \log \log n$ správ.

majme cestu z n procesorov, každý chce routovať práve dva pakety (červený a modrý), pričom červené aj zelené tvoria permutáciu. ukážte, že stačí n krokov

Problém dohody

- synchronný systém
- známe identifikátory
- každý má na vstupe 0/1
- správy sa môžu strácať
- každý proces sa musí rozhodnúť
- treba zaručiť
 - **Dohoda:** všetky procesy sa rozhodnú na tú istú hodnotu
 - **Terminácia:** každý proces sa rozhodne v konečnom čase
 - **Netrivialita:**
 - 1 Ak všetci začnú s hodnotou 0, musia sa dohodnúť na 0.
 - 2 Ak všetci začnú s hodnotou 1 a správy sa nestrácajú, musia sa dohodnúť na 1.

neexistuje deterministické riešenie

- 2 vrcholy, 1 linka
- sporom, nech existuje a trvá r kôl
- výpočet, kde začnú obaja s hodnotou 1 a nestrácajú sa správy
- dohodnú sa na 1
- stratí sa posledná správa, jeden z nich to nezistí
- výpočet, kde neprejde ani jedna správa a dohodnú sa na 1
- jeden z nich dostane na vstup 0
- aj druhý

randomizované riešenie (úplný graf)

komunikačný pattern

zoznam trojíc (i, j, t) : v čase t sa nestratí správa z $i \mapsto j$

(fixný) adversary = vstup a komunikačný pattern

Dohoda: $Pr[\text{nejaké dva procesy sa rozhodnú na rôznu hodnotu}] \leq \varepsilon$

algoritmus s $\varepsilon = 1/r$

daný adversary γ : dvojice (i, t) , kde i -procesor, t -čas majme usporiadanie:

- 1 $(i, t) \leq_{\gamma} (i, t')$, kde $t \leq t'$
- 2 ak $(i, j, t) \in \gamma$, tak $(i, t - 1) \leq_{\gamma} (j, t)$
- 3 tranzitivita

úroveň informovanosti

- 1 $level_{\gamma}(i, 0) = 0$
- 2 ak $t > 0$ a existuje $j \neq i$ také, že $(j, 0) \not\leq_{\gamma} (i, t)$, tak $level_{\gamma}(i, t) = 0$
- 3 nech l_j je $\max\{level_{\gamma}(j, t') \mid (j, t') \leq_{\gamma} (i, t)\}$
potom $level_{\gamma}(i, t) = 1 + \min\{l_j \mid j \neq i\}$

- 1 $level_\gamma(i, 0) = 0$
- 2 ak $t > 0$ a existuje $j \neq i$ také, že $(j, 0) \not\leq_\gamma (i, t)$, tak $level_\gamma(i, t) = 0$
- 3 nech l_j je $\max\{level_\gamma(j, t') \mid (j, t') \leq_\gamma (i, t)\}$
potom $level_\gamma(i, t) = 1 + \min\{l_j \mid j \neq i\}$

algorithmus

- prvý proces vygeneruje náhodný kľúč
- procesy si počítajú level
- rozhodnutie 1, ak všetci majú 1 a môj level je aspoň kľúč

```

rounds := rounds + 1
let  $(L_j, V_j, k_j)$  be the message from  $j$ , for each  $j$  from which a message arrives
if some  $k_j \neq \text{undefined}$  then  $key := k_j$ 
for all  $j \neq i$  do
  if some  $V_{i'}(j) \neq \text{undefined}$  then  $val(j) := V_{i'}(j)$ 
  if some  $L_{i'}(j) > level(j)$  then  $level(j) := \max\{L_{i'}(j)\}$ 
 $level(i) := 1 + \min\{level(j) : j \neq i\}$ 
if  $rounds = r$  then
  if  $key \neq \text{undefined}$  and  $level(i) \geq key$  and  $val(j) = 1$  for all  $j$  then
     $decision := 1$ 
  else  $decision := 0$ 

```

- **Dohoda:** $Pr[\text{nejaké dva procesy sa rozhodnú na rôznu hodnotu}] \leq \epsilon$
- **Terminácia:** každý proces sa rozhodne v konečnom čase
- **Netrivialita:**
 - 1 Ak všetci začnú s hodnotou 0, musia sa dohodnúť na 0.
 - 2 Ak všetci začnú s hodnotou 1 a správy sa neštrácajú, musia sa dohodnúť na 1.

