A note on conservativity relations among bounded arithmetic theories

Russell Impagliazzo*
Computer Science and Engineering
University of California, San Diego

Jan Krajíček†
Mathematical Institute‡
Academy of Sciences, Prague

Abstract

$T_1^{i+1}(\alpha)$ is not $\forall\Sigma_2^b(\alpha)$-conservative over $T_1^i(\alpha)$, all $i \geq 1$.[1]

It is known that the depth $d+1$ Frege system F_{d+1} has almost exponential ($\exp(\log(n)^{O(1)})$ vs. $\exp(n^{\Omega(1)})$) speed-up over the depth d system F_d, cf.[4]. The speed-up is realized on refutations of sets of depth d formulas (this can be improved to a single depth d formula using results in bounded arithmetic proved since then, cf. [1]). However, one would expect that the speed-up can occur already for refutations of sets of clauses and it is an interesting open problem to prove this or, at least, to find separating formulas of depth independent of d.

The exponential lower bound for F_d from [4] is simpler and based on different idea than later exponential lower bounds for PHP_n ([6, 8]). We think that a solution of the problem may yield a new insight into proof complexity of constant depth Frege systems and contribute to some other open problems about the systems that seem, so far, resistant to modifications of methods of [6, 8].

While discussing that problem we have observed that known facts can be combined to contribute towards a closely related problem of conservativity among bounded arithmetic theories. Specifically, it is known ([1]) that theory $T_2^{i+1}(\alpha)$ is not $\forall\Sigma_{i+1}^b(\alpha)$-conservative over $T_2^i(\alpha)$ (for $i=1$ one can get a better separation, cf. [2]) and again it is expected that the theories are not

*Research Supported by NSF Award CCR-9734911, Sloan Research Fellowship BR-3311, grant #93025 of the joint US-Czechoslovak Science and Technology Program, and USA-Israel BSF Grant 97-00188

†Partially supported by grant # A 101 99 01 of the Academy of Sciences of the Czech Republic and by project LN00A056 of The Ministry of Education of the Czech Republic.

‡Also member of the *Institute for Theoretical Computer Science* of the Charles University.

[1]MSC 2000: 03F30, 03F20. Keywords: bounded arithmetic, constant depth Frege systems.

$\forall\Sigma_1^b(\alpha)$-conservative or even $\forall\Pi_1^b(\alpha)$-conservative. We prove almost this good separation for theories without the smash function.

Theorem 0.1 *$T_1^{i+1}(\alpha)$ is not $\forall\Sigma_2^b(\alpha)$-conservative over $T_1^i(\alpha)$, all $i \geq 1$.*

We recall first four relevant facts and then give the proof of the theorem. More background information can be found in [5].

By $\mathrm{PHP}(\alpha, m)$ we denote the bounded $\Sigma_2^b(\alpha)$ formula expressing the ordinary pigeonhole principle: α cannot be a graph of a function mapping injectively m into $m-1$. PHP_m is the propositional translation of $\mathrm{PHP}(\alpha, m)$.

Fact 0.2 ([6, 8]) *PHP_m cannot be proved in the depth d Frege system F_d by a proof of size less than $\exp(m^{5^{-d}})$.*

Fact 0.3 ([7]) *Let $i, k \geq 1$ be fixed. If $T_1^i(\alpha)$ proves the formula*

$$\forall x, PHP(\alpha, |x|^k)$$

then all $PHP_{\log(n)^k}$ have F_i-proofs of size at most n^{c_k}, where constant c_k depends only on k.

This is the well known translation of bounded arithmetic proofs into propositional proofs. That $T_1^i(\alpha)$ proofs yield F_i proofs can be found in [5] (in fact, a bit better bound on the depth holds, cf. [4]).

