THE AMAZING POWER OF COMPOSITION

Toniann Pitassi

U. Toronto

STOC '94

THE AMAZING POWER OF PAIRWISE INDEPENDENCE

AVI WIGDERSON

HEBREW UNIVERSITY
JERUSALEM

PAIRWISE IND. RANDOM VARIABLES

trials

$\{Z_1, Z_2, \dots Z_x, \dots\}_{x \in U} \qquad Z_x \in T \qquad |T| = t$

(•) UNIFORM $\quad \forall x \in U \quad \forall \alpha \in T \quad \Pr[Z_x = \alpha] = \frac{1}{t}$

(••) PAIRWISE IND. $\quad \forall x \neq y \in U \quad \forall \alpha, \beta \in T \quad \Pr[Z_x = \alpha \wedge Z_y = \beta] = \frac{1}{t^2}$

$h : U \to T$

$Z_x = h(x) \qquad h \in_R H$

$H = H(U,T) =$

$\{h : U \to T\}$ SAT. (•) (••)

$$\begin{array}{c|ccccc|}
 & Z_1 & Z_2 & Z_3 & Z_4 & Z_5 \\
\hline
 & 0 & 1 & 0 & 1 & 1 \\
 & 1 & 0 & 0 & 0 & 1 \\
 & 0 & 0 & 1 & 0 & 1 \\
h & 1 & 1 & 0 & 0 & 0 \\
 & 0 & 0 & 0 & 1 & 0 \\
 & 1 & 1 & 1 & 1 & 1 \\
 & 1 & 0 & 1 & 1 & 0 \\
 & 0 & 1 & 1 & 0 & 0 \\
\hline
\end{array}$$

$U = \{1,2,3,4,5\}$

$T = \{0,1\}$

$\forall x \neq y \quad \Pr[h(x) = h(y)] = \frac{1}{t}$

[CW] Cohen Wigderson STOC/FOCS 89? similar to IZ "How to recycle random bits"

EFFICIENT CONSTRUCTION [CW]

$$H(U,U) = \{ h(x) = a + bx \mid a, b \in U \}$$

$$\begin{pmatrix} h(x) \\ h(y) \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}}_{\text{INVERTIBLE MATRIX}} \begin{pmatrix} a \\ b \end{pmatrix} \qquad U \text{ FIELD}$$

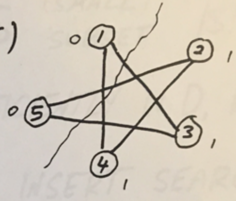
$$H(U,T) = \{ h(x) = a + bx \pmod{t} \mid a, b \in U \} \qquad t \mid |U|$$

PROPERTIES

- 2 SUCCINCTNESS $|H| = |U|^2$, $|h| = 2|x|$
- 3 EFFICIENCY $h(x) \in \mathrm{LOGSPACE}(|x|)$
- 1 PAIRWISE IND. $h(x), h(y)$ INDEPENDENT
- 2 LOW RANDOMNESS $2 \log |U|$ RANDOM BITS

DERANDOMIZING PROB. ALGORITHMS

MAX CUT $\quad G(U,E)$



CUT $\quad \chi : U \to \{0,1\}$

$c(\chi) = |(x,y) \in E : \chi(x) \neq \chi(y)|$

FIND χ WITH LARGE $c(\chi)$

χ RANDOM

$$\mathbb{E}[c(\chi)] = \sum_{(x,y)\in E} \Pr[\chi(x) \neq \chi(y)] = \frac{|E|}{2}$$ ($\frac{1}{2}$ APPROX. TO OPT.)

$h \in_R H(U, \{0,1\})$

$$\mathbb{E}[c(h)] = \sum_{E} \Pr[h(x) \neq h(y)] = \frac{|E|}{2}$$

NC' ALGORITHM

- TRY ALL $h \in H(U,\{0,1\})$ IN PARALLEL

TAKE h WHICH MAXIMIZES $c(h)$

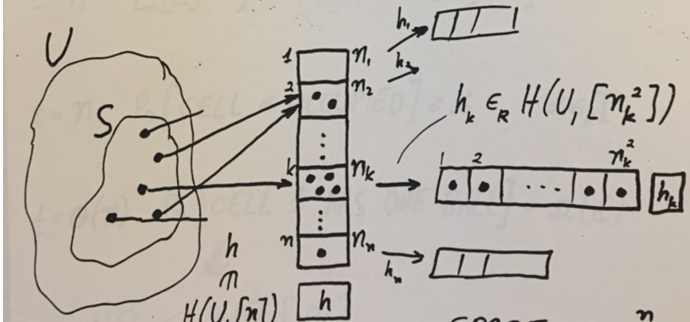
Fredman Komlos Szemeredi

THE (STATIC) DICTIONARY PROBLEM [FKS

U (LARGE) UNIVERSE $\quad U \supseteq S$ (SMALL) SUBSET $\quad |S| = n$

PROBLEM: STORE S EFFICIENTLY IN D, $|D| = O(n$

		INSERT	SEARCH
DETERMINISTIC	BALANCED TREES	$n \log n$	$\log n$
PROBABILISTIC	PERFECT HASHING [FKS]	n	2



$$\text{SPACE} = n + \sum_{k=1}^{n} n_k^2$$

n_k = # OF BALLS IN CELL k

$BPP \subseteq \Sigma^2$ (APPROX. UPPER BOUND) [S]

