Provably Total Search Problems of Second-Order Bounded Arithmetic

Sam Buss

Journes sur les Arithmétiques Faibles
JAF/MAMLS, New York City
July 7, 2015

Talk outline:

1. Weak theories of bounded arithmetic.
   Provably total functions & NP-search problems.
2. Frege and extended Frege propositional proof systems.
3. Consistency search problems.
   Many-one completeness for U_2^1 and V_2^1.

Second-order Bounded Arithmetic Theories U_2^1 and V_2^1.

S_2^1 is a bounded arithmetic theory for polynomial time (P).

U_2^1 and V_2^1 are second-order bounded arithmetic theories for polynomial space (PSPACE) and exponential time $(\mathrm{EXPTIME})$.

[B, 1985]

First-order language for (non-negative) integers:

Symbols: 0, S, $+$, $\cdot$, $\#$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $\leq$.

$|x|$ is the length of the binary representation of x.

$x\#y \ := \ 2^{|x|\cdot|y|}$ — gives polynomial growth rate functions.

First-order quantifiers range over integers:

Unbounded quantifiers: $\forall x$, $\exists x$.

Bounded quantifiers: $\forall x \leq t$, $\exists x \leq t$.

Sharply bounded quantifiers: $\forall x \leq |t|$, $\exists x \leq |t|$.

Second-order quantifiers range over sets of integers.

$\forall X$, $\forall Y$. Implicitly, but not explicitly, bounded.

Classifications of bounded formulas:

- Σ_i^b, Π_i^b - Formulas with $\leq i$ alternating blocks of bounded first-order quantifiers ignoring sharply bounded quantifiers. No unbounded quantifiers. May contain second-order variables, but no second-order quantifiers.
- $\Sigma_0^{1,b}$ - Formulas with no unbounded quantifiers, and no second-order quantifiers. Equals $\bigcup_i \Sigma_i^b$.
- $\Sigma_i^{1,b}$, $\Pi_i^{1,b}$ - Formulas with i alternating blocks of second order quantifiers, ignoring first-order quantifiers. No unbounded first-order quantifiers.

Normal forms:
W.l.o.g., negations are pushed in to atomic formulas, sharply bounded quantifiers are pushed inside bounded first-order quantifiers, and bounded first-order quantifiers are pushed inside second-order quantifiers.

Complexity characterizations

- Σ^b_1 and Π^b_1 formulas express exactly NP and coNP properties.
- Σ^b_i and Π^b_i formulas express exactly properties at the i-th level of the polynomial time hierarchy.
- $\Sigma^{1,b}_1$ formulas express exactly $\mathrm{NEXPTIME}$ properties.

Γ-IND induction axioms

Γ-IND: $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x{+}1)) \rightarrow \forall x \varphi(x)$; for $\varphi \in \Gamma$.

Γ-PIND/-LIND induction axioms

Γ-PIND: $\varphi(0) \wedge \forall x(\varphi(\lfloor \frac{1}{2}x \rfloor) \rightarrow \varphi(x)) \rightarrow \forall x \varphi(x)$; for $\varphi \in \Gamma$.

Γ-LIND: $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x{+}1)) \rightarrow \forall x \varphi(|x|)$; for $\varphi \in \Gamma$.

The PIND/LIND axioms are "feasible" forms of induction.

Bounded Arithmetic Theories

"BASIC" - universal axioms giving simple properties of the function and relation symbols.

$\Sigma_0^{1,b}$-comprehension axioms

$(\forall \vec{x})(\forall \vec{X})(\exists Z)(\forall y \leq t)[y \in Z \leftrightarrow \varphi(y, \vec{x}, \vec{X})]$, for $\varphi \in \Sigma_0^{1,b}$

Definition (S_2^1)

S_2^1 is BASIC + Σ_1^b-PIND.

Definition (U_2^1)

U_2^1 is BASIC + $\Sigma_1^{1,b}$-PIND + $\Sigma_0^{1,b}$-comprehension.

Definition (V_2^1)

V_2^1 is BASIC + $\Sigma_1^{1,b}$-IND + $\Sigma_0^{1,b}$-comprehension.

