Provability of the Circuit Size Hierarchy and Its Consequences

Dimitrios Tsintsilidas

The *Circuit Size Hierarchy* (CSH_b^a) states that if $a > b \geq 1$ then the set of Boolean functions on n variables computed by circuits of size n^a is strictly larger than the set of functions computed by circuits of size n^b. This result, which is a cornerstone of circuit complexity theory, follows from the *non-constructive* proof of the existence of functions of large circuit complexity obtained by Shannon in 1949 [Sha49].

Are there more "constructive" proofs of the Circuit Size Hierarchy? Can we quantify this? Motivated by these questions, we investigate the provability of CSH_b^a in theories of Bounded Arithmetic, which are fragments of Peano's Arithmetic that capture the notion of polynomial-time reasoning or incorporate induction principles corresponding to various levels of the polynomial-time hierarchy (see [Bus97, Kra95]).

Specifically, we are interested in identifying the weakest theory capable of establishing this hierarchy and related results and we present a tight connection between the computational and proof-theoretic perspectives. Among other contributions, we establish the following results:

(*i*) Given any $b > 1$, CSH_b^a is provable in Buss's theory T_2^2 for $a > b + 1$.

(*ii*) In contrast, if there are constants $a > b > 1$ such that CSH_b^a is provable in the theory T_2^1, then there is a constant $\varepsilon > 0$ such that P^{NP} requires non-uniform circuits of size $n^{1+\varepsilon}$.

(*iii*) Similarly, if there are constants $a > b > 1$ such that CSH_b^a is provable in the theory PV_1, then there is a constant $\varepsilon > 0$ such that P requires non-uniform circuits of size $n^{1+\varepsilon}$.

In other words, an improved *upper bound* on the proof complexity of CSH_b^a would lead to new *lower bounds* in complexity theory.

We complement these results with a proof of the *Formula Size Hierarchy* (FSH_b^a) in PV_1 with parameters $a > 2$ and $b = 3/2$. This is in contrast with typical formalizations of complexity lower bounds in bounded arithmetic, which require APC_1 or stronger theories and are not known to hold even in T_2^1.

This is joint work with Marco Carmosino, Valentine Kabanets, Antonina Kolokolova and Igor C. Oliveira.

[Bus97] Samuel R. Buss. Bounded arithmetic and propositional proof complexity. In *Logic of Computation*, pages 67–121. Springer Berlin Heidelberg, 1997. 1

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1995. 1

[Sha49] Claude E. Shannon. The synthesis of two-terminal switching circuits. *The Bell System Technical Journal*, 28(1):59–98, 1949. 1