# On the (Non) NP-Hardness of Computing Circuit Complexity

Cody D. Murray and Ryan Williams

presented by Radek Hušek

## Complexity ZOO

| Complexity class | Characterization |
|---|---|
| P | polytime deterministic algorithms |
| RP | polytime randomized algorithms with bounded one-size error[1] |
| BPP | polytime randomized algorithms with bounded two-size error |
| ZPP | randomized algorithms with average polytime complexity |
| AC0 | polysize circuits with unbounded fan-in and constant depth[2] |
| AC0[m] | AC0 + "mod $m$" gates |
| E | $\mathrm{TIME}(2^{O(n)})$ |
| EXP | $\mathrm{TIME}(2^{n^{O(1)}})$ deterministic algorithms |
| $\mathsf{P}_{/\mathsf{poly}}$ | polytime with polynomial advise |

The "N" prefix denotes non-deterministic variant of given complexity class: Input of non-deterministic algorithm is (except instance of given problem) a "certificate". For every YES-instance there exists certificate which makes algorithm answer yes, and for NO-instance no certificate can convince algorithm to answer yes.

Given complexity class $C$, language $L$ belongs into class i. o.-$C$ (infinitely often) iff $L \cap \{0,1\}^n = L' \cap \{0,1\}^n$ for some $L' \in C$ and infinitely many $n$, and $\mathsf{co}C := \left\{L : \overline{L} \in C\right\}$.

## Minimum Circuit Size Problem Complexity

**Definition 1.** *The* Minimum Circuit Size Problem (MCSP):
*Input is $(T, k)$ where $T \in \{0,1\}^n$ is truth-table of boolean function on $\log_2 n$ variables and $k \in \mathbb{N}$ (encoded binary or unary). Output is YES if there is circuit of complexity[3] at most $k$ which evaluates function $T$, and NO otherwise.*

We're encoding MCSP as string $Tx$, where $|T| = \max_{n\in\mathbb{N}} \{2^n < |Tx|\}$ and $x$ is binary encoding of parameter $k$.[4]

We will use machine model with random access to input such as random-access Turing machine.

[1] Only false-negatives.

[2] We allow only AND, OR and NOT gates.

[3] Complexity of is circuit is number of its gates and we're allowed to use AND, OR and NOT gates with fan-in at most 2.

[4] This encoding limits possible values of $k$ but it's not a problem because every Boolean function on $n$ variables has circuit complexity at most $(1 + o(1))2^n/n$ (Lupanov 59).

**Definition 2.** *An algorithm* $R : \Sigma^* \times \Sigma^* \to \{0,1,*\}$ *is* $\mathrm{TIME}(t(n))$ **reduction** *from* $L$ *to* $L'$ *if there is constant* $c \geq 0$ *such that* $\forall x \in \Sigma^*$*:*

- $R(x,i)$ *runs in* $O(t(|x|))$ *for all* $i \in \{0,1\}^{\lceil 2c\log_2 |x| \rceil}$,
- *There is an* $l_x \leq |x|^c + c$ *such that* $R(x,i) \in \{0,1\}$ *for all* $i \leq l_x$ *and* $R(x,i) = *$ *for all* $i > l_x$*, and*
- $x \in L \Leftrightarrow R(x,1)R(x,2)\ldots R(x,l_x) \in L'$.

**Proposition 3** (Skyum & Valiant 85; Papadimitriou & Yannakakis 86)**.** *SAT, Vertex Cover, Independent Set, Hamiltonian Path and 3-Coloring are* $\mathsf{NP}$*-complete under* $\mathrm{TIME}(poly(\log(n)))$ *reductions.*

**Theorem 4.** *For every* $\delta < \frac{1}{2}$*, there is no* $\mathrm{TIME}(n^\delta)$ *reduction from* $\textsc{Parity}$ *to* $\mathrm{MCSP}$*. Hence* $\mathrm{MCSP}$ *is not* $\mathsf{AC0}[2]$*-hard under* $\mathrm{TIME}(n^\delta)$ *reductions.*

**Theorem 5.** *If* $\mathrm{MCSP}$ *is* $\mathsf{NP}$*-hard under polytime reductions, then* $\mathsf{EXP} \neq \mathsf{NP} \cap \mathsf{P}_{/\mathsf{poly}}$*. Consequently* $\mathsf{EXP} \neq \mathsf{ZPP}$*.*

**Theorem 6.** *If* $\mathrm{MCSP}$ *is* $\mathsf{NP}$*-hard under logspace reductions, then* $\mathsf{PSPACE} \neq \mathsf{ZPP}$*.*

**Theorem 7.** *If* $\mathrm{MCSP}$ *is* $\mathsf{NP}$*-hard under logtime-uniform* $\mathsf{AC0}$ *reductions, then* $\mathsf{NP} \not\subset \mathsf{P}_{/\mathsf{poly}}$ *and* $\mathsf{E} \not\subset \mathrm{i.o.\text{-}SIZE}(2^{\delta n})$ *for some* $\delta > 0$*. As consequence* $\mathsf{P} = \mathsf{BPP}$*.*

## Proofs

**Lemma 8** (Williams 2013)**.** *There is a universal* $c \geq 1$ *such than for any binary string* $T$ *and any substring* $S$ *of* $T$*,* $CC(f_S) \leq CC(f_T) + c\log|T|$*.*

**Theorem 9** (Håstad 86)**.** *For every* $k \geq 2$*,* $\textsc{Parity}$ *cannot be computed by circuits with AND, OR and NOT gates of depth* $k$ *and size* $2^{o(n^{1/(k-1)})}$*.*

**Definition 10** (Cabanets & Cai 2000)**.** *A reduction from language* $L$ *to* $\mathrm{MCSP}$ *is* **natural** *if the size of all output instances and the size parameters* $k$ *depend only on length of the input to the reduction.*

**Claim 11.** *Let* $\varepsilon > 0$*. If there is* $\mathrm{TIME}(n^{1-\varepsilon})$ *reduction from* $\textsc{Parity}$ *to* $\mathrm{MCSP}$*, then there is* $\mathrm{TIME}(n^{1-\varepsilon}\log^2 n)$ *natural reduction from* $\textsc{Parity}$ *to* $\mathrm{MCSP}$*. Furthermore, the value of* $k$ *in this natural reduction is* $O(n^{1-\varepsilon} poly(\log(n)))$*.*

**Claim 12.** *If there is a* $\mathrm{TIME}(n^{1-\varepsilon})$ *reduction from* $\textsc{Parity}$ *to* $\mathrm{MCSP}$*, then there is a* $\Sigma_2\,\mathrm{TIME}(n^{1-\varepsilon} poly(\log(n)))$ *algorithm for* $\textsc{Parity}$*.*

**Theorem 13.** *If every sparse language in* $\mathsf{NP}$ *has polytime reduction to* $\mathrm{MCSP}$*, then* $\mathsf{EXP} \subseteq \mathsf{P}_{/\mathsf{poly}} \Rightarrow \mathsf{EXP} = \mathsf{NEXP}$*.*