Bounded arithmetic, ultrapowers, and replacement

Michal Garlík

University of Warsaw

Proof Complexity Workshop in St. Petersburg
2016

Motivations

- (Buss) The Σ_1^b-definable functions in S_2^1 are exactly those in FP.
- (Allen, Takeuti) The Σ_1^b-definable functions in R_2^1 are exactly those in uniform FNC.
- Separations of theories of bounded arithmetic shed insight into problems in computational complexity. There are known model construction tasks in bounded arithmetic which are equivalent to problems in complexity theory.
- With $strictR_2^1$ it looks like its Σ_1^b-consequences are a fair bit weaker than FNC, so there is a hope to separate it from S_2^1.
- Cook-Thapen: several separation results for theories below S_2^1. E.g.: If integer factoring is not possible in probabilistic polynomial time, then $PV_1 \neq S_2^1$.

First-order theories of bounded arithmetic

- $L_2 : 0, S, +, \cdot, =, \leq,$

$\lfloor x/2 \rfloor$	(x divided by 2 rounded down),
$\lvert x \rvert$	($= \lceil \log(x+1) \rceil$, the length of x in binary notation),
$x \# y$	($= 2^{\lvert x \rvert \cdot \lvert y \rvert}$),
$MSP(x, i)$	($= \lfloor x/2^i \rfloor$),
$x \dot{-} y$	(x minus y if this is greater than zero and zero otherwise)

- $BASIC$ is a finite set of open axioms fixing the basic properties of the language, like $x + S(y) = S(x+y)$, $|x \# y| = |x| \cdot |y| + 1, \ldots$
- $L^m IND_\phi$ induction axiom for a formula ϕ is

$$\phi(0) \wedge \forall x < |t|_m(\phi(x) \rightarrow \phi(S(x))) \rightarrow \phi(|t|_m),$$

  where t is a term and we are using $|x|_0 := x, |x|_m := ||x|_{m-1}|$.

Bounded arithmetic theories

- Bounded quantifiers: $\exists x \leq t$; $\forall x \leq t$
- Sharply bounded quantifiers: $\exists x \leq |t|$; $\forall x \leq |t|$
- A formula is called (sharply) bounded if all quantifiers in it are (sharply) bounded.
- Σ_0^b (or Π_0^b) is the class of sharply bounded formulas
- For $i > 0$, Σ_{i+1}^b (resp. Π_{i+1}^b) is the least class containing Π_i^b (resp. Σ_i^b) and closed under conjunction, disjunction, sharply bounded quantification and bounded existential (resp. universal) quantification.

- T_2^i is $BASIC + \Sigma_i^b - IND$
  S_2^i is $BASIC + \Sigma_i^b - LIND$
  R_2^i is $BASIC + \Sigma_i^b - LLIND$

Coding and Replacement

- Since we have MSP and $\dot{-}$ in the language, we can define a term $\beta_a(w, i)$, such that if w is the number whose binary representation consitst of 1 followed by binary representations of numbers $b_1, \ldots, b_\ell$, each padded with zeros to be of length $|a|$, then $\beta_a(w, i) = b_i$.
- Replacement scheme (also called sharply bounded collection scheme) $BB\Gamma$ for a class of formulas Γ is

$$
\begin{aligned}
&(\forall x \leq |s|)(\exists y \leq t)A(x, y) \rightarrow \\
&\qquad (\exists w \leq 2(t\#2s))(\forall x \leq |s|)\beta_t(w, x) \leq t \wedge A(x, \beta_t(w, x))
\end{aligned}
$$

  for each $A(x, y) \in \Gamma$ and for all terms s, t, such that $A(x, y), s, t$ may contain other free variables but t and s do not involve x or y. Here $2(t\#2s)$ is a bound on any string consisting of concatenating $|s| + 1$ strings of length $\leq |t|$.

