Weak Arithmetics & Unrelatized Independence Results

Chris Pollett
San Jose State University

LC 2003

Outline

1. Motivations
2. Bounded Arithmetic
3. Independence via definability
   (NP vs. coNP)
4. Independence via padding
   a. a success story
   b. towards something stronger
5. Conclusion

Motivations

1. Want to find stronger and stronger fragments of arithmetic that cannot prove $NP = coNP$
2. Eventually, hope this leads to a proof of $NP \neq coNP$
3. Want to understand how much mathematics is needed to prove Matiyasevich's Theorem

Bounded Arithmetic

Will work with one of the following languages:

$L_1 = \{0, S, +, \cdot, \dot{-}, \&, \lfloor \frac{x}{2^i} \rfloor, |x|, \leq\}$

$$x \dot{-} y := \begin{cases} x - y & \text{if } x > y \\ 0 \end{cases}$$

$x \& y :=$ bitwise and of x & y

$L_2 = L_1 \cup \{2^{|x||y|}\}$

$L_{exp} = L_2 \cup \{2^x\}$

Kind of formulas will consider:

E_i-formula: $\underbrace{\exists y_1 \leq t_1 \forall \leq \cdots}_{i\text{-alternations}}$ open

if ∞ means $\cup_i E_i$

(U_i if begin with $\forall y_1 \leq t_1$)

Σ_i^b-formula: An E_{i+1}-formula whose innermost quantifier is bdd by a term of form $|t|$. (Π_i^b if U_{i+1})

Facts: Bdd L_1-formula = LINH (W)

$E_i(L_2) = \Sigma_i^b(L_2) = \Sigma_i^p$ (K-H, J-M)

i.e. $\Sigma_1^b(L_2) = NP$

Independence via Definability

Let f be such that its graph, A_f, is $\Sigma_1^b(L_2)$, i.e., in NP, and

$\mathbb{N} \models \forall x \exists y \le t\, A_f(x,y)$, and

T cannot Σ_1^b-define f:

$T \nvdash \forall x \exists y \le t\, A_f'(x,y)$, for A_f', Σ_1^b graph of f.

By excluded middle:

$$T \vdash \exists y [(\exists z \le t\, A_f(x,z) \wedge z = y) \vee ((\neg \exists z \le t\, A_f(x,z)) \wedge y = t+1)]$$

Inside $[\cdots]$ can be made into a Σ_2^b-formula in T's want to consider.

So T can Σ_2^b-define f.

But if T proves every $\Sigma_1^b(L_2)$ formula is $\Pi_1^b(L_2)$. i.e., NP = coNP, then T could prove above def is a Σ_1^b definition.

$\therefore T \nvdash NP = coNP$

Choices of T argument works for

T	Function not definable
$\Sigma_1^b-L^3IND$	$\lfloor x/3 \rfloor$ $\lfloor x/9 \rfloor$ 4 lengths [P] [B-R]
TAC^0	Parity [P-P] [C-T]
$TAC^0[p]$	MOD_q [P-P]

Can give a slightly stronger argument to show these theories cannot prove PH↓.

Lower Bounds on Matiyasevich Thm

G-D & Kaye have shown
$E_1(L_{exp})$-IND can prove
Matiyasevich Thm.
(Σ_1-sets $= \exists_1$-sets)

<u>Thm</u> (W?) If a bdd theory $T \supseteq BASIC(L_1) \vdash$ Matiyasevich Thm then in its language $E_1 = U_1$. Hence, $NP = coNP$, if this language is L_2.

<u>proof</u>
Parikh's Theorems says if T is above & φ is bdd then if $T \vdash \exists y \varphi$ then $T \vdash \exists y \leq t \varphi$ for some term t.
Suppose $T \vdash$ M's Thm. Let $A \in U_1$
By M's Thm,

$$T \vdash A \Leftrightarrow \exists \vec{y}\ p = q$$ where q, p are polynomials.

