UNIVERSITY OF CALIFORNIA, SAN DIEGO UCSD

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

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

TELEPHONE: (858) 534-1177
FAX: (858) 534-5273

October 11, 2014

PhD Committee for J. Pich
Charles University
Prague
Czech Republic

To Whom It May Concern:

I am writing with my evaluation of the thesis "Complexity Theory in Feasible Mathematics" submitted by Jan Pich for his Ph.D. Doctoral Thesis. The thesis consists of two main parts in addition to an introductory chapter. The first main part is on the provability of circuit lower bounds in bounded arithmetic. I was already familiar with the first part, since I served as the editor for this paper when it was submitted to the Annals of Pure and Applied Logic; I am pleased to report that the paper was accepted for publication. The second part of the thesis concerns the formalization of the PCP theorem in bounded arithmetic, and I have reviewed this portion rather carefully in order to write this evaluation.

The introductory section gives an overview of the results of the thesis and makes several nice observations. To mention just one noteworthy item, on page 7, Pich defines a notion of "proof complexity generator": these give tautologies potentially hard for extended Frege systems, and it is argued that they are simpler and more natural than earlier proposals of Krajíček and Razborov.

The chapter on *Circuit Lower Bounds in Bounded Arithmetic* proves limitations on the provability of lower bounds on circuit complexity in fragments of bounded arithmetic that are weaker than PV_1 or S_1^2. Pich introduces a several new formulations of circuit lower bounds as $\forall\Sigma_2^b$-formulas, and discusses what it means to (provably) witness these circuit lower bound principles. These new formulations must be carefully phrased since these weak theories are not known to be able to define polynomial time computable functions. Under reasonable assumptions about the approximation of polynomial size circuits by subexponential size formulas, Pich then proves that these formulations of circuit lower bounds are not provable in the bounded arithmetic theories T_{NC1} and VNC^1 (see Corollaries 1.6.1 and 1.6.2). The proofs are technically quite difficult, and use the Yao-Hastad lower bounds for bounded depth circuits, NC^1 versions of Krajíček-Pudlák-Takeuti style Student-Teacher games, and Nisan-Wigderson random generators. This work represents a definite advance in the state of the art in establishing unprovability results, since the similar prior work (such as that due to Razborov) applied only to significantly weaker theories (e.g., V^0).

The chapter on *Logical Strength of Complexity Theory and a Formulazation of the PCP Theorem in Bounded Arithmetic* is even more ambitious. It begins with a review of the prior work on formalizing theorems about randomized feasible and near-feasible computation classes in bounded arithmetic. As a

warm-up, it proves that the Cook-Levin theorem is provable in PV_1 and (equivalently) in S_2^1. It then establishes the provability of the exponential version of the PCP theorem in the bounded arithmetic theory APC_1. The PCP theorem is a celebrated theorem about Probabilistically Checkable Proofs, and is widely regarded as one of the main achievements in the theory of the hardness of randomized, approximate computation. The theory APC_1 is a bounded arithmetic theory due to Jeřábek which can carry out approximate counting arguments. The thesis then turns to the much harder, full version of the PCP theorem about polynomial size proofs which are sampled only constantly many times. (The exponential version is a simpler result.) The full PCP theorem is shown to be formalizable and provable in PV_1. This is the main result of this chapter. Because of the central importance of the PCP theorem, and the naturalness of the bounded arithmetic theory PV_1, this result will probably be the most influential result of the thesis.

The proof methods, as formalized in PV_1 and in APC_1 to prove the PCP theorem, are by-and-large the usual methods used to prove the PCP theorem; however, some major modifications are needed. The most crucial modifications are as follows. First, the usual proof of the exponential PCP theorem cannot be formalized as is; fortunately, a proof method of Moshkovitz can be used instead. Second, the expansion properties of graphs cannot be proved by PV_1 via graph eigenvalues (as far as we know), and thus different methods must be used to obtain the needed expansion properties. The more minor, but still difficult, differences from the usual proof are that approximations involving computing norms of vectors, and using the Cauchy-Schwartz inequality, require introducing additional error terms, and considerable care is needed to handle these. In addition to these substantial modifications, there is considerable work required to show that the arguments are all formalizable in PV_1 and APC_1.

The thesis is overall well-written and accessible. There are various places where the English and technical exposition could be improved, but these do not detract from the readability. I omit listing these here for space reasons. There were a few places where the technical details of the proofs were unclear, and these might be addressed if possible before the thesis is finalized. I list these next; I think they are all easily fixed in any event.

Most importantly, the proof of Proposition 2.6.9 has some (fixable) technical problems. Here it should be stated that *b* greater than or equal to *e* as this is needed for the "Claim" on page 62 to hold. In addition, I am not sure if the conditions on *d* are sufficient for the needed expander graph to exist. It would be good to include a citation of an appropriate theorem from the literature about expander graphs. In addition, on page 63, I cannot see why the condition on line 10 is enough to prove the needed condition of line 8. The rest of that paragraph should be clarified as well.

In Definition 2.7.2, the value *W'* is first called an arbitrary constant, and then later a function of *q*.

In the last lines of page 66, if I understand correctly, the value *w* should be bounded by 2^{n_1}, not 2^{2^{n_1}}. On the next page, line six, I think 2^W is too large, and W or $\log W$ would be more appropriate.

There seems to be a mismatch in the factors on line -5 of page 71 and lines 20-22 of page 72.

In conclusion, this is a very strong and impressive thesis that makes important advances on two different topics. I recommend its acceptance for the Ph.D.

Sincerely,

Samuel R. Buss
Professor of Mathematics and Computer Science
Department of Mathematics
University of California, San Diego