A Relativization Perspective on Meta-Complexity

Harlin Ren
& Rahul Santhanam
University of Oxford

STACS '22

Meta-Complexity

"Complexity of complexity".

Minimum Circuit Size Problem (MCSP)

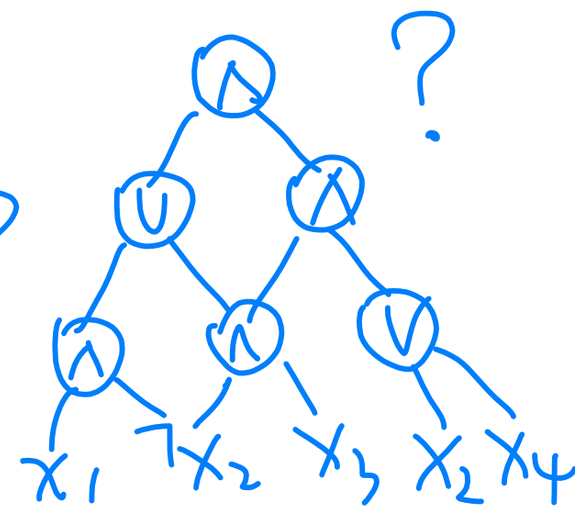
* Input: a truth table $tt \in \{0,1\}^N$ representing a Boolean function $f: \{0,1\}^n \to \{0,1\}$ — convention: $N = 2^n$

  a size parameter s — w.l.o.g $s \le N$

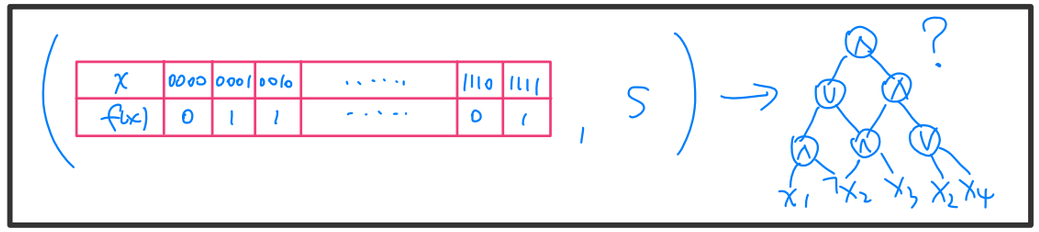
* Decide: Is f computable by a size-s circuit?

(| x | 0000 | 0001 | 0010 | ..... | 1110 | 1111 |
|---|---|---|---|---|---|---|
| f(x) | 0 | 1 | 1 | ..... | 0 | 1 |

, s) → ?



Why study MCSP?



Reason #1. Its complexity is mysterious.

MCSP $\in$ NP. (Just guess the circuit and notice that $S \leq 2^n/n < N$.)

If MCSP $\in$ P then $\nexists$ one-way functions. [RR97, KC00]

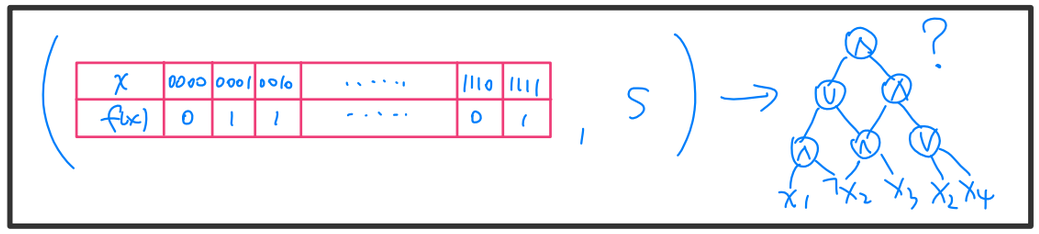
which means modern cryptography is not secure!

Q: Is MCSP NP-complete? BIG open question!

Intuition: we need to generate hard functions, if we want to reduce SAT to MCSP

* If MCSP is NP-complete under "nice" reductions then we can prove breakthrough lower bounds. [KC00, MW15, SS20, ...]
  e.g. EXP $\neq$ ZPP or EXP $\not\subseteq$ $P_{/poly}$
* This doesn't tell you if MCSP should be NP-complete at all!
  (Since we believe these lower bounds.)
  But it means that NP-completeness of MCSP would be hard to prove, if true.

