Report on the doctoral thesis "Model constructions for bounded arithmetic" by Michal Garlik

A model of bounded arithmetic is, typically, a structure with an order, addition and multiplication, which satisfies the axioms of an ordered semiring and also some restricted amount of induction. We think of elements of the model as generalized natural numbers.

Such structures are useful for studying foundational questions about what mathematics looks like if we are only allowed to use very weak axioms. They also have close connections with complexity theory. To fix on one in particular, NP=coNP if and only if there is a propositional proof system P in which every propositional tautology has a short proof. For fixed P and and a fixed family (τ_n) of tautologies, this can be seen as a question about models of bounded arithmetic. Roughly, if we can build a model with enough induction to prove that P is sound, but in which τ_n is false for some nonstandard n, then the family (τ_n) does not have short proofs in P, and vice versa.

It is, surprisingly, open whether the usual propositional proof systems taught in introductory logic courses have short proofs of every tautology. Jan Krajicek has a research programme to show that they do not, under some reasonable assumption from cryptography, by constructing suitable models. It turns out that here, and in many other situations, it is important to be able to grow a model by adding new "large" numbers that satisfy some property, while keeping the set of "small" numbers unchanged, so that certain desirable properties of the original model are preserved. This thesis deals with the question of when this sort of move is possible.

The thesis has the form of two papers, one already published in the Archive for Mathematical Logic last year, and the other submitted. These are followed by a few pages of extra results and discussion. The thesis is not padded out by any introduction to the subject, and inside the two papers this kind of material is kept to a minimum.

The first, published, paper gives a simplified proof of a 2007 result of Miklos Ajtai, about a version of Gödel's completeness theorem suitable for extending models while keeping an initial part fixed. Ajtai's result generalizes a construction that first appeared in his seminal work on complexity in the 1980s. Ajtai's paper gives some proofs only as sketches, with further details in an unpublished manuscript, while Garlik's is self-contained. Garlik mentions one issue he fixes, making an unstated assumption explicit in the statement of the theorem. His presentation of this result has been used in at least one course on models of arithmetic (at the university of Vienna).

The second paper gives two, quite different, ways of extending models while leaving an initial part fixed.

Construction A starts with a model of a weak theory, and the assumption that it is hard to witness a formula there in polynomial time. It extends this to a model in which the formula is false, which has no new small numbers, and in which a reasonable amount of induction holds.

Construction B starts with a model of a strong theory, in which it is with high probability hard to witness a formula by a kind of shallow circuit. It extends this to a model in which the formula is false, which has no new small numbers, and in which some induction holds, but exponentially less induction than in construction A.

Both constructions are interesting and, as far as I can tell, new. They combine techniques from witnessing theorems with an ultrapower construction in a neat way. Garlik gives no real new application for construction A. He uses construction B to answer an open problem, showing that two particular bounded arithmetic theories are distinct, under the assumption that cryptographic hard one-way functions exist. This result is strengthened slightly in the last section of the thesis. (It is a bit unfortunate that it does not seem to use the "no new small numbers" condition that is the stated purpose of the construction.)

I believe that this work will be useful to other researches, and the concluding remarks briefly outline some possible directions it could be taken, mentioning important problems for which these constructions seem relevant.

The thesis demonstrates mathematical skill and maturity, in how it handles abstract ideas and carries out some rather complicated constructions in detail. It is clearly written and I found no mistakes; although I will comment that at certain points even an expert reader would appreciate more high-level descriptions in plain language of what is going on, rather than relying on dry formulas. The thesis proves the author's ability for creative scientific work.

Neil Thapen 20 August 2015