Announcements

- Presentations on April 17 : Upload video by April 11
  Presentations on April 24 : Upload video by April 18

  Videos : 20 mins
  Class Presentation : 10 mins plus 5-10 mins discussion

- HW2 posted today (we will discuss)

- Scribe Notes : 1st draft due one week after lecture;
  Final draft due : one week after feedback. Thanks!

HW 2

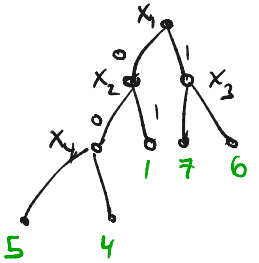
Q3: about deterministic vs randomized decision tree complexity

Let $S \subseteq \{0,1\}^n \times [m]$ be a search problem

S is <u>total</u> if $\forall \alpha \in \{0,1\}^n$, there exists at least one $j \in [m]$ such that $(\alpha, j) \in S$

Deterministic depth-d decision tree for some total search problem S:

T:



leaves labelled by some $j \in [m]$

$\forall \alpha \in \{0,1\}^n, \quad (\alpha, T(\alpha)) \in S$

this says for every assignment α to n vars, the output $T(\alpha)$ given by T is a valid solution to S on α

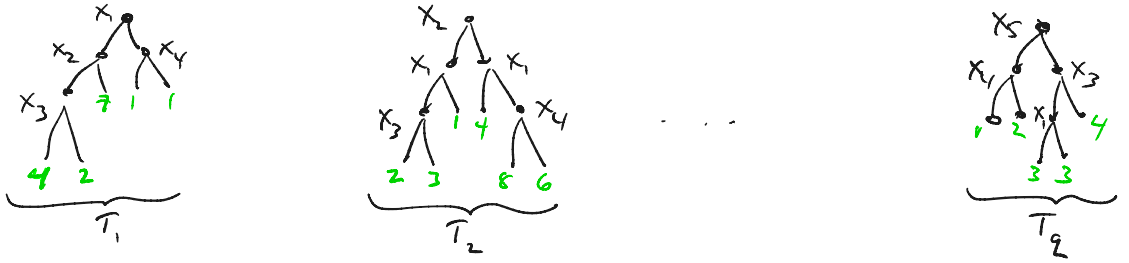
$D^{dt}(S)$ = min depth over all deterministic trees T for S.

HW 2

Randomized Decision tree for total search problem $S \subseteq \{0,1\}^n \times [m]$

$\mathcal{T} = \{T_1, \ldots, T_q\}$, each T_i is a deterministic dec. tree

$\mathcal{T}$:



Accuracy: $\forall \alpha \in \{0,1\}^n$, $\Pr_{i \in [q]} [(\alpha, T_i(\alpha)) \in S] \geq 2/3$

$R^{dt}(S) \stackrel{d}{=}$ min depth of any randomized DT $\mathcal{T}$ for S

For total Boolean functions, f: $D^{dt}(f) \leq \left[R^{dt}(f)\right]^2$

HW2, Q3: $R^{cc} \stackrel{?}{=} \text{poly}(D^{cc})$ for total search problems?

HW 2

Example: FIND 1

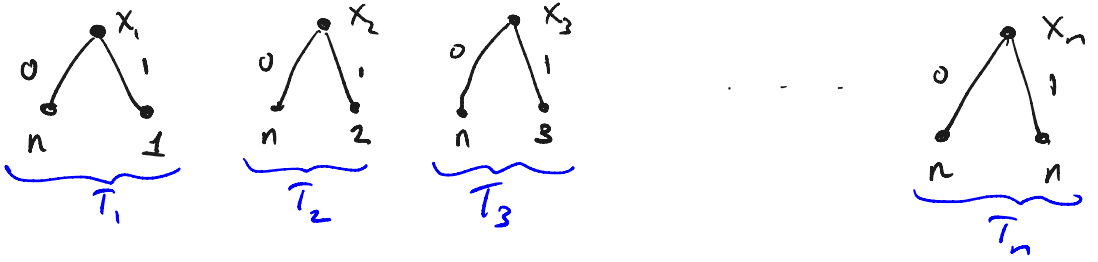
Input $x \in \{0,1\}^n$

Output:
- If #1's in x is $\geq \frac{3}{4}$ output $j \in [n]$ such that $x_j = 1$
- Otherwise output any $j \in [n]$.

} partial or "promise" search problem

Randomized Dec tree for FIND 1:

T:



Claim $\forall x \in \{0,1\}^n$ such that $(\#\text{1's in } x) \geq \frac{3n}{4}$:

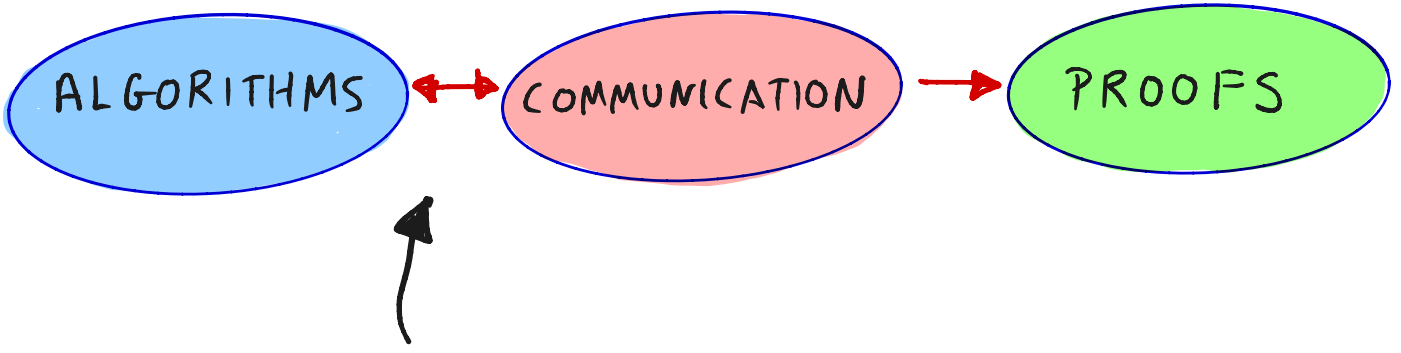
$$\Pr_{i \in [n]}\left[T_i(x) \text{ is correct}\right] \geq \frac{3}{4}$$

Applications

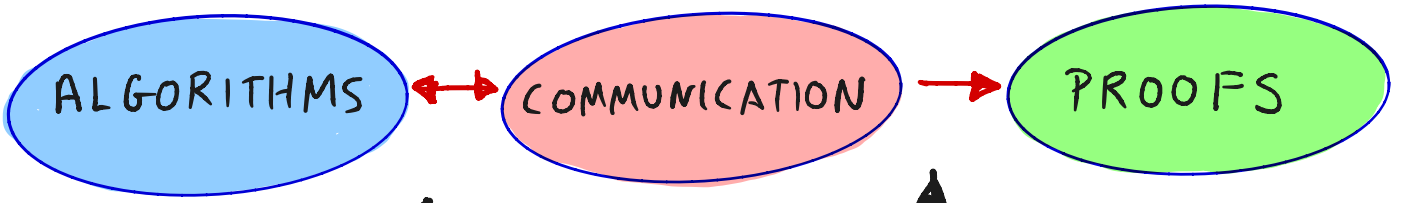
I. Lifting Proof Complexity Lower Bounds **TODAY**