Why study MCSP?

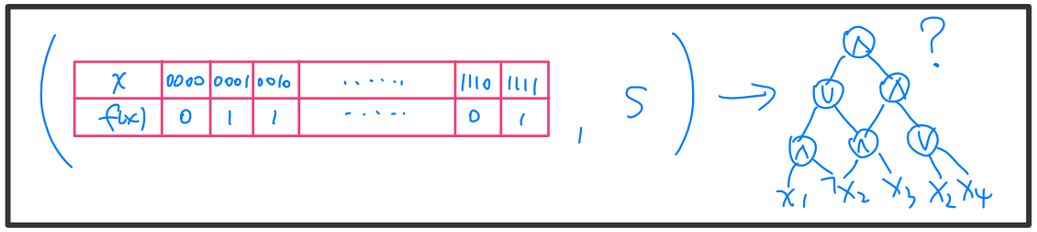


Reason #1. Its complexity is mysterious.

Q: Is there a search-to-decision reduction for MCSP?

* Given an oracle for the decision version of $MCSP := \{(tt, s) : CC(tt) \le s\}$ (Circuit Complexity),
  on input truth table $tt \in \{0,1\}^N$, find an optimal circuit for tt in $poly(N)$ time.
* Open since [KC'00]!
* If MCSP is NP-hard, the answer should be Yes!

Why study MCSP?



Reason #1. Its complexity is mysterious.

Q: Robustness of MCSP?

* w.r.t. allowed gates, circuit class, size parameter

SAT is robust: $\mathcal{C}$-SAT is NP-complete for any "interesting" $\mathcal{C}$.

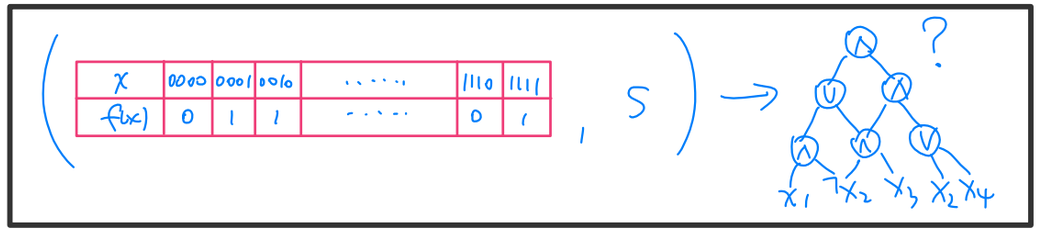
* case study: $MCSP[2^{n/2}]$ vs $MCSP[2^{n/4}]$. $MCSP[s(n)]$: size parameter is fixed.

