Nepomnjascij's Theorem and Independence Results in Bounded Arithmetic

Chris Pollett
CS Dept.
SJSU
Nov 22/'02

Outline

(1) Motivation

(2) Bounded Arimetic

(3) Dumb theories T such that
$T \nvdash NP = coNP$

(4) Towards stronger theories
  (a) Lower bound on MRDP
  (b) Lower bound on $\Sigma^b_{1,1} = \Pi^b_{1,1}$

(5) Conclusion

Motivation

- Want to exhibit any reasonable T such that $T \nvdash P = NP$ or $T \nvdash NP = coNP$

- Given we can show such a T find stronger and stronger T' such $T' \nvdash NP = coNP$

- Maybe get enough insight to actually show $NP \neq coNP$

Bounded Arithmetic

Will work with one of following languages:

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

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

Bounded arithmetic for this talk is the study of theories in one of these languages all of whose axiom schemas are over bounded formulas.

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

(U_i begin with $\forall y_1 \le t_1$)

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

Bdd L_1 - formulas = LINH

$\Sigma_i^b(L_2) = \Sigma_i^p$ (K-H) i.e. $\Sigma_1^b(L_2)$ = NP

Bounded Arithmetic & Complexity

<u>Def$^{\underline{n}}$</u> T can Ψ-define a function f if $T \vdash \forall x \exists y\, A_f(x,y)$ where $A_f \in \Psi$ and $\mathbb{N} \models A_f(x, f(x))$

Many complexity classes have characterizations in terms of definability in some bounded arithmetic theory:

Theory	Σ^b_1-def f$^{\underline{ns}}$
(Buss) S^1_2	P – p-time
	$\cup\vert$
(Allen, Tak, Clote) R^1_2	NC : poly size, uniform poly log depth circuits.
	$\cup\vert$
(Clote, Tak) TLS	L : Log space
	$\cup\vert$
(C, T, J, P) C^0_2	TC^0 : poly-size, uniform constant depth threshold circuits
	$\cup\times$
(C, T) $TAC^0[p]$	$AC^0[p]$: p-size, uniform, constant depth, $\wedge, \vee, \neg$, mod p circuits unbdd fan-in

Dumb Theories cannot prove NP = coNP

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

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

T cannot Σ_1^b-define f.

Note 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 Σ_2^b in T's want to consider.

So T can Σ_2^b-define f.

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

But assumed T does not Σ_1^b-def f.

Dumb Theories

- Above argument can be used to show $TAC^0[p] \not\vdash NP = coNP$ (Pollett)
- Lends itself to any new classes complexity theorist can prove $\neq NP$

$TAC^0[p]$ in a language without '$\cdot$' but with $x \cdot 2^{|y|}$

Strongest results for language with '$\cdot$'

[R-B] -0? $\quad BASIC + \Sigma_1^b - L^3 IND \leftarrow$ Pollett '00 had 4

$$\frac{A(x), \Gamma \to \Delta, A(sx)}{A(0), \Gamma \to \Delta, A(|||t|||)}$$

$A \in \Sigma_1^b$

Note: a slightly different argument can be used to show these theories cannot prove PHP

Towards Stronger Theories

It would be nice to have indepedence results which don't first rely on knowing some class is different from NP.

[Fortnow '00] has lately been considering time space trade-offs as a way to show $L \neq NP$.

These are based on an old result of Nepomnjascij. Can these techniques be applied in the bounded arithmetic setting?

Ans: Yes. Will use to show lower bounds on MRDP and on $\Sigma^b_1(L) = \Pi^b_1(L)$ (roughly NLIN

Matiyasevich's Theorem (MRDP)

sets of form:

$$\{\vec{x} \mid \exists \vec{y}\ p(\vec{x},\vec{y}) = q(\vec{x},\vec{y})\}$$

p, q polynomials over $\mathbb{N}$
are exactly the Σ_1-sets.

Known to be provable in
$I\Sigma_1 + \exp$ (Kaye, G-D).

Will show that at least one
of $I\Delta_0$ or TLS cannot
prove this theorem

induction
on bdd G_1-formulas

A theory for logspace

TLS (Proposed by Clote & Takeuti '95
Simplified using J-P '00)
(Theory below Σ_1^b-conservative over theirs)

in L_2 → ① BASIC + open-LIND

A open in $\dfrac{A(x), \Gamma \to \Delta, A(Sx)}{A(0), \Gamma \to \Delta, A(|t|)}$

② Σ_1^b-REPL

$$\frac{\Gamma \to \Delta, \forall x \le |s|\, \exists y \le t\, A(x, y, \vec{a})}{\Gamma \to \Delta, \exists w < bd(t, |s|)\, \forall x \le |s|\, A(x, \dot{\beta}(x, |t^*|, t, w))}$$

$A \in \Sigma_1^b$

③ Σ_1^b-WSN

$$\frac{b \le |k(j, \vec{a})| \to \exists! x \le |k(j, \vec{a})|\, A(j, \vec{a}, b, x)}{\exists w \le bd(|k|, |l|)\, \forall j < |l|\; A(j, \vec{a}, \hat{\beta}(j, |k^*|, w), \hat{\beta}(j+1, |k^*|, w))}$$

$A \in \Sigma_1^b$,

<u>Thm</u> (C-T '95) The Δ_1^b-predicates of TLS are precisely LOGSPACE. (Predicates TLS proves both Σ_1^b & Π_1^b)

A complexity tool

This research was motivated by Fortnow '97 research on time-space trade-offs for SAT using Nepomnjascij's Thm.

