ARNOLD BECKMANN. *Proving consistency of equational theories in bounded arithmetic.* ***Journal of symbolic logic,*** vol. 67 (2002). pp. 279–296.

One of the oldest outstanding problems in bounded arithmetic is whether the hierarchy of theories S_2^i collapses. It is known if this hierarchy collapses then in fact the polynomial time hierarchy collapses. Since the the theories S_2^i are defined in a way reminiscent to the theories $I\Sigma_k$ and the latter are known to be separable by Gödel-style arguments, it seems reasonable to try Gödel-style arguments to separate the theories S_2^i. So far this approach has not been successful and there have been results indicating the approach is unlikely to work. In particular, P. Pudlak (*A note on bounded arithmetic.* ***Fundamenta Mathematicæ***, vol. 136 (1990) pp. 85–89) has shown that $S_2 = \cup_i S_2^i$ does not prove the bounded consistency of S_2^1. By bounded consistency of a theory T, we mean the statement that T does not prove $0 = 1$ with a proof involving only formulas with bounded quantifiers. Due to this kind of results G.Takeuti (*Open Problems.* ***Arithmetic, Proof theory, and computional complexity***, edited by P.Clote and J. Krajíček. pp. 1–9) conjectured that S_2 cannot prove the consistency of the equational fragment $S_2^{-\infty}$ of S_2 which allows only equations of the form $s = t$ for closed terms and natural rules based on recursive definitions of the base symbols. The paper under review proves this latter conjecture is false and shows in fact that S_2^1 can prove the consistency of a reasonably broad class of equational theories.

More precisely, the paper defines what it means for a set of equations Ax involving the functions symbols $\mathcal{F}$ to be a *nice set of recursive axioms.* For Ax to be nice, $\mathcal{F}$ must contain a finite list of 0 or 1-ary constructors (at least one 0 and one 1-ary), $\mathcal{C}$, such that the closed terms (free algebra) over $\mathcal{C}$ can be used used as the numerals of Ax. Then for each $f \in \mathcal{F} \backslash \mathcal{C}$ and each $c \in \mathcal{C}$ there must exist exactly one equation $s = t$ in Ax such that s has the form $f(c, x_1, x_2 \ldots, x_n)$ if c has arity zero or has the form $f(c(x_0), x_1, x_2 \ldots, x_n)$ if c has arity one. Lastly, the only rules in Ax must be of the previously defined type. Given such an Ax, the paper defines the theory $\mathsf{EqT}(Ax)$ to be the theory consisting of closed instances of Ax and those equations derivable from Ax by using either the definition of equality as an equivalence relation or by using the compatibility of function symbols with equality. By fixing a 0-ary constructor c and a 1-constructor c', both in $\mathcal{C}$, $0 = 1$ can be defined as $c = c'(c)$, and $\mathsf{EqT}(Ax)$ is consistent if it does not contain a proof of this. The main result of the paper is then that

$$S_2^1 \vdash \mathsf{Con}(\mathsf{EqT}(Ax)).$$

The class of nice sets of recursive axioms mentioned above is quite general. The author gives several interesting examples. The running example throughout the paper is the theory that uses 0 and S to define numerals and then has equational axioms to define the symbols $+$, $\cdot$, and $\widetilde{\mathsf{exp}}$, denoting addition, multiplication and a kind of exponentiation. In addition to this example, the author shows how a nice set of recursive axioms can be given for the primitive and μ-recursive functions over $\mathbb{N}$, and how the system PV without the substitution and induction rules satisfies the definition of nice. Here PV is theory defined by Cook (*Feasibly constructive proofs and the propositional calculus.* ***Seventh annual ACM symposium on theory of computing***, pp. 83-97) for reasoning about polynomial time computable functions.

The proof of the main result uses a blend of a term rewriting argument together with an approximation scheme. Write $u \longrightarrow^1_{Ax} v$ to mean that there is some axiom $s = t$ in Ax and a ground substitution σ such that $s\sigma$ is a ground term and v is the result of replacing exactly one occurrence of $s\sigma$ in u by $t\sigma$. Define $u \longleftrightarrow^1_{Ax} v$ iff $u \longrightarrow^1_{Ax} v$ or $v \longrightarrow^1_{Ax} u$. Let $\longleftrightarrow^*_{Ax}$ and be the transitive closure of $\longleftrightarrow^1_{Ax}$. The article shows that S_2^1 can prove that if $u = v$ is provable in $\mathsf{EqT}(Ax)$ then $u \longleftrightarrow^*_{Ax} v$ and that if $u \longleftrightarrow^*_{Ax} v$ and u and v are numerals then the Gödel codes for u and v are the same.

Thus, $S_2^1 \vdash \mathsf{Con}(\mathsf{EqT}(Ax))$ because if $0 = 1$ is provable in $\mathsf{EqT}(Ax)$ then $0 \longleftrightarrow_{Ax}^* 1$ and hence 0 and 1 must have the same code which is a contradiction.

The result that S_2^1 proves if $u = v$ is provable in $\mathsf{EqT}(Ax)$ then $u \longleftrightarrow_{Ax}^* v$ is proven by a straightforward induction on the $\mathsf{EqT}(Ax)$ proof. The second result that S_2^1 proves that if $u \longleftrightarrow_{Ax}^* v$ and u and v are numerals then the Gödel codes for u and v are the same is the heart of the argument. To do this a new symbol $*$ is introduced and $u \lhd v$ is defined to mean roughly that v can be obtained from u by replacing some of the subterms of v by $*$. It is obvious that if $u \lhd v \lhd u$ then $u = v$. Using now terms over $\mathcal{F} \cup \{*\}$, a notion of evidence is defined which captures schematically (replacing non-relevant things by $*$) what happens in a given reduction sequence. A notion of one term approximating another given some evidence is also defined. The definition entails that if w approximates t then $t \lhd w$. It is shown that S_2^1 can prove that if u and v approximate the same term according to some evidence then either $u \lhd v$ or $v \lhd u$. By induction on the reduction sequence of $u \longleftrightarrow_{Ax}^* v$, S_2^1 proves that there is an evidence such u approximates v. By a similar induction, one can show with the same evidence that v approximates u. Thus, we get $u \lhd v \lhd u$, and hence, $u = v$.

The paper under review is very well written with many examples. There was only one typo that caused this reviewer some minor confusion: In the example on page 288 right after Definition 4.6, the f's in the given table should be replaced with $\widetilde{\mathsf{exp}}$'s. This same mix-up of f and $\widetilde{\mathsf{exp}}$ also occurs in the equation right after the third paragraph of page 287. Both the main result of the paper and the proof technique are interesting. The paper gives some hope to the program that consistency statements might eventually be used to separate non-trivial bounded arithmetic theories. By showing some consistency results provable in these theories it may also help as a guide in finding statements provable in one theory but not in another.

Chris Pollett

Department of Computer Science, San Jose State University, One Washington Square, San Jose, CA 95192 pollett@cs.sjsu.edu