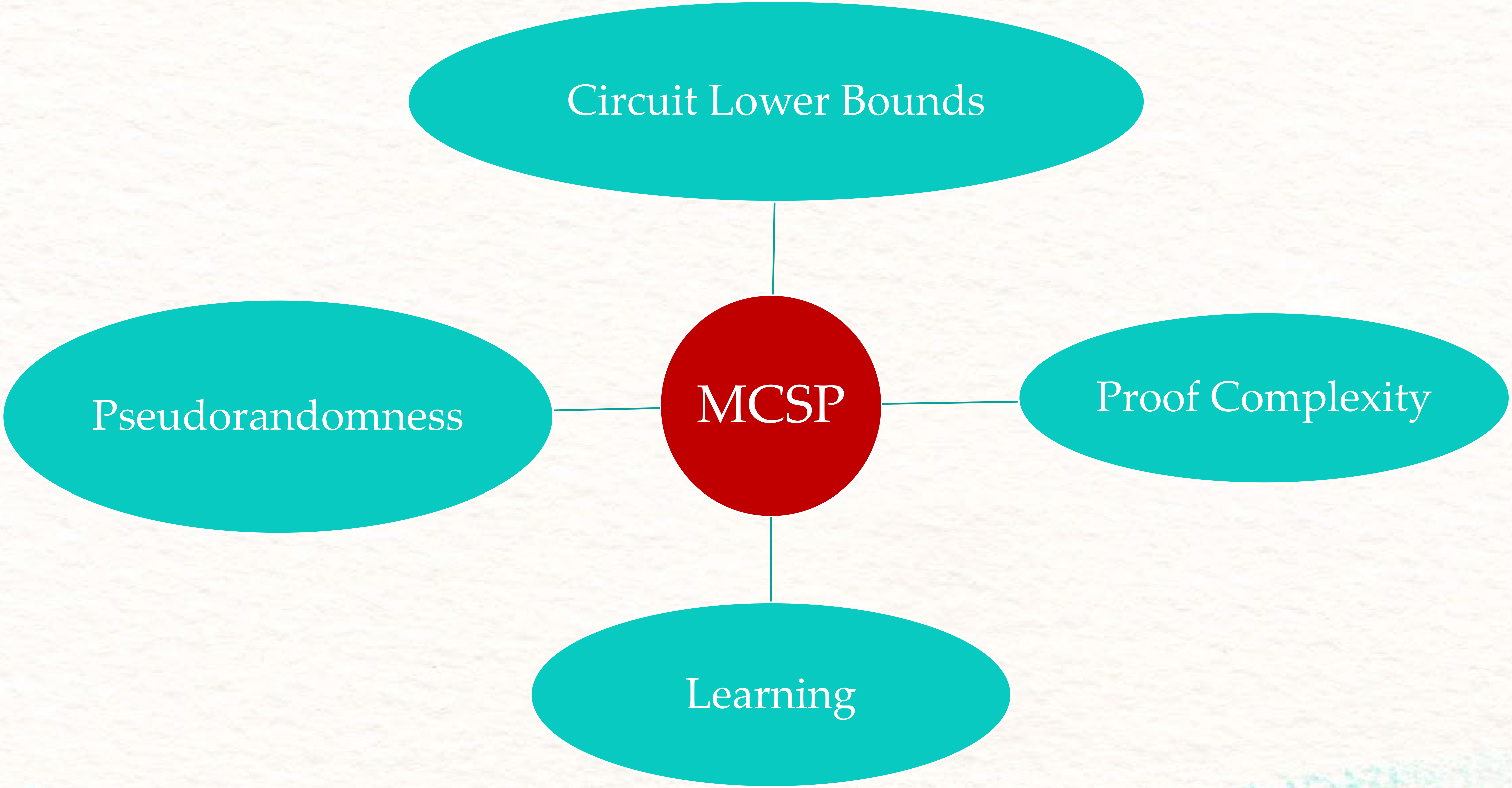
Natural Properties, MCSP, and Proving Circuit Lower Bounds

Valentine Kabanets

(based on joint works with Marco Carmosino, Russell Impagliazzo, Antonina Kolokolova & Ilya Volkovich)


Circuit Lower Bounds
Pseudorandomness
MCSP
Proof Complexity
Learning

Minimum Circuit Size Problem (MCSP):

MCSP (def)

Given: truth table T of $f: \{0,1\}^n \rightarrow \{0,1\}$, and $0 < s < 2^n$

Decide: is there a Boolean circuit C, of size s, computing f ?

