Set-Intersection & Applications

Randomised protocol $\underbrace{\Pi}_{}$ (cost c) is a probability dist. over deterministic protocols (cost $\le c$). Π computes $f: \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ with error $\varepsilon > 0$ if

$$\forall (x,y) \in \mathcal{X} \times \mathcal{Y}: \quad \Pr_{\pi \sim \Pi}\left[\pi(x,y) = f(x,y)\right] \geq 1 - \varepsilon$$

$R^{cc}_{\varepsilon}(f)$ = least cost of ε-error protocol for f

Ex $R^{cc}_{\varepsilon}(EQ_n) = O(\log \frac{1}{\varepsilon})$ $\quad r \in_R \{0,1\}^n$

$\underline{\langle x, r \rangle}_{\in \{0,1\}} = \langle y, r \rangle \mod 2$

Ex $R^{cc}_{\frac{1}{3}}(GT_n) = \tilde{O}(\log n)$ $\quad x = 1101011$
$\quad y = 1100101$

IDEA: binary search find firs (most significant) bit where $x_i \neq y_i$

Run $\log n$ many EQ tests, each with error $\varepsilon < \frac{1}{3} \cdot \frac{1}{\log n}$

$\Rightarrow$ Cost: $O(\log n \cdot \log \log n)$

Set-Intersection hype

Alice: $x \subseteq [n]$ $\quad$ output: $x \cap y \overset{?}{\neq} \emptyset$

Bob: $y \subseteq [n]$

- Easy ($\in NP^{cc}$) hard problem ($\notin BPP^{cc}$)
- "NP-complete" (Exercise)
- reductions from SI ubiquitous

• reductions from SI (disguised)

Thm [KS'87] $R^{cc}_{\frac{1}{3}}(SI_n) = \Omega(n)$ (Difficult proof)

Application to circuit complexity

Circuit size $\cong$ Time complexity

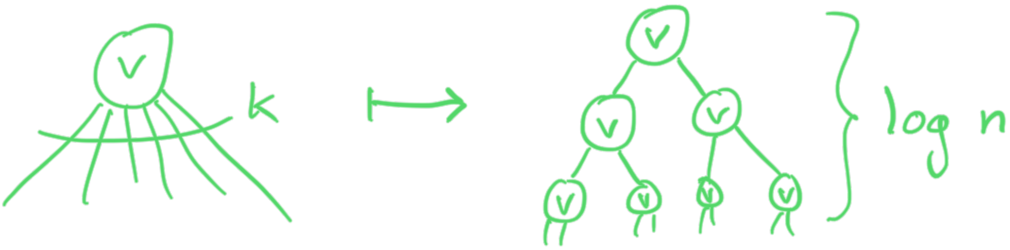
depth $\cong$ Parallel time compl.

$L \to NL \to \underbrace{NC}_{} \to P$

"Nick's Class"

= languages that admit uniform / Fan-in 2 polysized circuits of depth $(\log n)^{O(1)}$

uniform: $\exists$ polytime TM $1^n \mapsto C_n$



Surprise: Depth can be characterised communication language !

Fix $f: \{0,1\}^n \to \{0,1\}$

Monotone Karchmer–Wigderson game for f: ← monotone

Alice: $x \in f^{-1}(1)$

Bob: $y \in f^{-1}(0)$

$[\forall i: x_i \leq y_i \Rightarrow f(x) \leq f(y)]$, $f(x) = 1$, $f(y) = 0$

$x_i = 1, \quad y_i = 0$

Find: $i \in [n]$ s.t. ~~$x_i \neq y_i$~~

Thm $D^{cc}(KW_F^+) = \mathrm{depth}^+(F)$ $\quad \left[R^{cc}_{\frac{1}{3}}(KW_F) \leq O(\log n) \right]$

Note: Hopeless to prove lower bounds on $D^{cc}(KW_f)$ — would separate complexity classes