Theory	Induction formulas	Induction type
S_2^1	NP-predicates (Σ_1^b)	length (LIND)/polynomial (PIND)
T_2^1	NP-predicates (Σ_1^b)	successor (IND)
S_2^k	Σ_k^p-predicates (Σ_2^b)	length (LIND)/polynomial (PIND)
T_2^k	Σ_k^p-predicates (Σ_2^b)	successor (IND)
U_2^1	NEXPTIME $(\Sigma_1^{1,b})$	length (LIND)/polynomial (PIND)
V_2^1	NEXPTIME $(\Sigma_1^{1,b})$	successor (IND)

Definability of functions

Definition

Let Γ be a class of formulas, and T be a theory. Also suppose f is a total (multi)function, $f = f(\vec{a})$ or $f = f(\vec{a}, \vec{A})$. Then f *is* Γ*-definable by* T if, there is some $\varphi \in \Gamma$ which defines the graph of f such that

$$T \vdash \forall \vec{x} \exists y \, \varphi(\vec{x}, y)$$

or (respectively),

$$T \vdash \forall \vec{x}, \vec{X} \exists y \, \varphi(\vec{x}, \vec{X}, y).$$

In the many cases, y can be made provably unique by strengthening φ.

Theory	Function definition	Function class
S_2^1	Σ_1^b-definable	polynomial time (P) [B'85]
$S_2^2 \& T_2^1$	Σ_2^b-definable	P^{NP} [B'85]
$S_2^k \& T_2^k$	Σ_k^b-definable	$\mathrm{P}^{\Sigma_k^b - 1}$ [B'85]
$S_2^2 \& T_2^1$	Σ_1^b-definable	polynomial local search (PLS) [BK'94]
$S_2^3 \& T_2^2$	Σ_1^b-definable	Colored PLS [KST'06]
U_2^1	$\Sigma_1^{1,b}$-definable	PSPACE [B'85]
V_2^1	$\Sigma_1^{1,b}$-definable	EXPTIME [B'85]

Remark: The first-order inputs $\vec{x}$ are usual inputs. Any second-order inputs $\vec{X}$ are given as oracles.

Total NP Search Problems (TFNP)

Σ^b_1-Defined Functions:

Definition

A *Total NP Search Problem* is given by a polynomial time property $\varphi(x, y)$ and a polynomial p such that

$$\forall x \, \exists y \, [|y| \leq p(|x|) \wedge \varphi(x, y)].$$

Canonical examples include PLS [JPY'88]; PPAD, PPADS [MP'91,P'94], and many others.

Let T be a true theory, say U^1_2 or V^1_2.
Any Σ^b_1 definable function of T is a total NP search problem.
And is trivially in P^{NP} and hence PSPACE.

Goal: Characterize the provably total NP search problems of U^1_2 and V^1_2.

Definition (Many-one reduction)

Suppose that $(\forall x)(\exists y \leq t)\varphi(y,x)$ and $(\forall x)(\exists y \leq s)\psi(y,x)$ specify NP search problems, denoted $y = Q_\varphi(x)$ and $y = Q_\psi(x)$. A *many-one reduction* from Q_φ to Q_ψ consists of a pair of polynomial time functions g and h such that

$$\text{whenever } y = Q_\psi(g(x)), \text{ we have } h(y,x) = Q_\varphi(x).$$

We write $Q_\varphi \leq_m Q_\psi$ to denote that there is a many-one reduction from Q_φ to Q_ψ.

Definition

A theory proves that $Q_\varphi \leq_m Q_\psi$ provided that it proves

$$(\forall x)(\forall y)[y = Q_\psi(g(x)) \rightarrow h(y,x) = Q_\varphi(x)]$$

for some explicitly polynomial time functions g and h.

When second-order inputs are present, instead use:

Definition (Many-one reduction, relativized case)

Suppose that $(\forall x)(\exists y \leq t)\varphi(y, x, X)$ and $(\forall x)(\exists y \leq s)\psi(y, x, X)$ specify NP search problems, denoted $y = Q_\varphi(x, X)$ and $y = Q_\psi(x, X)$. A *many-one reduction* from Q_φ to Q_ψ consists of polynomial time functions α, g and h such that

whenever $y = Q_\psi(g(x), \alpha^X(x, \cdot))$, we have $h(y, x, X) = Q_\varphi(x, X)$.