Sipser

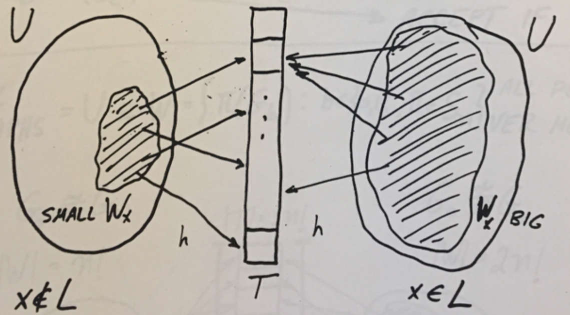
$L \in BPP$ $\qquad x \leftrightarrow W_x \subseteq \{0,1\}^n$

WITNESSES

$x \in L \Rightarrow |W_x| \geq \frac{2}{3} 2^n$ BIG

$x \notin L \Rightarrow |W_x| \leq \frac{1}{3} 2^{n/3}$ SMALL

$h \in_R H(U,T)$ $\quad U = \{0,1\}^n$ $\quad T = \{0,1\}^{\cancel{\frac{2n}{3}}\; n-1}$ INTERMEDIATE



$\Pr[h \text{ IS } 1\text{-}1] \geq \frac{1}{2}$ $\qquad$ h IS NOT 1-1

$x \notin L \Leftrightarrow \exists h \in H\ \forall y \neq z \in W_x\ [h(y) \neq h(z)]$

$IP(k) \subseteq AM(k+2)$ (APPROX. LOWER BOUND) [GS]

PRIVATE COINS $\equiv$ PUBLIC COINS

GRAPH NON-ISOMORPHISM $\in AM(2)$ [Sc]

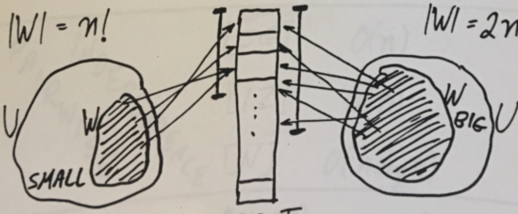
PROVER $\leftarrow G_0, G_1 \rightarrow$ VERIFIER

	$\xleftarrow{h,k}$	$h \in_R H$, $k \in_R T$
FIND $c \in \{0,1\}$, $\sigma \in S_n$ S.T. $h(\sigma(G_c)) = k$	$\xrightarrow{c,\sigma}$	ACCEPT IF $h(\sigma(G_c)) = k$

ALL GRAPHS $= U \supseteq W = \{\pi(G_b) : b \in \{0,1\}, \pi \in S_n\}$ ALL POSSIBLE VER. MESSAGES

$G_0 \cong G_1$ $\qquad$ $|T| = 2n!$ $\qquad$ $G_0 \not\cong G_1$

$|W| = n!$ $\qquad\qquad\qquad$ $|W| = 2n!$



$\alpha \in_R T$

$\Pr[\alpha \text{ NONEMPTY}] \le \frac{1}{2}$ $\qquad$ $\Pr[\alpha \text{ NONEMPTY}] \ge .6$

DETERMINISTIC AMPLIFICATION [KPS]

$L \in BPP$ $\quad x \leftrightarrow W_x \subseteq \{0,1\}^n$

$$\left.\begin{array}{l} x \in L \Rightarrow |W_x| \geq \frac{2}{3} 2^n \\ x \notin L \Rightarrow |W_x| \leq \frac{1}{3} 2^n \end{array}\right\} \begin{array}{l} n \text{ RANDOM BITS} \\ (\Pr[\text{error}] = \frac{1}{3}) \end{array}$$

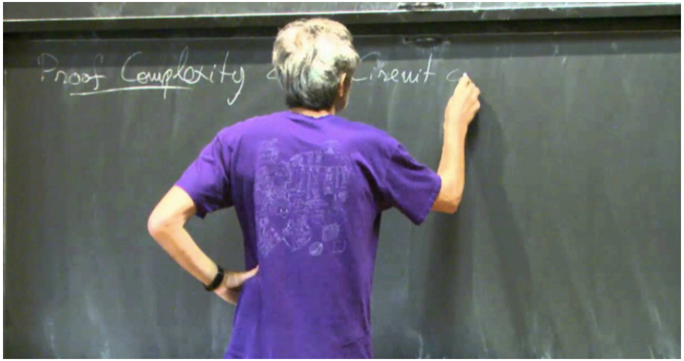
AMPLIFICATION ALGORITHM A:

GENERATE $G(\cdot) = (Y_1, Y_2 \cdots Y_k)$ $\quad Y_i \in \{0,1\}^n$

ACCEPT x IFF $MAJ\{Y_i \in W_x\}$

METHOD	REF.	#RANDOM BITS	$\Pr[\text{error}]$
INDEPENDENT SAMPLING		$O(n \cdot k)$	2^{-k}
PAIRWISE INDEPENDENCE	[CG] ~~[illegible]~~ Chor goldreigh	$O(n)$	n^{-c}
	[IZ]	$O(n)$	$2^{-\sqrt{n}}$
	[N] Nisan?	$O(n \log n)$	2^{-n}
EXPANDERS	[CW, IZ]	$n + O(k)$	2^{-k}

LEGEND



=

HARDNESS AMPLIFICATION

OLD SCHOOL:

f hard in worst case $\rightsquigarrow$

f' hard on average

HARDNESS AMPLIFICATION

OLD SCHOOL:

f hard in worst case $\rightsquigarrow$

f' hard on average

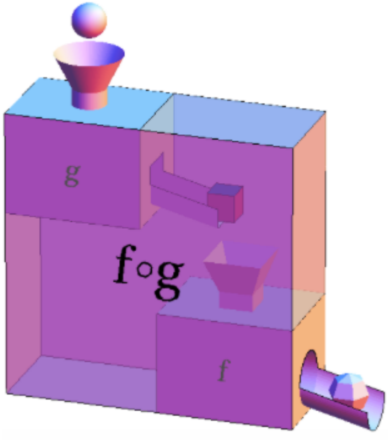
NEW SCHOOL: HARDNESS ESCALATION

f a little bit hard $\rightsquigarrow$

f' hard for a more powerful model

How to build f' ?