MCSP ∈ NP, but not known to be NP- complete.

Circuit Lower Bounds from an MCSP Algorithm

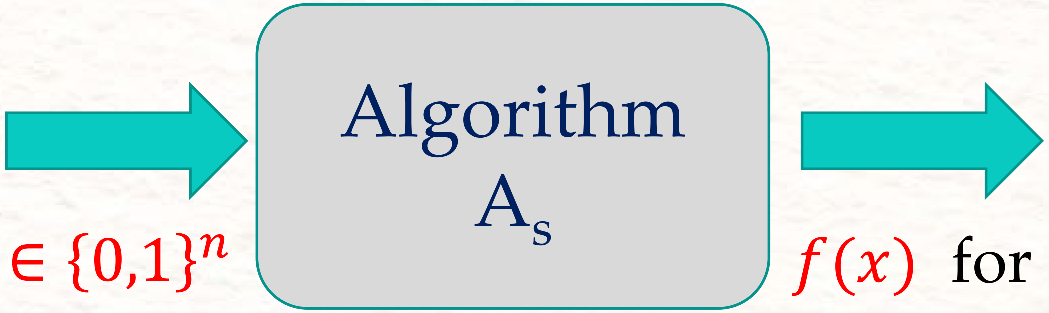
Generating Hard Functions

n → **Algorithm A_s** → Truth Table of $f : \{0,1\}^n \longrightarrow \{0,1\}$ with $SIZE(f) > s(n)$

- A_s in $BPTIME(2^n)$ for $s(n) = 2^n / n$ [Shannon 1949]
- A_s in $DTIME(poly(2^n))$ $\Leftrightarrow$ $EXP \not\subseteq SIZE(s)$
- A_s in $pseudo\text{-}DTIME(poly(2^n))$ $\Leftrightarrow$ $BPEXP \not\subseteq SIZE(s)$

(last two: weakly explicit)

Generating Hard Functions



$x \in \{0,1\}^n$ → $f(x)$ for some $f : \{0,1\}^n \longrightarrow \{0,1\}$ with $\text{SIZE}(f) > s(n)$

- A_s in DTIME (poly(n)) $\Leftrightarrow$ $P \not\subseteq \text{SIZE}(s)$
- A_s in NTIME (poly(n)) $\Leftrightarrow$ $NP \not\subseteq \text{SIZE}(s)$

} strongly explicit

Generating Hard Functions if MCSP Were Easy

Truth Table of $f : \{0,1\}^n \longrightarrow \{0,1\}$ with $\mathrm{SIZE}(f) > s(n)$

- A_s in ZPTIME (2^n) for $s(n) = 2^n / n$ if MCSP $\in$ P. (MCSP $\in$ P $\Rightarrow$ BPP = ZPP)
- BPEXP $\not\subseteq$ SIZE (poly) if MCSP $\in$ BPP [Impagliazzo, K, Volkovich 2018].

Open Question: EXP $\not\subseteq$ SIZE (poly) if MCSP $\in$ P ?

Interlude:

Explicit Constructions of Pseudorandom Objects

Pseudorandom Object	Property	Decision Complexity
Linear Error-Correcting Codes (Binary)	Min-Distance	NP-complete [Vardy 1997]
Expander Graphs	Expansion	coNP-complete [Blum, Karp, Vornberger, Papadimitriou, Yannakakis 1981]

1. There are explicit constructions of good Codes and Expanders despite the NP-hardness of testing Min-Distance and (Non-) Expansion.