* Padding: if $MCSP[2^{n/4}] \in P$, then $MCSP[2^{n/2}] \in P$

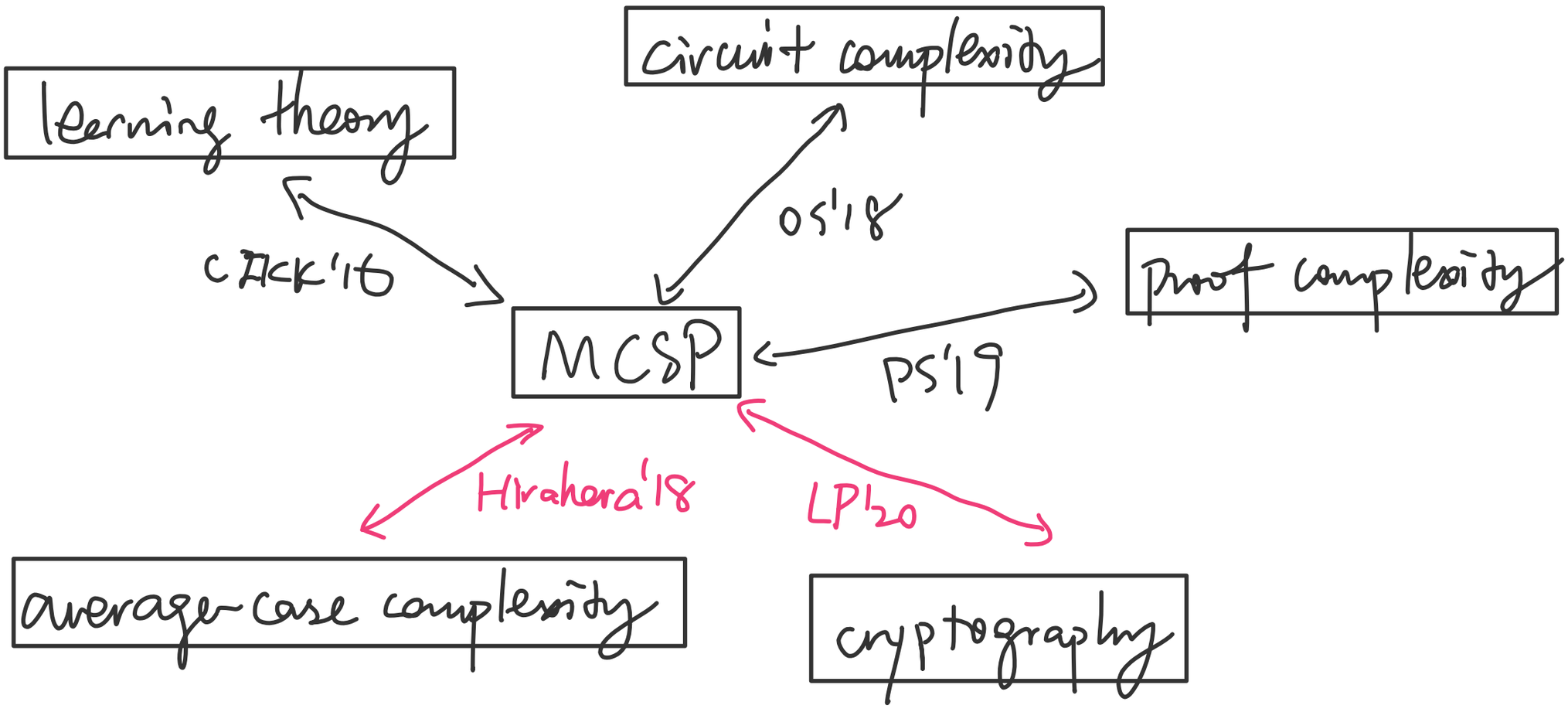
Proof: Let $f'(x_1 \cdots x_{2n}) = f(x_1 \cdots x_n)$, then $CC(f) \le 2^{n/2} \Leftrightarrow CC(f') \le 2^{2n/4}$. ■

* Open: is it possible that $MCSP[2^{n/2}]$ is very easy (in P)
but $MCSP[2^{n/4}]$ is very hard (require brute force)?

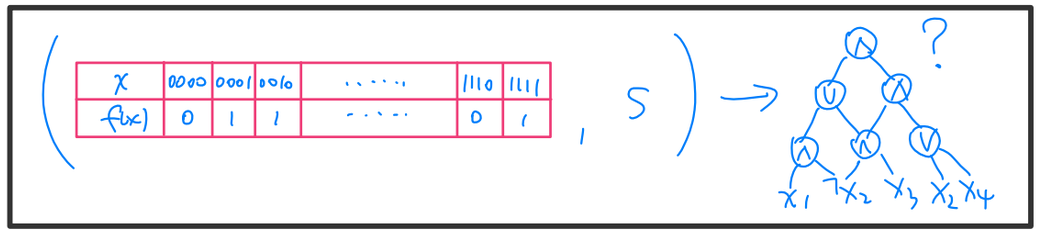
Why study MCSP?



Reason #2: connections to complexity theory.



Why study MCSP?



Reason #2. connections to complexity theory.

AVERAGE-CASE COMPLEXITY.

* If an approximation version of MCSP is NP-hard,
* then the worst-case and the (errorless) average-case complexities of NP are equivalent. [Hirahara'18]

CRYPTOGRAPHY

* The existence of one-way functions
is equivalent to
* the average-case hardness of (error-prone)

$MK^{Poly}P$. [LP'20]

certain Kolmogorov version of MCSP

... and so many recent progress!

[AD'14] [MW'15] [CIKK'16] [AH'17] [HS'17] [CZKK'17] [HOS'18]
[OS'18] [Hirahara'18] [OPS'19] [MMW'19] [PS'19] [CJW'19] [CHOPRS'20]
[Ilango'20 (ITCS)] [CJW'20] [Hirahara'20 (STOC)] [ILO'20] [Ilango'20 (CCC)] [Hirahara'20 (CCC)] [LP'20] [Ilango'22 (FOCS)]
[Hirahara'20 (FOCS)] [LP'21 (STOC)] [Hirahara'21] [RS'21] [LP'21 (CRYPTO)] [Ilango'21] this list is far from comprehensive.....