How to build f'?



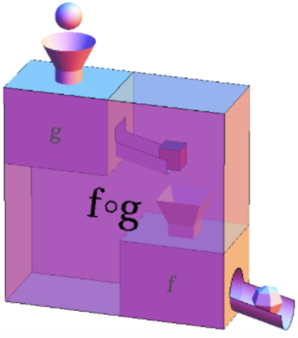
Function composition

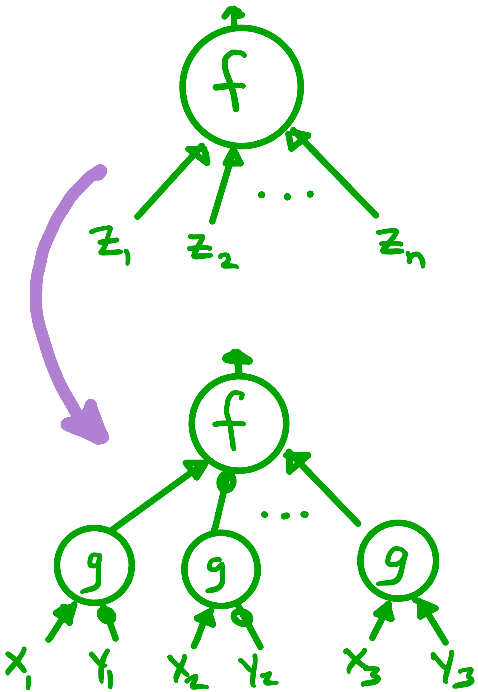
Already in early work:

Andreev '87

Karchmer-Raz-W '91

COMPOSED FUNCTIONS





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

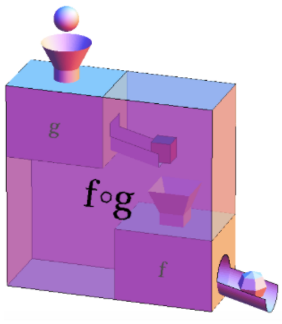
$g: \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

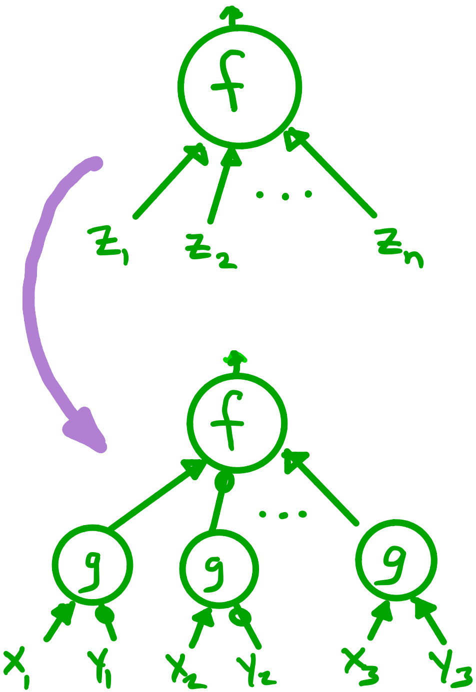
$F = f \circ g^n$

outer function

inner function (gadget)

COMPOSED FUNCTIONS





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

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

$F = f \circ g^n$

outer function

inner function (gadget)

LIFTING THEOREM

$CC(F) \approx$ decision-tree complexity (f)

or some variant

same variant in dec tree model

(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
Robere-P-Rossman-Cook '16	Razborov Rank	algebraic gap degree
Kothari-Meka-Raghavendra '16	Nonnegative Rank	Junta degree

A BLIZZARD OF APPLICATIONS

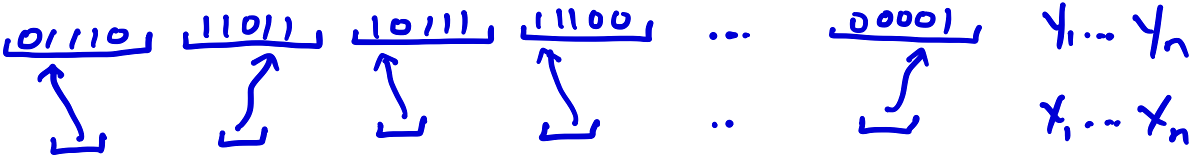
1. DETERMINISTIC CC LIFTING

Lifting Theorem for Deterministic CC

(Raz-McKenzie, Göös-P-Watson)

f : n-bit boolean function (or search problem)

$g(x,y) = y_x$, where $|y| = n^{\Theta(1)}$ pointer function



Theorem

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

Applications

1. Monotone circuit depth
   Proof complexity

2. Communication complexity
   - Partition vs deterministic CC
   - Log Rank conjecture LBs
   - clique/coclique (Göös)

APPLICATIONS TO CIRCUIT DEPTH & PROOF COMPLEXITY

UNSAT FORMULA (TSEITIN OR PEBBLING)

$\Downarrow$

CANONICAL SEARCH PROBLEM (SEARCH(TS_g))