We write $Q_\varphi \leq_m Q_\psi$ to denote that there is a many-one reduction from Q_φ to Q_ψ.

The following are known to be provably total, and many-one complete, NP-search problems of U_2^1 and V_2^1.

Theory	Many-one complete NP Search problem	
V_2^1	LI, Local Improvement	[KNT'11]
V_2^1	$\mathrm{LI}_{\log}$, LI with $O(\log n)$ rounds	[BB'14]
U_2^1	LLI, Linear LI	[BB'14]
U_2^1	$\mathrm{LLI}_{\log}$	[KNT'11]
V_2^1	RLI, Rectangular LI	[KNT'11]
V_2^1	$\mathrm{RLI}_{\log}$	[BB'14]
U_2^1	RLI_1	[BB'14]

This talk:

The consistency search problems for Frege and extended Frege proof systems are many-one complete for U_2^1 and V_2^1.

Part II. Frege proofs

Frege proofs are the usual "textbook" proof systems for propositional logic, using modus ponens as their only rule of inference.

Connectives: $\wedge$, $\vee$, $\neg$, and $\rightarrow$.

Modus ponens: $\dfrac{A \quad A \rightarrow B}{B}$

Axioms: Finite set of axiom schemes, e.g.: $A \wedge B \rightarrow A$

Defn: Proof *size* is the number of symbols in the proof.

Frege proofs and Extended Frege proofs

Frege proofs are the usual "textbook" proof systems for propositional logic, using modus ponens as their only rule of inference.

Connectives: $\wedge$, $\vee$, $\neg$, and $\rightarrow$.

Modus ponens: $\dfrac{A \quad A \rightarrow B}{B}$

Axioms: Finite set of axiom schemes, e.g.: $A \wedge B \rightarrow A$

Extended Frege proofs allow also the *extension axiom*, which lets a new variable x abbreviate a formula A:

$$x \leftrightarrow A$$

Defn: Proof *size* is still the number of symbols in the proof.

Open Question

Do Frege proofs (quasi)polynomially simulate extended Frege proofs?
That is, can every extended Frege proof of size n be transformed into a Frege proof of size $p(n))$ or $2^{p(\log n)}$, for some polynomial p?

Intuition: Extended Frege proofs can reason about Boolean circuits, Frege proofs about Boolean formulas.

It is generally conjectured that Boolean circuits can require exponential size to express as Boolean formulas.

By analogy, it is generally conjected Frege proofs can require exponential size to simulate extended Frege proofs.

For an example, consider the Pigeonhole Principle ...

The pigeonhole principle as a propositional tautology

Let $[n] = \{0, \ldots, n-1\}$.
Let i's range over members of $[n+1]$ and j's range over $[n]$.

$$\mathrm{Tot}_i^n \;:=\; \bigvee_{j\in[n]} x_{i,j}. \quad \text{“Total at } i\text{”}$$

$$\mathrm{Inj}_j^n \;:=\; \bigwedge_{0\le i_1<i_2\le n} \neg(x_{i_1,j} \wedge x_{i_2,j}). \quad \text{“Injective at } j\text{”}$$

$$\mathrm{PHP}_n^{n+1} \;:=\; \neg\Big(\bigwedge_{i\in[n+1]} \mathrm{Tot}_i^n \wedge \bigwedge_{j\in[n]} \mathrm{Inj}_j^n \Big).$$

PHP_n^{n+1} is a tautology.

Cook-Reckhow's $e\mathcal{F}$ proof of PHP_n^{n+1}

Code the graph of $f : [n+1] \to [n]$ with variables $x_{i,j}$ indicating that $f(i) = j$.

