Communication Lower Bounds via Critical Block Sensitivity

Mika Göös & Toniann Pitassi
University of Toronto

Communication complexity?

[Yao, STOC'79]

Alice

Bob

Communication complexity?

[Yao, STOC'79]

Alice

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

Bob

$y \in \{0,1\}^n$

Communication complexity?

[Yao, STOC'79]

Alice

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

Bob

$y \in \{0,1\}^n$

- **Goal** is to compute $f(x,y)$

Communication complexity? [Yao, STOC'79]

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

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

- **Goal** is to compute $f(x,y)$
- **Example:** $f(x,y) = 1$ iff $x = y$

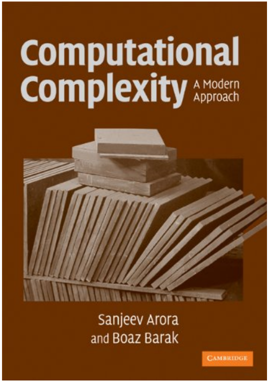
Communication complexity? [Yao, STOC'79]

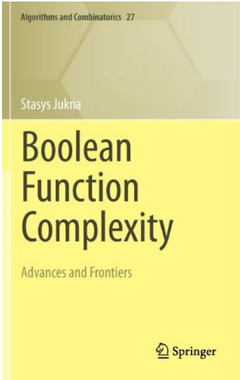
Alice **Bob**

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

- **Comm. complexity of f** is the least amount of communication required to compute f

Resources





2009 4%

2012 15%

1997 100%

Applications

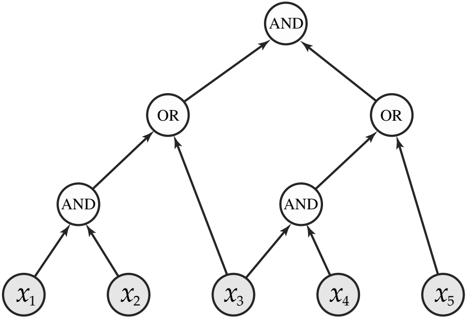
1. Distributed computations (duh)
2. Combinatorics
3. Circuit complexity (KW games)
4. Proof complexity (+ SAT algorithms)
5. Time–space tradeoffs for Turing machines
6. Extended formulations for LPs
7. Streaming algorithms
8. Property testing
9. Privacy
10. etc. . .

Applications

1. Distributed computations (duh)
2. Combinatorics
3. Circuit complexity (KW games)
4. Proof complexity (+ SAT algorithms)
5. Time–space tradeoffs for Turing machines
6. Extended formulations for LPs
7. Streaming algorithms
8. Property testing
9. Privacy
10. etc. . .

Our results: Applications

1. **Monotone circuit depth.** We exhibit an *explicit* (i.e., in **NP**) monotone function on n variables whose monotone circuits require depth $\Omega(n/\log n)$; previous best $\Omega(\sqrt{n})$ by Raz & Wigderson (JACM'92)



Our results: Applications

1. **Monotone circuit depth.** We exhibit an *explicit* (i.e., in **NP**) monotone function on n variables whose monotone circuits require depth $\Omega(n/\log n)$; previous best $\Omega(\sqrt{n})$ by Raz & Wigderson (JACM'92)

   We exhibit a function in monotone **P** with monotone depth $\Theta(\sqrt{n})$

   These lower bounds hold even if the circuits are allowed to err
   $\Longrightarrow$ average-case hierarchy theorem of Filmus et al. (FOCS'13)

Our results: Applications

1. **Monotone circuit depth.** We exhibit an *explicit* (i.e., in **NP**) monotone function on n variables whose monotone circuits require depth $\Omega(n/\log n)$; previous best $\Omega(\sqrt{n})$ by Raz & Wigderson (JACM'92)

   We exhibit a function in monotone **P** with monotone depth $\Theta(\sqrt{n})$

   These lower bounds hold even if the circuits are allowed to err
   $\Longrightarrow$ average-case hierarchy theorem of Filmus et al. (FOCS'13)

