

Weak Arithmetics  
ε  
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:

$$L_1 = \{0, s, +, \cdot, \div, \lfloor \frac{x}{2} \rfloor, |x|, \leq\}$$

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

$$x \& y := \text{bitwise and of } x \text{ \& } y$$

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

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

Kind of formulas will consider:

$E_i$ -formula:  $\exists y, st, \forall z \dots$  open

$\uparrow$   
if  $\infty$   
means  $\cup_i E_i$

$\underbrace{\hspace{10em}}$   
i-alternations

( $\cup_i$  if begin with  $\forall y, st$ )

$\Sigma_i^b$ -formula: An  $E_{i+1}$ -formula whose innermost quantifier is bdd by a term of form  $H$ . ( $\Pi_i^b$  if  $\cup_{i+1}$ )

Facts: Bdd  $L_1$ -formula = LINT (W)

$$E_i(L_2) = \Sigma_i^b(L_2) = \Sigma_i^P \quad \begin{matrix} (K-H) \\ (J-M) \end{matrix}$$

$$-4 - \text{ie } \Sigma_0^b(L_2) = NP$$

# Independence via Definability

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

$\mathbb{N} \models \forall x \exists y \leq t A_f(x, y)$ , and  
 $T$  cannot  $\Sigma_1^b$ -define  $f$ :

$T \not\vdash \forall x \exists y \leq t A_f(x, y)$ , for  $A_f$ ,  $\Sigma_1^b$  is graph of  $f$ .

By excluded middle:

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

Inside [...] can be made into a  $\Sigma_2^b$ -formula in  $T$ 's want to consider.

So  $T$  can  $\Sigma_2^b$ -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  $\Sigma_1^b$  definition.

$\therefore T \not\vdash NP = coNP$

# Choices of T argument works for

T

Function not  
definable

$\Sigma_1^b - L^3 \text{IND}$

$\lfloor x/3 \rfloor$   $\lfloor x/5 \rfloor$

$[P]$   $[B-R]$

4 lengths  $\rightarrow$

$\text{TAC}^0$

Parity

$[P-P]$   $[C-T]$

$\text{TAC}^0 [P]$

$\text{MOD}_9$   
 $[P-P]$

---

Can give a slightly stronger  
argument to show these theories  
cannot prove  $\text{PTh}$ .

# Lower Bounds on Matiyasevich Thm

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

( $\Sigma_1$ -sets =  $\exists_1$ -sets)

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

proof

Parikh's Theorem says if  $T$  is a bdd  
&  $\varphi$  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,

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

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

$$-7- \quad T \vdash A \rightarrow \exists y' \leq t t_1 = t_2.$$

## Lower Bounds M's Thm cont'd

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

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

Corollary  $\Sigma_1^b$ -LIND,  $TAC^0$ ,  
 $TAC^0[P]$  cannot prove  
Matiyasevich Theorem.

Note: above methods only  
work if  $T$ 's  $\Sigma_1^b$ -definable fns  
known to be different from NP.  
For most interesting  $T$ 's this is  
open.

So need better methods...

# Independence via Padding

Lemma (\*)  $\exists$  an  $\Sigma_1^b$ -formula  $\psi$  such that for any  $\Sigma_1^b(L_2)$ -formula  $A(x)$   
 $\text{BASIC}(L_2) \vdash \psi(e_A, x, t_A(x)) \leftrightarrow A(x)$ . Note the 1

proof idea:  $\text{BASIC}(L_2)$  can do Gödel coding for terms as only finite number of operations. Can check  $w = x \# y$  with  $|w| = S|x||y| \wedge w = \lfloor \frac{2^{|w|}}{2} \rfloor$ .  $\square$

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

i.e., the predicates  $\text{TLS}$  could prove equivalent to both  $\Sigma_1^b$  &  $\Pi_1^b$  formulas ( $\Delta_1^b$ -predicates) were exactly LOGSPACE.

$\text{TLS}$  can prove consistency of Frege proof so considered "reasonably strong."

