CONSISTENCY PROOF OF A FEASIBLE ARITHMETIC INSIDE A BOUNDED ARITHMETIC

YORIYUKI YAMAGATA

Ever since Buss showed the relation of his hierarchy of bounded arithmetic $S^i_2, i = 1, 2, \ldots$ to polynomial-time hierarchy of computational complexity [2], the question of whether his hierarchy is collapsed at some $i = n$ or not, has become one of the central questions of bounded arithmetic. This is because the collapse of Buss's hierarchy implies the collapse of polynomial-time hierarchy. In particular, $S^1_2 = \bigcup_{i=1,2,\ldots} S^i_2$ (the right hand side will be denoted by S_2.) implies $P = NP$, because S^1_2 characterizes polynomial time-computable functions P.

A classical way to prove the separation of theories is the use of the second incompleteness theorem of Gödel. If it is proved that S^2 proves the consistency of S^1_2, $S^1_2 \neq S_2$ is obtained, because S^1_2 cannot prove its own consistency.

Unfortunately, Wilkie and Paris showed that S_2 cannot prove the consistency of Robinson arithmetic Q [8], a much weaker system. Although this result stems more from the free use of unbounded quantifiers than from the power of arithmetic, Pudlák showed that S_2 cannot prove the consistency of bounded proofs (proofs of which the formulas only have bounded quantifiers) of S^1_2 [6]. The result was refined by Takeuti [7] and Buss and Ignjatović [3], who showed that, even if the induction were to be removed from S^1_2, S_2 would still not be able to prove the consistency of its bounded proofs.

Thus, it would be interesting to delineate theories which can be proven to be consistent in S_2 and S^1_2, to find a theory T that can be proven to be consistent in S_2 but not in S^1_2. In particular, we focus on Cook and Urquhart's system PV, which is essentially an equational version of S^1_2. Buss and Ignjatović stated that PV cannot prove the consistency of PV^-, a system based on PV from which induction has been removed. On the other hand, Beckmann [1] later proved that S^1_2 can prove the consistency of a theory which is obtained from PV^- by removing the substitution rule.

In this talk, I will present a proof that S^1_2 is capable of proving the consistency of purely equational PV^- with the substitution rule. This result apparently contradicts that of Buss and Ignjatović. However, their proof actually shows that PV cannot prove the consistency of the extension of PV^- that contains propositional logic and $BASIC^e$ axioms. On the other hand, our PV^- is strictly equational, which is a property on which our proof relies.

The consistency of PV^- can be proven by using the following strategy. Beckmann uses a rewriting system to prove consistency of PV^- excluding the substitution rule. According to the terminology of programming language theory, the use of a rewriting system to define the evaluation of terms, is referred to as *small-step semantics* (referred to as *structural operational semantics* in [5]).

Date: April 27, 2015.

However, there is an alternative competing manner in which to perform the abovementioned definition, namely *big-step semantics* (referred to as *natural semantics* in [4]). In big-step semantics, the relation $\langle t, \rho\rangle \downarrow v$ where t is a term, ρ is an assignment to free variables in t, and v is the value of t under assignment ρ, are defined. We treat $\langle t, \rho\rangle \downarrow v$ as a statement in a derivation, and provide rules with which to derive $\langle t, \rho\rangle \downarrow v$. For technical reasons, it is assumed that derivations are DAGs (Directed Acyclic Graphs).

Using big-step semantics, it is also possible to prove the consistency of PV^- excluding the substitution rule. For each inference of $t = u$ in PV^-, it can be proven that $\langle t, \rho\rangle \downarrow v$ implies $\langle u, \rho\rangle \downarrow v$ for any given ρ by induction on the construction of the proof of $t = u$. We refer to this as the main theorem. Based on the properties of semantics, it is easy to prove that $\langle 0, \rho\rangle \downarrow 1$ is never derived, thus the main theorem implies that PV^- never proves $0 = 1$.

However, it would still not be possible to prove the induction step for the substitution rule, which would require the introduction of the notion of *complete development*. The sequence of substitution ρ is a complete development of t if $t\rho$ is a closed term. Although it is generally not possible to compute $t\rho$ polynomially, the decision as to whether ρ is a complete development could be made by using polynomial time.

Then, we attempt to prove that $\langle t, \rho\rangle \downarrow v$ implies $\langle u, \rho\rangle \downarrow v$ for any given ρ by induction on the construction of the proof r of $t = u$ under the assumption that r is a sub-proof of a PV^--proof π of $0 = 1$. It is possible to set bounds for all quantifiers which appear in the induction hypothesis of this induction by setting a bound of ρ and bounds of the derivation of $\langle t, \rho\rangle \downarrow v$ and $\langle u, \rho\rangle \downarrow v$. Thus, the proof can be carried out inside S_2. The bound of $||\rho||$ is given by $||\pi|| - ||r||$ where $||\alpha||$ is the number of symbols in α.

