APPLICATIONS

- Streaming
- Property Testing
- game theory
- TIME/SPACE Turing Machine LBs

Last class

- Circuit complexity
- Proof complexity
- Extension Complexity
- clique/coclique, graph Theory, Learning Partial Functions

Main cc Lower Bounds

UDISJ : disjointness with promise that either $|x \cap y| = 0$ or $|x \cap y| = 1$

Theorem

$$BPP^{cc}(DISJ) = \Omega(n)$$

$$BPP^{cc}(UDISJ) = \Omega(n)$$

$$coNP^{cc}(UDISJ) = \Omega(n)$$

Theorem

The k-player NOF randomized cc of DISJ, UDISJ is $\Omega\left(\frac{n}{2^k}\right)$

We will prove these in a couple of weeks

APPLICATIONS

- Streaming
- Property Testing
- game theory
- TIME/SPACE Turing Machine LBs
- Circuit complexity
- Proof complexity
- Extension Complexity
- Monotone Span Programs / Linear Secret Sharing Schemes
- Clique-Coclique, graph Theory, Learning

all USE LIFTING TECHNIQUE

COMMUNICATION FOR SEARCH PROBLEMS

10111

00110

$S \subseteq \{0,1\}^n \times \{0,1\}^n \times \Theta$

Example 1 (KW Search)

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

Output $i \in [n]$ such that $x_i \neq y_i$

COMMUNICATION FOR SEARCH PROBLEMS

10111

00110

$S \subseteq \{0,1\}^n \times \{0,1\}^n \times \mathcal{O}$

Example 2 (CNF Search)

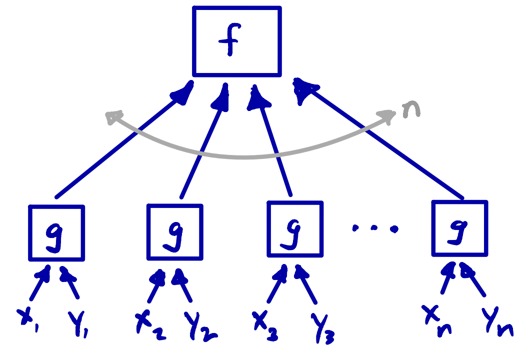
Fix an unsatisfiable CNF $\mathcal{C}$ over $x_1 \dots x_n$ $y_1 \dots y_n$

Alice: $x \in \{0,1\}^n$ Bob: $y \in \{0,1\}^n$

Output clause C_i falsified by (x,y)

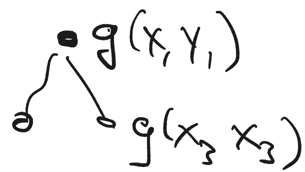
QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \mathcal{O}$ $\rightsquigarrow$ F :



DT for f :

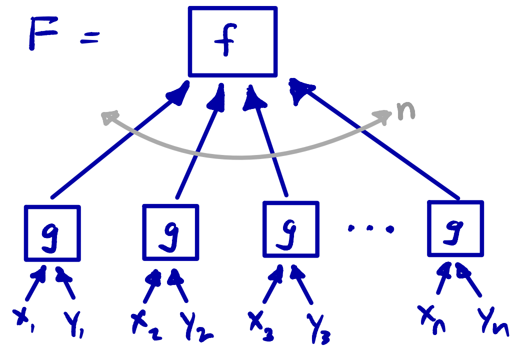
T



$$\text{cost} \approx \underbrace{\text{cost of } g}_{\substack{O(\log n) \\ O(1)}} \cdot \text{dt-ht of } T$$

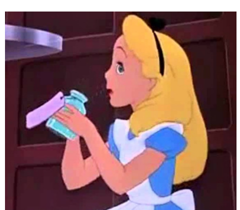
QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to \mathcal{O}$ $\rightsquigarrow$ $F =$



LIFTING THEOREM

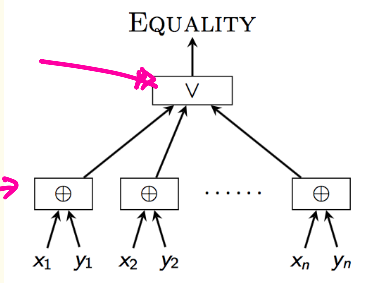
Communication Complexity of F $\approx$ Query complexity of f