II. Proof complexity UPPER BOUNDS for random CSPs and connections

LOWER BOUND PROGRAM



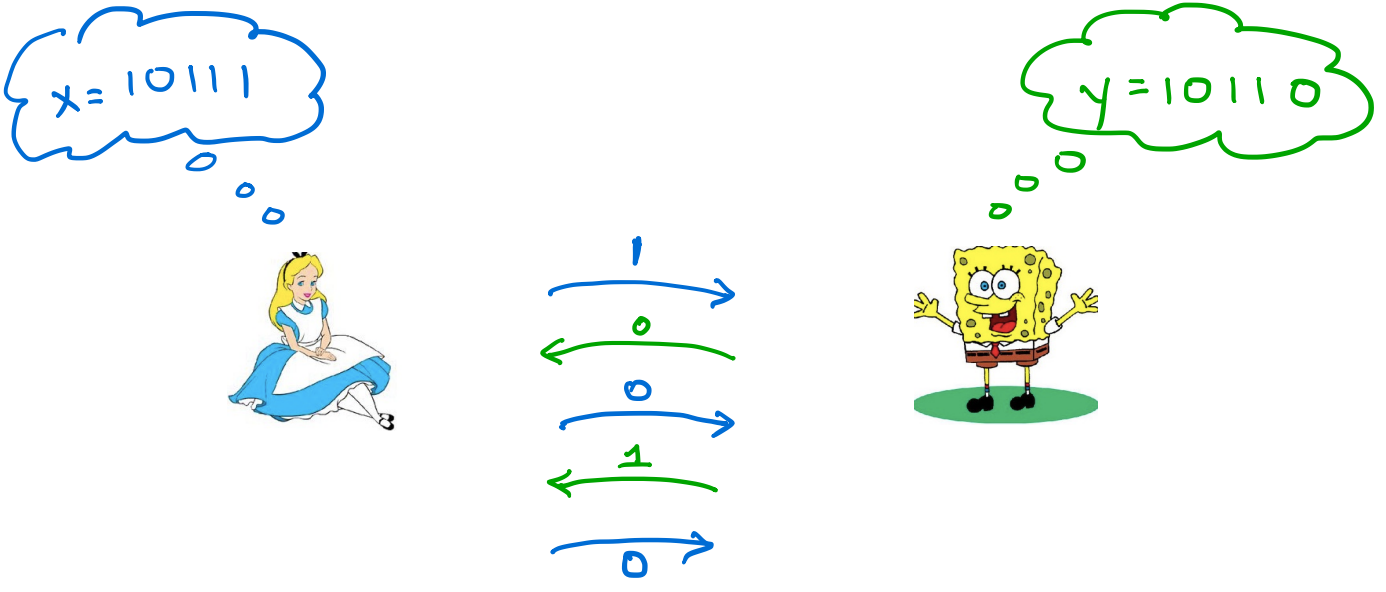
LOWER BOUND PROGRAM



Use communication complexity to capture underlying class of algorithms

New LIFTING THEOREMS to reduce communication lower bounds to simpler proof complexity lower bounds

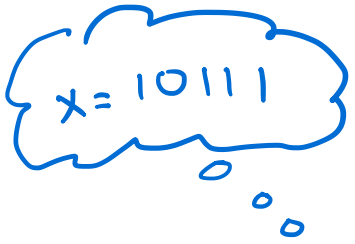
Communication complexity (Yao '79)



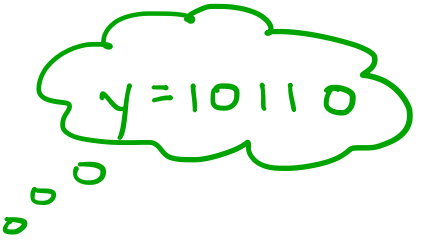
$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

$$cc(f) = \min_{\pi \text{ computing } f} cc(\pi)$$

Example: EQUALITY(x,y)



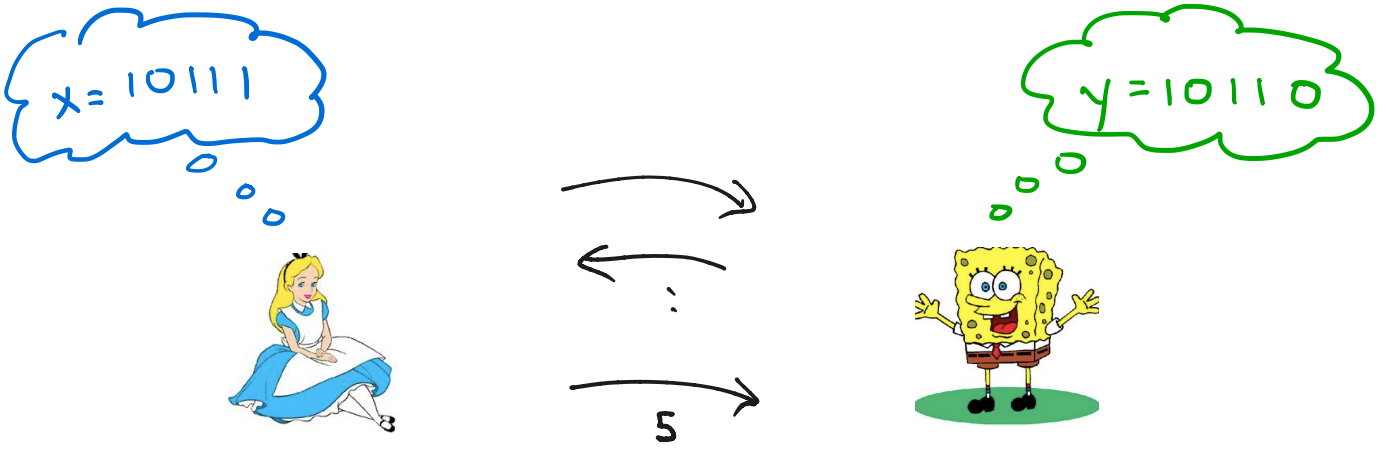
$x \stackrel{?}{=} y$



Deterministic CC = $\Omega(n)$

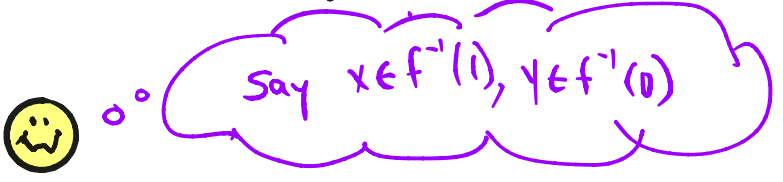
Randomized CC = $O(1)$

COMMUNICATION FOR TOTAL SEARCH PROBLEMS

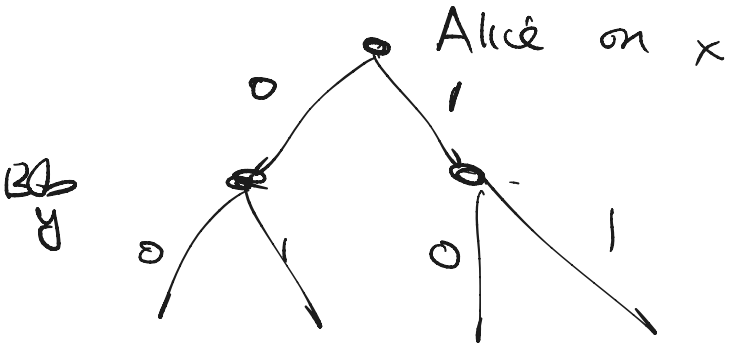


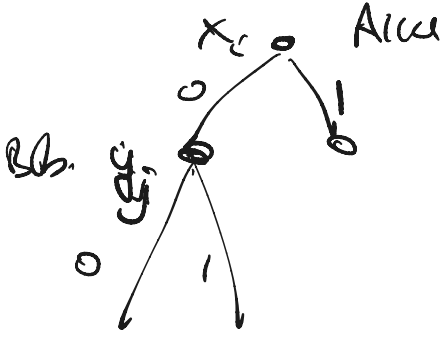
Example: Alice x Bob y

Promise $x \neq y$ Find i such that $x_i \neq y_i$

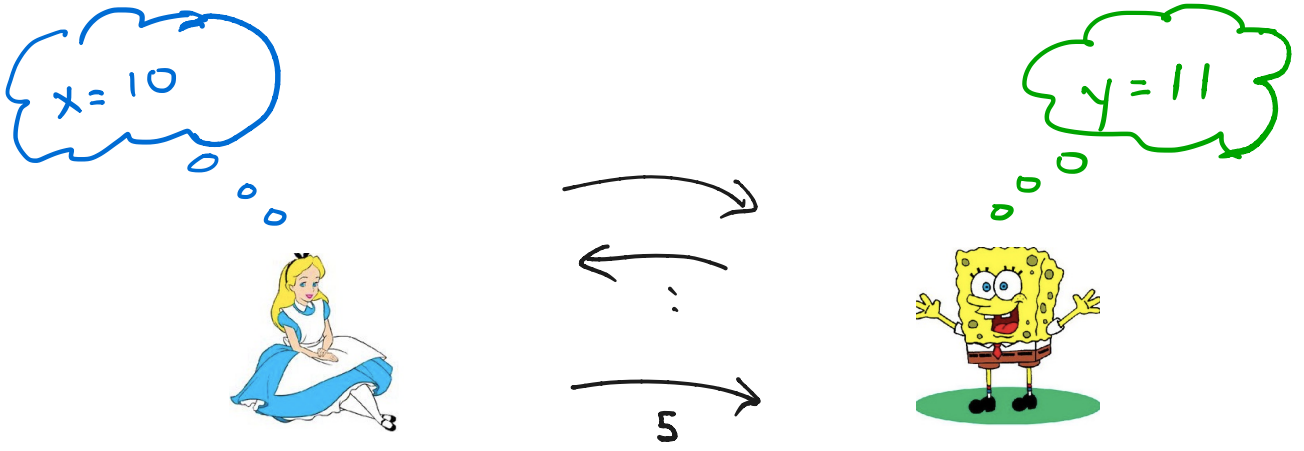


Protocol tree:





COMMUNICATION FOR TOTAL SEARCH PROBLEMS

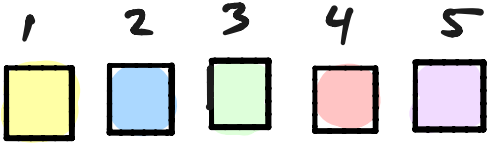


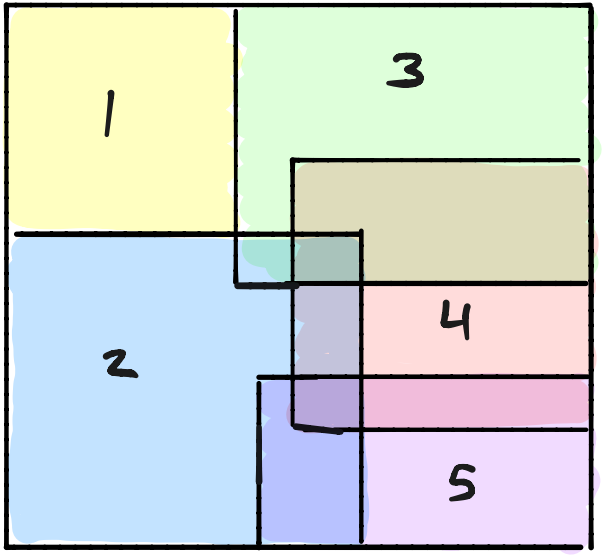
Example: Unsatisfiable CNF over $x_1 .. x_n, y_1 .. y_n$

Alice x Bob y Output falsified claus

$$C = \overset{1}{(x_1 \vee y_1)} \wedge \overset{2}{(\bar{x}_1 \vee y_1)} \wedge \overset{3}{(x_2 \vee \bar{y}_2)} \wedge \overset{4}{(\bar{x}_2 \vee \bar{y}_1)} \wedge \overset{5}{(y_2)}$$