2. The NP-hardness proofs for Min-Distance and (Non-) Expansion use explicit constructions of good Codes and Expanders.

Why Proving Hardness of MCSP is Hard

- SAT $<_p^m$ MCSP (via ``standard'' reductions) $\Rightarrow$ EXP $\not\subseteq$ P/poly [K. & Cai 2000]
- SAT $<_p^m$ MCSP $\Rightarrow$ EXP $\neq$ ZPP [Murray, Williams 2015; Hitchcock, Pavan 2015]

- SAT $\not<_p^{local}$ MCSP [Murray, Williams 2015] (local reduction: each output bit in time $< n^{0.49}$)
- SAT $\not<_p^{oracle-independent}$ MCSP, unless P = NP [Hirahara, Watanabe 2016]

(oracle-independent reduction from L to MCSP: L $\in P^{MCSP^A}$ for every oracle A, where $MCSP^A$ asks about the A-oracle circuit size).

MCSP Algorithms from Constructive Proofs of Circuit Lower Bounds

Natural Properties

Most known proofs of s(n) circuit lower bounds for weak circuit classes **C** yield efficient (poly(2^n)-time) algorithms for "Average-Case s(n)-MCSP" (aka Natural Property with usefulness s(n)) : [Razborov, Rudich 1997]

Given: Truth table T of $f: \{0,1\}^n \rightarrow \{0,1\}$

Output: "Easy" if **C**-SIZE(f) $\leq$ s(n),

"Hard" for at least ½ of functions f with **C**-SIZE(f) > s(n).

Natural Properties Yield MCSP Algorithms

Average-Case s(n)-MCSP (aka Natural Property with usefulness s(n)) :

Given: Truth table T of $f: \{0,1\}^n \to \{0,1\}$

Output: "Easy" if SIZE(f) ≤ s(n), "Hard" for at least ½ of functions f with SIZE(f) > s(n).

(easy, hard) - GapMCSP :

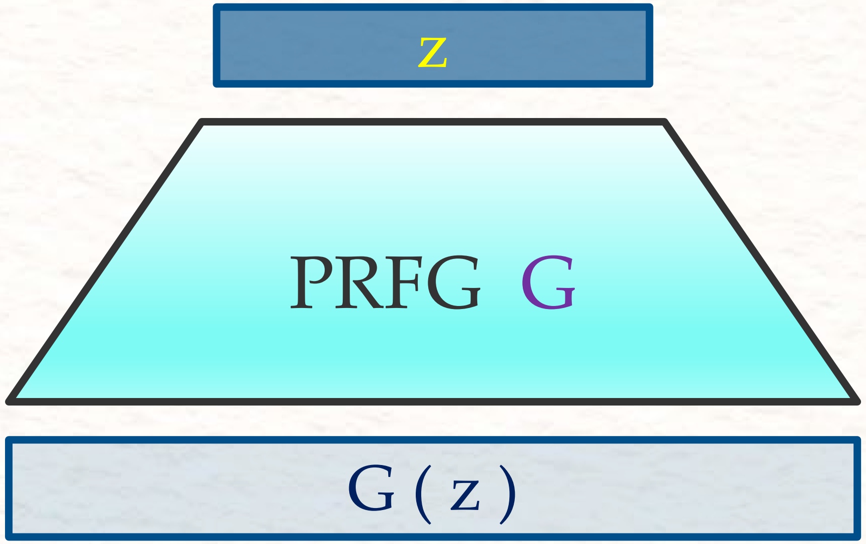
Given: Truth table T of $f: \{0,1\}^n \to \{0,1\}$

Output: "Easy" if SIZE(f) ≤ easy(n), "Hard" if SIZE(f) ≥ hard(n).

Theorem ([Carmosino, Impagliazzo, K, Kolokolova 2016] , [Hirahara 2018]):

If Average-Case $2^{0.1\,n}$ -MCSP is in BPP , then ($2^{0.01\,n}$, $2^{0.99\,n}$) –GapMCSP is in BPP.

