UNIVERSITY OF CALIFORNIA, SAN DIEGO UCSD

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

SAM BUSS, PROFESSOR
DEPARTMENT OF MATHEMATICS, 0112
9500 GILMAN DRIVE
LA JOLLA, CALIFORNIA 92093-0112

Phone: (858) 534-3590
Email: sbuss@ucsd.edu
Url: http://math.ucsd.edu/∼sbuss

September 28, 2023

Evaluation of *(Im)possibility Results in Proof Complexity and Arithmetic* submitted by Erfan Khaniki

The thesis consists of four papers. The first three papers address different questions in logic related to open problems in computational complexity, specifically questions about the complexity of proofs in propositional logic. These questions are closely related to the fundamental open question of whether P = NP, or more precisely whether NP = coNP, and to open questions about the difficulty of proof search. The first paper contains new lower bounds for propositional proof systems. The second paper gives a new method for obtaining lower bounds for constant depth Frege proofs. The third paper investigates methods for producing tautologies which require large propositional proofs.

The fourth paper is about the intuitionistic first-order theory of arithmetic, Heyting arithmetic. It resolves an open question about Kripke pmodels of Heyting arithmetic that was first posed in 1986.

In more detail, Paper A gives new lower bounds and size-width tradeoffs for the propositional proof systems $Res(\mathsf{PC}_{d,R})$ and $Res(\mathsf{PC}_{d,\mathbb{F}})$ which are resolution proof systems in which clauses contain polynomials of degree at most d. The size-width bounds are similar to the Ben-Sasson–Wigderson tradeoffs for resolution. This paper also gives size lower bounds for $Res(\mathsf{PC}_{d,R})$-proofs of a number of principles including mod q Tseitin tautologies, random k-CNFs, and pigeonhole principles. These latter results are based on previously known degree lower bounds for $\mathsf{PC}_{\mathbb{F}}$-proofs. The contribution of this paper is that the systems $Res(\mathsf{PC}_{d,R})$ and $Res(\mathsf{PC}_{d,\mathbb{F}})$ are stronger than systems such as resolution and $Res(\mathsf{PC}_{d,R})$.

Paper B shows that Nisan-Wigderson generators can be used as hard proof complexity generators for constant-depth Frege proofs. This can based on any sufficiently hard symmetric Boolean-valued function in NP ∩ coNP.

Paper C introduces several new constructions of implicit proofs and candidate jump operators. The one is the central constructions is an implicit proof system $[\mathsf{IP}, P]$ which is a MA (Merlin-Arthur) proof system. The system IP is a MA system based on the randomized sum-check protocol of Lund-Fortnow-Karloff-Nisan. Another candidate jump operator comes from the possibility of polynomial time computable stretching maps which are P-provably hard for P. Finally, it is shown that there is a partial computable construction for a jump operator if and only if, for suitably strong theories, a jump operator can be explicitly constructed by adding statements that posit the consistency of adding consistency statements.

Paper D proves a number of results about Kripke models for Heyting arithmetic. The most notable new result is the construction of a Kripke model for Heyting arithmetic which is not locally PA; i.e., not all "worlds" in the Kripke model are models of Peano arithmetic. This resolves a question

posed by van Dalen, Mulder, Krabbe and Visser in 1986. In fact, is shown that there are Kripke models for HA that are not locally $I\Delta_1$.

The thesis is overall very well written, with very few typos and I did not discover any substantial errors. However, joining the four papers together did introduce some small problems with cross references, namely on page 39, there are cross references to Lemma 9.1 and Theorem 19.2 that refer to a different paper.

In summary, this work contains several new scientific results on important topics in the logic, proof complexity and theoretical computer science. The author has clearly demonstrated the ability for creative scientific work, and the work is very high quality for a Ph.D. thesis. I am happy to recommend it be accepted as a doctoral thesis.

Sincerely,

Samuel R. Buss
Distinguished Professor of Mathematics and Computer Science & Engineering
University of California, San Diego