2. **Proof complexity.** Rank and length–space lower bounds for semi-algebraic proof systems, including Lovász–Schrijver and Lasserre systems. This extends and simplifies Beame et al. (SICOMP'07) and Huynh and Nordström (STOC'12)

Our results: Communication complexity

1. **Starting point:** Simple proof of the following theorem

Huynh & Nordström (STOC'12)

Let S be a *search problem*. The communication complexity of a certain *two-party lift* of S is at least the **critical block sensitivity (cbs)** of S.

2. **New cbs lower bounds:** **Tseitin** and **Pebbling** problems

Critical block sensitivity

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

- On input $\alpha \in \{0,1\}^n$ the goal is to find a $q \in Q$ s.t. $(\alpha, q) \in S$
- Input α is **critical** if there is a unique feasible solution for α

Critical block sensitivity

[Huynh & Nordström, STOC'12]

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

- On input $\alpha \in \{0,1\}^n$ the goal is to find a $q \in Q$ s.t. $(\alpha, q) \in S$
- Input α is **critical** if there is a unique feasible solution for α

Critical block sensitivity (cbs)

- Let $f \subseteq S$ be a **function** solving S

Critical block sensitivity

[Huynh & Nordström, STOC'12]

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

- On input $\alpha \in \{0,1\}^n$ the goal is to find a $q \in Q$ s.t. $(\alpha, q) \in S$
- Input α is **critical** if there is a unique feasible solution for α

Critical block sensitivity (cbs)

- Let $f \subseteq S$ be a **function** solving S
- Let $\mathrm{bs}(f, \alpha)$ be the **block sensitivity** of f at α

$$\mathrm{bs}(f,\alpha) \;=\; \max k \text{ such that there are disjoint blocks } B_1, \ldots, B_k \subseteq [n] \text{ with } f(\alpha) \neq f(\alpha^{(B_i)}) \text{ for all } i \in [k]$$

Critical block sensitivity [Huynh & Nordström, STOC'12]

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

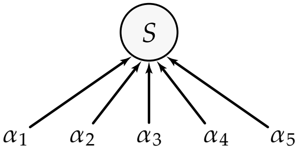
- On input $\alpha \in \{0,1\}^n$ the goal is to find a $q \in Q$ s.t. $(\alpha, q) \in S$
- Input α is **critical** if there is a unique feasible solution for α

Critical block sensitivity (cbs)

- Let $f \subseteq S$ be a **function** solving S
- Let $\mathrm{bs}(f, \alpha)$ be the **block sensitivity** of f at α

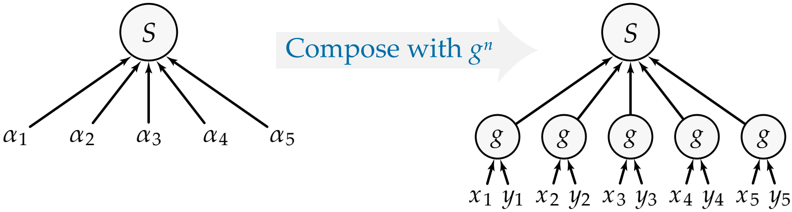
$$\mathrm{cbs}(S) := \min_{f \subseteq S} \max_{\text{critical } \alpha} \mathrm{bs}(f, \alpha)$$

Lifted problems



How do we turn $S \subseteq \{0,1\}^n \times Q$ into a **two-party** communication problem?