MCSP Algorithms Yield Learning Algorithms



Def: Function Generator G is s-local if, for every seed z, MCSP(G(z), s) is True, where $s \ll |G(z)|$.

Observation: MCSP(, s) will "break" every s-local Function Generator G.

- [Razborov, Rudich 1997]: If MCSP ∈ BPP, the every candidate One-Way Function can be inverted in BPP (by locality of the GGM PRFG construction).

- [Carmosino, Impagliazzo, K, Kolokolova 2016]: If MCSP ∈ BPP, then every f ∈ SIZE(poly) can be PAC-learned (with membership queries, under uniform distribution) in BPP (by locality of the NW PRG construction).

MCSP Algorithms Yield SAT Algorithms

SAT Algorithm from MCSP, assuming IO exist

Theorem [Impagliazzo, K, Volkovich 2018]: Suppose Indistinguishability Obfuscators exist. Then MCSP $\in$ BPP $\Leftrightarrow$ SAT $\in$ BPP.

Definition (IO): A randomized polytime transformation of circuits to circuits is an IO if

- **correctness:** For every circuit C, IO(C) $\equiv$ C.
- **polynomial slowdown:** $|$IO(C)$|$ < poly($|$C$|$).
- **indistinguishability:** for all pairs of circuits C, C′, if C $\equiv$ C′, and $|$C$|$ = $|$C′$|$, then the distributions IO(C) and IO(C′) are computationally indistinguishable.

MCSP yields Hard Tautologies

Constructive Circuit Lower Bound Proofs

Most known proofs of s(n) circuit lower bounds for weak circuit classes **C** are constructive: can be formalized in V_1^1 (bounded arithmetic system with "polytime reasoning") [Razborov 1995]

Theorem: If V_1^1 proves Shannon's counting argument that

" there exists a truth table of $f: \{0,1\}^n \rightarrow \{0,1\}$ with $\mathrm{SIZE(f)} > \mathrm{s(n)}$ ",

then $\mathrm{EXP}^{\mathrm{NP}} \not\subseteq \mathrm{SIZE}\,(\mathrm{s(n)})$.

