Corrigendum for
Uniform Constant-Depth Threshold Circuits for Division and Iterated Multiplication

William Hesse[1]

School of Computer Science
University of Massachusetts
Amherst, MA 01003-4610

E-mail: whessedk@gmail.com

and

Eric Allender[2]

Dept. of Computer Science
Rutgers University
Piscataway, NJ 08854-8019

E-mail: allender@cs.rutgers.edu

and

David A. Mix Barrington

School of Computer Science
University of Massachusetts
Amherst, MA 01003-4610

E-mail: barring@cs.umass.edu

In this corrigendum, we retract part of our Corollary 6.6, which was presented as an immediate and obvious consequence of our main theorem, which showed that division lies in Dlogtime-uniform TC^0.

Key Words: Division, threshold circuits, uniformity, proof theory

[1]Current affiliation: Google, Inc.
[2]Supported in part by NSF grants CCF-0832787 and CCF-1064785.

1. INTRODUCTION

The main theorem of our earlier paper [4] is the presentation of an algorithm for integer division that can be implemented in Dlogtime-uniform TC^0. We recently became aware that Corollary 6.6 in [4], which we presented as an immediate corollary of our main theorem, must be scaled back considerably.

Corollary 6.6 concerns a logic system that was introduced by Johannsen and Pollett [8] (see also [6]), in the framework of bounded arithmetic. Specifically, Johannsen and Pollett showed [8] that the bounded arithmetic theory C_2^0 has the property that the Σ_1^b-definable functions of C_2^0 are precisely the functions computed by Dlogtime-uniform TC^0 circuits. In a later paper [7], Johannsen augmented C_2^0 with a function symbol $\div$ for integer division (along with some axioms stating that $x \div 0 = 0$ and $(x > 0) \Rightarrow (y \div x) \cdot x \leq y < ((y \div x) + 1) \cdot x$). He called this new system C_2^0[*div*].

Part of Johannsen's motivation for introducing this system was to gain a better understanding of a class known as K introduced by Constable in 1973 [2]. Johannsen showed [7] that the Σ_1^b-definable functions of C_2^0[*div*] are precisely Constable's class K.

We are now ready to state Corollary 6.6 of [4] (which is not known to hold):

Corollary 6.6: [Parts 1 and 3 are now retracted.]

1. C_2^0[*div*] = C_2^0.
2. DLOGTIME-uniform TC^0 is equal to Constable's class K [2].
3. The Δ_1^b theorems of C_2^0 do not have Craig-interpolants of polynomial circuit size, unless the Diffie-Hellman key exchange protocol is insecure.

Part 2 of Corollary 6.6 is easily seen to hold, by following the strategy used by Johannsen to prove Corollary 5 of [7]. In that proof, Johannsen builds on earlier work of Clote and Takeuti [1] to (essentially) show that the Σ_1^b-definable functions of C_2^0[*div*] are precisely the functions computable by Dlogtime-uniform TC^0 circuits augmented with gates for integer division. Since integer division itself is in Dlogtime-uniform TC^0 [4], the result is now immediate from [7, 8]. Thus the Σ_1^b-definable functions of C_2^0[*div*] and the Σ_1^b-definable functions of C_2^0 both coincide exactly with K.

However, even though the integer division function is Σ_1^b-definable in C_2^0, it does not follow that C_2^0 can prove that this function satisfies the defining axiom of division: $(x > 0) \Rightarrow (y \div x) \cdot x \leq y < ((y \div x) + 1) \cdot x$). Whether this can be proved is explicitly stated as Open Problem IX.7.6 on page 360 of [3], and is also discussed briefly in [5]. In order to resolve this question, one would need to show that the algorithm of [4] (or some other division algorithm) can be formulated and proved correct within C_2^0. Thus part 1 of Corollary 6.6 remains very much unsolved.

Part three of Corollary 6.6 similarly is not easily seen to follow from [7] and from the main theorem of [4]. Thus this seems also to be open. A discussion of related issues can be found in [9, Chapter 4].

ACKNOWLEDGMENT

We thank Emil Jeřábek and Jan Johannsen for helpful comments.

REFERENCES

1. P. Clote and G. Takeuti. First order bounded arithmetic and small Boolean circuit complexity classes. In *Feasible Mathematics II*, pp. 154–218. Birkhäuser, 1995.

2. R. Constable. Type 2 computational complexity. In *Proc. 5th ACM Symposium on Theory of Computing (STOC)*, 1973, pp. 108–121.
3. S. A. Cook and P. Nguyen, Logical Foundations of Proof Complexity. Cambridge University Press, New York, 2010.
4. W. Hesse, E. Allender, and D. A. M. Barrington. Uniform constant-depth threshold circuits for division and iterated multiplication. Journal of Computer and System Sciences **65**:695–716, 2002.
5. E. Jeřábek. Root finding with threshold circuits. *Theoretical Computer Science*, **462**:59–69, 2012.
6. J. Johannsen. A bounded arithmetic theory for constant depth threshold circuits. In *Proc. GÖDEL '96*, P. Hájek, editor. Lecture Notes in Logic 6, Springer-Verlag, 1996, pp. 224–234.
7. J. Johannsen. Weak bounded arithmetic, the Diffie-Hellman problem, and Constable's Class K. In *Proc. 14th IEEE Symposium on Logic in Computer Science (LICS)*, pp. 268–274, 1999.
8. J. Johannsen and C. Pollett. On proofs about threshold circuits and counting hierarchies. In *Proc. 13th IEEE Symposium on Logic in Computer Science (LICS)*, pp. 444–452, 1998.
9. S. Müller. On the Power of Weak Extensions of V^0. Doctoral Thesis, Charles University, 2012. Available on ECCC.