$\mathrm{PHP}_n^{n+1}(\vec{x})$: "$f$ is not both total and injective"

Use **extension** to introduce new variables

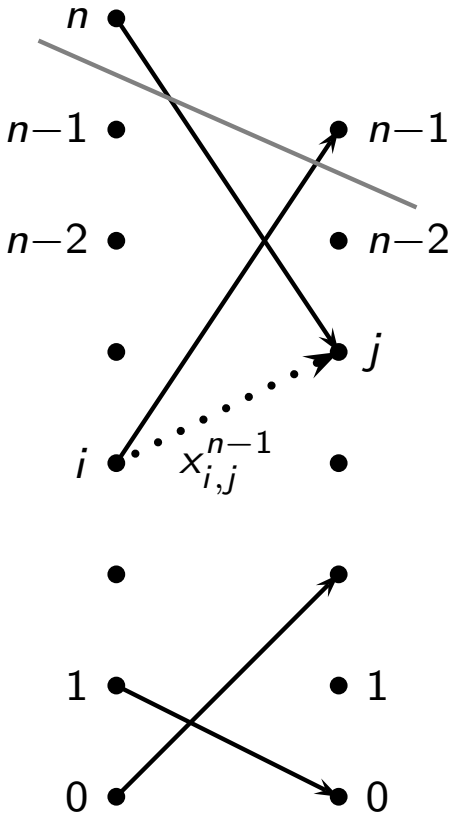
$$x_{i,j}^{\ell-1} \leftrightarrow x_{i,j}^{\ell} \vee (x_{i,\ell-1}^{\ell} \wedge x_{\ell,j}^{\ell}).$$

for $i \leq \ell$, $j < \ell$; where $x_{i,j}^{n} \leftrightarrow x_{i,j}$.

Prove, for each ℓ that

$$\neg PHP_{\ell}^{\ell+1}(\vec{x}^{\ell}) \to \neg PHP_{\ell-1}^{\ell}(\vec{x}^{\ell-1}).$$

Finally derive $\mathrm{PHP}_n^{n+1}(\vec{x})$ from $\mathrm{PHP}_1^2(\vec{x}^1)$. $\square$



Alternate construction of $e\mathcal{F}$ proofs of PHP_n^{n+1} via S_2^1

Theorem

$S_2^1 \vdash \forall x$, x does not code a set of pairs defining a function violating the pigeonhole principle".
Or: $S_2^1(f) \vdash (\forall x)\neg(f : [|x|+1] \xrightarrow{1-1} [|x|])$.

Definition

Let $\varphi(x)$ be a polynomial time property, and $n \geq 1$.
Then $[\![\varphi]\!]_n$ is a polynomial-size propositional formula which is a tautology iff $\mathbb{N} \models (\forall x < 2^n)\varphi(x)$

Theorem (Cook'75)

If $\varphi(x)$ is a polynomial time property, and $S_2^1 \vdash (\forall x)\varphi(x)$, then the tautologies $[\![\varphi]\!]_n$ have polynomial size extended Frege proofs.

Frege proof consistency as a total NP search problem

Code an (exponentially long) Frege proof P with an oracle X. The value $X(i)$ gives the i-th symbol of P.

Search problem: Show that X does not code a valid Frege proof of a contradiction.

Frege Consistency Search Problem - *Informal*

Input: Second-order X and first-order x.
Output: A set of values $i_1, \ldots, i_\ell$ so that the values $X(i_1), \ldots, X(i_\ell)$ show X does not code a valid Frege proof of a contradiction.

Since the Frege proof is exponentially long, it may contain exponentially long formulas.

However, ℓ should be polynomially bounded by $|x|$: Frege proofs need to be carefully encoded to allow this.

Frege proofs encoded by oracle $X(i)$ contain:

- Fully parenthesized formulas, terminated by commas.
- Each parenthesis has a pointer to
  a. Its matching parenthesis, and
  b. The principal connective inside the parentheses.
- Each comma has the type of inference for the previous formula, plus pointers to the formulas used as hypotheses.

This allows any syntactic error in the Frege proof to be identified by constantly many positions $i_1, \ldots, i_\ell$ in X.

Theorem

The Frege Consistency Search Problem *is provably total in* U^1_2.

Theorem (Beckmann-B, i.p.)

The Frege Consistency Search Problem *is* U^1_2*-provably many-one complete for the Total NP Search Problems of* U^1_2.

Theorem

The Extended Frege Consistency Search Problem *is provably total in* V^1_2.

Theorem (Beckmann-B, i.p.)