Thm If $\Sigma_i^b(L_1) = \Pi_i^b(L_1)$ then $LOGSPACE \neq NP$

To prove need:

① Nepomnjascij's Thm

$$LOGSPACE \subseteq \bigcup_k TimeSpace(n^k, n^{1-\epsilon})$$
$$\subseteq LINH$$

② $\Sigma_i^b(L_1) \neq \Pi_i^b(L_2)$

Idea: There is a $U(e_\varphi, x) \in \Sigma_i^b(L_2)$ such that $\forall \varphi \in \Sigma_i^b(L_1)$, $\varphi \equiv U(e_\varphi, x)$

Consider $\neg U(x,x) \in \Pi_i^b(L_2)$.

Proof:

Suppose $\Sigma_i^b(L_1) = \Pi_i^b(L_1) \overset{\text{by ①}}{\supseteq} LOGSPACE = NP$.

Then as LOGSPACE closed under complement. we get $\Sigma_i^b(L_1) \supseteq \Pi_i^b(L_2)$

A contradiction.

Matiyasevich Lower Bound

Note: G&D then Kaye have shown if 2^x in language then BASIC + E_1 - induction proves Matiyasevich Thm.

<u>Thm</u> ⊛⊛ At least one of the theories $I\Delta_0$ and TLS does not prove Matiyasevich Thm.

Will need:

① Parikh's Thm ('71)

Let T be $I\Delta_0$ or TLS. Let φ be a bounded formula.
Then if $T \vdash \exists y\, \varphi$ then there is a term t in the language such that
$T \vdash \exists y \le t\, \varphi$.

One more lemma is needed to prove Thm ⊛⊛ ...

Lemma ⊛⊛⊗

① If $I\Delta_0 \vdash$ M's Thm then $\Sigma_1^b(L_1) = \Pi_1^b(L_1)$

② If TLS $\vdash$ M's Thm then LOGSPACE $= \Sigma_1^b(L_2) = \Pi_1^b(L_2)$

$\Sigma_1^b(L_2) = NP$, $\Pi_1^b(L_2) = coNP$

<u>pr</u> Both proved in same way. So prove ①

Suppose $I\Delta_0 \vdash$ M's Thm. Let $A \in \Pi_1^b$. By M's Thm,

$I\Delta_0 \vdash A \equiv \exists \vec{y}\; p = q$ where p, q polynomials over $\mathbb{N}$.

Since terms in lang for pair can get

$I\Delta_0 \vdash A \equiv \exists y'\; t_1 = t_2$

In particular, $I\Delta_0 \vdash A \to \exists y'\; t_1 = t_2$

can rewrite apply Parikh to get:

$I\Delta_0 \vdash A \to \exists y' \leq t\; t_1 = t_2$.

But $\exists y' \leq t\; t_1 = t_2 \Rightarrow \exists y'\; t_1 = t_2$

So $I\Delta_0 \vdash A \equiv \exists y' \leq t\; t_1 = t_2 \in \Sigma_1^b(L_1)$ $\boxed{\text{Lem}}$

<u>pf</u> Thm ⊛⊛

Follow from Thm ⊛ & above $\boxed{\text{Lem}}$

Another Application of Thm (*)

Thm TLS does not prove
$$\Sigma_1^b(L_1) = \Pi_1^b(L_1).$$

Lemma $\exists$ an L_1 (note 1) -formula U_i such that for any $\Sigma_i^b(L_2)$-formula $A(x)$,
$TLS \vdash U_i(e_A, x, t_A(x)) \Leftrightarrow A(x)$.

Pf Idea: can ck $\omega = x \# y$ with
$$|\omega| = s|x||y| \wedge \omega = \left\lfloor \frac{2^{|\omega|}}{2} \right\rfloor$$

pf Thm: Suffices to show
$TLS \vdash \Sigma_1^b(L_1) = \Pi_1^b(L_1) \Rightarrow \Sigma_1^b(L_2) = \Pi_1^b(L_2)$
since this implies $TLS \vdash \text{LOGSPACE} = \Delta_1^b = \Sigma_1^b(L_2) = NP$
contradicting Thm (*).
Let $A \in \Sigma_1^b(L_2)$. So $TLS \vdash U_1(e_A, x, z) \equiv U_1'(e_A, x, z)$.
$\Pi_1^b(L_1)$

$\therefore TLS \vdash A \Leftrightarrow U_1'(e_A, x, t_A(x)) \in \Pi_1^b(L_2)$
$\Rightarrow \Leftarrow$ $\boxed{}$

Conclusion

1. Can add a symbol for $2^{|x|\,\|y\|}$ to L_1 & L_2. Then bdd L_1-formulas the quasi linear time hierarchy. Above results still work.

2. Much stronger results might be possible depending on the formalizability of results like

$$NP = coNP \Rightarrow NE = coNE$$