terminácia a netrivialita sú zrejmé
pre fixný pattern, aká je pravdepodobnosť nezhody?
levely sa líšia max o 1, preto jediný problém je ak $key = \max\{l_j\}$

dolný odhad

ľubovoľný r -kolový algoritmus má pravdepodobnosť nezhody aspoň $\frac{1}{r+1}$

orez

pre adversary B s patternom γ a proces i , $B' = \text{prune}(B, i)$

- 1 ak $(j, 0) \leq_{\gamma} (i, r)$ tak sa vstup j zachová, inak znuluje
- 2 trojica (j, j', t) je v kom. patterne B' , akk je v γ a $(j', t) \leq_{\gamma} (i, r)$

$$P^B[i \text{ sa rozhodne } 1] = P^{\text{prune}(B,i)}[i \text{ sa rozhodne } 1]$$

lema

Ak majú na vstupe všetci 1, $P[i \text{ sa rozhodne } 1] \leq \varepsilon(\text{level}(i, r) + 1)$

lema

Ak majú na vstupe všetci 1, $P[i \text{ sa rozhodne } 1] \leq \varepsilon(\text{level}(i, r) + 1)$

- indukcia na $\text{level}(i, r)$: nech $\text{level}(i, r) = 0$:
- $B' = \text{prune}(B, i) = \text{prune}(B', i)$
- $P^B[i \text{ sa rozhodne } 1] = P^{B'}[i \text{ sa rozhodne } 1]$
- od j -čka neprišla správa, $B'' = \text{prune}(B', j) = \text{prune}(B'', j)$ je triviálny adversary
- $P^{B'}[j \text{ sa rozhodne } 1] = P^{B''}[j \text{ sa rozhodne } 1]$
- lenže $P^{B''}[j \text{ sa rozhodne } 1] = 0$, takže $P^{B'}[j \text{ sa rozhodne } 1] = 0$
- pst' nezhody je ε , $\Rightarrow |P^{B'}[i \text{ sa rozhodne } 1] - P^{B'}[j \text{ sa rozhodne } 1]| \leq \varepsilon$
- preto $P^{B'}[i \text{ sa rozhodne } 1] \leq \varepsilon$ a $P^B[i \text{ sa rozhodne } 1] \leq \varepsilon$
- nech $\text{level}(i, r) > 0$
- $B' = \text{prune}(B, i) = \text{prune}(B', i)$
- existuje j , že $\text{level}_{B'}(j, r) \leq l - 1$
- podľa i.p. $P^{B'}[j \text{ sa rozhodne } 1] \leq \varepsilon(\text{level}(j, r) + 1) \leq \varepsilon l$
- pst' nezhody je ε , $\Rightarrow |P^{B'}[i \text{ sa rozhodne } 1] - P^{B'}[j \text{ sa rozhodne } 1]| \leq \varepsilon$
- preto $P^{B'}[i \text{ sa rozhodne } 1] \leq \varepsilon(l + 1)$ a $P^B[i \text{ sa rozhodne } 1] \leq \varepsilon(l + 1)$

Problém dohody

- synchrónny systém
- známe identifikátory
- každý má na vstupe 0/1
- proces môže havarovať (uprostred posielania správ)
- maximálne f havarovaných procesov
- každý proces sa musí rozhodnúť
- treba zaručiť
 - **Dohoda:** všetky procesy (ktoré nehavarovali) sa rozhodnú na tú istú hodnotu
 - **Terminácia:** každý proces (ktorý nehavaroval) sa rozhodne v konečnom čase
 - **Netrivialita:** ak všetci začnú s rovnakou hodnotou i , musia sa dohodnúť na i .

algorithmus

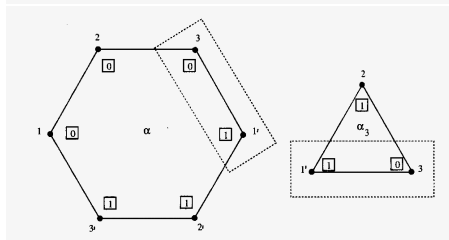
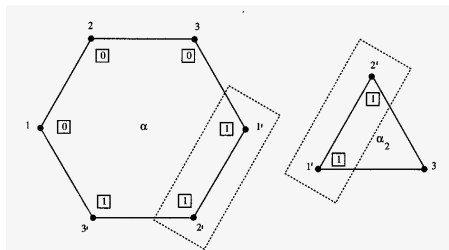
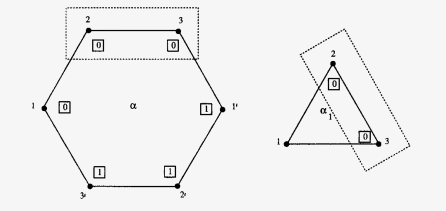
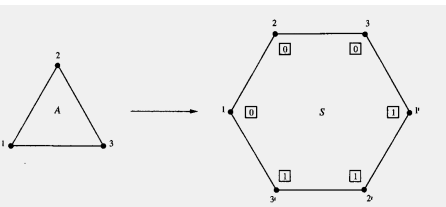
flood počas $f + 1$ kôl; ak je iba jedna hodnota, rozhodni sa, inak (default) 0