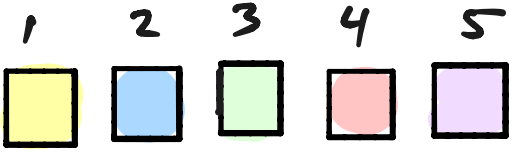
THE COMMUNICATION MATRIX

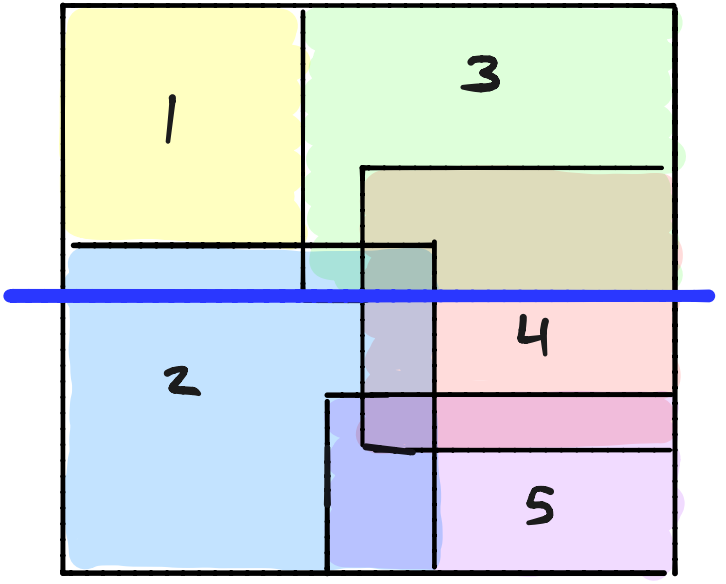




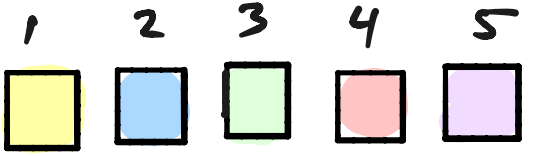
$$S(x, y) \subseteq \{1, 2, 3, 4, 5\}$$

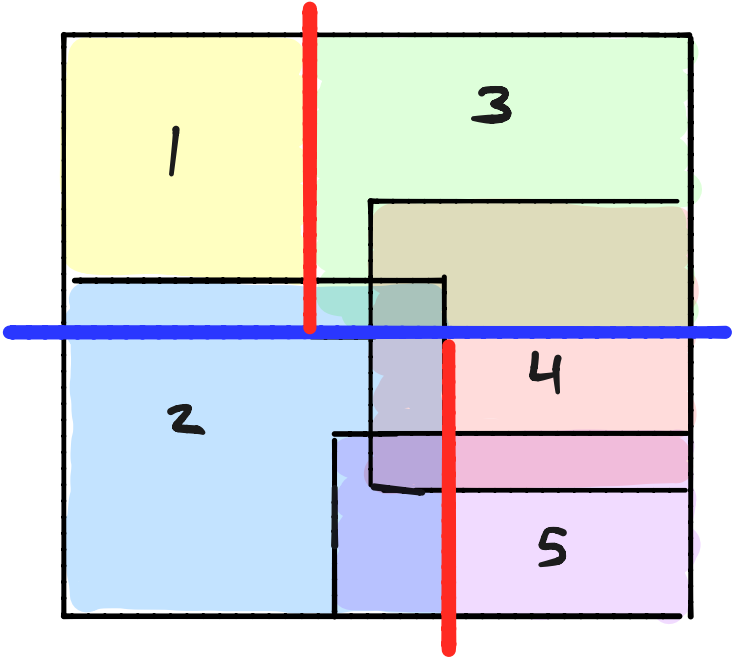
THE COMMUNICATION PROTOCOL



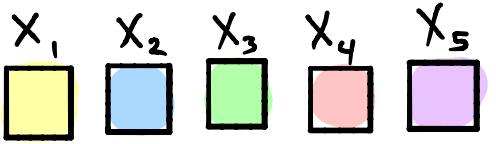


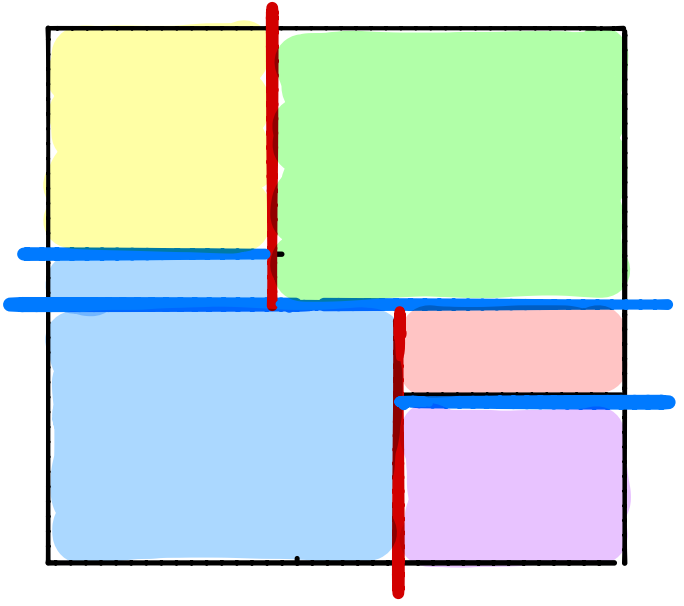
THE COMMUNICATION PROTOCOL





Protocol Partitions
Matrix into monochromatic rectangles

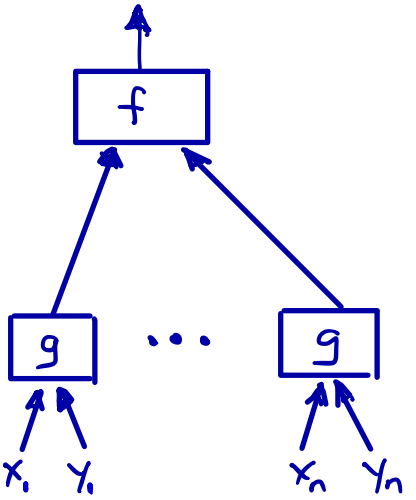




So cc is a rank-like measure

QUERY TO COMMUNICATION LIFTING

$f : \{0,1\}^n \to R$ ⇝ $F =$



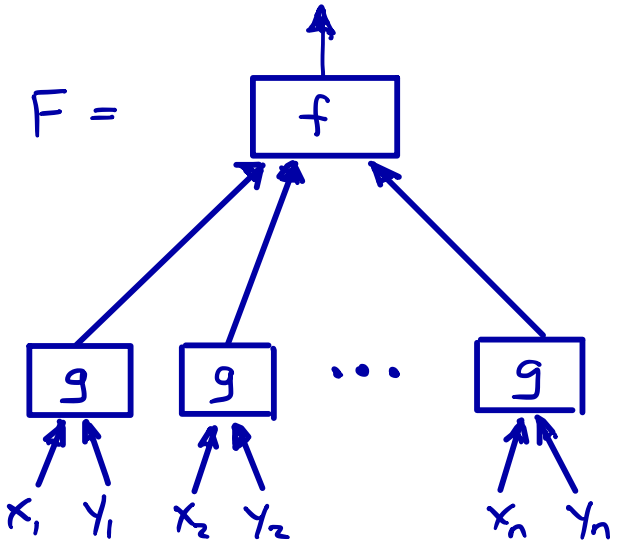
(f a total or partial function or a search problem)

degree/query measure

rank-like measure

QUERY TO COMMUNICATION LIFTING

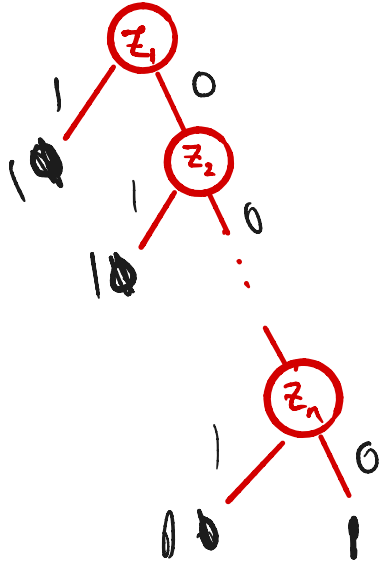
$f : \{0,1\}^n \to R$ $\rightsquigarrow$ $F =$



Lifting Theorem

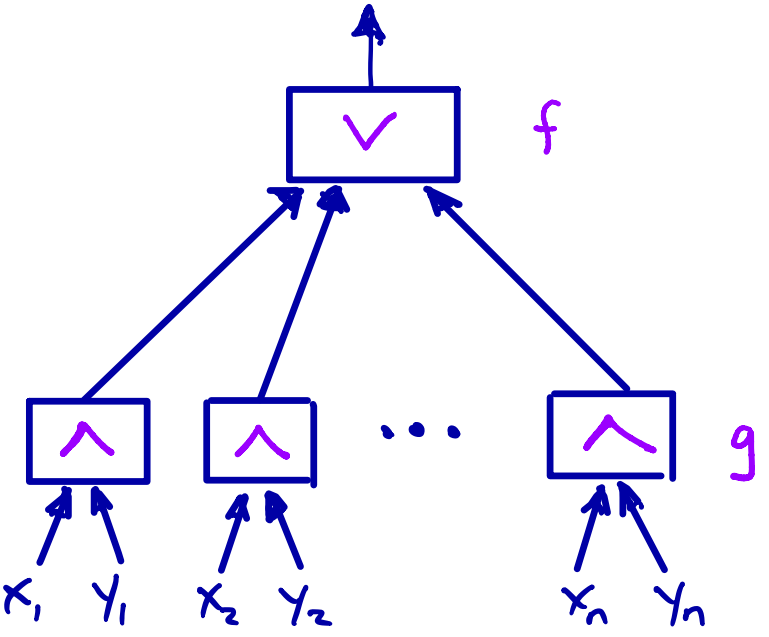
Query Complexity of f $\approx$ Communication Complexity of $F = f \circ g^n$

EXAMPLE : DISJOINTNESS



OR

$DT(f) = \Theta(n)$



$CC(f \circ g^n) = \Theta(n)$

SOME LIFTING THEOREMS

[Raz, Mckenzie '97, göös-P-Watson '15] dec tree $\leftrightarrow$ cc

[Sherstov '01] Poly degree $\rightarrow$ rank (pattern matrix method)

[göös, Lovett, Meka, Watson, Zuckerman '15]

Nonnegative Junta degree $\rightarrow$ nonneg rank

[Chattopadhyay, Koucky, Loff, Mukhopadhyay '17], [Wu, Yao, Yuen '17]

* with inner product gadget

[göös, P, Watson '17] (BPP LIFTING)

randomized dec tree $\leftrightarrow$ randomized cc

MORE LIFTING THEOREMS

[Razborov '03] approximate degree → quantum query

[P-göös] Critical block sensitivity → NOF cc

[gLMWZ '15] Approx Junta degree ⟷ nondet cc

[Lee, Raghavandra, Steurer '15] sos degree ⟷ PSD rank

[KMR '16] Junta degree ⟷ nonneg rank

[P, Robere, Rossman Cook '16], [P, Robere '17, '18]

Nullstellensatz degree ⟷ Razborov Rank / Algebraic Tiling

LIFTING THEOREMS

f: n-bit boolean function / search problem

g: index gadget $\quad g(x,y) = y_x$

$|y| = n^{20}$, $|x| = 20 \log n$

Theorem 1 (Deterministic Lifting) [Raz, McKenzie, Göös, P, Watson]

$$DT(f) \cdot \Theta(\log n) = CC(f \circ g^n)$$

Theorem 2 (Randomized Lifting) [Göös-P-Watson]

$$rDT(f) \cdot \Theta(\log n) = rCC(f \circ g^n)$$

Theorem 3 [Chattopadhyay, Filmus, Koroth, Meir, P]

unified proof of Theorems 1 and 2 using either index or inner product gadget. (any "low discrepancy" gadget)

Theorem 4 [Robere, P]

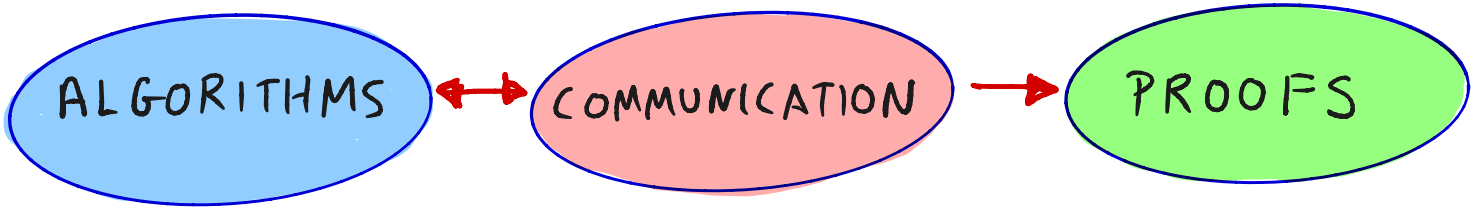
$$2^{NS(f)} \approx \text{monotone-span}(f \circ g^n)$$

← any "nontrivial" constant-sized gadget

Applications of Lifting (for Lower Bounds)

- monotone formulas
- monotone circuits
- monotone span programs
- linear secret sharing schemes
- extended formulations of Linear programs
- game theory (Nash equilibria)
- Graph theory (Alon-Saks-Seymour Conjecture)
- Proof complexity
- Communication complexity
  - log rank conjecture
  - partition vs communication
- Quantum Computing