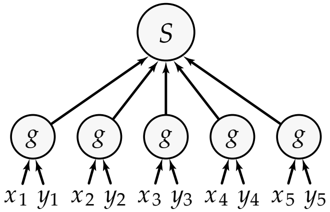
Lifted problems



Lifting: We consider a **composed** problem $S \circ g^n$ where $g\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ is some small two-party function (called "gadget")

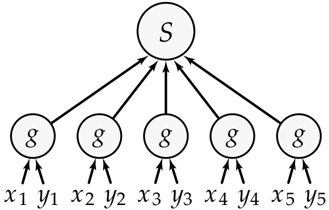
- **Alice** holds $x \in \mathcal{X}^n$
- **Bob** holds $y \in \mathcal{Y}^n$

Lower bounds via **cbs**



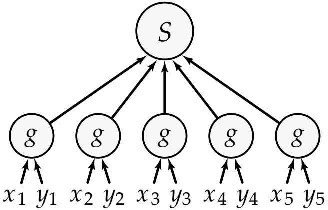
Lower bounds via **cbs**

Let $g = \begin{array}{|c|c|c|c|}\hline 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline \end{array}$



Lower bounds via **cbs**

Let $g = \begin{array}{|c|c|c|c|}\hline 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline \end{array}$

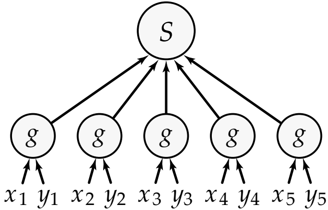


Theorem (Lower bounds via cbs)

Randomised comm. complexity of $S \circ g^n$ is $\Omega(\mathrm{cbs}(S))$

Lower bounds via **cbs**

Let $g = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$



Theorem (Lower bounds via cbs)

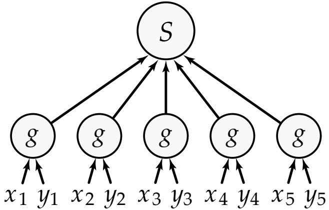
Randomised comm. complexity of $S \circ g^n$ is $\Omega(\text{cbs}(S))$

Comparison with [Huynh & Nordström, 2012]:

- Slightly different gadgets
- We reduce from **set-disjointness**; [HN'12] use information theory
- Our proof generalises to multi-party models (NIH, NOF)

Lower bounds via **cbs**

Let $g = \begin{array}{|c|c|c|c|} \hline 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline \end{array}$



Theorem (Lower bounds via cbs)

Randomised comm. complexity of $S \circ g^n$ is $\Omega(\mathrm{cbs}(S))$

Proof...

Proof strategy

Proof is by a reduction from **set-disjointness**:

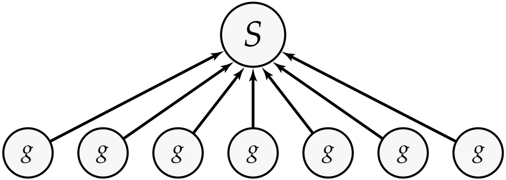
$$\mathrm{DISJ}_{\mathrm{cbs}} \leq S \circ g^n$$

where DISJ_m is defined as follows:

- **Alice** holds $A \subseteq [m]$
- **Bob** holds $B \subseteq [m]$
- **Goal** is to decide whether $A \cap B = \emptyset$

It is known that DISJ_m requires $\Theta(m)$ bits of communication (even randomised protocols)

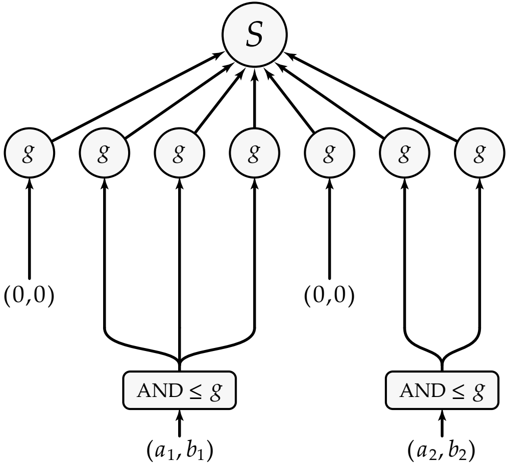
Reduction $\mathrm{DISJ}_{\mathrm{cbs}} \leq S \circ g^n$ [Zhang, ISAAC'09]