Using pairing,

$$T \vdash A \Leftrightarrow \exists y'\ t_1 = t_2.$$

So $T \vdash A \Rightarrow \exists y' t_1 = t_2$. Can rewrite apply Parikh to get

$$T \vdash A \Rightarrow \exists y' \leq t\ t_1 = t_2.$$

Lower Bounds M's Thm cont'd

So as $\exists y' \leq t\ t_1 = t_2 \to \exists y'\, t_1 = t_2$

get $T \vdash A \Leftrightarrow \underbrace{\exists y' \leq t\ t_1 = t_2}_{E_1}$ $\boxed{/\!/}$

<u>Corollary</u> Σ_1^b-L^3IND, TAC^0, $TAC^0[p]$ cannot prove Matiyasevich Theorem.

Note: above methods only work if T's Σ_1^b-definable $f^{\underline{ns}}$ known to be different from NP. For most interesting T's this is open.

So need better methods...

Independence via Padding

Lemma (*) $\exists$ an $\Sigma_1^b(L_1)$ - formula U_1 such that for any $\Sigma_1^b(L_2)$ - formula $A(x)$ Note the 1

$$BASIC(L_2) \vdash U_1(e_A, x, t_A(x)) \Leftrightarrow A(x).$$

proof idea: BASIC(L_2) can do Gödel coding for terms as only finite number of operations. Can check $\omega = x \# y$ with

$$|\omega| = S|x||y| \wedge \omega = \left\lfloor \frac{z^{|\omega|}}{2} \right\rfloor .$$

$\boxed{}$

Clote & Takeuti '95 had a theory TLS $\supset$ BASIC(L_2) for reasoning about LOGSPACE:

i.e., the predicates TLS could prove equivalent to both Σ_1^b & Π_1^b formulas (Δ_1^b - predicates) were exactly LOGSPACE.

TLS can prove consistency of Frege proof so considered "reasonably strong."

Thm $TLS \nvdash \Sigma_1^b(L_1) = \Pi_1^b(L_1)$

proof: First need following claim:

Claim: $\Sigma_1^b(L_1) = \Pi_1^b(L_1) \Rightarrow LOGSPACE \neq \Sigma_1^b(L_2)$.

proof of claim: By Nepomnjascij's Thm $LOGSPACE \subseteq LINH = \bigcup_i \Sigma_i^b(L_1)$. So if $\Sigma_1^b(L_1) = \Pi_1^b(L_1)$ and $LOGSPACE = \Sigma_1^b(L_2)$. Then $\Pi_1^b(L_1) = \Sigma_1^b(L_2)$. However, can show that there is a fixed t such that for all A in $\Pi_1^b(L_1)$ $\neg U_1(e_{\neg A}, x, t(x)) \Leftrightarrow A$. So $U_1(x, x, t(x)) \notin \Pi_1^b(L_1)$. $\boxtimes$

Suppose $TLS \vdash \Sigma_1^b(L_1) = \Pi_1^b(L_1)$
Let $A \in \Sigma_1^b(L_2)$. So

$$TLS \vdash U_1(e_A, x, z) \Leftrightarrow \underset{\Pi_1^b(L_1)}{U_1'}(e_A, x, z)$$

Padding. $\therefore TLS \vdash A \Leftrightarrow U_1'(e_A, x, t_A(x)) \in \Pi_1^b(L_2)$

$\therefore TLS \vdash \Sigma_1^b(L_1) = \Pi_1^b(L_1) \rightarrow \underbrace{\Sigma_1^b(L_2) = \Pi_1^b(L_2)}_{\Delta_1^b \text{ in } TLS = LOGSPACE}$

$\Rightarrow\Leftarrow$

How powerful is this padding idea?

Def$^{\underline{n}}$ Let $\Sigma^b_{\infty,2}(open_{exp})$ be the formulas with matrix from L_{exp} but all quantifiers are bounded by L_2-terms.