- existuje kolo, v ktorom nikto nehavaruje; potom sa udržiavajú rovnaké hodnoty
- $(f + 1)n^2$ správ
- zlepšenie: posielat' iba keď sa zmení hodnota $\Rightarrow O(n^2)$ správ

Problém dohody

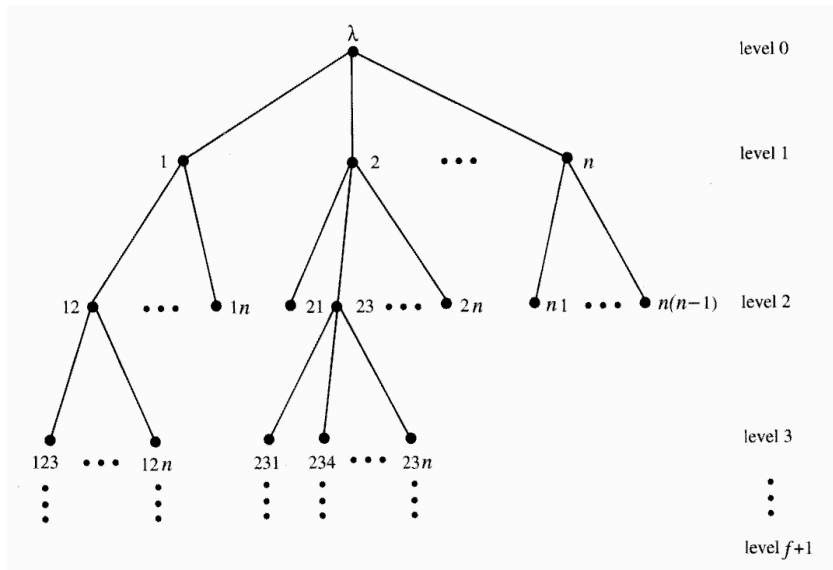
- synchronný systém
- známe identifikátory
- každý má na vstupe 0/1
- niektoré procesy sú *zlé*
- maximálne f zlých procesov
- každý proces sa musí rozhodnúť
- treba zaručiť
 - **Dohoda:** všetky dobré procesy sa rozhodnú na tú istú hodnotu
 - **Terminácia:** každý dobrý proces sa rozhodne v konečnom čase
 - **Netrivialita:** ak všetci dobrí začnú s rovnakou hodnotou i , všetci dobrí sa musia dohodnúť na i .

dolný odhad na počet zlých: jeden zlý spomedzi troch



pre viac: simulácia

EIG algoritmus



$newval(x)$: väčšina z $newval(x_j)$

dôkaz

lema

Po $f + 1$ kolách platí: nech $j, j, k, i \neq j$ sú tri dobré procesy. Potom $val(xk)_i = val(xk)_j$ pre všetky x .

lema

Po $f + 1$ kolách platí: nech k je dobrý proces. Potom existuje v , že $val(xk)_i = newval(xk)_i = v$ pre všetky dobré procesy i

lema

keď všetci začnú s rovnakou hodnotou, musia sa na nej dohodnúť

vrchol x je *dobrý*, ak všetky dobré procesy i majú po $f + 1$ kolách $newval(x)_i = v$ pre nejaké v

lema

Po $f + 1$ kolách je na každej ceste z koreňa do listu dobrý vrchol

lema

Po $f + 1$ kolách: ak existuje pokrytie podstromu vo vrchole x dobrými vrcholmi, potom x je dobrý.

konzistentný broadcast

- ak dobrý proces i poslal (m, i, r) v kroku r , dobrí ju akceptujú najneskôr v $r + 1$
- ak dobrý proces i neposlal (m, i, r) v kroku r , nikto dobrý ju neakceptuje
- ak je správa (m, i, r) akceptovaná dobrým j v r' , najneskôr v $r' + 1$ ju akc. všetci dobrí

algoritmus

- i pošle $(init, m, i, r)$ v kole r
- ak dobrý dostane $(init, m, i, r)$ v kole r , pošle $(echo, m, i, r)$ všetkým dobrým v kole $r + 1$
- ak pred kolom $r' \geq r + 2$ dostane dobrý od $f + 1$ echo, pošle $(echo, m, i, r)$ v r'
- ak dostal echo od $n - f$, akceptuje

dohoda

- dvojkrovové fázy
- v prvom kole bcastujú všetci s 1
- v kole $2s - 1$ pošlú tí, čo akceptovali od $f + s - 1$ a ešte nebcastovali
- ak po $2(f + 1)$ kolách i akceptoval od $2f + 1$ procesov, tak 1, inak 0