A pesky theory of bounded arithmetic

Leszek Kołodziejczyk
University of Warsaw

(based on joint work with Buss-Thapen and Buss-Zdanowski)

Kotlarski-Ratajczyk conference, Będlewo, July 2012

Bounded arithmetic: quick review

Language: symbols for all polytime computable functions & relations on the natural numbers. In particular, no 2^x, but we do have $x^{\log y}$.

$\hat{\Sigma}^b_n$ formulas: $\exists x_1 < t_1 \forall x_2 < t_2 \ldots Q x_n < t_n\, \psi$, where ψ open. Correspond to properties in the n-th level of the polynomial hierarchy.

- Full BA: induction for bounded formulas in this language. Essentially a notational variant of $I\Delta_0 + \Omega_1$.
- The fragment T^n_2: induction for $\hat{\Sigma}^b_n$.
- Role of T^0_2 played by PV: a basic theory for polynomial time. (PV is to polytime as PRA is to primitive recursive).

Bounded arithmetic: motivation

- connections to computational complexity:
  - witnessing theorems: if $T \vdash \forall x\, \exists y\, A(x, y)$ for A of the right form, then y can be found by a given kind of algorithm/search process,
  - natural framework for stating complexity-theoretical questions, with the hope of getting independence results,
- connections to propositional proof complexity: arithmetical proofs can be translated into short propositional proofs.
- desire to understand how much combinatorics, number theory, logic etc. can be done without the exponential function.

Bounded arithmetic: relativized setting

Fundamental (and seemingly hopeless) open problem:
Do the theories T_2^n form a strict hierarchy?

More open problems come from relativized BA,
where we have a new "oracle" predicate α and allow the ptime functions/relations to query α (which gives $\hat{\Sigma}_n^b(\alpha), T_2^n(\alpha), \mathrm{PV}(\alpha)$ etc.)

For instance, is is known that $\mathrm{PV}(\alpha) \subsetneq T_2^1(\alpha) \subsetneq T_2^2(\alpha) \subsetneq T_2^3(\alpha) \ldots$
(Krajíček-Pudlák-Takeuti 1991).

Two current major open problems

1. Can the theories $T^n_2(\alpha)$ be separated by a $\forall\hat{\Sigma}^b_1(\alpha)$ sentence?
   - only $\mathrm{PV}(\alpha) \not\preccurlyeq_{\forall\hat{\Sigma}^b_1(\alpha)} T^1_2(\alpha) \not\preccurlyeq_{\forall\hat{\Sigma}^b_1(\alpha)} T^2_2(\alpha)$ known.
2. An “interesting” independence result for $\mathrm{BA}(\alpha)$ with a parity quantifier, “there is an odd number of $x < t$ such that”.
   - e.g. for PHP: “α is not a 1-1 function from $x + 1$ to x”, already known to be independent from $\mathrm{BA}(\alpha)$.

Two current major open problems

1. Can the theories $T^n_2(\alpha)$ be separated by a $\forall\hat{\Sigma}^b_1(\alpha)$ sentence?
   - only $\mathrm{PV}(\alpha) \not\succcurlyeq_{\forall\hat{\Sigma}^b_1(\alpha)} T^1_2(\alpha) \not\succcurlyeq_{\forall\hat{\Sigma}^b_1(\alpha)} T^2_2(\alpha)$ known.
2. An "interesting" independence result for $\mathrm{BA}(\alpha)$ with a parity quantifier, "there is an odd number of $x < t$ such that".
   - e.g. for PHP: "α is not a 1-1 function from $x+1$ to x", already known to be independent from $\mathrm{BA}(\alpha)$.

Main theme of this talk: in both problems, the same kind of theory seems to show up as an obstacle.

Detour: approximate counting

Weak pigeonhole principles

iWPHP($\mathcal{F}$): injective WPHP for function class $\mathcal{F}$:
no function $f \in \mathcal{F}$ is injective from $y \gg x$ into x,
sWPHP($\mathcal{F}$): surjective WPHP for function class $\mathcal{F}$:
no function $f \in \mathcal{F}$ is surjective from x onto $y \gg x$.

Typically, $y \gg x$ means $y = x^2, 2x$, at times has to be $x(1 + 1/\log x)$.