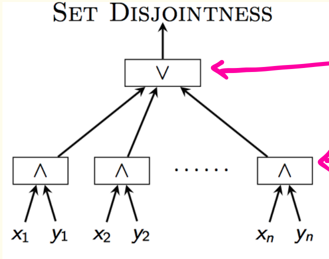


INTUITION: MOST HARD COMMUNICATION PROBLEMS ARE COMPOSED FUNCTIONS $f \circ g^n$

f : OR

g: =



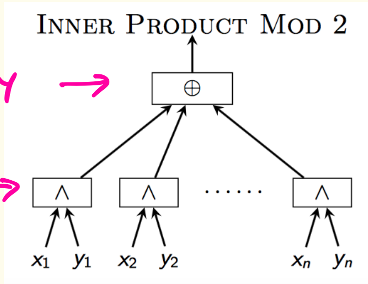


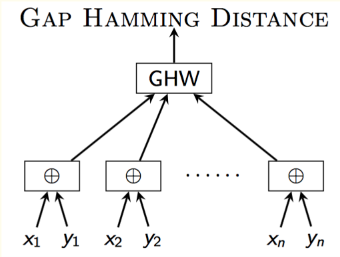
f : OR

g: AND

f: PARITY

g: AND





(SOME) LIFTING THEOREMS

	Measure on $f \circ g^n$	Measure on f
Raz-McKenzie '99	Deterministic CC	Decision tree
Razborov '03	Quantum CC	approx. degree
Sherstov '07	discrepancy, sign rank, unbded error	Threshold degree
Göös-P '14	Randomized CC	(critical) Block Sensitivity
GLMWZ '15	Nondeterministic CC, Partition	approx. Junta degree
Lee-Raghavendra Steurer '15	Semidefinite Rank	SOS degree
RPRC '16 PR '17, PR '17b	Razborov Rank/ Algebraic Tiling	algebraic gap degree Nullsatz. degree
KMR '16	Nonnegative Rank	Junta degree
Göös-P-Watson '17	Randomized CC	Randomized dec. tree

Lifting Theorems Makes Lower Bounds Easy!

2 step Recipe:

1. Prove problem specific query lower bound

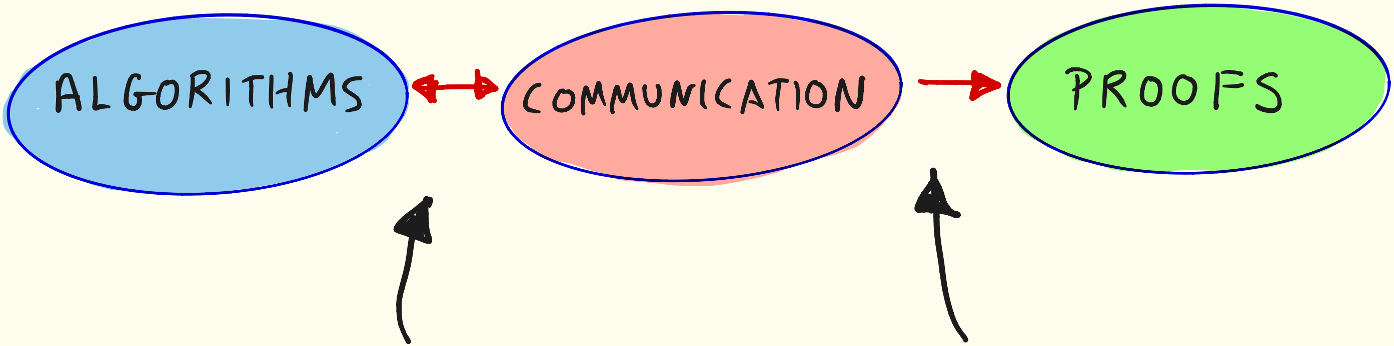
2. Apply Lifting theorem to obtain communication complexity lower bound

APPLICATIONS

- Streaming
- Property Testing
- game theory
- TIME/SPACE Turing Machine LBs
- Circuit complexity
- Proof complexity
- Extension Complexity
- clique/coclique, Graph Theory, Learning Partial Functions

