Models of bounded arithmetic by restricted reduced powers (Abstract)

Michal Garlík *
Faculty of Mathematics and Physics
Charles University in Prague

This abstract presents some results of the author's paper [7] (submitted to Archive for Mathematical Logic), namely, Theorems 1 and 2 below, and contains some new observations.

It is well known that some problems in complexity theory can be reformulated as problems of constructions of expanded extensions of models of bounded arithmetic ([1], [2], [6],[9], [10]). These models are usually required to satisfy some form of bounded induction but at the same time not introduce any new lengths of strings. Modifications of the ultrapower construction can make it easier to meet the last requirement. Restricted ultrapowers were used by Kochen and Kripke [8] to obtain nonelementary extensions of models of arithmetic and by Buss [4] in the context of bounded arithmetic. Theorem 1 below is an attempt in this direction.

Restricted reduced product is defined in the same way as the ordinary *reduced product* except instead of the cartesian product in the definition we only consider some suitable subset of the cartesian product. *Restricted reduced power* is a special case of restricted reduced product in which all factors are equal.

Assume that M is a countable nonstandard model of true arithmetic, $n \in M \setminus \mathbf{N}$, $\Omega \subseteq \{0,1\}^n$. Suppose that $\mathcal{L}$ is a first-order language whose nonlogical symbols are a binary relation $\leq$ and a finite set of function symbols $F_{\mathcal{L}}$ containing a unary symbol S and constant symbols $0, \tilde{n}$. The intended interpretation of each of these function symbols is some function definable in M, with S interpreted by the successor function, $\tilde{n}$ by n, and 0 and $\leq$ interpreted as usual. Assume further that $\psi(x, y, z_1, \ldots, z_{k_0})$ is a $\Delta_0^{<\tilde{n}}$ formula in the language $\mathcal{L}$, i.e., each of its quantifiers is of the form $(\exists w < \tilde{n})$ or $(\forall w < \tilde{n})$. Let $X \in M$ be a set containing the following functions from Ω to M: the identity function id_Ω, for each $v \leq n$ the constant function c_v with value v, and some functions $h_1(x), \ldots, h_{k_0}(x) \in M$.

*Supported by grant GAUK 5732/2012

We define a *straight-line program* (SLP) over $F_{\mathcal{L}}$ of size t with input variables $x_1, \ldots, x_k$ to be a sequence of instructions of the following form: the ith instruction ($i = 1, \ldots, t$) applies a function from $F_{\mathcal{L}}$ to some of the input variables or previously assigned variables $y_1, \ldots, y_{i-1}$ and assigns the outcome of this operation to y_i. Given an assignment of the input variables, the output of the program is the value of y_t. The size of an SLP P will be denoted by $size(P)$.

We will consider SLPs inside M: let $P \in M$ be an SLP over $F_{\mathcal{L}}$ of size $t \in M$ with input variables of the form x_g, $g \in X$. We define $Fct_X(P)$ to be the set consisting of all functions $f : \Omega \to M$ where either $f \in X$ or there is some $i = 1, \ldots, t$ such that $f(u)$ is the value at y_i computed by P with the following assignment of the input variables: the value of x_g is $g(u)$.

Fix a parameter $m \in M$, a nonstandard number with $m < n$, and a parameter q, which is a rational number in M and satisfies $0 < q < 1$. Assume further the following hypothesis:

$$\begin{aligned} &\textit{There is a nonstandard } s \in M \textit{ such that for every SLP } P \in M \\ &\textit{of size } m^s \textit{ and every } f \in Fct_X(P)\textit{:} \\ &\qquad \Pr_{u \in \Omega}[\psi(u, f(u), h_1(u), \ldots, h_{k_0}(u))] < q. \end{aligned} \tag{H}$$

In M define the *master tree* to be the tree of SLPs of size $\leq m^s$. The empty SLP is the root of the master tree and the partial order of the tree is defined by "P is an initial part of Q". For $\ell \geq 0$ put $FCT(\ell) := \bigcup_P Fct_X(P)$, P ranging over SLPs from the master tree of size $\leq \ell$. Denote $FCT := FCT(m^s)$.

The following relation between the parameters n, m and q will be required:

$$q^{1/m^i} < \frac{1}{n} \quad \text{for every } i \in \mathbf{N}. \tag{R}$$

This forces Ω to be large with respect to $\{0,1\}^n$.

Theorem 1. *Let $M, n, \Omega, \mathcal{L}, \psi, X$ be as above. Assume that the parameters m, q as above satisfy the hypothesis* (H) *and the relation (R).*

Then there is $\mathcal{F} \subseteq FCT$ and a filter $\mathcal{G}$ on the M-definable subsets of Ω such that the restricted reduced power $\mathcal{F}/\mathcal{G}$ enjoys the following properties:

(FG 1) *$X \subseteq \mathcal{F}$ and $\mathcal{F}$ is closed under the functions from $F_{\mathcal{L}}$.*

(FG 2) *$\mathcal{F}/\mathcal{G}$ contains no new lengths $\leq n$, i.e., if $f \in \mathcal{F}$ and $\mathcal{F}/\mathcal{G} \models [f] \leq [c_n]$, then there is $v \leq n$ in M such that $\mathcal{F}/\mathcal{G} \models [f] = [c_v]$.*

(FG 3) *Łoś's theorem holds for $\Delta_0^{<\tilde{n}}$ formulas, i.e., for functions $f_1, \ldots, f_k \in \mathcal{F}$ and for an $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_k)$ which is $\Delta_0^{<\tilde{n}}$, we have*

$$\mathcal{F}/\mathcal{G} \models \varphi([f_1], \ldots, [f_k]) \quad \textit{iff} \quad \{u \in \Omega \mid M \models \varphi(f_1(u), \ldots, f_k(u))\} \in \mathcal{G}.$$