Strict theories

- The strict variant of Σ_i^b, the *strict*Σ_i^b-formulas, are of the form
$$(\exists x_1 \leq t_1)(\forall x_2 \leq t_2)\ldots(Qx_i \leq t_i)\phi,$$
where Q is $\exists$ if i is odd and $\forall$ if i is even, and ϕ is sharply bounded.
- A *strict*Π_i^b-formula is defined similarly but with the outer quantifier being universal.
- Does it make any difference if we define T_2^i, S_2^i, R_2^i using $strict\Sigma_i^b - L^m IND$ rather than $\Sigma_i^b - L^m IND$ ($m = 0, 1, 2$, respectively)? Denote these theories by $strictT_2^i, strictS_2^i, strictR_2^i$.
- Makes no difference for T_2^i and S_2^i: The strict theory proves $BB\Sigma_i^b$, and so it proves that each formula is equivalent to its strict form.
- For R_2^i it is unknown. We don't know whether $strictR_2^i$ proves $BB\Sigma_i^b$.
- R_2^i proves $BB\Sigma_i^b$ (Allen): Use LLIND on
$$(\forall u \leq |s|)(\exists w \leq 2(t\#2s))(\forall x \leq |s|)$$
$$[(x \leq 2^{\min(j,||s||)} \wedge u + x \leq |s|) \rightarrow A(u + x, \beta_t(w, x))]$$

Our framework

Definable ultrapower

- Skolem: the first historical construction of a nonstandard model of PA
- Paris, Hájek-Pudlák: constructions of extensions of models of arithmetic

Restricted ultrapower

- Kochen-Kripke: reproved Paris-Harrington theorem
- Máté: suggests it as a possible method to tackle problems in computational complexity
- Krajíček: similar method of Boolean-valued models based on random variables

A general construction task

Let M be a countable nonstandard model of arithmetic, $n \in M$ a nonstandard element and $\psi(x, y)$ an L_2-formula. We are looking for a construction of models of S^1_2 of the form $\mathcal{F}/G$, such that:

- $\mathcal{F}$ is some set of functions $f \in M$ with domain $\Omega \subseteq M$
- G is a filter on M-definable subsets of Ω
- $\mathcal{F}/G$ coincides with M up to n
- $\mathcal{F}/G \models (\forall y)\neg\psi([id_\Omega], y)$.

Hardness assumption

Definition (ϵ-OWP)

Let $\epsilon : \mathbf{N} \to [0,1]$ be a function. A polynomial-time function $g : \{0,1\}^* \to \{0,1\}^*$ is called an ϵ-*OWP (one-way permutation)* if 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 $p(n)$,

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

We will need $\epsilon(x) := 2^{-x^\delta}$ where $\delta > 0$ is some rational number.

Results

Theorem

Let M be a nonstandard model of true arithmetic and let $n \in M$ be nonstandard. Let $\epsilon(x) := 2^{-x^{\delta}}$ where $\delta > 0$ is some (standard) rational number and assume that an ϵ-OWP exists. Denote g the ϵ-OWP in M and Let $\tilde{g}$ be a function symbol interpreted in M by g. Then there exists a model N of strict$R^1_2(\tilde{g})$ such that N restricted to $Log(N)$ coincides with M restricted to $\{x \in M \mid x \leq n^k \text{ for some } k \in \mathbf{N}\}$ and the following instance of $BB\Sigma^b_0(\tilde{g})$ does not hold in N:

$$(\forall x)\big((\forall i < n)(\exists z < 1\#LSP(x,n))\,\tilde{g}(z) = \beta_{LSP(x,n)}(x,i)$$
$$\rightarrow (\exists y)(\forall i < n)\,\tilde{g}(\beta_{LSP(x,n)}(y,i)) = \beta_{LSP(x,n)}(x,i)\big).$$

Results

Theorem

Let $\delta > 0$ be a rational number and let $\epsilon(x) := 2^{-x^{\delta}}$. If an ϵ-OWP exists and is in NC, then strictR^1_2 is weaker than R^1_2.

Theorem

Let $\delta > 0$ be a rational number, $\epsilon(x) := 2^{-x^{\delta}}$ and suppose that an ϵ-OWP exists. Then $PV_1 + strict\Sigma^b_1(PV) - \mathrm{LLIND}$ is weaker than $PV_1 + \Sigma^b_1(PV) - \mathrm{LLIND}$.

Theorem

For a new unary relation symbol α, strict$R^1_2(\alpha)$ is weaker than $R^1_2(\alpha)$.

Thank you!