Very Similar use of Lifting Plus other common ideas

INTRO : LIFTING QUERY TO CC LOWER BOUNDS



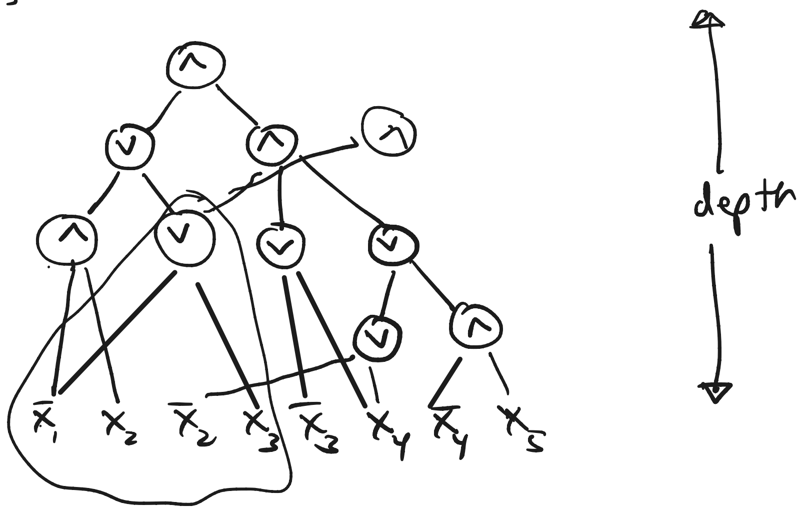
Use communication complexity to capture underlying class of algorithms

New **LIFTING THEOREMS** to reduce communication lower bounds to much simpler Lower bounds on query complexity of search problems

CIRCUIT DEPTH / FORMULA SIZE

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

formula for f :



size (F) = # vertices

<u>Lemma</u> $\log(\text{size}(f)) = \Theta(\text{depth}(f))$

Monotone CIRCUIT DEPTH (+ FORMULA SIZE) LBS (a little history)

Thm [Karchmer-Wigderson]
any monotone formula for STCONN requires depth $\Omega(\log^2 n)$

Thm [Raz-McKenzie]
For any $d \geq 1$ $\exists$ monotone $f_d : \{0,1\}^n \to \{0,1\}$ st.

$$f \in \text{mdepth}(\log^{d+1} n), \quad f \notin \text{mdepth}(\log^d n)$$

Thm [Raz-Wigderson]
any monotone circuit for matching (n^2 inputs)
requires depth $\Omega(n)$

Thm [Razborov]
Monotone circuits for CLIQUE on G_n require size 2^{n^ε} for some $\varepsilon > 0$

MONOTONE CIRCUIT DEPTH LBS VIA LIFTING

Theorem [Göös-Pitassi]

$\exists$ explicit monotone $f \in NP$ requiring monotone circuit depth $\Omega(n/\log n)$

$\exists$ explicit monotone $f \in P$ requiring monotone ckt depth $\Omega(\sqrt{n})$

Proof

Lifting Theorem from critical Block sensitivity to Randomized CC

a reduction to UDISJ
gadget has constant size
even works for NOF cc

Alternative Proof [Raz-McKenzie, GPW'15]

Deterministic Lifting Theorem (Decision tree to cc)

harder proof
gadget Larger
but Lifting theorem stronger

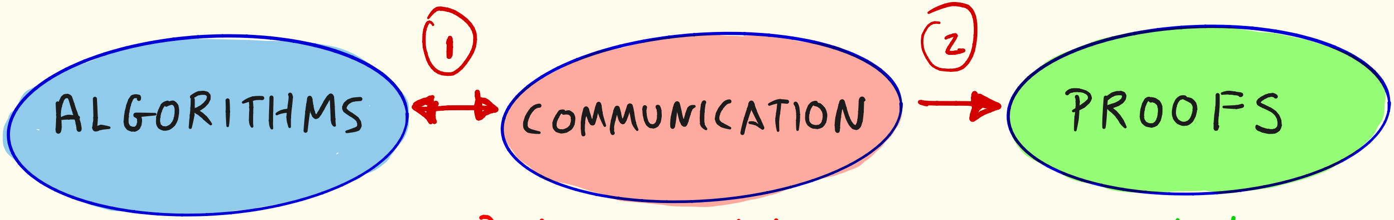
MONOTONE CIRCUIT SIZE LBS VIA LIFTING

[GGKS] give alternative LB on monotone circuit size via dag-like dec tree $\rightarrow$ dag-CC lifting

