Higher polynomial local search for fragments of bounded arithmetic

Leeds Research Workshop in Proof Theory and Constructivism
July 7, 2009

Sam Buss
Department of Mathematics
Univ. of Calif., San Diego

(joint work with Arnold Beckmann)

Bounded Arithmetic and Provably Total Functions.

Recall some systems:

- PV - Induction on polynomial time predicates (Cook 1975)
- $I\Delta_0$ - Induction on linear time hierarchy predicates (Parikh, 1971).
- Ω_1 - Totality of $x^{\log x}$ ("smash" function, $\#$)
- T_2^k -Induction on Σ_k^b-predicates, at k-th level of polynomial time hierarchy.
  T_2^1 - Induction on NP predicates. (Buss 1985)
- S_2^k -Length or polynomial induction on Σ_k^b-predicates. [ibid]

$$PV \preccurlyeq S_2^1 \subseteq T_2^1 \preccurlyeq S_2^2 \subseteq T_2^2 \preccurlyeq S_2^3 \subseteq \cdots \qquad \cdots I\Delta_0 + \Omega_1.$$

S_2^{k+1} is $\forall\Sigma_{k+1}^b$-conservative over T_2^k.

Analogy (weak): $S_2^k \approx I\Sigma_k$ and (polynomial time)$\approx$(primitive recursive).

Provably total functions.

Theory	Graph	(Multi)Function class
S_2^1	Σ_1^b-defined	P, polynomial time functions
T_2^1	Σ_1^b-defined	PLS, polynomial local search multifunctions.
S_2^k	Σ_k^b-defined	$P^{\Sigma_{k-1}^b}$ functions.
T_2^k	Σ_k^b-defined	$PLS^{\Sigma_{k-1}^b}$ multifunctions.
S_2^{k+1}	Σ_k^b-defined	$PLS^{\Sigma_{k-1}^b}$ multifunctions.
T_2^2	Σ_1^b-defined	Colored PLS. (Krajíček-Skelley-Thapen, 2006)
T_2^k	Σ_1^b-defined	Herbrand analysis (Pudlák, 2006).
"	"	k-turn games (Skelley-Thapen, 200?).
T_2^2	Σ_1^b-defined	Iterated PLS (Arai, 200?)
T_2^k	Σ_i^b-defined	Π_k^b-PLS with Π_{i-1}^b-goal $(1 \leq i \leq k)$ - (this talk)

(P:Buss 1985. PLS: Buss-Krajíček 1994).

Polynomial Local Search (PLS) problems.

(Johnson-Papadimitriou-Yannakakis, 1988). A *PLS problem* defines a total multifunction f with polynomial time graph $f(x) = y$. It has:

- A set $F(x) := \{s : F(x,s)\}$ of feasible points $\leq t(x)$,
- An initial point $i(x) \in F(x)$.
- A cost function $c(x,s)$.
- A neighborhood function $N(x,s)$.
- F, N, c, i and t are polynomial time.
- For all $s \in F(x)$, $N(x,s) \in F(x)$ and
  either $N(x,s) = s$ or $c(N(x,s)) < c(s)$.
- If $s \in F(x)$ and $N(x,s) = s$, then $y = (s)_1$ is a value of $f(x)$.

$f(x) = y$ holds if and only if $s \in F(x)$ and $N(x,s) = s$ and $(s)_1 = y$.

Algorithm: Start with $s = i(x)$ and iterate N. Is in PSPACE.
Open question: Are PLS problems in P?

Π_k^p-PLS — relativizing PLS

($PLS^{\Pi_k^p}$ has F, c, N, i in $P^{\Pi_k^p}$.)

Π_k^p-PLS has $F \in \Pi_k^p$, but N, c, i are polynomial time.
Π_k^p-PLS problems by definition satisfy (α)-(δ):

(α) $\forall x \forall s(F(x,s) \rightarrow |s| \leq d(|x|))$, d a polynomial.

(β) $\forall x(F(x, i(x)))$.

(γ) $\forall x \forall s(F(x,s) \rightarrow F(x, N(x,s)))$.

(δ) $\forall x \forall s(N(x,s) = s \vee c(x, N(x,s)) < c(x,s))$.