Suppose S is a **function** with 2-sensitive input

$$\alpha = 0\underline{000}0\underline{00}$$

Reduction $\mathrm{DISJ}_{\mathrm{cbs}} \leq S \circ g^n$ [Zhang, ISAAC'09]

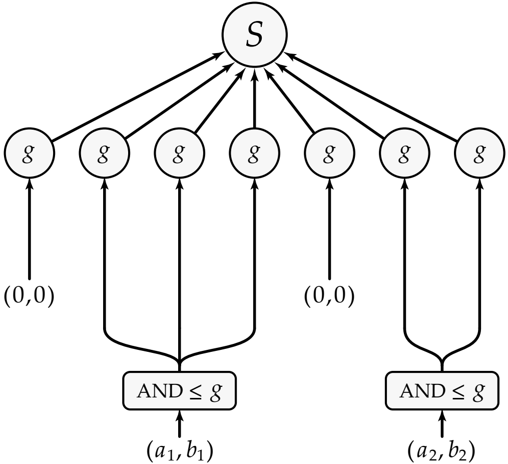


Suppose S is a **function** with 2-sensitive input

$$\alpha = 0\underline{000}0\underline{00}$$

Reduction $\mathrm{DISJ}_{\mathrm{cbs}} \leq S \circ g^n$

[Zhang, ISAAC'09]



Suppose S is a **function** with 2-sensitive input

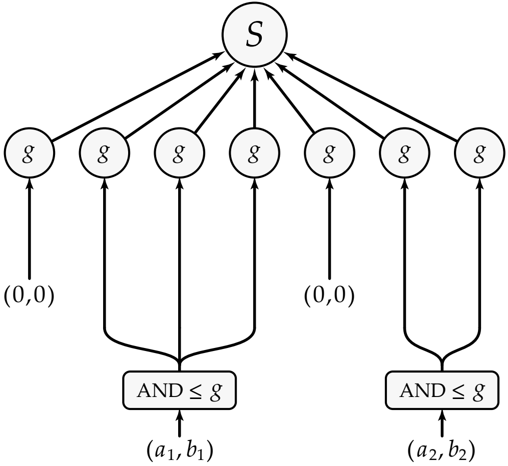
$$\alpha = 0\underline{000}0\underline{00}$$

AND $\leq g$

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

Reduction $\text{DISJ}_{\text{cbs}} \leq S \circ g^n$

[Zhang, ISAAC'09]

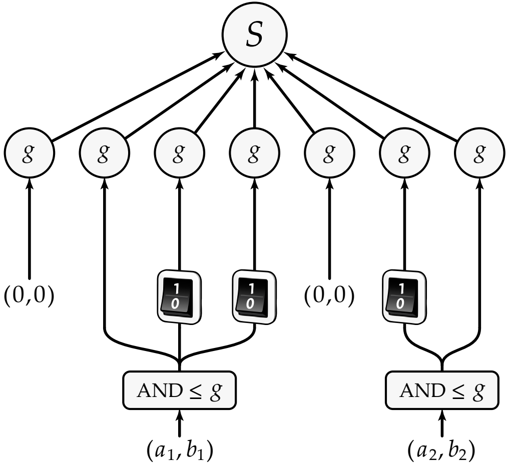


Suppose S is a **function** with 2-sensitive input

$$\alpha = 0\underline{011}0\underline{10}$$

Reduction $\text{DISJ}_{\text{cbs}} \le S \circ g^n$

[Zhang, ISAAC'09]