I. MONOTONE FORMULA LOWER BOUNDS



Monotone formulas

Deterministic CC of KW game

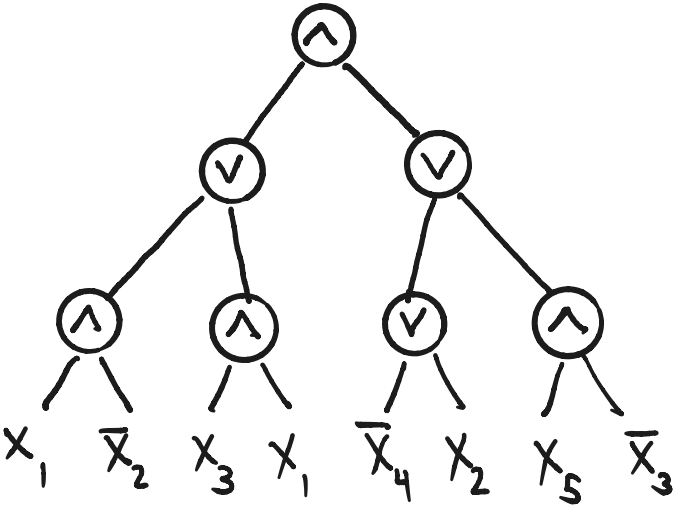
Resolution depth

KARCHMER-WIGDERSON GAME KW_f^{cc}

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

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

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



Characterization of Formula Size by KW-game CC

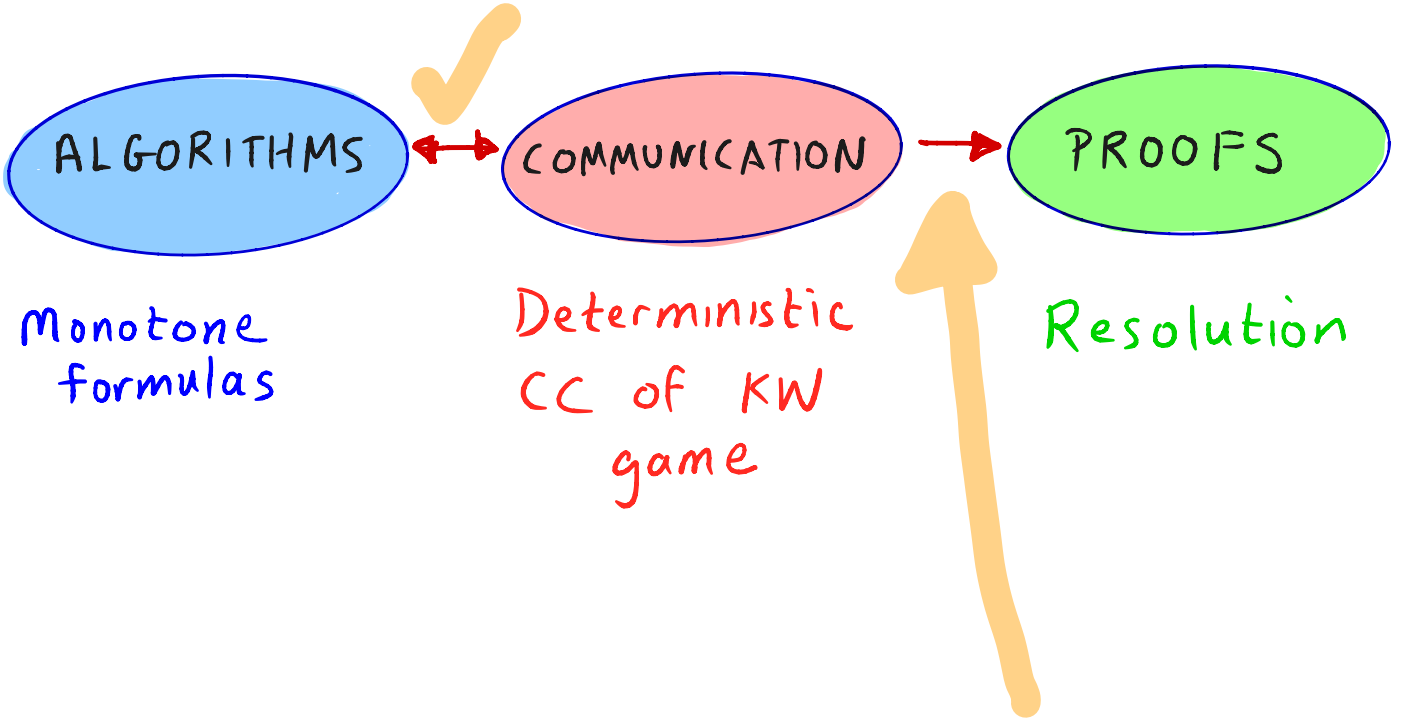
THEOREM [KW]

FORMULA-SIZE(f) is equal to the communication complexity of KW_f^{cc}

THEOREM (monotone version) f monotone

Monotone-FORMULA-SIZE(f) is equal to the cc of monotone-KW_f^{cc} (find i such that $x_i > y_i$)

I. MONOTONE FORMULA LOWER BOUNDS



CANONICAL SEARCH PROBLEM

UNSAT

KCNF $\quad \mathcal{C} = C_1 \wedge C_2 \wedge \cdots \wedge C_t \quad$ over $z_1, \ldots, z_n$

Search($\mathcal{C}$): given $\alpha \in \{0,1\}^n$, find a falsified clause (C_i such that $C_i(\alpha) = 0$)

LIFTED SEARCH PROBLEM

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

Alice gets x
Bob gets y
Find a falsified clause

Theorem [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($\mathcal{C} \circ g^n$)

Proof sketch $\mathcal{C} = C_1 \wedge \cdots \wedge C_t$ UNSAT K-CNF over $z_1 \ldots z_n$

Search ($\mathcal{C} \circ g^n$): Alice gets n pointers $x_1 \ldots x_n$ $x_i \in [m]$
Bob gets n m-bit vectors $y_1 \ldots y_n$ $y_i \in \{0,1\}^m$

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

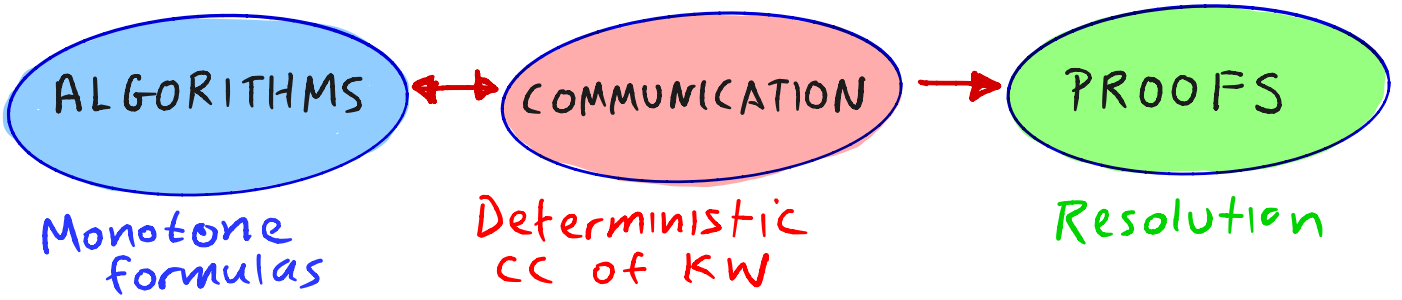
α is a $|\mathcal{C}|(mn)^K$ indicator vector for a K-SAT instance over mn variables V_{ij} with constraints from $\mathcal{C}$

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

Alice: $x \longrightarrow \mathcal{C}$ over the renamed vars $V_{1,x_1}, \ldots, V_{n,x_n}$

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

I. MONOTONE FORMULA LOWER BOUNDS



monotone f-size $(F_e) \geq 2^{n^\varepsilon}$ ⟵ $cc(F_e) = \Omega(n)$ ⟵ Resolution Depth$(e) = \Omega(n)$

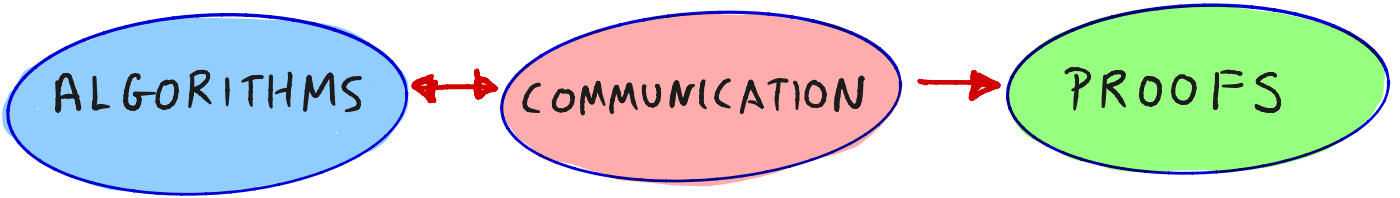
KW equiv.