Defines a multifunction $f(x) = y$ by:

$$f(x) = y \;\Leftrightarrow\; (\exists s \leq 2^{d(|x|)})[F(x,s) \wedge N(x,s) = s \wedge y = (s)_1].$$

Same algorithm applies, and is still in PSPACE.

Π_k^p-PLS with Π_g^p-goal G

A Π_k^p-PLS problem with Π_g^p-goal $G(x,s)$ satisfies the additional property:

$(\epsilon)\ \forall x \forall s (G(x,s) \leftrightarrow [F(x,s) \wedge N(x,s) = s])$.

The graph of the multifunction can now be defined by

$$f(x) = y \ \Leftrightarrow \ (\exists s \leq 2^{d(|x|)})[G(x,s) \wedge y = (s)_1],$$

so f has a Σ_{g+1}^b-definition.

Formalized Π_k^p-PLS problems: The predicates F and G are given by Π_k^b- and Π_g^b-formulas, N, i, c are polynomial time functions, and the base theory S_2^1 proves conditions (α)-(ϵ).

Formalized Π_k^p-PLS problems are called Π_k^b-PLS problems.

Existence of solutions to Π_k^b-problems

Thm 1. Let $\mathcal{P}$ be a Π_k^b-PLS problem. Then T_2^{k+1} proves that, for all x, $\mathcal{P}(x)$ has a solution:

$$\forall x \exists s (F(x,s) \wedge N(x,s) = s),$$

or

$$\forall x \exists s (G(x,s)).$$

This is a Σ_{k+1}^b- (resp., Σ_{g+1}^b-) definition of a multifunction.

Pf. Use Σ_{k+1}^b-minimization to find the least c_0 satisfying

$$\exists s \le 2^{d(|x|)} (c_0 = c(x,s) \wedge F(x,s)).$$

Exact characterization of Σ_i^b-definable functions of T_2^{k+1}.

Main Thm 2 Let $0 \le g \le k$ and $A(x, y) \in \Sigma_{g+1}^b$. Suppose

$$T_2^{k+1} \vdash (\forall x)(\exists y) A(x, y).$$

Then there is a Π_k^b-PLS problem $\mathcal{P}$ with Π_g^b-goal G such that S_2^1 proves

$$\forall x \forall s (G(x, s) \rightarrow A(x, (s)_1)).$$

Note that the conclusion is provable in S_2^1, but T_2^{k+1} is needed to prove the existence of s.

For $k = g = 0$, states that the Σ_1^b-definable functions of T_2^1 are in PLS.

Why formalization in S_2^1 is important (#1)

Consider a total multifunction defined by $(\forall x)(\exists y \leq t)A(x,y)$, where $A \in \Delta_0^b$. Here is a Π_1^p-PLS search problem for it:

- Initial function: $i(x) = 0$.
- Cost function: $c(x,y) = t - y$.
- Neighborhood function: $N(x,y) = \begin{cases} y & \text{if } A(x,y) \text{ or } y \geq t(x) \\ y+1 & \text{otherwise.} \end{cases}$
- Feasible set: $F(x,y) \;\Leftrightarrow\; [A(x,y) \vee (\forall y' < y)(\neg A(x,y'))] \wedge y \leq t(x)$.
- Goal: $G(x,y) \;\Leftrightarrow\; A(x,y) \wedge y \leq t(x)$.

This is a correct Π_1^p-PLS problem independently of provability in T_2^{k+1}. But it is not formalizable in S_2^1, so is not a Π_1^b-PLS problem.

Thm 2's proof strategy: Fix $k \geq 0$.

Defn Let $A(\vec{c}) \in \Sigma^b_{k+1}$. $Wit_A(u, \vec{c})$ is a Π^b_k-formula that states u codes values for the outermost existential quantifiers of $A(\vec{c})$ making $A(\vec{c})$ true.

Witnessing Lemma. If T_2^{k+1} proves a sequent

$$\Gamma \longrightarrow \Delta$$

of Σ^b_{k+1}-formulas with free variables $\vec{c}$, then there is a multifunction f defined by a Π^b_k-PLS problem such that

$$S^1_2 \ \vdash \ Wit_{\wedge\Gamma}(u, \vec{c}) \wedge y = f(\langle u, \vec{c} \rangle) \rightarrow Wit_{\vee\Delta}(y, \vec{c}).$$

Proof is by induction on length of a free-cut free proof. Part of the proof requires finding a Π^b_k-PLS problem for determining the truth of a Π^b_k-formula.