Still, the following basic problems about MCSP remain open:

Q: Is MCSP NP-complete?

Q: Is there a search-to-decision reduction for MCSP?

Q: Robustness of MCSP?

Our perspective: relativization?

Quick reminder on relativization:
give an oracle O to everyone for free.
a technique relativizes if it works for any O.

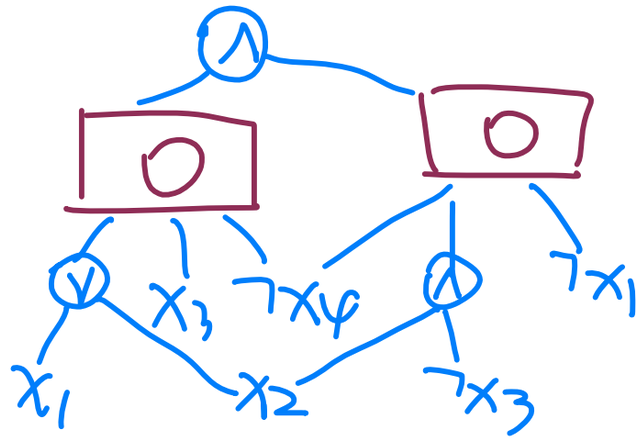
$\exists O_1, P^{O_1} = NP^{O_1}$; $\exists O_2, P^{O_2} \neq NP^{O_2}$ [BGS'75]

⇒ we need non-relativizing techniques to solve P vs NP!

Observation 1: it makes sense to talk about relativization of MCSP!

$MCSP^O$ ← O is an oracle.

* Input: a truth table $tt \in \{0,1\}^N$
  a size parameter s
* Decide: Is f computable by a size-s oracle circuit?



Observation 2: many meta-complexity results relativize!
e.g. [Hirahara'18] & [LP'20]

Our results: relativization barriers

Result 1: $\exists$ oracle O, s.t. $MCSP^O$ is easy ← in P^O

but search-$MCSP^O$ is "very hard" ← requires $2^{\Omega(N/\log N)}$ time

Finding a search-to-decision reduction for MCSP needs non-relativizing techniques!

Result 2: $\exists$ oracle O, s.t. $MCSP^O[2^{n/2}]$ is easy ← in P^O

but $MCSP^O[2^{n/4}]$ is "very hard" ← requires $2^{\Omega(N^{1/4}/\log N)}$ time

Reducing $MCSP[2^{n/4}]$ to $MCSP[2^{n/2}]$ needs non-relativizing techniques!

Our results on Kt

Levin's Kt complexity: $Kt(x) := \min\{|d| + \log_2 t : U(d) \text{ outputs } x \text{ in } t \text{ steps}\}$.

Known [ABKMR'02]: MKtP is EXP-complete under P/poly-tt reductions and MP-Turing reductions.

MKtP: Minimum Kt Problem

Open: is MKtP $\in$ P? An EXP-complete problem shouldn't be in P, but we don't know!

Our result: a relativized world where Kt^O can be (2+ε)-approx. in P^O.

Actually, $\widetilde{Kt}^O$ is exactly computable in P^O!

$\widetilde{Kt}$: a non-standard version of Kt, defined in our paper

Remark. [ABKMR'02] is already non-relativizing (using IP=PSPACE).
However, in our oracle world, EXP=ZPP (thus IP also = PSPACE).
Open: find an algebrization barrier against proving MKtP$\notin$P!

Discussions

Main open question: using non-relativizing techniques to study MCSP?

Candidate 1: Ilango's "gate elimination" techniques

Candidate 2: PCP theorem?

Personal opinion: I don't think our results indicate, e.g. "search-to-decision reduction for MCSP is impossible". They are reminders that non-relativizing techniques are needed, and hope to inspire some!

Good news There is a poly-time search-to-decision reduction for MFSP (Min Formula Size Problem). [Ilango '21]

* doesn't relativize
* highly dependent on defn of "formula".

THANK YOU!

Questions are welcome