Lifting in same spirit used to prove

1. Extension complexity LBs
2. Monotone Span Program / Secret sharing scheme LBs

I. MONOTONE FORMULA/CIRCUIT DEPTH LBS



Monotone Circuit Depth

Deterministic CC of KW

Resolution

(Decision Tree OR BLOCK sensitivity of search problem)

1 CIRCUIT DEPTH & CC EQUIVALENCE

Defn Let $f : \{0,1\}^n \to \{0,1\}$.

$\mathrm{Search}_f \subseteq \{0,1\}^n \times \{0,1\}^n \times [n]$

Alice receives $x \in f^{-1}(1)$
Bob receives $y \in f^{-1}(0)$

Output $i \in [n]$ such that $x_i \neq y_i$

$\mathrm{mSearch}_f$: f monotone

output $i \in [n]$ such that $x_i = 1$, $y_i = 0$

Thm $cc(\mathrm{Search}_f) = \text{ckt-depth}(f)$

$cc(\mathrm{mSearch}_f) = \text{mono. ckt -depth}(f)$

Theorem 1 $\quad cc(\mathrm{Search}_f) = F\text{-depth}(f)$

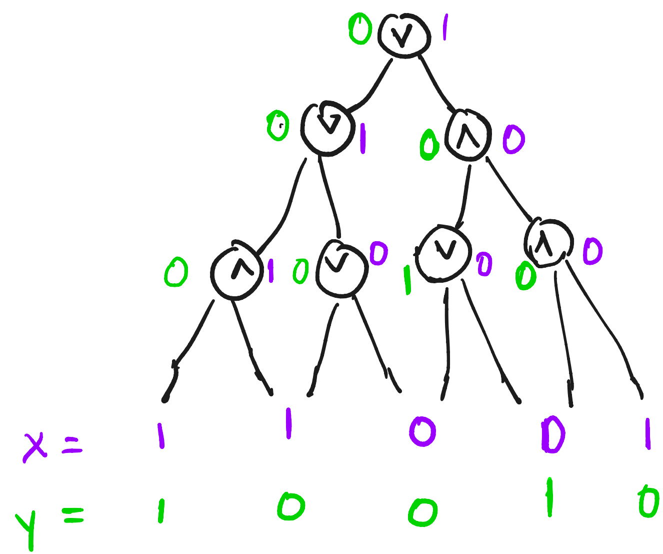
$cc(\mathrm{mSearch}_f) = \text{monotone } F\text{-depth}(f)$

Pf ($\Rightarrow$) Let F be a formula for f. Then $cc(\mathrm{Search}_f) \leq \mathrm{depth}(F)$

Let F be a monotone formula for f (monotone). Then $cc(\mathrm{mSearch}_f) \leq \mathrm{mdepth}(F)$

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

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



Theorem 1 $cc(\text{Search}_f) = \text{F-depth}(f)$

$cc(\text{mSearch}_f) = \text{monotone F-depth}(f)$

Pf ($\Rightarrow$) Let F be a formula for f. Then $cc(\text{Search}_f) \leq \text{depth}(F)$

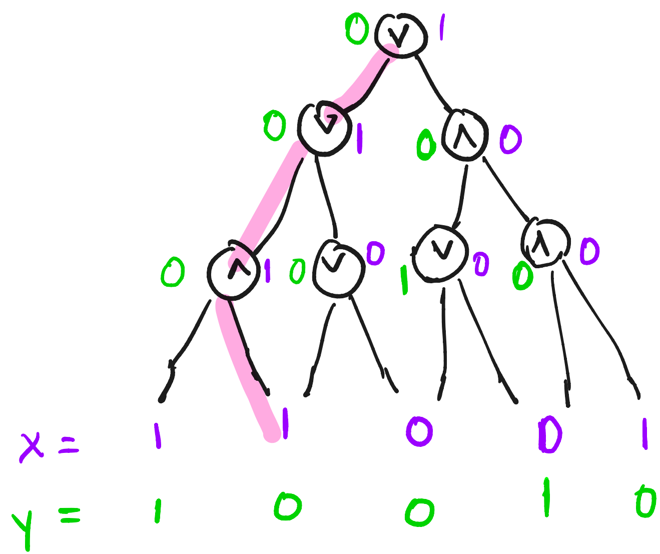
Let F be a monotone formula for f (monotone). Then $cc(\text{mSearch}_f) \leq \text{mdepth}(F)$