LIFTING THM

Applications of Lifting (for Lower Bounds)

- monotone formulas
- monotone circuits
- monotone span programs
- linear secret sharing schemes
- extended formulations of linear programs
- game theory (Nash equilibria)
- graph theory (Alon-Saks-Seymour Conjecture)
- Proof complexity
- Communication complexity
  - log rank conjecture
  - partition vs communication
- Quantum Computing

II. SPAN PROGRAM/SECRET SHARING LOWER BOUNDS



Linear Secret Sharing Schemes

III

Monotone Span Programs

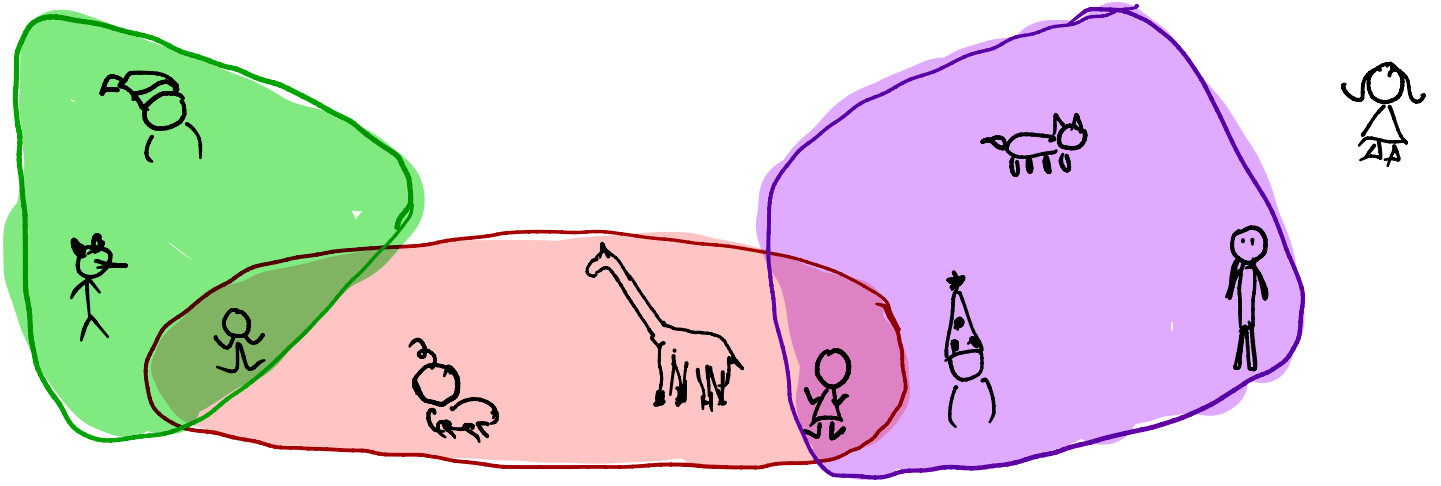
Algebraic Tiling Protocol

Nullstellensatz Proofs

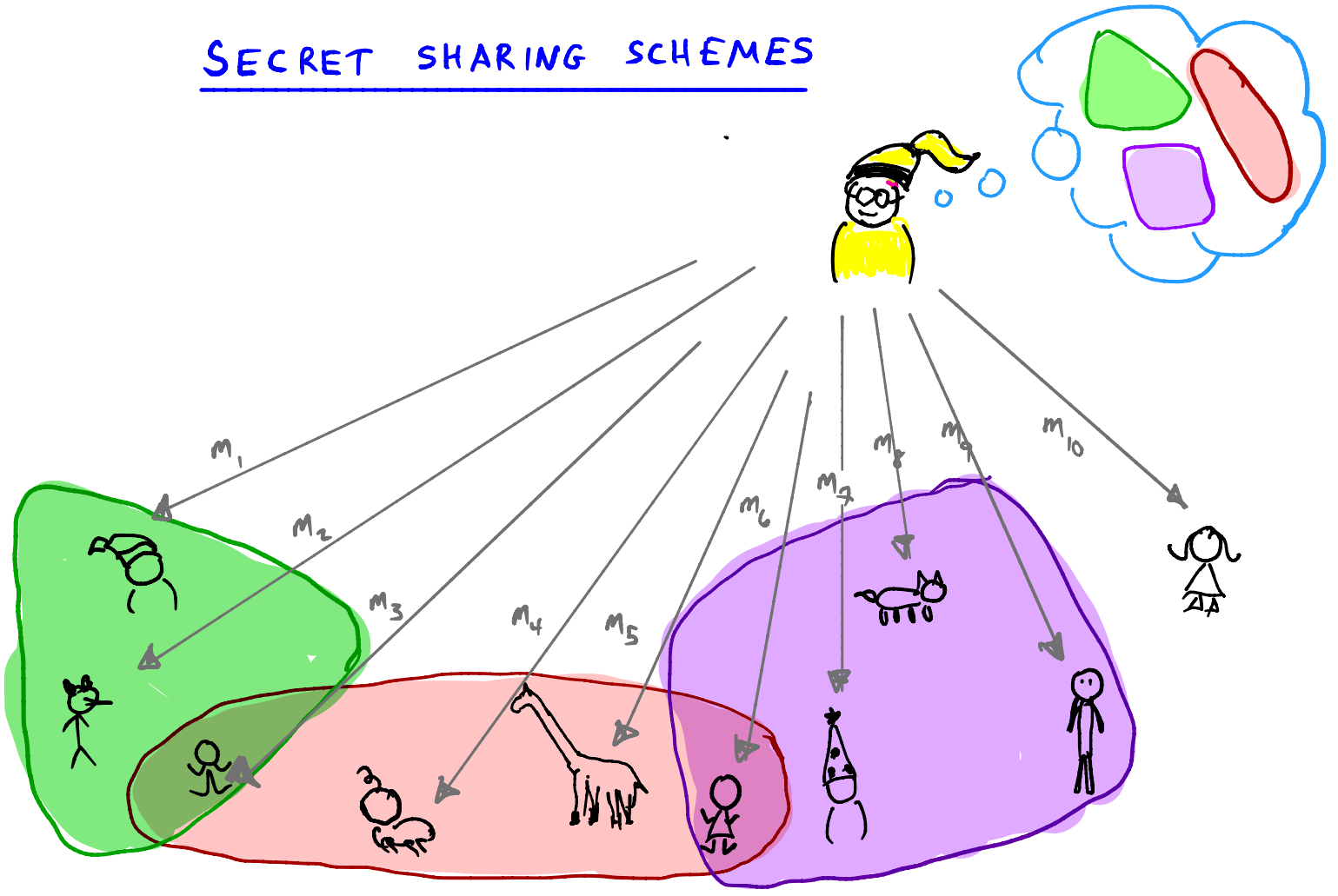
SECRET SHARING SCHEMES

share secret s

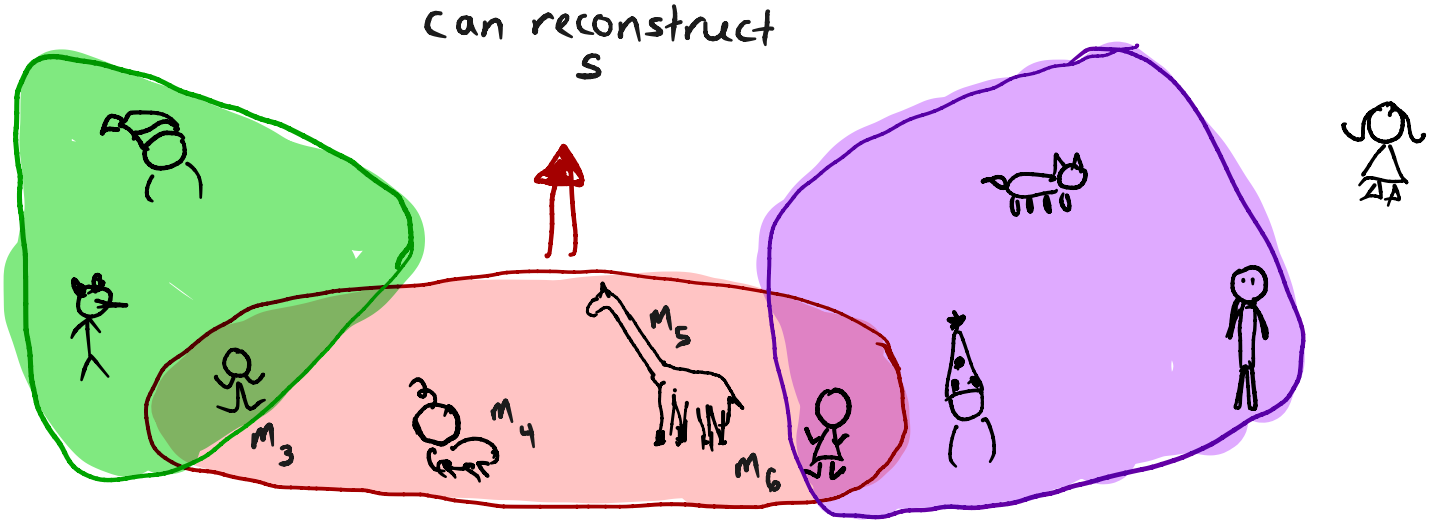
with select groups