Suppose S is a **function** with 2-sensitive input

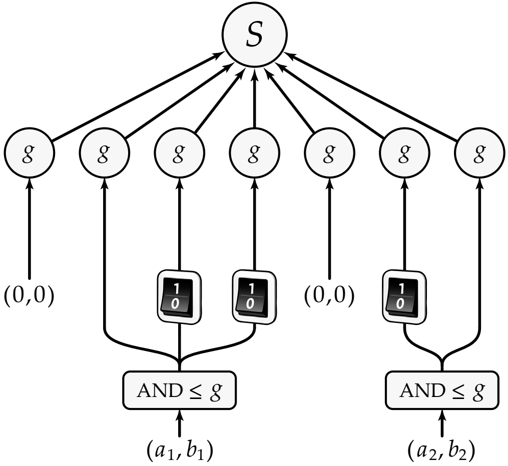
$$\alpha = 0\underline{011}0\underline{10}$$

Flippability:

$\neg g \le g$

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

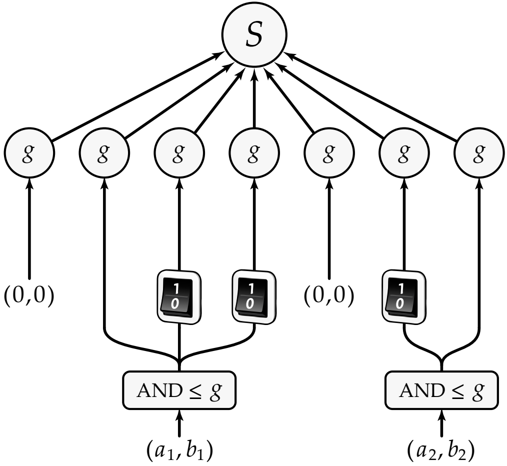
Reduction $\mathrm{DISJ}_{\mathrm{cbs}} \leq S \circ g^n$



What if S is a **search problem**?

- How do we define $f \subseteq S$?
- Protocol's output can depend on the *encoding* (x, y) of $\alpha = g^n(x, y)$!

Reduction $\text{DISJ}_{\text{cbs}} \leq S \circ g^n$

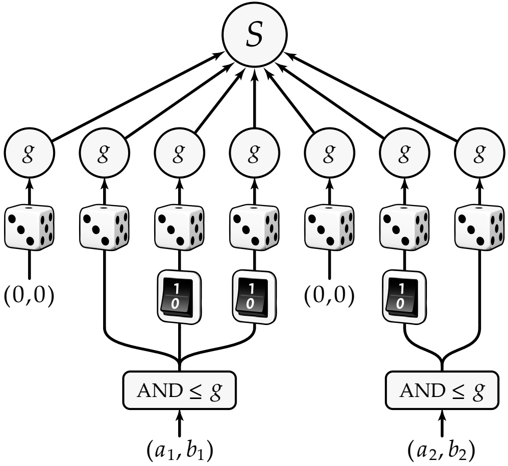


Solution: Consider **random** encodings!

Define $f(\alpha)$ to be the *most likely* solution output by the protocol on a random encoding of α

Apply a **random-self-reduction** to map any particular encoding (x, y) of $\alpha = g^n(x, y)$ into a random one

Reduction $\mathrm{DISJ}_{\mathrm{cbs}} \leq S \circ g^n$



Random-self-reduction:

$$(x, y) \in g^{-1}(z)$$
$$\downarrow$$
$$(X, Y) \in_R g^{-1}(z)$$

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

Proof complete!

Theorem (Lower bounds via cbs)

Randomised comm. complexity of $S \circ g^n$ is $\Omega(\text{cbs}(S))$

Note: Extension to multi-party setting uses **random-self-reducible** multi-party gadgets

Next up:

We need **cbs** lower bounds for interesting search problems
Focus of this talk: **Tseitin search problems**