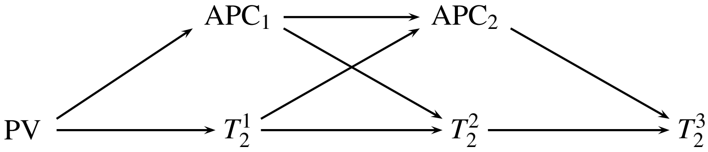
- easy: $\mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}(\alpha)}) \vdash \mathrm{iWPHP}(\alpha)$,
- likewise, $\mathrm{iWPHP}(\mathrm{FP}^{\mathrm{NP}(\alpha)}) \vdash \mathrm{sWPHP}(\alpha)$,
- $T^2_2(\alpha) \vdash \mathrm{iWPHP}(\alpha), \mathrm{sWPHP}(\alpha)$ (Maciel-Pitassi-Woods 2002).

Approximate counting

Jeřábek 2005-2009:

- $\mathrm{APC}_1 = \mathrm{PV} + \mathrm{sWPHP}(\mathrm{FP})$ can approximate the size of polytime set $X \subseteq 2^n$ up to $1/\mathrm{poly}(n)$ fraction of 2^n.
- $\mathrm{APC}_2 = T^1_2 + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}})$ can do the same for $X \in \mathrm{P}^{\mathrm{NP}}$, while for $X \in \mathrm{NP}$ it finds surjections witnessing $m \twoheadleftarrow X \twoheadleftarrow m + m/\mathrm{polylog}(m)$.

APC theories within the hierarchy



Peskiness of APC_2

Empirical observation:

The $\forall\hat{\Sigma}_1^b(\alpha)$ principles used to separate low levels of the $\mathrm{BA}(\alpha)$ hierarchy from the rest are either complete for some level (hence hard to work with) or provable in $\mathrm{APC}_2(\alpha)$.

Mathematical result:

Bounded arithmetic with the parity quantifier, $\mathrm{BA}^{\oplus}$,
is equal to a "parity version" of APC_2 (and this relativizes).

The non-parity case

Typical separating principles

Some $\forall\hat{\Sigma}^b_1(\alpha)$ principles separating $T^1_2(\alpha)$ from stronger theories:

- iWPHP(α),
- Ramsey's principle: the graph determined by α on $[0,x)$ has a homogeneous set of size $(\log x)/2$,
- ordering principle OP: if α is a linear ordering on $[0,x)$, then it has a least element (has to be Herbrandized to become $\forall\hat{\Sigma}^b_1(\alpha)$).

All these, and many similar principles, are either known or easily seen to be provable in $\mathrm{APC}_2(\alpha)$.

Example: $\mathrm{APC}_2(\alpha) \vdash \mathrm{OP}$.

- Given x, prove by induction on $y < \log x$ that there exists $z < x$ such that the set of elements α-smaller than z has size approximately less than than $x/2^y$.
- Inductive step involves some additional counting arguments to show that there is z' α-smaller than approximately at least half of the elements α-smaller than the current z.
- Induction formula is $\Sigma^b_2(\alpha)$, but the induction is only up to $\log x$, so there is a conservativity result that lets us use it.

APC_2 and $\forall\hat{\Sigma}_1^b$

Question:

Is there a $\forall\hat{\Sigma}_1^b(\alpha)$ sentence separating $\mathrm{APC}_2(\alpha)$ from full $\mathrm{BA}(\alpha)$?

APC_2 and $\forall\hat{\Sigma}^b_1$

Question:

Is there a $\forall\hat{\Sigma}^b_1(\alpha)$ sentence separating $\mathrm{APC}_2(\alpha)$ from full $\mathrm{BA}(\alpha)$?

?????

APC_2 and $\forall\hat{\Sigma}^b_1$

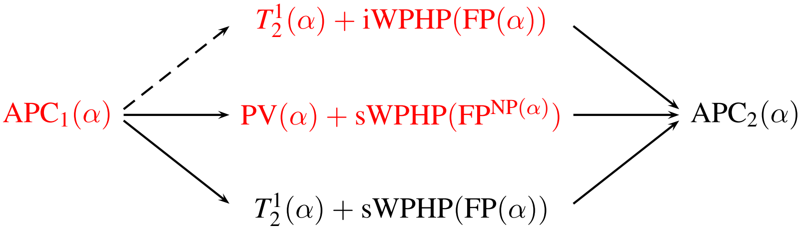
Question:

Is there a $\forall\hat{\Sigma}^b_1(\alpha)$ sentence separating $APC_2(\alpha)$ from full $BA(\alpha)$?

?????

So, why not first consider natural fragments of APC_2?
(Obtained by limiting induction or WPHP somewhat.)