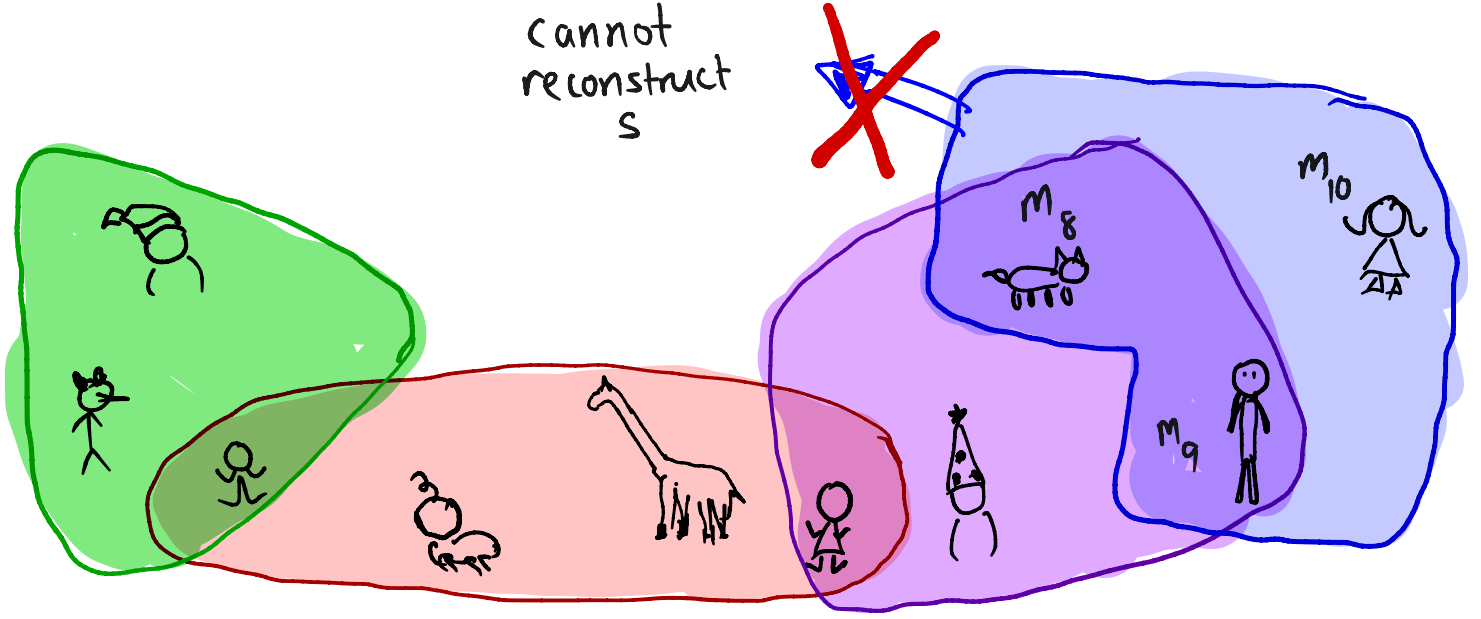
SECRET SHARING SCHEMES



SECRET SHARING SCHEMES



SECRET SHARING SCHEMES



SECRET SHARING SCHEMES (Shamir '79)

OPEN QUESTION: n parties, and subsets of allowed groups $P_1, \ldots, P_m$, how long must the messages be?

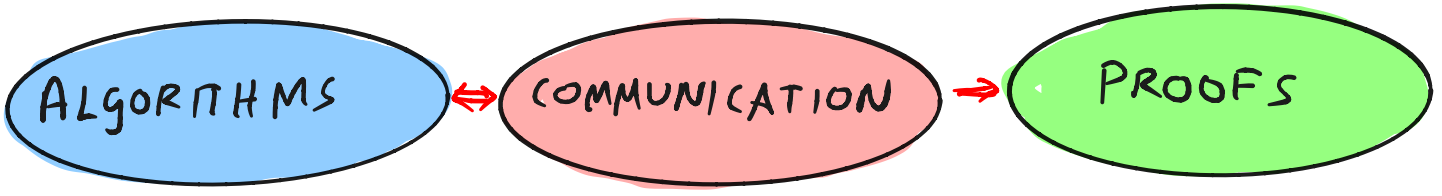
Nearly all schemes are LINEAR...
How long must messages be for LINEAR schemes?

A long line of work led to $n^{\Omega(\log n)}$ LOWER BOUNDS [Gál '01]

THEOREM [P, Robere '18] $\forall n$ there is a collection of allowed groups such that any linear sss for these groups requires $2^{\Omega(n)}$ message length.

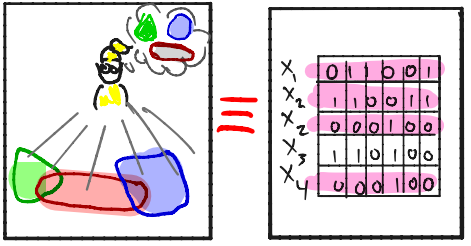
COROLLARIES $2^{\Omega(n)}$ LOWER BOUNDS FOR
- MONOTONE SPAN PROGRAMS
- MONOTONE BRANCHING PROGRAMS
- MONOTONE FORMULAS

