

Nepomnjascij's Theorem
and
Independence Results
in
Bounded Arithmetic

Chris Pollett
CS Dept.
SJSU
Nov 22/'02

Outline

- ① Motivation
- ② Bounded Arithmetic
- ③ Dumb theories T such that
 $T \not\vdash NP = coNP$
- ④ Towards stronger theories
 - Ⓐ Lower bound on MRDP
 - Ⓑ Lower bound on $\Sigma_{1,1}^b = \Pi_{1,1}^b$
- ⑤ Conclusion



Motivation

- Want to exhibit any reasonable T such that $T \neq P = NP$ or $T \neq NP = coNP$
- Given we can show such a T find stronger and stronger T' such $T' \neq NP = coNP$
- Maybe get enough insight to actually show $NP \neq coNP$

Bounded Arithmetic

Will work with one of following languages:

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

$$L_2 = L_1 \cup \{2^{|\alpha||\beta|}\}$$

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 $\exists y_1 \leq t, \forall \dots$ open

i -alternations
(U_i begin with $\forall y, st, \dots$)

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

$$\Sigma_i^b(L_2) = \Sigma_i^p(K-H) \quad \text{i.e.} \quad \Sigma_i^b(L_2) = NP$$

Bounded Arithmetic & Complexity

Defⁿ T can Ψ -define a function f if $T \vdash \forall x \exists y A_f(x, y)$ where $A_f \in \Psi$ and $N \models A_f(x, f(x))$

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

Theory

Σ_1^b -def fns

(Buss) S_2^1

P - p-time

(Allen Tak clove) R_2^1

UI : poly size, uniform
 NC : poly log depth circuits.

(clove tak) TLS

L : Log space

(C, T, J, P) C_2^0

UI
 TC^0 : poly-size, uniform
 UT : constant depth, threshold circuits

(E, T) $TAC^0[p]$

$AC^0[p]$: p-size, uniform, constant depth, $\wedge, \vee, \neg, \text{mod } p$ 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

$$IN = \forall x \exists y \text{ st } A_f(x, y), \text{ and}$$

T cannot Σ_1^b -define f .

Note by excluded middle:

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

Inside [...] can be made Σ_2^b in T' 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 $TAC^0[FP] \neq NP_{coNP}$ (Pollett)
- Lends itself to any new classes complexity theorist can prove $\neq NP$

$TAC^0[FP]$ in a language without $'\cdot'$
but with $x \cdot 2^{191}$

Strongest results for language with $'\cdot'$

$[R-B]_{-0?}$ BASIC + Σ_1^b - L^3 IND ← Pollett '00 had 4

$$A(x), \Pi \rightarrow \Delta, A(sx)$$

$$A(0), \Pi \rightarrow \Delta, A(\text{ITEM})$$
$$A \in \Sigma_1^b$$

Note: a slightly different argument can be used to show those theories cannot prove PH

Towards Stronger Theories

It would be nice to have independence 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 $\Sigma_1^b(L) = \Pi_1^b(L)$ (roughly $NLIN$ ~~with~~)

Matiyasevich's Theorem (MRDP)

Sets of form:

$$\Sigma_1^1 \mid \exists \vec{y} \quad p(\vec{x}, \vec{y}) = q(\vec{x}, \vec{y}) \exists$$

p, q polynomials over \mathbb{N}
are exactly the Σ_1^1 -sets.

Known to be provable in
 $IE_1 + \text{exp}$ (Kaye, G-D).

Will show that at least one
of ID_0 or TLS cannot
prove this theorem

induction
on bdd Σ_1^1 -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 $\xrightarrow{\text{①}}$ BASIC + open-LIND
 $\xrightarrow{\text{②}}$ Σ_1^b -REPL

A open in $\frac{\widehat{A}(x), \Gamma \rightarrow \Delta, A(sx)}{A(0), \Gamma \rightarrow \Delta, A(1)}$

$$\frac{\Gamma \rightarrow \Delta, \forall x \leq |s| \exists y \leq t A(x, y, \vec{a})}{\Gamma \rightarrow \Delta, \exists w \leq b \wedge (t, |s|) \forall x \leq |s| A(x, \hat{\beta}(x, t^q, t, w))}$$

$A \in \Sigma_1^b$

③ Σ_1^b -WSN

$$b \leq |K(j, \vec{a})| \rightarrow \exists ! x \leq |K(j, \vec{a})| A(j, \vec{a}, b, x)$$

$$\exists w \leq |K(k, \vec{a})| \forall j \in |t| A(j, \vec{a}, \hat{\beta}(j, |K^q|, w), \hat{\beta}(j+1, |K^q|, w))$$

$A \in \Sigma_1^b$,

Thm (C-T '95) The Δ_1^b -predicates of TLS are precisely LOGSPACE. (Predicates TLS proves to be $\Sigma_1^b \in \Pi_1^b$)

A complexity tool

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

Thm ① IF $\Sigma_i^b(L_1) = \Pi_i^b(L_1)$
then $\text{LOGSPACE} \neq \text{NP}$

To prove need:

① Nepomnjaschij's Thm
 $\text{LOGSPACE} \subseteq \bigcup_k \text{TimeSpace}(n^k, n^{1-\epsilon})$
 $\subseteq \text{LINH}$

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 $\Sigma_i^b(L_1) = \Pi_i^b(L_1) \stackrel{\text{by ①}}{\subseteq} \text{LOGSPACE} = \text{NP}$

Then as LOGSPACE closed under complement.

we get $\Sigma_i^b(L_1)^c \supseteq \Pi_i^b(L_2)$

A contradiction.

Matiyasevich Lower Bound

Note: Gödel then Kaye have shown if \exists^x in language then BASIC + E_1 - induction proves Matiyasevich Thm.

Thm ^(*) At least one of the theories ID_0 and TLS does not prove Matiyasevich Thm.

Will need:

① Parikh's Thm ('71)

Let T be ID_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 $T \vdash \exists y \leq t \varphi$.

One more lemma is needed to prove Thm ^(*)...