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

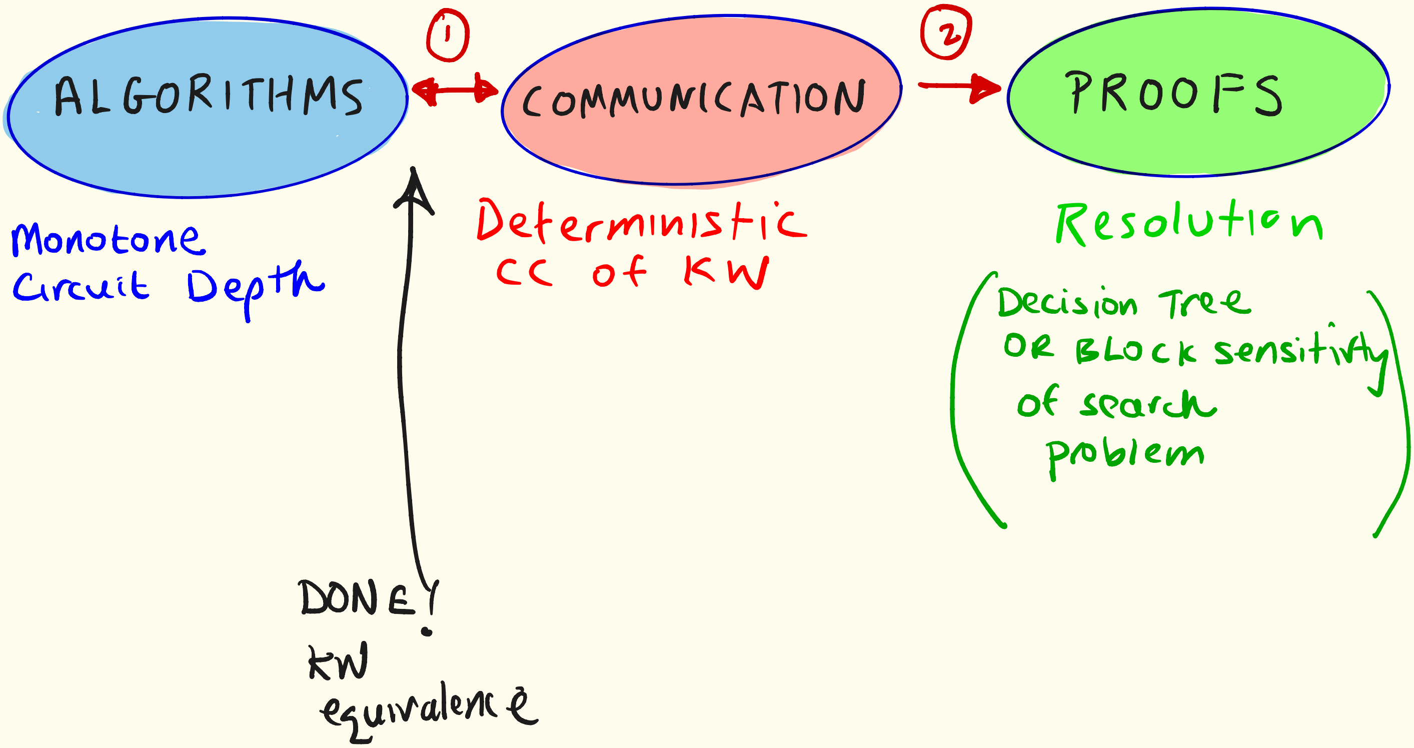
$y \in f^{-1}(0)$

at $\vee$ gate:
Alice sends bit

at $\wedge$ gate:
Bob sends bit



I. MONOTONE FORMULA/CIRCUIT DEPTH LBS



(2) CONSTRUCTING A HARD MONOTONE FUNCTION

* This is a main theme!