Some fragments of APC_2



For the theories marked in red, we have a separation from $\mathrm{BA}(\alpha)$ (in fact, from $\mathrm{APC}_2(\alpha)$). For the others, still no separation known.

A useful principle

HOP:
"For all z, it is not true that $\preccurlyeq$ is a linear order on $[0, z)$ for which h is the predecessor function".
(Oracle α provides $\preccurlyeq$ and the bitgraph of h.)

A useful principle

HOP:

"For all z, it is not true that $\preccurlyeq$ is a linear order on $[0, z)$ for which h is the predecessor function".
(Oracle α provides $\preccurlyeq$ and the bitgraph of h.)

Theorem

HOP is unprovable in:

- $T^1_2(\alpha) + \mathrm{iWPHP}(\mathrm{FP}(\alpha))$,
- $\mathrm{PV}(\alpha) + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}(\alpha)})$.

Provable in $\mathrm{APC}_2(\alpha)$. Status in $T^1_2(\alpha) + \mathrm{sWPHP}(\mathrm{FP}(\alpha))$ unknown!

$\mathrm{PV} + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}})$

Theorem

$\mathrm{PV}(\alpha) + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}(\alpha)}) \nvdash \mathrm{HOP}$.

(note: $x \to 2x$ version; some issues about formalization of $\mathrm{FP}^{\mathrm{NP}}$.)

$\mathrm{PV} + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}})$

Theorem

$\mathrm{PV}(\alpha) + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}(\alpha)}) \nvdash \mathrm{HOP}$.

(note: $x \to 2x$ version; some issues about formalization of $\mathrm{FP}^{\mathrm{NP}}$.)

Proof ingredients:

- logic: (generalizations of) so-called KPT witnessing for $\forall\exists\forall$ and more complex consequences of PV,
- simplified case: $x \to x^2$ version of sWPHP for single $\mathrm{FP}^{\mathrm{NP}}$ function f, where x is a term depending only on z,
- witnessing gives constant round Student-Teacher game: given $v < x^2$, Student produces $u < x$ and computation w witnessing $f(u) = v$, or witness to HOP; Teacher gives counterexamples showing that w contains a false 'No' answer to an NP query.

$\mathrm{PV} + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}})$: arguing against Student

- Construction in stages $1, \dots, k = \mathrm{lh}$ of S-T game. At each stage, $\preceq$ defined on all of $[0, z)$, but only part is settled (initially $\emptyset$), the points below it are tentative;
- Always $\gg x$ v's (initially all x^2) are active, the rest is discarded.

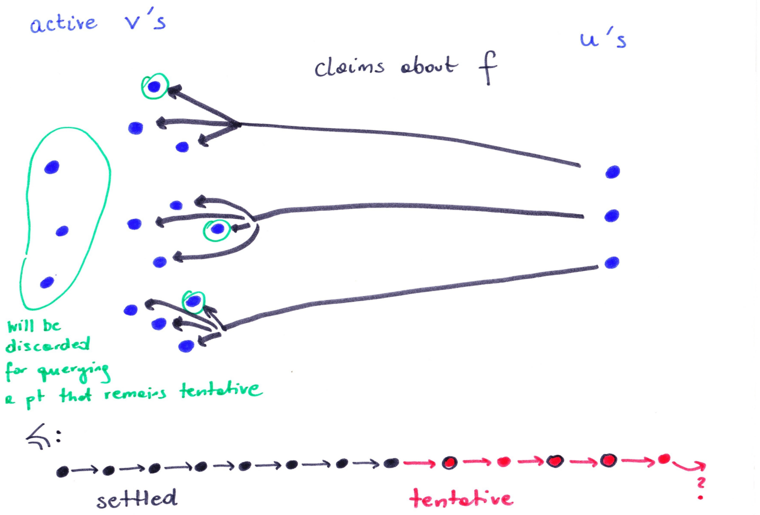
PV + sWPHP(FP^{NP}): arguing against Student

- Construction in stages $1, \ldots, k = \mathrm{lh}$ of S-T game. At each stage, $\preceq$ defined on all of $[0, z)$, but only part is settled (initially $\emptyset$), the points below it are tentative;
- Always $\gg x$ v's (initially all x^2) are active, the rest is discarded.
- At stage i order the tentative part randomly and only keep a $1/\mathrm{polylog}(z)$ fraction tentative, so that the least point remains tentative and at most half the active v's query a point that remains tentative. Discard those v's.