$\Downarrow$ DECISION TREE LOWER BOUND

HIGH DECISION TREE COMPLEXITY

$\Downarrow$ LIFTING THM

HIGH CC FOR LIFTED SEARCH PROBLEM

HIGH MONOTONE CIRCUIT DEPTH

HIGH PROOF COMPLEXITY (RANK, LENGTH-SPACE)

CANONICAL SEARCH PROBLEM

UNSAT

kCNF $\mathcal{C} = C_1 \wedge C_2 \wedge \ldots \wedge C_m$ over $z_1, \ldots, z_n$

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

LIFTED

CANONICAL SEARCH PROBLEM

<u>KCNF</u> $\mathcal{C} = C_1 \wedge C_2 \wedge \dots \wedge C_m$ over $z_1, \dots, z_n$

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

<u>Search($\mathcal{C} \circ g^n$), $g: \mathcal{X} \times \mathcal{Y} \to \{0,1\}$:</u>

Alice gets $x \in \mathcal{X}^n$

Bob gets $y \in \mathcal{Y}^n$

Output C_i such that

$$C_i(g(x_{i_1}, y_{i_1}), g(x_{i_2}, y_{i_2}), g(x_{i_3}, y_{i_3})) = 0$$

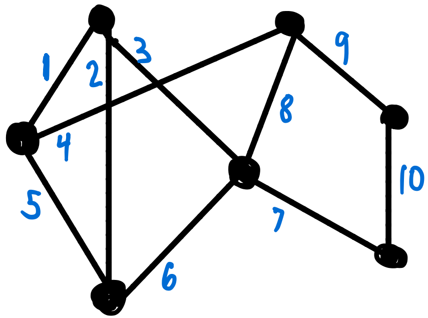
Tseitin Contradictions

A system of unsatisfiable mod 2 equations,
each variable occurs twice

$G = (V, E)$ n node, bounded-degree graph, n odd

TS_G : variables: x_e, $e \in E$

constraints: For each node v, sum of edges incident to v is odd



$$\begin{aligned}
x_1 + x_2 + x_3 &= 1 \quad (\text{mod } 2) \\
x_1 + x_4 + x_5 &= 1 \\
x_4 + x_8 + x_9 &= 1 \\
x_2 + x_5 + x_6 &= 1 \\
x_6 + x_7 + x_8 &= 1 \\
x_9 + x_{10} &= 1
\end{aligned}$$

Tseitin Contradictions

A system of unsatisfiable mod 2 equations, each variable occurs twice

$G = (V, E)$ n node, bounded-degree graph, n odd

TS_G: variables: x_e, $e \in E$

constraints: For each node v, sum of edges incident to v is odd

$Search(TS_G)$: given an assignment α to variables, output a violated constraint

LEMMA For expanding G,

$$DT(Search(TS_G)) = \Omega(n)$$

Tseitin Contradictions

A system of unsatisfiable mod 2 equations, each variable occurs twice

$G = (V, E)$ n node, bounded-degree graph, n odd

TS_G : variables: x_e, $e \in E$

constraints: For each node v, sum of edges incident to v is odd

Search(TS_G): given an assignment α to variables, output a violated constraint

COROLLARY OF DETERMINISTIC LIFTING THEOREM

$$CC(\text{Search}(TS_G \circ g^m)) = \Omega(n \log n)$$

APPLICATIONS TO CIRCUIT DEPTH & PROOF COMPLEXITY

UNSAT FORMULA (TSEITIN OR PEBBLING)

CANONICAL SEARCH PROBLEM (SEARCH(TS_g))

DECISION TREE LOWER BOUND

HIGH DECISION TREE COMPLEXITY

LIFTING THM

HIGH CC FOR LIFTED SEARCH PROBLEM

HIGH MONOTONE CIRCUIT DEPTH

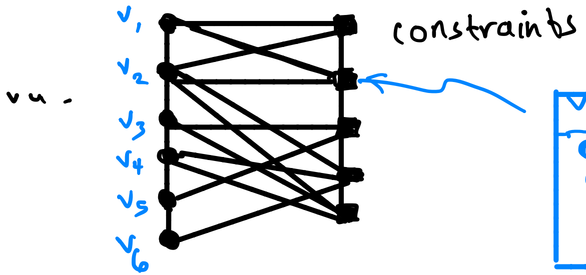
$\Omega(n^{\varepsilon})$

HIGH PROOF COMPLEXITY (RANK, LENGTH-SPACE)

Cutting Planes

MONOTONE CIRCUIT DEPTH (RM, GPW, Oliveira)

Monotone K-SAT / K-CSP



v_1	v_2	
0	0	1
0	1	1
1	0	0
1	1	0

$\binom{n}{K} 2^K$ variables

variables of monotone K-SAT

Input is a KSAT φ

Output 1 iff φ is satisfiable

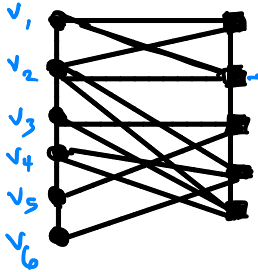
<u>Lemma</u> $\max_{\text{unsat } \varphi} [CC(Search(\varphi \circ g^n))] \le mDepth(\text{monotone K-CSP})$

lifted search problem

lifted K-CSP

MONOTONE CIRCUIT DEPTH (RM, GPW, Oliveira)

Monotone K-SAT / K-CSP



v_1	v_2	
0	0	1
0	1	1
1	0	0
1	1	0

$\binom{n}{K} 2^K$ variables

variables of monotone K-SAT

Input is a KSAT φ
Output 1 iff φ is satisfiable

Lemma $\max_{\text{unsat } \varphi} [CC(\text{Search}(\varphi \circ g^n))] \leq \text{mDepth}(\text{monotone K-CSP})$

