Komunikační složitost

- Alice a Bob mají bitové řetězce x, y délek n
- oba se chtějí dozvědět výsledek $f(x,y)$ nějaké fce $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$
- Alice a Bob mají neomezené výpočetní prostředky
- ALE ⚠ nevidí vstupy toho druhého
- takže spolu musí Alice a Bob komunikovat
- mohou si posílat zprávy neomezené délky a mohou si dopředu dohodnout strategii, která může záviset na konkrétní fci f, ale určitě ne na vstupech x,y
  - takové strategii se říká **komunikační protokol pro f**
- pozn: v protokolu si zprávidla jeden spočítá $f(x,y)$ a jako poslední zprávu tuto hodnotu pošlou druhému
- a co měříme u nějakého konkrétního protokolu je maximální množství bitů přes všechny vstupy x,y, které si musí Alice a Bob musí učinit, aby spočítali $f(x,y)$
- **komunikační složitost fce f** $CC(f)$ je # bitů, které si musí vyměnit nejlepší strategie
  - tj. min přes protokoly a max přes vstupy

Triv. horní odhad pro libovolnou f je $n+1$

- jeden pošle celý vstup, druhý výsledek $f(x,y)$

Parita

- $f(x,y) = \sum x_i + \sum y_i \mod 2$

protokol

- Alice pošle $\sum x_i \mod 2 = p$
- Bob pošle $\left(\sum y_i + p\right) \mod 2$
- $CC(\text{parita}) \leq 2$, je to ostré?

· 1 bit znamená, že nám jeden a ten se nic nedozví od toho druhého

---

Majorita

· $f(x,y) = \begin{cases} 1 & \text{pokud } \# \text{jedniček je aspoň } n \\ 0 & \text{jinak} \end{cases}$

protokol

· Alice pošle # jedniček

· Bob pošle $f(x,y)$

→ $\lg n + 1$ bit

· lower bound?

Medián

· Alice a Bob mají prvky podmnožiny $X, Y \subseteq [n]$ resp. char. vektory $x_i = 1 \Leftrightarrow i \in X$ $\forall i \in [n]$

· chceme spočítat medián multimnožiny $X \cup_{multi} Y$

$O(\lg^2 n)$ protokol přes binární půlení

· Alice i Bob si udržují interval $[i,j]$ ve kterém může být medián $X \cup Y$

· Alice pošle # prvků menších než $\frac{i+j}{2}$ a # prvků větších než $\frac{i+j}{2}$

· Bob zjistí, jestli medián $\leq \frac{i+j}{2}$ nebo ne a pošle 1 zpět

→ $O(\lg n)$ fází, $O(\lg n)$ bitů v každé fázi

Alternativní $O(\lg^2 n)$ protokol, ze kterého vzniknou $\lg n$

· BÚNO n je mocnina dvou

· můžeme si v $\lg n$ vyměnit velikosti $|X|, |Y|$

· přidáme spárovaný # přesně $-\infty$ a $+\infty$ než tomu šlo hůře

· Alice si udržuje X' = mn. potenciálních mediánů v jejím vstupu, Bob Y' obdobně

· na začátku $X' = X$, $Y' = Y$

· Alice pošle medián $X' = a$, Bob medián $Y' = b$

· $a = b$? $a = b$ je medián

· $a < b$? prvky menší než a určitě nebudou medián $\Rightarrow$ z X' vyhodím čísla menší než a

Y' — " — větší než b

větší: — " —

· $a > b$ naopak

· $X \cup_{multi} Y$ se seřadí v lineárním čase o příčku

· pokud $|X'| = |Y'| = 1$, pak menší z těch dvou je medián

snížení na $\log n$

· kombinace na "$a < b$"? lze dělat od nejvýznamnějších bitů

· pokud např $a < b$, pak medián je mezi a a b

· takže v další fázi se pokračuje mediány lineárně shodovat na těch významných bitech,

na kterých se shodují a a b

→ každé z $\log n$ sečtřídění si vyžádá $\leq$ jednou

→ $O(\log n)$ složitost

Složitost s nápovědou

Věta: Pokud pro nějaký stream. problém umíme stream alg pracující v prostoru $s(n)$, pak umíme i problém s $O(s(n))$ bity. (konst. je asi 8)

myšlenka:
- vstup stream alg si rozdělíme na první půlku x a druhou půlku y
- Alice si odsimuluje stream alg na x a pošle svůj obsah paměti na linci
- Bob si obsah paměti obnoví ze zprávy a dojede si alg na zbytku

→ regulární jazyky mají konst. kom. problém

aplikace: dolní odhad na kom. složitost ⇒ dolní odhad na stream. algoritmy

---

Karchmer - Widgerson games

- mějme bool. fci $f: \{0,1\}^n \to \{0,1\}$ a zajímá nás min hloubka (AND, OR, NOT) obvodu pro f, kde hradla mají aritu ≤ 2
- hra: Alice má $x \in \{0,1\}^n$ a Bob $y \in \{0,1\}^n$ t.ž. $f(x) \neq f(y)$.
  - cíl: najít $i \in [n]$ t.ž. $x_i \neq y_i$ (kdyby neexistovalo, pak $f(x) = f(y) \Leftarrow x = y$)
    (lg n bitů)

Věta: min hloubka obvodu pro f $= \Theta(CC(f))$

Dk:

$CC(f) \leq depth(f)$

- skonstruujeme protokol na základě obvodu
- BÚNO nejpravější hradlo je AND, $f(x)=0$, $f(y)=1$
- pokud $f(x)=0$ ⇒ alespoň jeden ze dvou vstupů vrcholu hradla je 0 pro Alici
- ale $f(y)=1$ ⇒ oba vstupy pro vrchní hradlo Boba jsou 1

→ Alice řekne, jestli levý či pravý bit je 0 → 1 bit komunikace

. rekurzivně zvýše o hladinu níže

. eventuálně dojdeme ke vstupnímu bitu, na kterém se číst (vstup je tedy kvantk. posloupnost 0 nebo 1)

$depth(f) \leq cc(f)$

. dá se udělat, ale není důležité pro nás

. je potřeba si uvědomit, co protokol dělá

. na základě čeho se rozhodnje Alice, jestli první poslaný b.t je 0 či 1?

. podle vstupu

. kořen tedy reprezentuje všechny možné vstupy a vnitřní vrcholy zase podmn. vstupů

. no a z toho se nějak určí obvod