Tools for proving the Witnessing Lemma include the following.

Π^b_k-PLS problems:

- are closed under polynomial time operations
- closed under composition
- are closed under "pseudoiteration": exponentially long, polynomial space bounded iteration that preserves a Π^b_k-property. (Needed to handle induction inferences.)
- can decide the truth of Π^b_k-properties. (Needed to handle $\forall \le$:right inferences.)

For deciding truth of Π^b_k-formulas, see next page ...

Determining truth of a Π^b_k-formula

Lemma Let $A(x) = (\exists y{\le}t)B(y,x) \in \Sigma^b_k$, with $B \in \Pi^b_{k-1}$. There is a Π^b_k-PLS problem $\mathcal{P}_A$ that explicitly determines the truth of $A(x)$ by computing

$$\mathcal{P}_A(x) = \begin{cases} \langle 0, t+1 \rangle & \text{if } \neg A(x) \\ \langle 1, i \rangle & \text{if } i{\le}t \text{ is the least value s.t. } B(i,x). \end{cases}$$

Pf. Define initial function $i(x) := \langle 0, 0 \rangle$. Define

$$N(x, \langle 0, i \rangle) = \begin{cases} \langle 0, i+1 \rangle & \text{if } \neg B(i,x),\ i \le t. \\ \langle 1, i \rangle & \text{otherwise} \end{cases}$$

$$N(x,s) = s \text{ for all other } s.$$

For $k > 1$, determining $\neg B(i,x)$ involves calling $\mathcal{P}_B$, a Π^b_{k-1}-PLS problem.

Then define $F(x, \langle 0, i \rangle) \Leftrightarrow i{\le}t+1 \land (\forall j{<}i)(\neg B(j,x))$ and
$F(x, \langle 1, i \rangle) \Leftrightarrow i{\le}t \land B(i,x) \land (\forall j{<}i)(\neg B(j,x))$.
$F(x,s)$ is false for all other s. Note $F \in \Pi^b_k$.
Cost function $c(x, \langle j, i \rangle) = t + 1 - i$.

Skolemization: A stronger version of Π_k^b-PLS witnessing

Skolemization: For a Boolean combination of formulas, create equivalent prenex form by the following procedure. Find all outermost blocks of quantifiers not yet processed. Bring out all universal ones first, then all existential ones. Repeat until in prenex form. Then Skolemize with terms.

Example: If F is $\forall y \exists z F_0(y, z)$, then (γ) is Skolemized as follows:

Recall (γ) is: $\forall x, s(F(x, s) \rightarrow F(x, N(x, s)))$.

Prenex form: $\forall x, s, y_2 \exists y_1 \forall z_1 \exists z_2 (F_0(x, s, y_1, z_1) \rightarrow F_0(x, s, y_2, z_2))$.

Skolem form: $\forall x, s, y_2, z_1 (F_0(x, s, r(x, s, y_2), z_2) \rightarrow F_0(x, s, y_1, t(x, s, y_2, z_1)))$.

where r and t are terms (over the language $0, S, +, \cdot, \dot{-}, MSP$ that allows simple fixed-length sequence coding.) r and t are polynomial time.

Defn A Π_k^b-PLS problem with Π_g^b goal is *formalized in Skolem form* provided the functions N, c, and i are defined by terms, the formulas F and G are "strict" formulas (with no sharply bounded quantifiers in front of bounded quantifiers, etc.) and provided S_2^1 proves all the conditions (α)-(δ) plus

(ϵ') $\forall x \forall s (G(x,s) \rightarrow [F(x,s) \wedge N(x,s) = s])$

(ϵ'') $\forall x \forall s ([F(x,s) \wedge N(x,s) = s] \rightarrow G(x,s))$

in Skolem form using terms as Skolem functions.

Thm If $\mathcal{P}$ is formalized in Skolem form, it is also formalized in the usual form.

Pf. This is trivial.