Tseitin contradictions

Let G be a **bounded-degree** graph with an **odd** number of nodes

Tseitin contradiction F_G

- **Variables:** x_e for each edge e
- **Clauses:** For each node v,

$$\sum_{e:v\in e} x_e \equiv 1 \pmod 2$$

Tseitin contradictions

Let G be a **bounded-degree** graph with an **odd** number of nodes

Tseitin contradiction F_G

- **Variables:** x_e for each edge e
- **Clauses:** For each node v,

$$\sum_{e: v \in e} x_e \equiv 1 \pmod 2$$

Canonical search problem

- **Input:** Assignment to the variables of F_G
- **Output:** Violated clause

Tseitin contradictions

Let G be a **bounded-degree** graph with an **odd** number of nodes

Tseitin contradiction F_G

- **Variables:** x_e for each edge e
- **Clauses:** For each node v,

$$\sum_{e : v \in e} x_e \equiv 1 \pmod 2$$

Canonical search problem

- **Input:** Assignment to the variables of F_G
- **Output:** Violated clause

If G is an expander...

Known: Deterministic query complexity $\Theta(n)$ [Urq'87]
Randomised query complexity $\Omega(n^{1/3})$ [LNNW'95]

We prove: Critical block sensitivity $\Omega(n/\log n)$

Tseitin sensitivity

κ-routability

G is κ**-routable** iff there is a set of terminals

$$T \subseteq V(G), \quad |T| = \kappa,$$

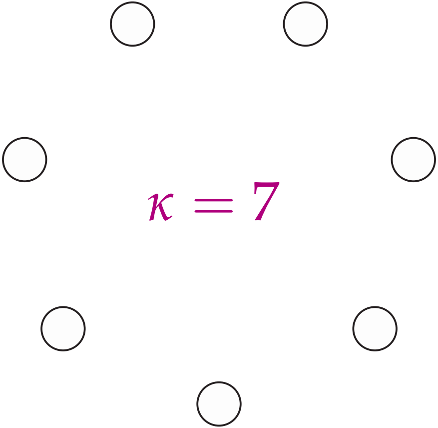
such that for every pairing of the nodes of T there are edge-disjoint paths in G connecting every pair

Example: $\kappa = \Theta(n/\log n)$ on an expander

Theorem (Tseitin sensitivity)

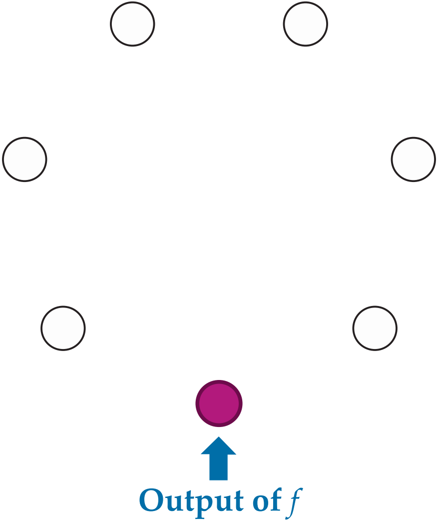
$\text{cbs}(\text{Tseitin}) = \Omega(\kappa)$

Tseitin sensitivity: Proof



Let f be a function solving the Tseitin problem

Tseitin sensitivity: Proof

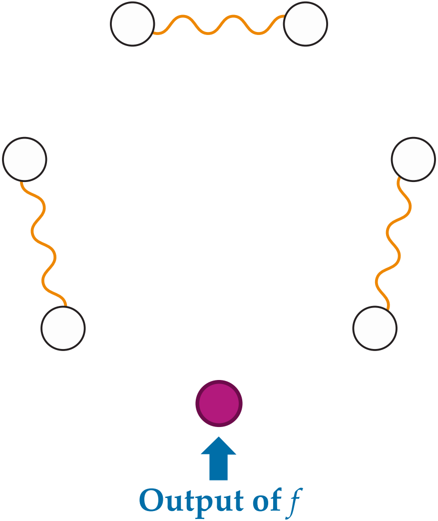


Let f be a function solving the Tseitin problem

Consider a **configuration**:

- Unique violation at a terminal

Tseitin sensitivity: Proof

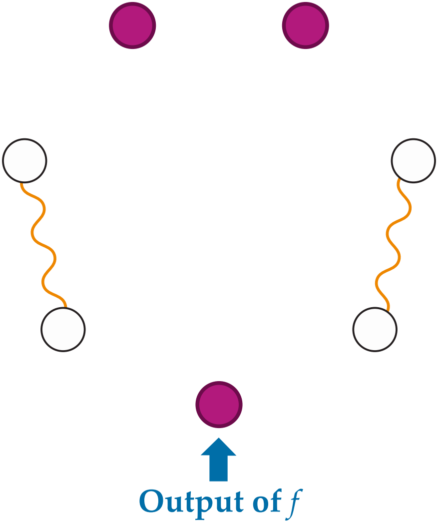


Let f be a function solving the Tseitin problem

Consider a **configuration**:

- Unique violation at a terminal
- Blocks are edge-disjoint paths pairing the remaining terminals

Tseitin sensitivity: Proof

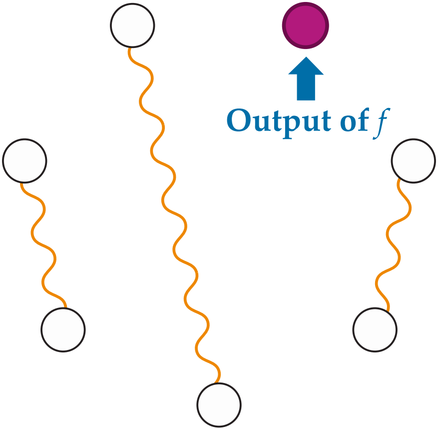


Let f be a function solving the Tseitin problem

Consider a **configuration**:

- Unique violation at a terminal
- Blocks are edge-disjoint paths pairing the remaining terminals

Tseitin sensitivity: Proof

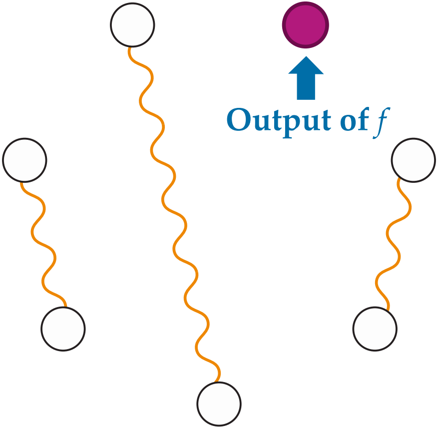


Let f be a function solving the Tseitin problem

Consider a **configuration**:

- Unique violation at a terminal
- Blocks are edge-disjoint paths pairing the remaining terminals

Tseitin sensitivity: Proof



Let f be a function solving the Tseitin problem

Consider a **configuration**:

- Unique violation at a terminal
- Blocks are edge-disjoint paths pairing the remaining terminals

Show that a **random config** is sensitive to $\Omega(\kappa)$ blocks in expectation!

Putting everything together

Unsatisfiable CNF formula
(**Tseitin** or **Pebbling**)

$\rightsquigarrow$

Canonical search problem

$\rightsquigarrow$

Thm: High critical block sensitivity

$\rightsquigarrow$

Thm: High communication complexity for lifted problem

$\swarrow$ $\searrow$

High monotone circuit depth
[KW'88], [RM'99], [FPRC'13]

High proof complexity
(rank & length–space)
[IPU'94], [BPS'07], [HN'12]

Open problem

Conjecture

There exists a two-party gadget g such that for all

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

- **Deterministic** comm. complexity of $f \circ g^n$ $\approx$ **deterministic** query complexity of f
- **Randomised** comm. complexity of $f \circ g^n$ $\approx$ **randomised** query complexity of f

Open problem

Conjecture

There exists a two-party gadget g such that for all

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

- **Deterministic** comm. complexity of $S \circ g^n$ $\approx$ **deterministic** query complexity of S
- **Randomised** comm. complexity of $S \circ g^n$ $\approx$ **randomised** query complexity of S

Questions?