II. LINEAR SECRET SHARING LOWER BOUNDS



Algebraic Tiling

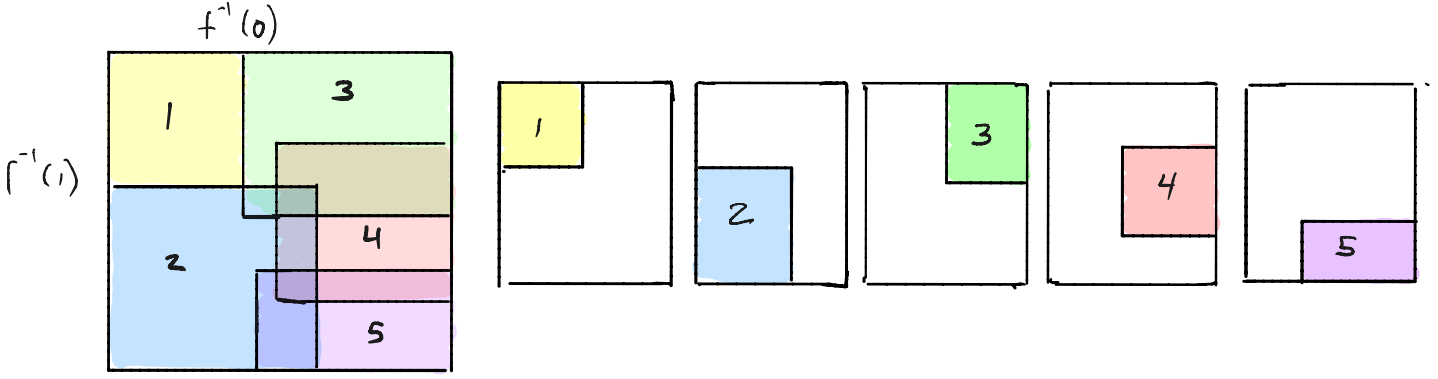
Nullstellensatz Proofs



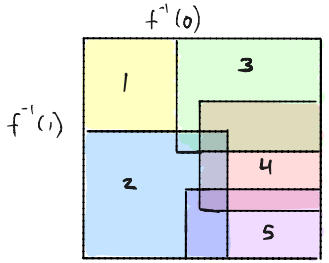
Linear SSS

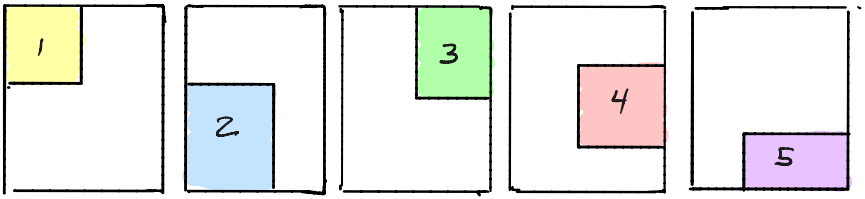
Monotone SPAN

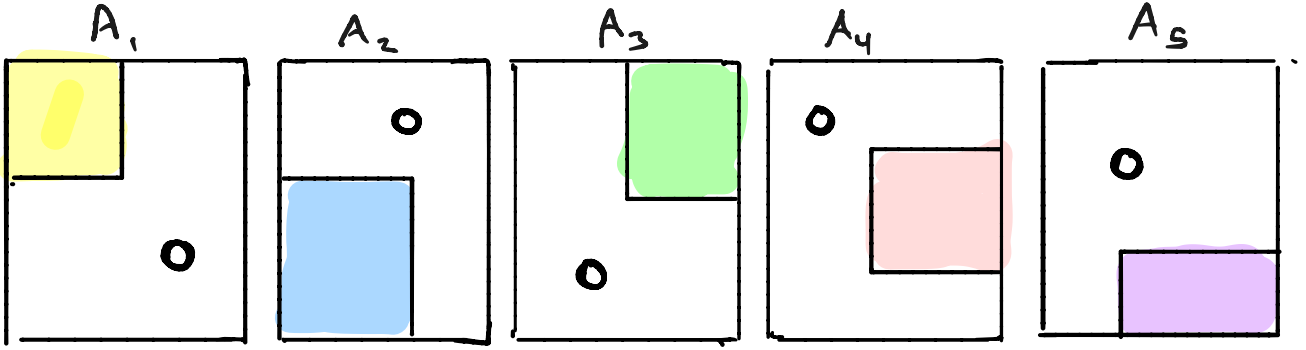
ALGEBRAIC TILING [gál]



ALGEBRAIC TILING [gál]



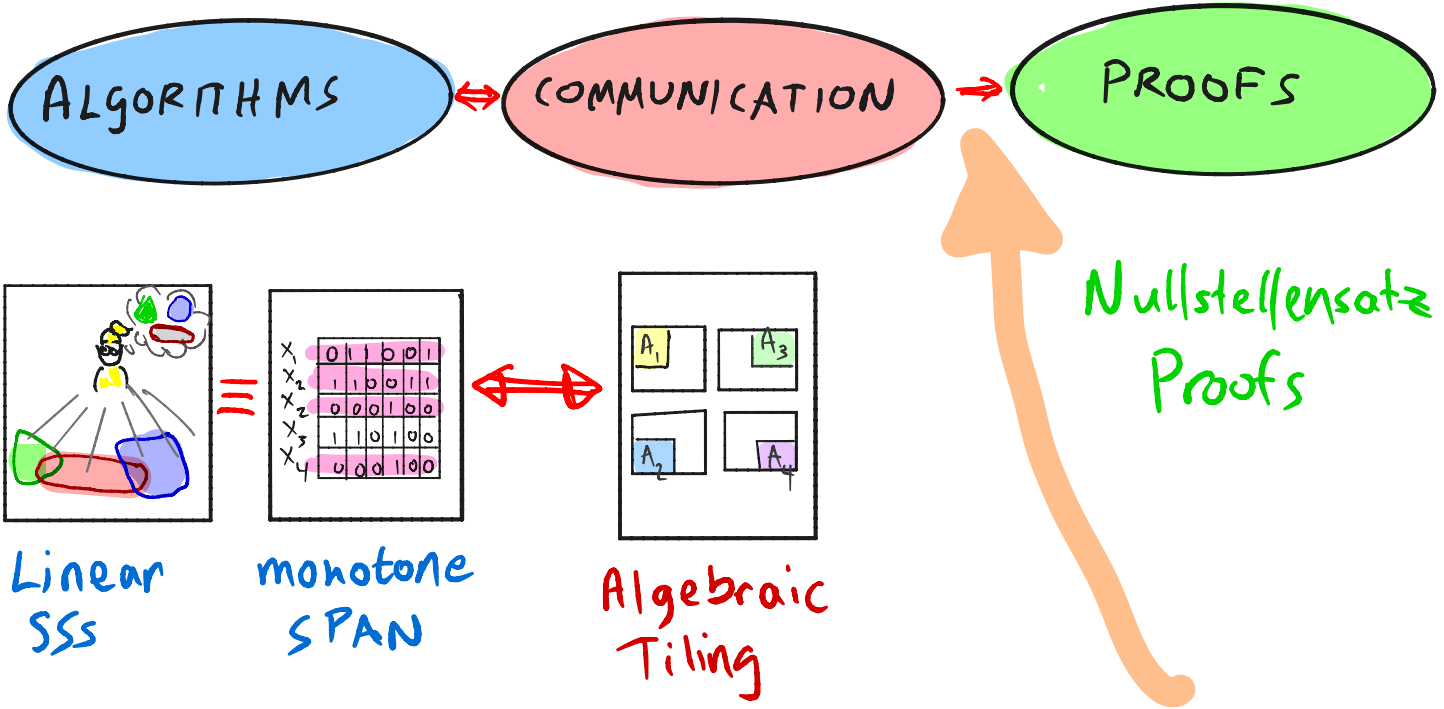




$$A_1 + A_2 + A_3 + A_4 + A_5 = 1$$

$$\text{Complexity of Tiling} = \sum_i \text{rank}(A_i)$$

II. LINEAR SECRET SHARING LOWER BOUNDS



Nullstellensatz Proofs

Let $P = \{p_1 = 0, p_2 = 0, \ldots, p_m = 0\}$ be an unsat system of poly equations over $\mathbb{F}$

A **Nullstellensatz Refutation** of P is $Q = \{q_1, \ldots, q_m\}$ such that $\sum_{i=1}^{m} p_i q_i = 1$

$NS_{\mathbb{F}}(P)$ = min degree of Nullstellensatz refutation

Lemma $NS_{\mathbb{F}}(P) \approx$ min degree of polynomial that solves search problem for P

LIFTING THEOREM (degree / algebraic tiling)

Theorem 4 [Robere, P]

$$2^{NS(f)} \approx \text{monotone-span}(f \circ g^n)$$

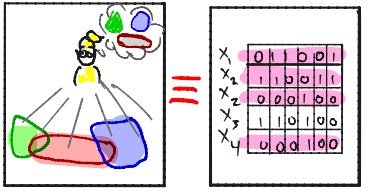
↑ constant-sized gadget

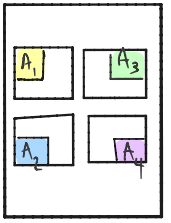
$$2^{NS(\mathcal{C})} \approx \text{algebraic-tiling}(\mathcal{C} \circ g^n)$$

$$= \text{monotone-span}(F_{\mathcal{C}})$$

II. LINEAR SECRET SHARING LOWER BOUNDS

ALGORITHMS ⇔ COMMUNICATION → PROOFS





Nullstellensatz

LIFTING THM

Linear sss
size $= 2^{\Omega(n)}$

Algebraic
Tiling $(F_e) = 2^{\Omega(n)}$

$NS_F(e) = \Omega(n)$

Applications of Lifting (from proof complexity LBs)

Model of computation	Proof System
monotone formulas	Tree-like Resolution
monotone circuits	(DAG-like) Resolution
monotone span programs / Linear SSS	Nullsatz
extended formulations of Linear programs	Sherali Adams (SA)
extended formulations of semi-definite programs	Sum-of-Squares (SOS)