A Relativization Perspective on Meta-Complexity

Harlin Ren
& Rahul Santharoubam
University of Oxford
STACS '22
Meta-Complexity

"Complexity of complexity"

Minimum Circuit Size Problem (MCSP)

* Input: a truth table $t \in \{0,1\}^N$ representing a Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$

*a size parameter $s$ \hspace{1cm} \text{w.l.o.g.} \ s \leq N

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

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>0000</th>
<th>0001</th>
<th>0010</th>
<th>\ldots</th>
<th>1110</th>
<th>1111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(x)$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>\ldots</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Why study MCSP?

Reason #1: Its complexity is mysterious. MCSP $\in$ NP. (Just guess the circuit and notice that $5 \leq 2^{\log N} = N$.)

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!

* If MCSP is NP-complete under "nice" reductions then we can prove breakthrough lower bounds. [KC00, MW15, SS20, ...]

  e.g. EXP #P  $\neq$ EXP $\neq$ PSPACE

* 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.

Intuition: we need to generate hard functions, if we want to reduce SAT to MCSP.
Why study MCSP?

Reason #1: Its complexity is mysterious.

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

*Given an oracle for the decision version of MCSP: \( f(\mathbf{t}, s): C(\mathbf{t}) \leq S \),

on input truth table \( \mathbf{t} \in \{0,1\}^N \), find an optimal circuit for \( \mathbf{t} \) in \( \text{poly}(N) \) time.

*Open since [KC'00]!

*If MCSP is \( \text{NP} \)-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: E-SAT is NP-complete for any "interesting" E.

   * Case study: $\text{MCSP}[2^{n/2}]$ vs $\text{MCSP}[2^{n/4}]$. $\text{MCSP}[\text{fl}(n)]$: size parameter is fixed.

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

   Proof: Let $f'(x_1, \ldots, x_m) = f(x_1, \ldots, x_n)$, then $\text{CC}(f) \leq 2^{n/2} \Rightarrow \text{CC}(f') \leq 2^{n/4}$. □

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

Reason #2: connections to complexity theory.

- Learning theory (CJCK'16)
- Circuit complexity (05'18)
- Proof complexity (PS'19)
- Average-case complexity (Hirahara'18)
- Cryptography (LP'20)
Why study MCSP?

Reason #2: connections to complexity theory.

**AVERAGE-CASE COMPLEXITY.**

* If an approximation version of MCSP is \textbf{NP}-hard, then the worst-case and the average-case complexities of \textbf{NP} are equivalent. [Hirahara'18]

**CRYPTOGRAPHY.**

* The existence of \underline{one-way functions} is equivalent to the \underline{average-case hardness of $\text{MK}^{\text{poly}} \vDash P$}. [LP'20]

* Certain Kolmogorov version of MCSP
... and so many recent progress!

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 $O$.

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

We need non-relativizing techniques to solve P vs NP!

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

$$MCSP^O \leftrightarrow O$$ is an oracle.

* Input: a truth table $f \in \{0,1\}^N$
* 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: \( \exists \text{ oracle } O, \text{ s.t. } \text{MCSP}\overset{0}{=} \text{easy} \) but \( \text{search-MCSP}^{O} \) is "very hard" \( \leftarrow \) requires \( 2^{\Omega(N/\log N)} \) time

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

Result 2: \( \exists \text{ oracle } O, \text{ s.t. } \text{MCSP}^{O}[2^{n/2}] \text{ is easy} \) but \( \text{MCSP}^{0}[2^{n/4}] \) is "very hard" \( \leftarrow \) requires \( 2^{\Omega(N^{1/3} \log N)} \) time

Reducing \( \text{MCSP}[2^{n/4}] \) to \( \text{MCSP}[2^{n/2}] \) needs non-relativizing techniques!
Our results on $K_t$

Levin's $K_t$ complexity: $K_t(x) := \min \{ d_1 + \log_2 t : U(d) \text{ outputs } x \text{ in } t \text{ steps} \}.$

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

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 $Kt^0$ can be $(2+\epsilon)$-approx. in $P^0$.

Actually, $Kt^0$ is exactly computable in $P^0$!

Remark: [ABKMR'02] is already non-relativizing (using $IP=PSpace$). However, in our oracle world, $EXP=2PP$ (thus IP also = PSPACE). Open: find an algebrization barrier against proving $MKtP \notin P$!
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 😊