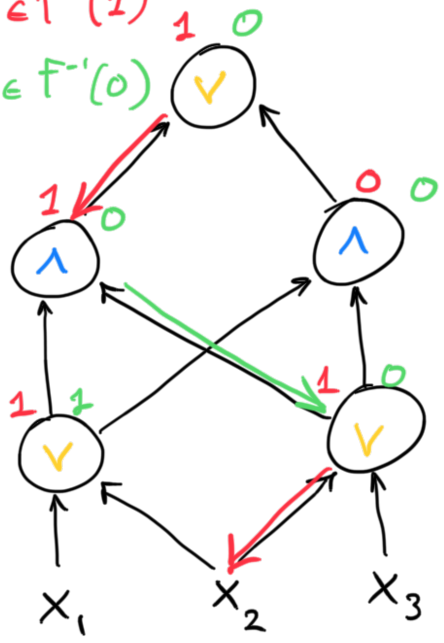
Relaxation: Monotone circuits (no $\neg$-gates) only $\wedge$, $\vee$

f monotone $\iff$ $x \leq y$ $(\forall i: x_i \leq y_i)$ $\Rightarrow f(x) \leq f(y)$

Proof $D^{cc}(KW_F^+) \leq \mathrm{depth}^+(f)$

A: $x \in f^{-1}(1)$

B: $y \in f^{-1}(0)$



Start at the top gate g

$$\boxed{\begin{array}{l} g(x) = 1 \\ g(y) = 0 \end{array}}$$

invariant

Move to child of g

- comm. 1 bit
- retain invariant

End up in leaf

$x_i = 1$

$y_i = 0$

Thm [RW92] Mon. circuits for $\underbrace{\text{matching}}_{\mathrm{Match}: \{0,1\}^{\binom{n}{2}} \to \{0,1\}}$ need depth $\Omega(n)$

Cor: $D^{cc}(KW^+_{\ \ }) \geq \Omega(n)$

Show $D(KW_{Match}) \geq \Omega(n)$

by reduction from SI_n

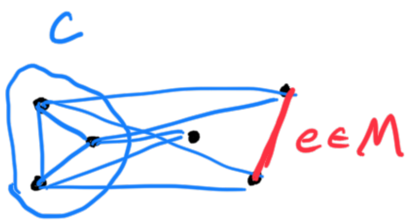
KW^+_{Match} $m = 3n+2$, Match $= 1$ iff $\exists$ Match size $\geq n+1$

Alice: matching $M \subseteq \binom{[3n+2]}{2}$, $|M| = n+1$

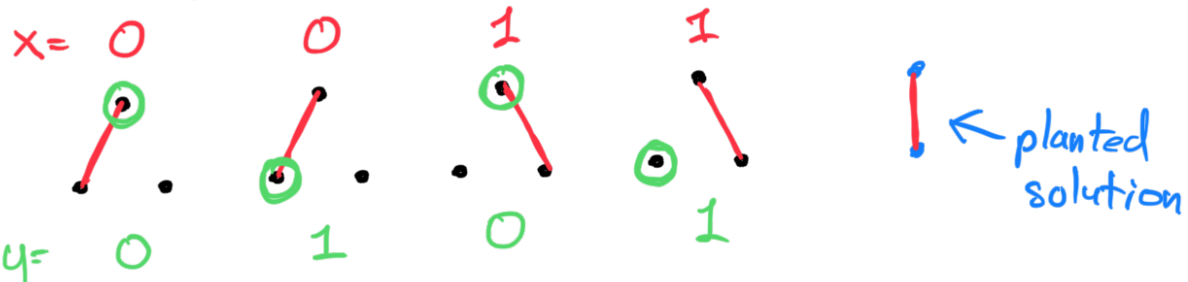
Bob: set $C \subseteq [3n+2]$, $|C| = n$

Find $e \in M$ disjoint from C

Bob's graph



Let $x, y \in \{0,1\}^n$ be inputs to SI_n



#sols to KW^+ is $|x \cap y| + 1$

- Reduction $(x,y) \longmapsto (M, C)$
- Randomly relabel nodes
- Run hypothetical KW^+ protocol

  ↳ if returns planted, output disjoint

  non-plant, output inter

if disjoint $\Rightarrow$ out disjoint w.p. 1

intersect $\Rightarrow$ out intersect w.p. $\frac{1}{2}$