Bounded Arithmetic, Threshold Circuits and Counterexample Computations

Jan Johannsen, Dept. of Mathematics, U.C. San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0112. Email: `johannsn@math.ucsd.edu`
Chris Pollett, Dept. of Mathematics and Computer Science, Clark University, Worcester, MA 01610. Email: `cpollett@aleph0.clark.edu`

The rule Δ^b_1-$COMP$ is defined as follows: If a predicate $A(x)$ has been proven to be Δ^b_1, i.e., equivalent to both a Σ^b_1- and a Π^b_1-predicate, then we conclude the comprehension axiom for A

$$\exists y < 2^{|a|}\, \forall x < |a| \; \bigl(Bit(y,x) = 1 \;\leftrightarrow\; A(x) \bigr) \;.$$

We consider the theory of Bounded Arithmetic Δ^b_1-CR axiomatized by $BASIC$, *open*-$LIND$ and the Δ^b_1-$COMP$ rule, and show that this theory is closely related to the complexity class (uniform) TC^0.

First, the Σ^b_1-definable functions of Δ^b_1-CR are TC^0. In fact, we show that the theory C^0_2 of [1], whose Σ^b_1-definable functions are TC^0, is $\forall\Sigma^b_1$-conservative over Δ^b_1-CR.

Moreover, a closer relationship between Δ^b_1-CR and TC^0 is established by the following witnessing theorem using counterexample computations:

Theorem 1 *Assume* Δ^b_1-$CR \vdash \exists x\, \forall y\, A(a,x,y)$ *, where* A *is* Δ^b_1 *w.r.t.* Δ^b_1-CR*. Then there are* $k \in \mathbb{N}$ *and functions* $f_1, \ldots, f_k \in TC^0$*, that are* Σ^b_1*-definable in* Δ^b_1-CR*, s.t.* Δ^b_1-CR *proves*

$$A(a, f_1(a), b_1) \vee A(a, f_2(a,b_1), b_2) \vee \ldots \vee A(a, f_k(a, b_1, \ldots, b_{k-1}), b_k) \;.$$

As in [2], this is used to show that a collapse of arithmetic theories implies a collapse of complexity classes.

Theorem 2 *If* $S^1_2 = \Delta^b_1$-CR*, then* NP *is contained in non-uniform* TC^0*.*

References

[1] J. Johannsen and C. Pollett. On proofs about threshold circuits and counting hierarchies (extended abstract). In *Proc. 13th IEEE Symposium on Logic in Computer Science*, pages 444–452, 1998.

[2] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52:143–153, 1991.