Fact 0.4 ([7]) *Let $k \geq 1$ be fixed. Then theory $T_1(\alpha)$ proves the formula $\forall x, PHP(\alpha, |x|^k)$*

This is proved in [7, Thm.7] for all Δ_0-relations α and we need to verify the uniformity of the proof in oracle α. The proof is based on Δ_0-counting of Δ_0-sets of polylogarithmic size. In particular, if $A \in \Delta_0$ and $A_n := \{m < n \mid \langle n, m\rangle \in A\}$ has size at most $\log(n)^{O(1)}$, and $A_n \subseteq \{0,1\}^{\log(n)^\epsilon}$ for some $\epsilon < 1$, then the counting function $F : n \to |A_n|$ is Δ_0-definable. The construction uses only Nepomnjascij's theorem $\mathrm{TimeSpace}(n^{O(1)}, n^\delta) \subseteq \Delta_0$, $\delta < 1$, which is oracle uniform. The assumption $A_n \subseteq \{0,1\}^{\log(n)^\epsilon}$ is in [7] removed via hashing but we do not need to do that as even $\alpha \subseteq \log(n)^{2k}$.

Fact 0.5 ([3]) *If $T_1(\alpha)$ is not $\forall\Sigma_2^b(\alpha)$-conservative over $T_1^i(\alpha)$ then $T_1^{i+1}(\alpha)$ is not $\forall\Sigma_2^b(\alpha)$-conservative over $T_1^i(\alpha)$ as well, all $i \geq 1$.*

This is the "no gap theorem" of [3, Thm.5.3]. The theorem is stated in [3] for theories with the smash function (as those are the theories studied there) and for theory $S_2^{i+1}(\alpha)$ in place of $T_2^i(\alpha)$ (as that gives a stronger statement). The smash function is used at one place only in the whole construction [3, 5.1-5.3]: To have $S_2^{i+1}(\alpha)$ in the theorem one uses that it is $\forall\Sigma_{i+1}^b(\alpha)$- conservative over

$T_2^i(\alpha)$. That is not known for the theories without the smash function and so we use only $T_1^i(\alpha)$.

We can prove the theorem now. First observe

Claim: *For any $i \geq 1$ there is $k \geq 1$ such that $T_1^i(\alpha)$ does not prove the formula $\forall x, PHP(\alpha, |x|^k)$*

Assume otherwise. Then, by Fact 0.3, $\mathrm{PHP}_{\log(n)^k}$ has F_i-proofs of size at most n^{c_k}. By Fact 0.2 it must hold for all n:

$$n^{c_k} \geq \exp(\log(n)^{k \cdot 5^{-i}})$$

which is impossible if we pick $k > 5^i$.

By Fact 0.4 and by the claim $T_1(\alpha)$ is not $\forall\Sigma_2^b(\alpha)$-conservative over $T_1^i(\alpha)$, and the theorem follows by Fact 0.5.

References

[1] S. Buss and J. Krajíček, An application of boolean complexity to separation problems in bounded arithmetic, *Proceedins of the London Mathematical Society*, **69(3)**, (1994), pp. 1-21.

[2] M. Chiari and J. Krajíček, Witnessing functions in bounded arithmetic and search problems, *J. of Symbolic Logic*, **63(3)**, (1998), pp. 1095-1115.

[3] M. Chiari and J. Krajíček, Lifting independence results in bounded arithmetic, *Archive for Mathematical Logic*, **38(2)**, (1999), pp.123-138.

[4] J. Krajíček, Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic*, **59(1)** (1994) 73-86.

[5] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[6] J. Krajíček, P. Pudlák, and A. Woods, Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, *Random Structures and Algorithms*, **7(1)**, (1995), pp.15-39.

[7] J. Paris and A. J. Wilkie, Counting problems in bounded arithmetic, in: *Methods in Mathematical Logic*, Ed. C.A.DiPrisco, LNM 1130, (1985), pp.317-340. Springer.

[8] T. Pitassi, P. Beame, and R. Impagliazzo, Exponential lower bounds for the pigeonhole principle, *Computational complexity*, **3**, (1993), pp.97-308.