Fact: $\Sigma^b_{\infty,2}(open_{exp})$ predicates are the $\Sigma^b_{\infty,2}$ predicates $=$ PH.
(can show $open_{exp}$ predicate can be checked in p-time)

Def$^{\underline{n}}$ Let S_2, exp be sequent calculus system (1) $BASIC_{exp}$, (2) cuts only on $\Sigma^b_{\infty,2}(open_{exp})$ formulas, & with

(3) $\Sigma^b_{\infty,2}(open_{exp})$-IND: $\dfrac{A(x), \Gamma \to \Delta, A(Sx)}{A(0), \Gamma \to \Delta, A(t)}$

all formulas must $\Sigma^b_{\infty,2}(open_{exp})$.

Remark: restriction on (2) & (3) to prevent getting $I\Delta_0 + exp$

Thm The predicates $S_{2,exp}$ proves equivalent to both a $E_{1,exp}(\Sigma^b_{\infty,2}(open_{exp}))$ & $U_{1,exp}(\Sigma^b_{\infty,2}(open_{exp}))$ formula ($\nabla_{1,exp}$) are precisely the $\Sigma^b_{\infty,2}(open_{exp})$ predicates.

proof Witnessing argument.

Cor S_2,exp does not prove Matiyasevich Thm.

proof If could then $E_{1,exp} = U_{1,exp}$ $\Rightarrow E_{1,exp} = \Sigma_{\infty,exp}$. By above then

$$\nabla_{1,exp} = E_{1,exp} = \Sigma_{\infty,exp} = \Sigma^b_{\infty,2}(open_{exp}) = PH \quad \rightarrow\leftarrow$$

elementary

Remark S_2 might still prove Matiyasevich in its language.

<u>**Lemma**</u> For any $A \in E_{1,exp}$ there is a $U_A \in E_{1,2}$ & a L_{exp} term t_A such that

$$BASIC_{exp} \vdash U_A(a, t(a)) \Leftrightarrow A(a)$$

<u>proof:</u> similar to before.

Note: by cut-elim for $BASIC_{exp}$ know above provable in $S_{2,exp}$.

Does $S_{2,exp}$ prove

$$\underbrace{E_{1,2}}_{NP} = \underbrace{U_{1,2}}_{coNP} \rightarrow E_{1,exp} = U_{1,exp}\ ?$$

If could then as $\nabla_{1,exp} \neq \Sigma^b_{\infty,exp}$ we would have $S_{2,exp} \nvdash NP = coNP$.

Problem: Our restriction on cut prevents us from doing the term substitution we'd like to do to show this.

Def$^{\underline{n}}$ Call a derivation in $S_{2,exp}$ of $\Gamma(a) \to \Delta(a)$ uniform if can substitute any t in L_{exp} for a in this proof & get a valid $S_{2,exp}$ proof.

Thm $S_{2,exp}$ does not prove $NP = coNP$ using only uniform proofs.

proof Suppose did. Let $A \in E_{1,exp}$.
Then $S_{2,exp} \vdash A \Leftrightarrow U_A(a, t_A)$.
& $S_{2,exp} \vdash U_A(a,z) \Leftrightarrow U'_A(a,z)$

$U_{1,2}$

This proof is uniform so

$$S_{2,exp} \vdash A(a) \Leftrightarrow U(a,t_A) \Leftrightarrow U'(a,t_A).$$

so $S_{2,exp} \vdash E_{1,exp} = U_{1,exp}$ $\Rightarrow\Leftarrow$

$\blacksquare$

Cor $IOpen_{exp} \nvdash NP = coNP$.

Conclusion

Can try to use second order theories like V_2^1 rather than $S_{2,exp}$ but run into similar difficulties.

So question is: can one find a strong system for which this kind of argument works? Or is padding actually hard to prove in weak systems?

Can one still get this proof to work via some kind of easy case hard case argument?

Can we say anything about provability of Matiyasevich in S_2 from its non provability in $S_{2,exp}$?