(1) Start with a hard UNSAT CNF $\mathcal{C} = C_1 \wedge C_2 \wedge \dots \wedge C_m$ over $z_1 \dots z_n$

Search($\mathcal{C}$): given $\alpha \in \{0,1\}^n$, output some clause C_i falsified by α

Decision tree complexity of $\mathcal{C}$ $\equiv$ Resolution Depth of refuting $\mathcal{C}$

(2) Lift $\mathcal{C}$ to get a 2-player search problem hard for CC

$$\text{Search}(\mathcal{C}) \xrightarrow[\text{using } g]{\text{Lift}} \text{Search}(\mathcal{C} \circ g^n)$$

$\mathcal{C}$: $(z_1 \vee z_2)(\bar{z}_1 \vee z_3)$ $\quad$ $\mathcal{C} \circ g^n$: $(g(x_1, y_1) \vee g(x_2 y_2))(\overline{g(x_1, y_1)} \vee g(x_3 y_3))$

(3) Show that Alice's input x to Search($\mathcal{C} \circ g^n$) $\xrightarrow{\text{maps to}}$ 1-input of some monotone $F_{\mathcal{C}}$

Bob's input y " " $\rightarrow$ 0-input of $F_{\mathcal{C}}$

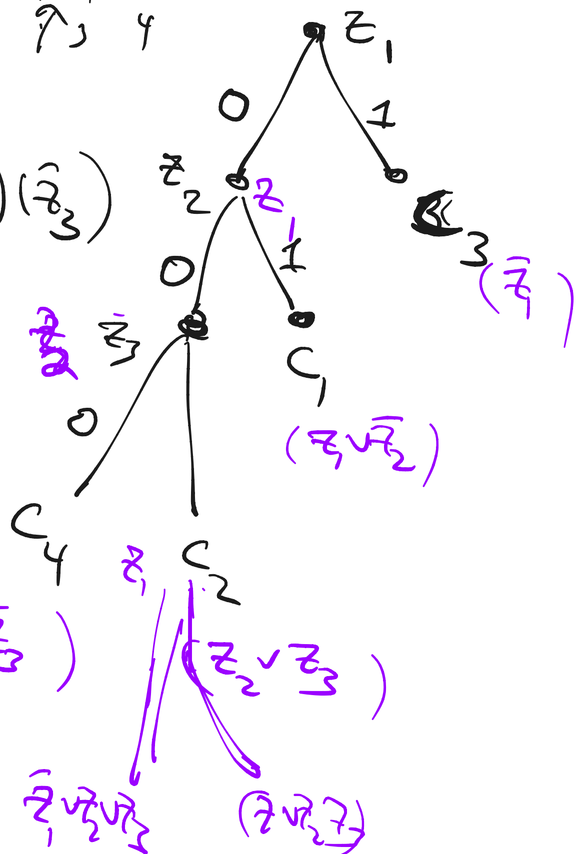
A DT for Search(φ)

$\varphi = C_1 \wedge \dots \wedge C_m$ over $z_1 \dots z_n$

$C = \underbrace{(z_1 \vee \bar{z}_2)}_{1} \underset{2}{(z_2 \vee z_3)} \underset{3}{(\bar{z}_1)} \underset{4}{(\bar{z}_3)}$

$(\bar{z}_2) \, (z_2 \vee z_3) \, (\bar{z}_3)$

1 2



Res: $\{C_1, C_2, \dots, C_m\}$

Rule $\underbrace{(x \vee C)}, \underbrace{(\bar{x} \vee D)}$

$((C \vee D))$

Res Ref of $C_1 \dots C_m$ is a derivation of empty clause starting with $C_1 \dots C_m$

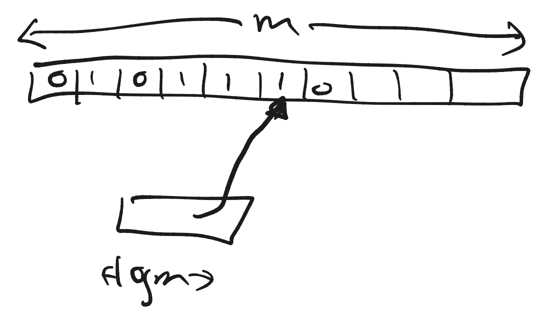
<u>Index gadget</u> with parameter m

$$g : X \times Y \to \{0,1\}$$

$$X = \{0,1\}^{\log m}$$

$$Y = \{0,1\}^{m}$$

$$g(x,y) \stackrel{d}{=} y_x$$



@ CNF over n variables

usually pick $m = n^2$ $\quad \log m = O(\log n)$

so $CC(\text{index gadget}_m) = (\log m) = O(\log n)$

LIFTED SEARCH PROBLEM

Search($\mathcal{C} \circ g^n$):

Alice gets x
Bob gets y
Find a falsified clause

This is saying that we can always transform lifted search problem to an equivalent KW game!