Proof: Buss's Witnessing Theorem. QED

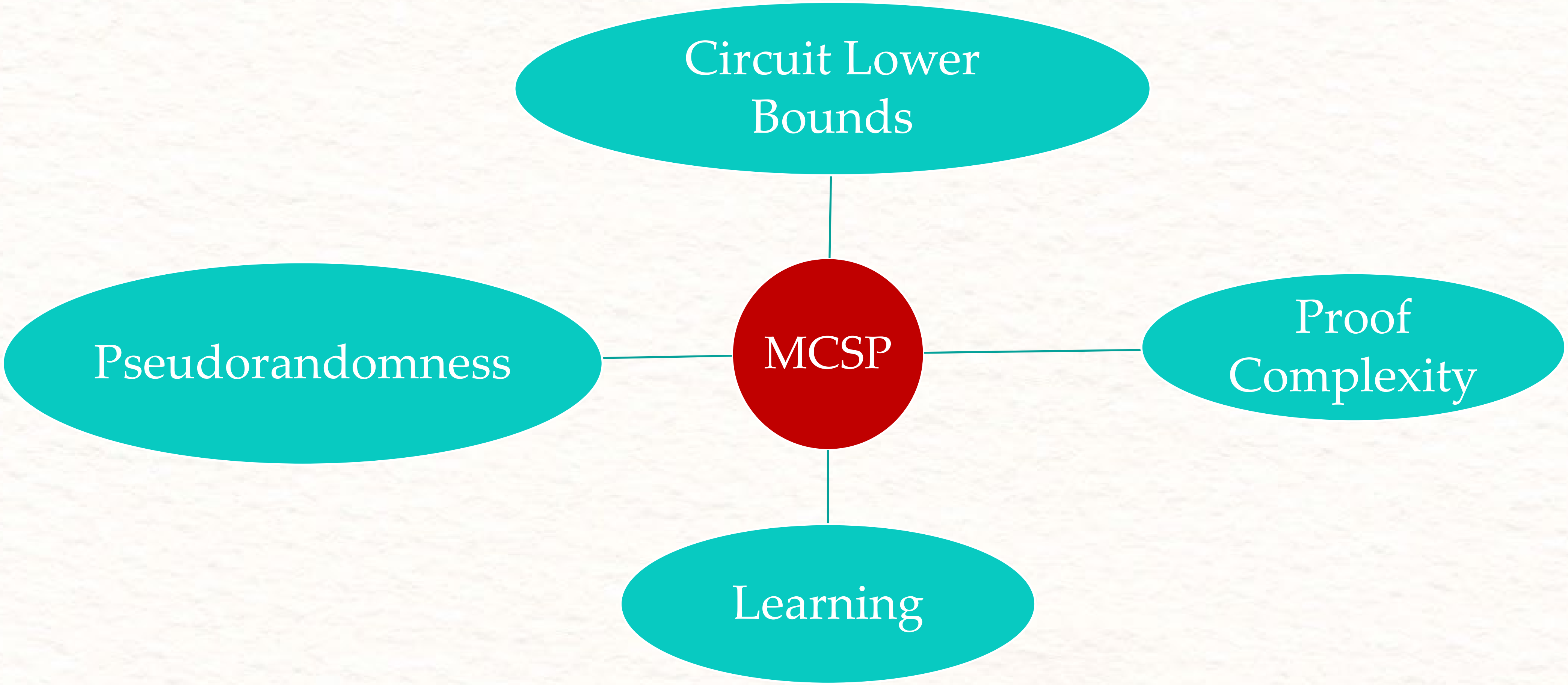
Candidate Hard Tautologies for Extended Frege

$\neg$ MCSP(f_n, s) = " function f_n requires SIZE(f_n) > s "

Question: Are there poly(2^n)-size Extended Frege proofs of $\neg$ MCSP(f_n, $2^{n^{\varepsilon}}$) ?

Lower Bounds for Res(ε log n) [Razborov 2015] (uses the "PRGs against Proof Systems" approach [Alekhnovich, Ben-Sasson, Razborov, Wigderson 2004, Krajicek 2004, …])

So far the strongest proof system where the unprovability of NP $\not\subseteq$ P/poly is known.



$\text{MCSP} \in \text{BPP} \iff \text{SAT} \in \text{BPP}$?

$\text{MCSP} \notin AC^0[2]$?

More connections ?

Thank you !

Proof of Theorem

Theorem: Suppose Indistinguishability Obfuscators exist. Then MCSP $\in$ BPP $\Leftrightarrow$ SAT $\in$ BPP.

Proof: $\Leftarrow$ is trivial. For $\Rightarrow$, consider $f_s(r) = IO(\perp_s, r)$, where $\perp_s$ is a canonical unsatisfiable circuit of size s, and r is internal randomness of IO. (similar idea in [Goldwasser, Rothblum 2007; Komargodski, Moran, Naor, Pass, Rosen, Yogev 2014])

MCSP $\in$ BPP $\Longrightarrow$ f_s can be inverted in BPP [Allender et al. 2006]

Algorithm for SAT: Given a circuit C of size s, let $C' = IO(C, r)$, for random r.

Attempt to invert f_s to find $r' = f_s^{-1}(C')$. If $IO(\perp_s, r') = C'$, output ``Unsat'' else ``Sat''.

Analysis: If C is satisfiable, then so is C' and $IO(\perp_s, r') \neq C'$ by correctness of IO.

If C is unsatisfiable, $IO(C)$ and $IO(\perp_s)$ are indistinguishable by the inverting algorithm, and so inverting succeeds with high probability.

Hence, SAT $\in$ BPP. QED