Alice X : ⊔ ⊔ ⊔ ⊔ .. ⊔

Bob Y : ⊔ ⊔ ⊔ .. ⊔

output violated clause

$\Rightarrow$

X describes a maxterm (unSAT lifted version of φ)

Y describes a minterm (SAT φ – all constraints consistent with y)

PROOF COMPLEXITY

Basic idea from Lovasz - Naor - Newman - 

- Height r refutation, each line has low cc
  $\Rightarrow$ low cc protocol for search problem

- Small size, small space refutation, each line low cc
  $\Rightarrow$ low cc protocol for search problem

APPLICATIONS TO CIRCUIT DEPTH & PROOF COMPLEXITY

UNSAT FORMULA (TSEITIN OR PEBBLING)

CANONICAL SEARCH PROBLEM (SEARCH(TS_g))

DECISION TREE LOWER BOUND

HIGH DECISION TREE COMPLEXITY

LIFTING THM

HIGH CC FOR LIFTED SEARCH PROBLEM

HIGH MONOTONE CIRCUIT DEPTH

$\Omega(n^{\varepsilon})$

HIGH PROOF COMPLEXITY (RANK, LENGTH-SPACE)

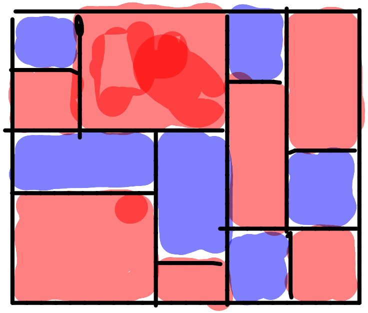
Cutting Planes

DETERMINISTIC LIFTING: CC APPLICATIONS

- Partition vs Deterministic CC
- Log Rank Conjecture
- Clique vs co-Clique

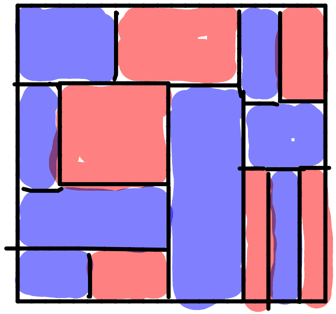
PARTITION VS. DETERMINISTIC CC

DETERMINISTIC CC



$CC(F)$ = det cc of F

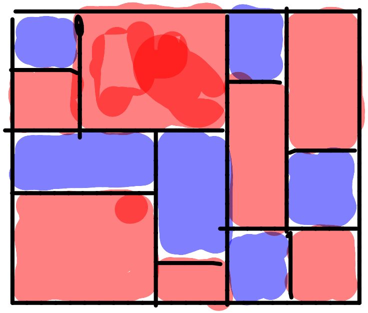
PARTITION



Partition number $\chi(F)$:
least # of monochrom. rectangles to cover matrix

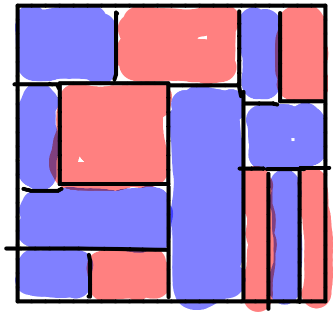
PARTITION VS. DETERMINISTIC CC

DETERMINISTIC CC



CC(F) = det cc of F

PARTITION



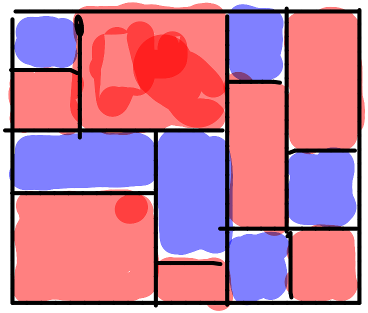
Partition number $\chi(F)$: least # of monochrom. rectangles to cover matrix

$$\chi(F) = \chi_0(F) + \chi_1(F)$$

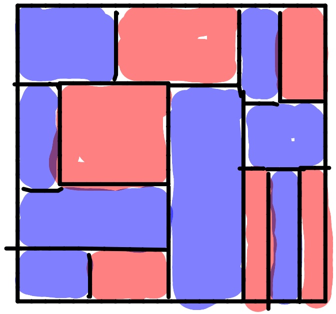
min # rectangles to partition 0's

PARTITION VS. DETERMINISTIC CC

DETERMINISTIC CC



PARTITION



Theorem (Göös-P-Watson)

$\exists F \quad cc(F) \geq \tilde{\Omega}(\log^{1.5} \chi(F))$

$\exists F \quad cc(F) \geq \tilde{\Omega}(\log^{2} \chi_1(F))$

$\forall F \quad cc(F) \leq O(\log^2 \chi(F))$
[Aho, Ullman, Yann. '83]

tight
[Yannakakis '88]

LOG-RANK CONJECTURE (Lovász-Saks '88)

$$\forall F \quad CC(F) \overset{?}{=} \log^{O(1)} \mathrm{rank}(F)$$

THEOREM (Kushilevitz-Nisan-)

$$\exists F \quad CC(F) \geq \Omega(\log^{1.63} \mathrm{rank}(F))$$

COROLLARY OF GPW

$$\exists F \quad CC(F) \geq \Omega(\log^{2} \mathrm{rank}(F))$$

since $\chi_1(F) \geq \mathrm{rank}(F)$

2. Randomized CC Lifting

* Proof easy + gadget constant-size
* Works in number-on-forehead CC model!