Theorem 2 [Göös-P]

For any unsatisfiable boolean formula $\mathcal{C}$ there is a Boolean function $F_{\mathcal{C}}$ such that monotone KW game for $F_{\mathcal{C}}$ equals Search($\mathcal{C} \circ g^n$)

g = index gadget with $m \sim n^2$

Proof sketch

$\mathcal{C} = C_1 \wedge \dots \wedge C_t$ UNSAT K-CNF over $z_1 \dots z_n$

Search$(\mathcal{C} \circ g^n)$:

Alice gets n pointers $x_1 \dots x_n$ $x_i \in [m]$

Bob gets n m-bit vectors $y_1 \dots y_n$ $y_i \in \{0,1\}^m$

Monotone Function $F_{\mathcal{C}}(\alpha)$:

α is a length $|\mathcal{C}|(mn)^k$ indicator vector for a K-SAT instance over mn variables with constraints from $\mathcal{C}$

$F_{\mathcal{C}}(\alpha) = 1$ iff α is UNSAT

$m \cdot n$ variables underlying CNF instance α are $v_{11} \dots v_{1m} \dots v_{n1} \dots v_{nm}$

Proof sketch

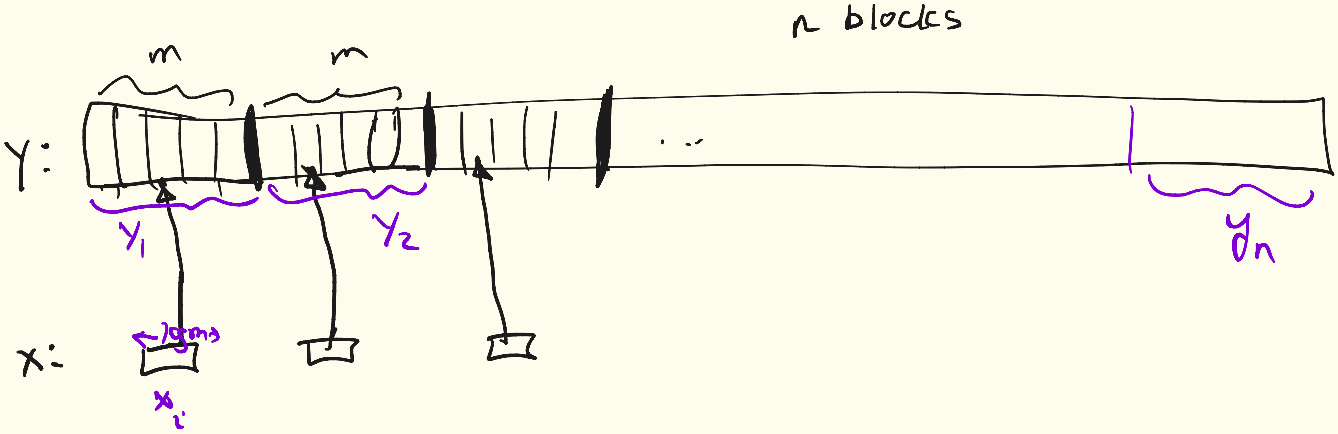
$\varphi = C_1 \wedge \dots \wedge C_t$ UNSAT k-CNF over $z_1 \dots z_n$

Search($\varphi \circ g^n$):

Alice gets n pointers $x_1 \dots x_n$ $x_i \in [m]$

Bob gets n m-bit vectors $y_1 \dots y_n$ $y_i \in \{0,1\}^m$

picks n out of nm variables and apply φ to these variables



Proof Sketch

$e = C_1 \wedge \dots \wedge C_t$ UNSAT K-CNF over $z_1 \dots z_n$

Search$(e \circ g^n)$:

Alice gets n pointers $x_1 \dots x_n$ $x_i \in [m]$

Bob gets n m-bit vectors $y_1 \dots y_n$ $y_i \in \{0,1\}^m$

Monotone Function $F_e(\alpha)$:

α is a length $|e|(mn)^k$ indicator vector for a K-SAT instance over mn variables v_{ij} with constraints from e

$F_e(\alpha) = 1$ iff α is UNSAT

Alice: $x \longrightarrow e$ over the renamed vars $v_{1,x_1}, \dots, v_{n,x_n}$

picks n out of nm variables and apply e to these variables

Bob: $y \longrightarrow$ all constraints satisfied by the assignment y

include all constraints over $v_{11} \dots v_{1m}\ v_{21} \dots v_{2m} \dots v_{n1} \dots v_{nm}$ satisfied by y

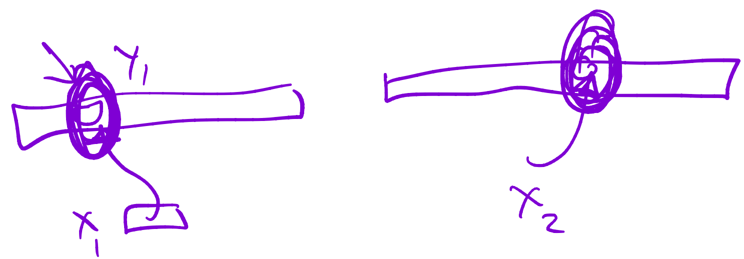
$C_1 \in \mathcal{C} \; : \; z_1 \vee z_2$

$C_1 \circ g \; : \; \underbrace{g(x_1, y_1)} \vee \underbrace{g(x_2 y_2)}$

$\underbrace{\mathcal{C} \circ g^n}$

true iff

the x_1^{th} bit of y_1 is true



$$\underbrace{(V_{1x_1} \vee V_{2x_2})}$$

Monotone Circuit Depth LBs : Putting it all together

Thm 1 [KW equivalence]

$$\text{mCktDepth}(F) = cc(mKW_F)$$

Thm 2 [Lifted CNF search $\equiv KW_F$]

$\text{Search}(\mathcal{C} \circ g^n) \equiv KW_{F_\mathcal{C}}$ for an associated monotone $F_\mathcal{C}$

Thm 3 [Deterministic Lifting]

For any search problem (ie $\text{Search}(\mathcal{C})$)

$$\text{Dec-Tree}(\text{Search}(\mathcal{C})) \simeq CC(\text{Search}(\mathcal{C} \circ g^n))$$

Thm 4 (LBs for $\text{Search}(\mathcal{C})$)

There exist unsat kCNF $\mathcal{C}$ over $z_1 \ldots z_n$ st.

$$\text{DecTree}(\text{Search}(\mathcal{C})) = \Omega(n)$$

Monotone Circuit Depth LBs : Putting it all together

Thm 1 [KW equivalence]

$\text{mCktDepth}(F) = cc(mKW_F)$

DONE ✓

Thm 2 [Lifted CNF search $\equiv KW_F$]

$\text{Search}(\mathcal{C} \circ g^n) \equiv KW_{F_\mathcal{C}}$ for an associated monotone $F_\mathcal{C}$

DONE ✓

Thm 3 [Deterministic Lifting]

For any search problem (ie $\text{Search}(\mathcal{C})$)

$\text{Dec-Tree}(\text{Search}(\mathcal{C})) \simeq CC(\text{Search}(\mathcal{C} \circ g^n))$

TO DO

Thm 4 (LBs for $\text{Search}(\mathcal{C})$)

There exist unsat kCNF $\mathcal{C}$ over $z_1 \ldots z_n$ st.

$\text{DecTree}(\text{Search}(\mathcal{C})) = \Omega(n)$

TO DO

Proofs $\longrightarrow$ Communication $\longrightarrow$ Algorithms

$DT(\text{Search}(\mathcal{C})) = \Omega(n)$ — Thm 4

$CC(\text{search}(\mathcal{C} \circ g^n)) = \Omega(n)$ — Thm 3

$CC(KW_{F_\mathcal{C}}) = \Omega(n)$ — Thm 2

$\text{mCkt depth}(F_\mathcal{C}) = \Omega(n)$ — Thm 1