The Extended Frege Consistency Search Problem *is* V^1_2*-provably many-one complete for the Total NP Search Problems of* V^1_2.

Theorem

The Frege Consistency Search Problem is provably total in U_2^1.

Proof Sketch. Argue inside U_2^1.

Suppose X is a Frege proof of a contradiction of length x.

W.l.o.g., there are no variables in the Frege proof. (!)

Define, using a Δ_1^b-predicate, the PSPACE property that the formula at position i in X is true.

"PSPACE" means $\mathrm{SPACE}(|x|^{O(1)})$ relative to the oracle X.

Prove by induction on i that every formula in the proof coded by X is true.

□

Theorem (Beckmann-B, i.p.)

The Frege Consistency Search Problem is U^1_2-provably many-one complete for the Total NP Search Problems of U^1_2.

Proof Sketch

Suppose $U^1_2 \vdash (\exists y \leq a)(\varphi(y, a, A)$, where φ is a sharply bounded formula.

Construct a Frege proof in stages. The Frege proof is variable-free and is coded by a second-order predicate which is polynomial time relative to A.

First stage: For each value of $y \leq a$:
If $\varphi(y, a, A)$ is false, give a Frege proof of $\neg[\![\varphi(y, a, A)]\!]$.
This a true variable-free formula.
However, if $\varphi(y, a, A)$ is true, include the formula $\neg[\![\varphi(y, a, A)]\!]$ and (incorrectly) label it as being an axiom.

Use a special case of the new-style witnessing theorem for U_2^1:

Theorem (New-style witnessing for U_2^1, Beckmann-B '14)

Suppose U_2^1 proves $(\exists y)\varphi(y, a, A)$ for φ a Σ_1^b-formula. Then there is a polynomial space oracle Turing machine M such that S_2^1 proves "If Y encodes a complete computation of $M^A(a)$, then $\varphi(out(Y), a, A)$ is true."

By the witnessing theorem for S_2^1, it follows that there is a polynomial time procedure $f^{A,Y}(a)$, which provably in S_2^1, given a, A, Y, either finds a mistake in Y's encoding of $M^A(a)$'s computation or produces a value $y = out(Y)$ satisfying $\varphi(y, a, A)$.

Second phase of Frege proof: Use the Nepomnjaščiĭ-Savitch divide-and-conquer method to give exponential size formulas $\psi_{t,p}$ which define the entire computation of M. ($\psi_{t,p}$ gives the p-th bit of the configuration at time t.)

Third phase of Frege proof: For each possible settings of Cook-Levin extension variables defining a complete run of $f^{A,Y}(a)$, prove that one of the following holds

a. Some Cook-Levin extension variable is incorrect.
b. Some query to A or M gives an incorrect answer.
c. It finds a place where the definition of the $\psi_{t,p}$'s are incorrect.
d. It finds a value y such that $\varphi(y, a, A)$ holds, and hence $[\![\varphi(y, a, A)]\!]$ holds.

Fourth phase of Frege proof: Put all these together to derive a contradiction ($\perp$). QED

Separating Frege and extended Frege with combinatorial principles?

There has been sustained effort to find combinatorial tautologies which might exponentially separate Frege and extended Frege proof lengths:

Tautology	Poly size $e\mathcal{F}$ proof	Quasipoly size $\mathcal{F}$ proof
PHP_n^{n+1}	Cook-Reckhow '79	B '87
Ramsey's Theorem	Krishnamurthy '85	Pudlák '92
Frankl's Theorem	Bonet-B-Pitassi '95	Aisenberg-Bonet-B '15
$AB = I \Rightarrow BA = I$	Soltys-Kulinicz '01	Hruběs-Tzameret '13
RLI_k, $k \geq 2$	Beckmann-B '14	open
Kneser-Lovasz	Istrate-Crãciun '14	A-B-B-C-I '15
Truncated Tucker_1^n	A-B-B-C-I 'ip	open

It is unlikely, but if V_2^1 is Σ_1^b-conservative over U_2^1, then Frege proofs quasipolynomially simulate extnded Frege proofs.

A-B-B-C-I is Aisenberg-Bonet-B-Crãciun-Istrate

Thank You!