2. Randomized CC Lifting

* Proof easy + gadget constant-size
* works in number-on-forehead CC model!

- complexity measure for f a (stronger) variant of dec trees
- works for total search problems

SEARCH PROBLEMS & CRITICAL BLOCK SENSITIVITY

(Huynh + Nordstrom)

Let $S \subseteq \{0,1\}^n \times Q$ be a search problem.

$$cbs(S) \stackrel{d}{=} \min_{f \subseteq S} \max_{\alpha} bs(f,\alpha)$$

critical block sensitivity

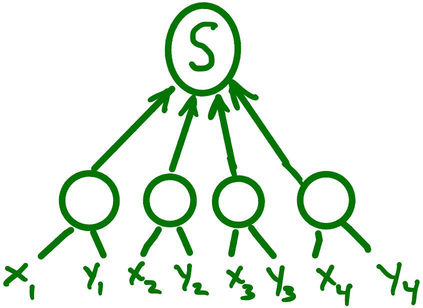
f is a function solving S

α a critical assignment

block sensitivity

* when S a function, $cbs(S) = bs(S)$

LIFTING THEOREM FOR RANDOMIZED CC (of Search)



$S \circ g^n$

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

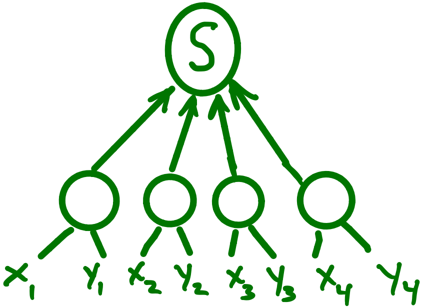
Lifting Theorem [Zhang, Huynh-Nordström, Göös-P]

$$\text{Randomized-CC}(S \circ g^n) = \Omega(\text{cbs}(S)),$$

$g =$

0	0	1	1
0	1	1	0
1	1	1	0
1	0	0	1

Lifting Search Problems



$$S \circ g^n$$

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

Lifting Theorem (Göös, P)

$$\text{Randomized-CC}\,(S \circ g^n) = \Omega(\text{cbs}(S)), \quad g = $$

0	0	1	1
0	1	1	0
1	1	0	0
1	0	0	1

- Proof: a reduction to DISJ!
- Works in NOF model!
- constant-sized gadget ☺

Tseitin Contradictions

A system of unsatisfiable mod 2 equations, each variable occurs twice

$G = (V, E)$ n node, bounded-degree graph, n odd

TS_G : variables: x_e, $e \in E$

constraints: For each node v, sum of edges incident to v is odd

$Search(TS_G)$: given an assignment α to variables, output a violated constraint

THEOREM (Göös-P)

For expanding G, $cbs(Search(TS_G)) = \Omega(n/\log n)$

Tseitin Contradictions

A system of unsatisfiable mod 2 equations, each variable occurs twice

$G = (V, E)$ n node, bounded-degree graph, n odd

TS_G: <u>variables</u>: x_e, $e \in E$

<u>constraints</u>: For each node v, sum of edges incident to v is odd

Search(TS_G): given an assignment α to variables, output a violated constraint

COROLLARY OF RANDOMIZED LIFTING

$$CC(\text{Search}(TS_G \circ g^n)) = \Omega(n/\log n)$$

* g constant sized, and also holds for NOF cc

Putting Everything Together

UNSAT FORMULA (TSEITIN OR PEBBLING)

$\Downarrow$

CANONICAL SEARCH PROBLEM (SEARCH(TS_g))

$\Downarrow$ PREVIOUS THM

HIGH CRITICAL BLOCK SENSITIVITY

$\Downarrow$ LIFTING THM

HIGH CC FOR LIFTED PROBLEM

HIGH MONOTONE CIRCUIT DEPTH

$\Omega(n/\log n)$

Best Previous $\sqrt{n}$

Raz-

HIGH PROOF COMPLEXITY (RANK, LENGTH-SPACE)

SOS, LS^+, CP, SA

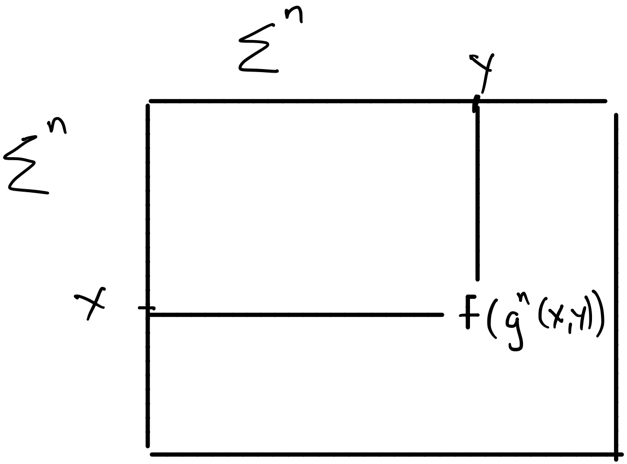
3. Rank Lifting

Razborov rank

Non-neg rank

LIFTING RANK

(Sherstov)