PV + sWPHP(FP^{NP}): arguing against Student

- Construction in stages $1, \ldots, k = \mathrm{lh}$ of S-T game. At each stage, $\preceq$ defined on all of $[0, z)$, but only part is settled (initially $\emptyset$), the points below it are tentative;
- Always $\gg x$ v's (initially all x^2) are active, the rest is discarded.
- At stage i order the tentative part randomly and only keep a $1/\mathrm{polylog}(z)$ fraction tentative, so that the least point remains tentative and at most half the active v's query a point that remains tentative. Discard those v's.
- When Student claims "$f(u) = v$" for a given u and many v's, for all but a single v Teacher can use the other v's to find a counterexample to a 'No' answer in the computation. For each u, that "bad" v is discarded.
- At the end of the S-T game, there are still a lot of active v's for which Student does not have a good u. □

PV + sWPHP(FP$^{\text{NP}}$) proof: picture of a stage



Open problem

Separate $T^1_2(\alpha) + \mathrm{sWPHP}(\mathrm{FP}(\alpha))$ from $\mathrm{BA}(\alpha)$!

- Candidate hard problems: HOP, iWPHP, etc.
- Characterizations of provability in $T^1_2(\alpha) + \mathrm{sWPHP}(\mathrm{FP}(\alpha))$ in terms of “randomized” propositional proofs and algorithmic search procedures are known.

The parity case

Limiting the use of $\oplus$

$\oplus x < y$:= "there is an odd number of $x < y$ such that".

$\hat{\Sigma}_n^{b,\oplus \mathrm{P}}$ formulas: $\exists x_1 < t_1 \forall x_2 < t_2 \dots Q x_n < t_n \, \psi$,
where ψ open except for perhaps $\oplus$ in front of polytime formulas.

$T_2^{n,\oplus \mathrm{P}}$: induction for $\hat{\Sigma}_n^{b,\oplus \mathrm{P}}$. Note that $\bigcup_n T_2^{n,\oplus \mathrm{P}} \neq \mathrm{BA}^{\oplus}$.

This all relativizes smoothly to α.

The collapse result

$$\mathrm{APC}_2^{\oplus \mathrm{P}} = T_2^{2,\oplus \mathrm{P}} + \mathrm{sWPHP}(\mathrm{FP}^{\mathrm{NP}^{\oplus \mathrm{P}}}).$$

Theorem

$\mathrm{BA}^{\oplus}$ *is conservative over* $\mathrm{APC}_2^{\oplus \mathrm{P}}$*, and this relativizes.*

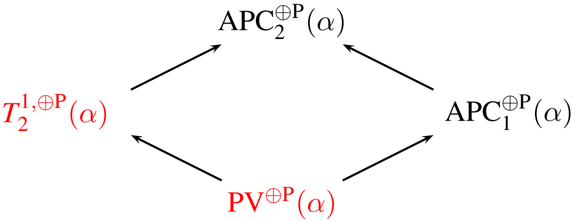
Remark

This has implications for propositional proof complexity: constant depth systems with parity gates are (for simple enough formulas) quasipolynomially simulated by depth 3 systems with formulas in a particular form (or even depth 2 systems with additional axioms corresponding to sWPHP).

The collapse result: comments on proof

- Toda's Theorem: each problem in the closure of the polynomial hierarchy under the parity quantifier has a probabilistic polytime reduction to $\oplus$Sat, the problem whether a given propositional formula has an odd number of satisfying assignments.
- We inductively assign to each bounded formula with $\oplus$ a "$\Delta_1^{b,\oplus P}$ translation" correct on a bounded interval, more or less following the usual proof of Toda's Theorem. The translation is well behaved in $APC_2^{\oplus P}$, which is strong enough to handle various probabilistic/counting arguments involved.
- Example of place where $APC_2^{\oplus P}$ seems needed: when we say that given a formula φ in n variables, there is $k \leq n$ such that φ has between 2^{k-2} and 2^k satisfying assignments.

Current picture



- Unprovability of PHP (and some variants of HOP) in $T_2^{1,\oplus \mathrm{P}}(\alpha)$ follows easily from known results in proof complexity.
- For the theories involving sWPHP, something can be done if $\oplus$ is allowed only in the induction part, not the sWPHP part.
- Independence of, say, PHP from even $\mathrm{APC}_1^{\oplus \mathrm{P}}(\alpha)$ is open, and seems hard.