The bounds for derivations are more difficult to obtain. Although it would be possible to bound the number of *nodes* in derivations such as the above in a similar way as ρ, the bounds for the *Gödel numbers* of these derivations are not trivially obtained, because there are no (obvious) bounds for those terms that appear in the derivations. This difficulty was overcome by employing the *call-by-value* style of big-step semantics, in which a derivation has the form

$$\frac{\langle f_1(\overline{v}), \rho\rangle \downarrow w_1, \quad \ldots \quad \langle f_k(\overline{v}, \overline{w}), \rho\rangle \downarrow w_k, \quad \langle t_1, \rho\rangle \downarrow v_1, \quad \ldots, \quad \langle t_m, \rho\rangle \downarrow v_m,}{\langle f(\overline{t}), \rho\rangle \downarrow v} \tag{1}$$

where $\overline{v}$ and $\overline{w}$ are all numerals. Because the numbers of the symbols in $\overline{t}$ and $\overline{f}$ are bounded by $||f(\overline{t})||$, and the size of the numerals appearing in the derivation are bounded by the number of nodes in the derivation, the size of the terms that appear in this derivation could be bound by the number of nodes and the size of the conclusions of the derivation.

Thus, an induction hypothesis is obtained of which all the quantifiers are bounded by the Gödel number of π. Although the induction hypothesis may appear to be a Π^b_2-formula, the derivation of $\langle u, \rho\rangle \downarrow v$ could be constructed by using a polynomial-time function from $\langle t, \rho\rangle \downarrow v$; thus, the induction hypothesis could be written as a Π^b_1-formula. Therefore, proving the main theorem would only require S^1_2.

The part of the induction step that is most difficult to prove is the soundness of the substitution rule. The proof is divided into two parts. First, it is proven that if σ derives $\langle t_1[u/x], \rho\rangle \downarrow v_1, \ldots$, then there is τ that derives $\langle t_1, [u/x]\rho\rangle \downarrow v_1, \ldots$

(Substitution I). Next, it is proven that if σ derives $\langle t_1, [u/x]\rho\rangle \downarrow v_1, \ldots$, then there is τ that derives $\langle t_1[u/x], \rho\rangle \downarrow v_1, \ldots$ (Substitution II).

The intuition behind the proof of Substitution I is explained as follows. The naïve method, which uses induction on the length of σ, is ineffective. This is because an assumption of the last inference of σ may be used an assumption of another inference; thus, it may not be a conclusion of σ_1, which is obtained from σ by removing the last inference. Thus, it would not be possible to apply the induction hypothesis to σ_1. The formulation of conclusions for all the assumptions requires us to increase the length of σ_1 from σ by duplicating the inferences from which the assumptions are derived. Therefore, induction cannot be used on the length of σ.

Instead, we use induction on $||t_1[u/x]|| + \cdots + ||t_m[u/x]||$. Then, we prove that for all $|||\sigma||| \leq U - ||t_1[u/x]|| - \cdots - ||t_m[u/x]||$ where U is a large integer, we have τ which derives $\langle t_1, [u/x]\rho\rangle \downarrow v_1, \ldots$ and satisfies $|||\tau||| \leq |||\sigma||| + ||t_1[u/x]|| + \cdots + ||t_m[u/x]||$. Because τ can be constructed from σ by using a polynomial-time function, the proof only requires induction of which the induction hypothesis is a Π^b_1-formula, thus it is only necessary to know S^1_2 to prove Substitution I.

Acknowledgment

The author is grateful to Toshiyasu Arai, Satoru Kuroda, and Izumi Takeuti for discussions and comments. I would like to thank Editage (www.editage.jp) for English language editing.

References

[1] Arnold Beckmann. Proving consistency of equational theories in bounded arithmetic. *Journal of Symbolic Logic*, 67(1):279–296, March 2002.
[2] Samuel R. Buss. *Bounded arithmetic*. Bibliopolis, 1986.
[3] Samuel R. Buss and Aleksandar Ignjatović. Unprovability of consistency statements in fragments of bounded arithmetic. *Annals of pure and applied logic*, 74:221–244, 1995.
[4] G. Kahn. Natural semantics. In *Proceedings of the First Franco-Japanese Symposium on Programming of Future Generation Computers*, pages 237–257, Amsterdam, The Netherlands, The Netherlands, 1988. Elsevier Science Publishers B. V.
[5] Gordon D. Plotkin. A structural approach to operational semantics. Technical report, Computer Science Department, Aarhus University Denmark, 1981.
[6] P. Pudlák. A note on bounded arithmetic. *Fundamenta mathematicae*, 136:85–89, 1990.
[7] Gaisi Takeuti. Some relations among systems for bounded arithmetic. In PetioPetrov Petkov, editor, *Mathematical Logic*, pages 139–154. Springer US, 1990.
[8] A. Wilkie and J. Paris. On the scheme of induction for bounded arithmetic formulas. *Annals of pure and applied logic*, 35:261–302, 1987.

National Institute of Advanced Science and Technology (AIST), 3-11-46 Nakoji, Amagasaki, Hyogo 661-0974, Japan
E-mail address: yoriyuki.yamagata@aist.go.jp