Thm  $TLS \not\vdash \Sigma_1^b(L_1) = \Pi_1^b(L_1)$

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 Nepomnjaschij's Thm  
 $LOGSPACE \subseteq LINH = U_1 \Sigma_1^b(L_1)$ .

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  $\Pi_1^b(L_1)$   
 $\neg U_1(e_A, x, t(x)) \Leftrightarrow A$ . So

$U_1(x, x, t(x)) \notin \Pi_1^b(L_1)$ .  $\square$

Suppose  $TLS \vdash \Sigma_1^b(L_1) = \Pi_1^b(L_1)$

Let  $A \in \Sigma_1^b(L_2)$ . So

$TLS \vdash U_1(e_A, x, z) \Leftrightarrow U'_1(e_A, x, z)$

Adding  $\therefore TLS \vdash A \Leftrightarrow U'_1(e_A, x, t_A(x)) \in \Pi_1^b(L_2)$

[  $\therefore TLS \vdash \Sigma_1^b(L_1) = \Pi_1^b(L_1) \rightarrow \Sigma_1^b(L_2) = \Pi_1^b(L_2)$

$\Rightarrow \Leftarrow$

$\Delta_1^b$  in  $TLS = LOGSPACE$

How powerful is this padding idea?

Def<sup>n</sup> Let  $\Sigma_{\infty,2}^b(\text{open}_{\text{exp}})$  be the formulas with matrix from  $L_{\text{exp}}$  but all quantifiers are bounded by  $L_2$ -terms.

Fact:  $\Sigma_{\infty,2}^b(\text{open}_{\text{exp}})$  predicates are the  $\Sigma_{\infty,2}^b$  predicates  $\equiv$  PH.

(can show  $\text{open}_{\text{exp}}$  predicate can be checked in  $p$ -time)

Def<sup>n</sup> Let  $S_{2,\text{exp}}$  be sequent calculus system ① BASIC<sub>exp</sub>, ② cuts only on  $\Sigma_{\infty,2}^b(\text{open}_{\text{exp}})$  formulas, & with

③  $\Sigma_{\infty,2}^b(\text{open}_{\text{exp}})$ -IND:  $\frac{A(x), \Gamma \rightarrow \Delta, A(Sx)}{A(0), \Gamma \rightarrow \Delta, A(t)}$

all formulas must  $\in \Sigma_{\infty,2}^b(\text{open}_{\text{exp}})$ .

Remark: restriction on ② & ③ to prevent getting  $IND_{\text{exp}}$

Thm The predicates  $S_{2, \text{exp}}$  proves equivalent to both a  $E_{1, \text{exp}}(\Sigma_{\infty, 2}^b(\text{open}_{\text{exp}}))$  &  $U_{1, \text{exp}}(\Sigma_{\infty, 2}^b(\text{open}_{\text{exp}}))$  formula ( $\nabla_{1, \text{exp}}$ ) are precisely the  $\Sigma_{\infty, 2}^b(\text{open}_{\text{exp}})$  predicates.


proof Witnessing argument.

Cor  $S_{2, \text{exp}}$  does not prove Matiyasevich Thm.

proof If could then  $E_{1, \text{exp}} = U_{1, \text{exp}}$

$\Rightarrow E_{1, \text{exp}} = \Sigma_{\infty, \text{exp}}$ . By above

then  $\nabla_{1, \text{exp}} = E_{1, \text{exp}} = \Sigma_{\infty, \text{exp}} \stackrel{?}{\leq} \text{elementary}$   
 $\Sigma_{\infty, 2}^b(\text{open}_{\text{exp}}) = \text{PH} \not\leq$

Remark  $S_2$  might still prove Matiyasevich in its language. 

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

$BASIC_{exp} \vdash U_A(a, t(a)) \leftrightarrow A(a)$   
proof: similar to before.

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

Does  $S_{2,exp}$  prove

$E_{1,2} = \underbrace{U_{1,2}}_{NP} \rightarrow E_{1,exp} = \underbrace{U_{1,exp}}_{coNP}?$   
If could then as  $\Delta_{1,exp} \neq \Sigma_{\infty,exp}^b$   
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.