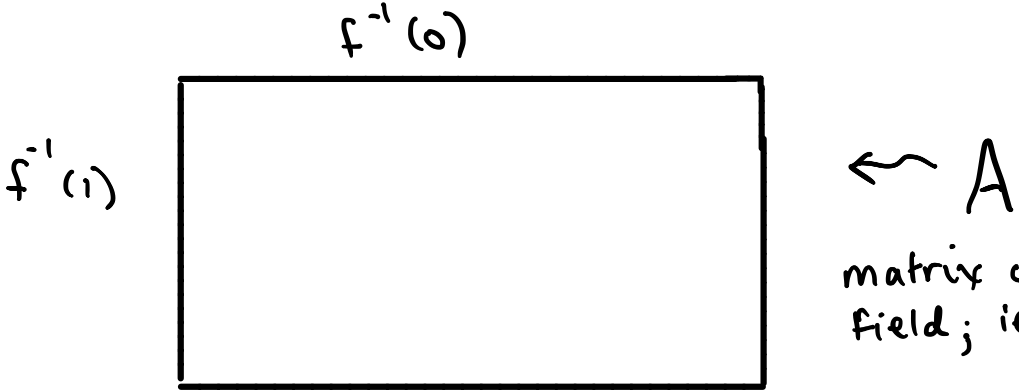
$M_f^g \in \mathbb{R}^{\Sigma^n \times \Sigma^n}$

Want to relate a rank measure for M_f^g to a degree measure for f

<u>Sherstov</u> $\text{Rank}(M_f^g) \approx \text{Degree}(f)$

Razborov's Rank Measure

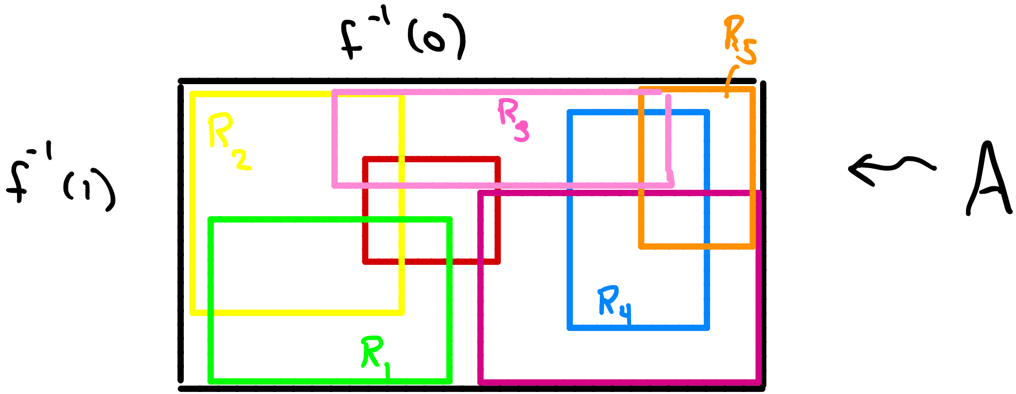
$f : \{0,1\}^n \to \{0,1\}$ monotone



matrix over a field; ie. $\mathbb{R}$

Razborov's Rank Measure

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



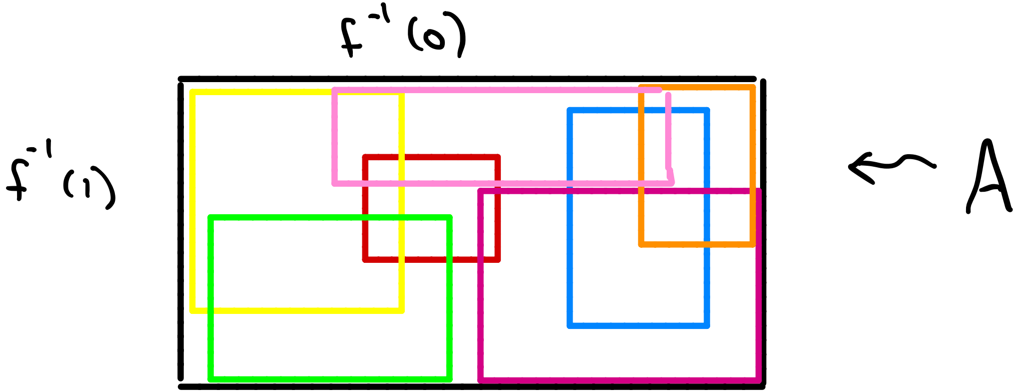
KW subrectangles: $R_i = \{(x,y) \in f^{-1}(1) \times f^{-1}(0) \mid x_i = 1, y_i = 0\}$

RANK MEASURE

$$\mu_A(f) = \frac{\operatorname{rank}(A)}{\max\limits_{i \in [n]} \operatorname{rank}(A_i)}$$

Razborov's Rank Measure

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



Theorem $\forall$ fields $\mathbb{F}$, $\forall$ Boolean f, $\forall A$ over $\mathbb{F}$

$$\mu_A(f) \leq mSPAN_{\mathbb{F}}(f) \leq mL(f) \leq mNC^1(f)$$

$$\mu_A(f) \leq mCC(f)$$

Razborov's Rank Measure

Best previous Lower bound : $n^{\Omega(\log n)}$ for a monotone function in NP

NEW (Robere, P, Rossman, Cook '16)

$\exists f$ in mP, and real matrix A s.t.

$$\mu_A(f) \geq 2^{n^{\varepsilon}}$$

$\exists g$ in mNL, and real matrix B s.t.

$$\mu_B(g) \geq n^{\Omega(\log n)}$$

PROOF IS A NEW LIFTING THEOREM

$$\mu_A(f \circ g^n) \approx \text{"algebraic gap" degree of } f$$

Applications

Monotone Span Programs

Monotone formula size + branching programs

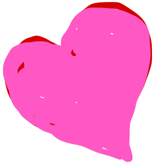
Monotone Comparator Circuits

SPAN PROGRAMS

(Karchmer - )

$$\begin{array}{c} \\ x_1 \\ x_2 \\ \bar{x}_2 \\ x_3 \\ \bar{x}_4 \\ x_5 \end{array}
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline
\end{array}$$