Exact characterization revisited, Skolemized form

Main Thm 3. Let $0 \le g \le k$ and $A(x,y) \in \Sigma^b_{g+1}$. Suppose

$$T_2^{k+1} \vdash (\forall x)(\exists y)A(x,y).$$

Then there is a Π^b_k-PLS problem $\mathcal{P}$ with Π^b_g-goal G which is formalized in Skolem form such that S^1_2 proves a Skolemization of:

$$\forall x \forall s (G(x,s) \rightarrow A(x,(s)_1)).$$

The proof of the theorem is similar to before, but much more delicate.

One potential problem. For $A \in \Pi_k^b$, $k \geq 2$, the formula

$$A \rightarrow A \wedge A$$

may not be provable in Skolem form by S_2^1.

This is needed to handle (implicit) contractions in the free-cut free T_2^i-proof.

Solution: Use $\mathcal{P}_A$, the Π_k^b-PLS problem that determines the truth of A. The formula

$$A(x) \wedge y = \mathcal{P}_A(x) \rightarrow A(x) \wedge A(x)$$

is provable in Skolem form by S_2^1.

A separation conjecture

We can set up a "generic" Skolemized Π^b_k-PLS problem with Π^b_0-goal as follows: Adjoin a new predicate symbol for G and a new predicate symbol F_0 for the sharply bounded subformula of F, and adjoin new functions symbols which are used as Skolem functions for the Π^b_k-PLS problem's defining conditions.

Then, the Skolemized definition of the Π^b_k-PLS problem can be expressed as a single $\forall\Delta^b_0$-formula.

Encoding the new functions and predicates by a single new predicate α, we can encode this $\forall\Delta^b_0$-formula as a single $\forall\Delta^b_0$-formula $\forall x \Psi(x, \alpha)$.

Consider the formula

$$\forall x \Psi(x) \to \forall x \exists y {\le} x (y = N(x,y) \wedge G(x,y)).$$

By the relativized version of the main theorems, it is provable in $T_2^{k+1}(\alpha)$.

On the other hand, by the conjectured properness of the bounded arithmetic and polynomial time hierarchies, we expect this is not provable in $T_2^k(\alpha)$.

This gives a single $\forall\Sigma_1^b(\alpha)$-formula that is known to be provable in $T_2^{k+1}(\alpha)$ but conjectured to not be provable by $T_2^k(\alpha)$.

Why formalization in S_2^1 is important (#2). Since the Skolem functions are polynomial time (in fact, are given by simple terms), they can be conservatively added to S_2^1, T_2^k, etc., and can be used freely in induction axioms. Thus, it is reasonable to allow $T_2^{k+1}(\alpha)$ use the new predicate α freely in induction axioms.

Conjectured separation for constant depth propositional proofs

By using the Paris-Wilkie translation, we get a conjectured separation for bounded depth propositional proof systems. The Paris-Wilkie translation converts existential and universal quantifiers to OR's and AND's, and atomic formulas to either *True* or *False* or, for $\alpha(t)$, to a propositional variable $p_{\underline{t}}$.

A *depth* k *Tait system* has sequents of formulas of depth k, where depth is measured by alternations of AND's and OR's. (Poly)logarithmic depth fanin at the bottom level counts as a $1/2$ depth. The $T_2^{k+1}(\alpha)$ proof of Thm 1 translates to a depth $k-1$ proof by the Paris-Wilkie translation (after several careful transformations).

The end result gives, for each $x \in \mathbb{N}$, a set Ξ_k of sequents of literals such that Ξ_k is known to have depth $k-1$ Tait-style refutations, but is conjectured to not have depth $k-1\frac{1}{2}$ depth refutations.

Some open problems

1. Can depth k propositional proofs be separated from depth $k-1$ proofs, for low depth tautologies?

2. Is there a non-uniform version of the witnessing theorems for T_2^k that will apply to depth $k-\frac{1}{2}$ propositional proofs?

3. Are there good analogues of Thms 2 or 3 for fragments of Peano arithmetic?

Advertisements:
- Problem session (Beckmann, Buss, and ? — today at 2:00.)
- Friday at 9:00am, Arnold will speak on related material?

Happy Birthday, Stan!