(FG 4) *$\mathcal{F}/\mathcal{G} \models (\forall y)\neg\psi([id_\Omega], y, [h_1], \ldots, [h_{k_0}])$*

(FG 5) *Let $\varphi(x)$ be an $\mathcal{L}$-formula of the form*

$$(\exists y_1)\dots(\exists y_{k'})\alpha$$

such that $\alpha(x, y_1, \dots, y_{k'}, [g_1], \dots, [g_k])$ is $\Delta_0^{<\tilde{n}}$ and has $[g_1], \dots, [g_k]$ as parameters, where $g_1, \dots, g_k \in \mathcal{F}$. Then

$$\mathcal{F}/\mathcal{G} \models \neg\varphi([c_0]) \vee \varphi([c_m]) \vee (\exists x < [c_m])\big(\varphi(x) \wedge \neg\varphi(S(x))\big),$$

i.e., in $\mathcal{F}/\mathcal{G}$ induction for φ holds up to m.

(For $f \in \mathcal{F}$, $[f]$ denotes the equivalence class of f in $\mathcal{F}/\mathcal{G}$.) The theorem is proved by constructing $\mathcal{F}$ and $\mathcal{G}$ in countably many stages. The main ingredient of the proof is the way in which induction is ensured. This is done by cutting the master tree in a binary search fashion and at the same time performing binary search on the interval $[0, n]$ and making smaller the sets of the filter.

We use the construction to separate theories $R^1_2(g)$ and $strictR^1_2(g)$ assuming that g is a one-way function hard against polynomial-size circuits. A polynomial-time function $g : \{0,1\}^* \to \{0,1\}^*$ is called an *ϵ-OWP (one-way permutation)* if $\epsilon : \mathbf{N} \to [0,1]$, for every n, g is a permutation of $\{0,1\}^n$, and for any polynomial p, for all sufficiently large n and for every boolean circuit C of size at most $p(n)$,

$$\Pr_{x\in\{0,1\}^n}[g(C(x)) = x] < \epsilon(n).$$

Theorem 2. *Let $\epsilon(x) := 2^{-x^\delta}$. If an ϵ-OWP exists then $strictR^1_2(\tilde{g})$ is weaker than $R^1_2(\tilde{g})$. If an ϵ-OWP is definable by a term in the language of R^1_2, then $strictR^1_2$ is weaker than R^1_2.*

Here $\tilde{g}$ is a new function symbol. The theorem is proved by the construction in Theorem 1 with some modifications to its setup. Namely, Ω consists of all sequences in M containing n items such that each item is a number of length n. Moreover, SLPs are allowed to use an additional instruction to find the preimage under $\tilde{g}$ of an item of a sequence (where the interpretation of $\tilde{g}$ in M is the ϵ-OWP g) . To translate the ϵ-OWP assumption into hypothesis (H) we use an argument similar to that of S. Cook and N. Thapen [5] described in the footnote on page 7 of [5] and attributed there to R. Impagliazzo. Theorem 1 then gives a model $\mathcal{F}/\mathcal{G}$ of $strictR^1_2(g)$ in which the following instance of *sharply bounded collection scheme* does not hold:

$$(\forall x)\big((\forall i < n)(\exists z)\, g(z) = [x]_i \to (\exists y)(\forall i < n)\, g([y]_i) = [x]_i\big),$$

where sequence coding $[x]_i$ is definable by a term of R^1_2. The rest of the theorem follows from the result of B. Allen [3] that R^i_2 proves the sharply bounded collection for Σ^b_i formulas for $i \geq 1$.

The results up to this point are taken from [7]. We add some new observations regarding Theorem 1.

One observation is that by a small change in the construction we can achieve that $\mathcal{F}/\mathcal{G}$ satisfies (in addition to (FG 1) - (FG 5)) the minimization principle for $\forall\Delta_0^{<\tilde{n}}$-formulas on the interval $[0, m]$.

Another observation is that we can modify the construction in Theorem 1 to prove

Theorem 3. *strict*$R_2^1(g) \neq R_2^1(g)$.

Here we got rid of the OWP assumption, but nothing favourable can be said about the function g.

References

[1] M. Ajtai, *Generalizations of the Compactness Theorem and Gödel's Completeness Theorem for Nonstandard Finite Structures*, Proceedings of the 4th international conference on Theory and applications of models of computation (2007) 13-33.

[2] M. Ajtai, *A Generalization of Gödel's Completeness Theorem for Nonstandard Finite Structures*, manuscript (2011)

[3] B. Allen, *Arithmetizing Uniform NC*, Annals of Pure and Applied Logic 53 (1991) l-50

[4] S. Buss, *Weak End Extensions of Models of Bounded Arithmetic*, unpublished manuscript (1986)

[5] S. Cook, N. Thapen, *The strength of replacement in weak arithmetic*, ACM Transactions on Computational Logic 7 (2006) 749-764

[6] M. Garlík, *A New Proof of Ajtai's Completeness Theorem for Nonstandard Finite Structures*, Archive for Mathematical Logic 54(3-4), (2015), pp. 413-424.

[7] M. Garlík *Construction of models of bounded arithmetic by restricted reduced powers*, submitted, February 2015

[8] S. Kochen, S. Kripke, *Non-standard models of Peano Arithmetic*, Enseign. Math. 28(2) (1982) 211-231.

[9] J. Krajíček, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge University Press, 1995

[10] A. Máté, *Nondeterministic polynomial-time computations and models of arithmetic*, Journal of the Association for Computing Machinery, 37(1) (1990) 175-193