M



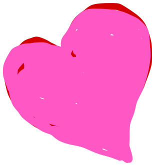
SPAN PROGRAMS

(K- )

$$
\begin{array}{c}
x_1 \\ x_2 \\ \bar{x}_2 \\ x_3 \\ \bar{x}_4 \\ x_5
\end{array}
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline
\end{array}
\qquad M
$$

Given $\alpha \in \{0,1\}^n$, M accepts α iff

M_α spans $\vec{1}$



SPAN PROGRAMS

(K- )

x_1	1	0	0	0	0	0	0	0
x_2	0	1	0	0	0	0	0	0
$\bar{x}_2$	0	1	0	0	0	0	0	0
x_3	0	1	0	1	0	1	0	1
$\bar{x}_4$	0	0	1	1	1	1	1	1
x_5	0	0	1	1	1	1	1	1

M

Example $\alpha = 10011$

SPAN PROGRAMS (k- )

$$
\begin{array}{c|cccccccc}
x_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\bar{x}_2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
x_3 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\bar{x}_4 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
x_5 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}
\qquad M_\alpha
$$

Example $\alpha = 10011$

is accepted !

SPAN PROGRAMS

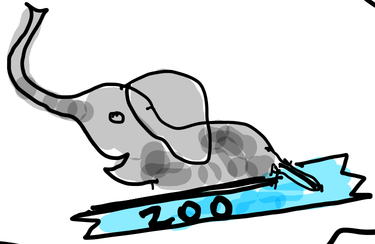
(K- )

x_1	1	0	0	0	0	0	0	0
x_2	0	1	0	0	0	0	0	0
$\bar{x}_2$	0	1	0	0	0	0	0	0
x_3	0	1	0	1	0	1	0	1
$\bar{x}_4$	0	0	1	1	1	1	1	1
x_5	0	0	1	1	1	1	1	1

M

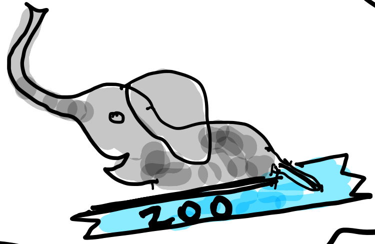
M is <u>monotone</u> if rows labelled with only positive literals

- Monotone span programs equivalent to linear secret sharing schemes

SPAN PROGRAMS AND THE 

$$
\begin{array}{ccccccccc}
mNC^1 & \subseteq & mL & \subseteq & mNL & \subseteq & mNC & \subseteq & mP \\
 & & \rotatebox{-90}{$\subseteq$} & & & & & & \\
 & & mSPAN_F & & & & & &
\end{array}
$$

SPAN PROGRAMS AND THE



$$m\mathrm{NC}^1 \subsetneq m\mathrm{L} \subsetneq m\mathrm{NL} \subsetneq m\mathrm{NC} \subsetneq m\mathrm{P}$$

$$\rotatebox{90}{$\supseteq$}$$

$$m\mathrm{SPAN}_F \subsetneq m\mathrm{P}$$

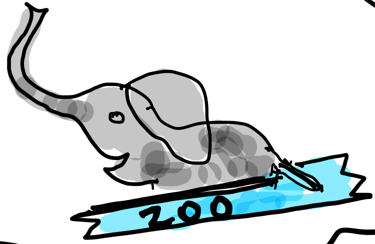
Karchmer-  '88

Babai, Gal,  '99

Potechin '10

Raz, McKenzie '99

SPAN PROGRAMS AND THE



$$\mathrm{mNC}^1 \subsetneq \mathrm{mL} \subsetneq \mathrm{mNL} \subsetneq \mathrm{mNC} \subsetneq \mathrm{mP}$$

$$\rotatebox{90}{$\subseteq$}$$

$$\mathrm{mSPAN}_F \subsetneq \mathrm{mP}$$

Karchmer–  '88

Babai, Gal,  '99

Potechin '10

Raz, McKenzie '99

<u>Robere-P-Rossman-Cook</u>

Lifting Theorem for Razborov's Rank gives all of these separations plus more

See Robert's talk!

Lifting Theorem for Non-Neg Rank

$b = 10 \log_2 n$

$g(\alpha, \beta) := \sum_{i=1}^{b} \alpha_i \beta_i \mod 2$

$\deg_+(f) := \min d$ such that $f = \sum h_i$,
h_i non-negative d-junta

[Kothari-Meka-Raghavendra '16]

$$nnr(M_f^g) \approx \exp\left(\Omega\left(b \cdot \deg_+\left(f + \frac{100}{n}\right)\right)\right)$$

[Göös-Lovett-Meka-Watson-Zuckerman '15]

$$\text{approx-}nnr(M_f^g) \approx \exp\left(\Omega\left(\log n \cdot \text{approx-}\deg_+(f)\right)\right)$$

Lifting Theorem for Non-Neg Rank

Corollary

Beating the trivial algorithms for MAX-3SAT, MAX-3XOR requires $\exp(n^{\varepsilon})$ sized extended formulations

(Natural family of LPs must have exponential size)

What's Left ?

What's Left?

- Karchmer-  : nonmonotone case

What's Left ?

- Karchmer-  : Nonmonotone case
- Extended Formulations :
  models where polytope can
  depend on instance

What's Left?

- Karchmer-  : nonmonotone case
- Extended Formulations:
  models where polytope can
  depend on instance
- 60 more years!


Thanks!