Bounded Versions of HTP & NP = co-NP

C. Pollett
Oberwolfach
2003

Outline

1. Motivation
2. Implications of Gaifman & Dimitricopoulus
3. Theories $I\mathcal{E}_{n,n+1}$
4. Independence Results
5. Conclusion

Motivation

Try to show $T \nvdash NP = coNP$ for stronger & stronger T until see why $NP \neq coNP$.

Work in weak arithmetics.

In these systems, provability of $NP = coNP$ closely connected with HTP.

<u>Ex</u> (Folklore) Wilkie? If $S_2 \vdash MRDP$ then $S_2 \vdash NP = coNP$

Gaifman & Dimitricopoulos '82

Showed $I\Delta_0(2^x) \vdash MRDP$

Q + induction on bounded formulas in language with 2^x

Seems to imply if $T \supseteq I\Delta_0(2^x)$ cons. then $T \vdash MRDP$.

Not entirely...

What was shown was that $I\Delta_0(2^x)$ can prove any formula of form:

$\exists \vec{y}$ bdd formula

is equivalent to a formula

$\exists \vec{y}\ P(\vec{x},\vec{y}) = Q(\vec{x},\vec{y})$ But...

(G-D cont'd)

The terms bounding the bounded quantifiers always exponential in size.

<u>Parikh's Thm</u> (holds any theory considered today)

$I\Delta_0(2^x) \vdash \exists y\, A(a,y)$

then $I\Delta_0(2^x) \vdash \exists y \le t\, A(a,y)$

t term in language.

So $I\Delta_0(2^x)$ cannot reason about superexponential growth fns!

If expand language to include such a fn but keep induction somehow restricted so can't reason about it, maybe can't eliminate the bounded quantifiers in proof of MRDP

System $I\mathcal{E}_{3,4}$

Let

$L_4 := \{ \leq, 0, S, +, \cdot, \lfloor x/2 \rfloor, \dot{-}, \&_2, 2^{|x|\|y|}, \ast,$

limited subtraction

bitwise and

$|x|, |x|^*, 2_x \}$

$\lceil \log_2(x+1) \rceil$

$2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \} x$ of height x

$|2_x|^* = x$

Observations

① Pairing and projection of blocks of bits $\beta_{|x|}(i, w)$ can be defined as ~~terms~~.

② $L_4^- := L_4 \setminus \{2^x, 2_x\}$ p-computable operations $\quad E_{1,4}^-$-sets $=$ NP

$L_3 := L_4 \setminus \{2^x\}$

$\exists x$ open in L_4^-

$\text{open}_4 :=$ open formulas L_4

③ $\Delta_{0,3} :=$ bdd formulas L_3

Language

$\Delta_{0,3}$-sets $= \mathcal{E}_3$-sets (Grzegorczyk Hierachy)

$\Delta_{0,4}$-sets $= \mathcal{E}_4$-sets

Known $\mathcal{E}_3$-sets $\subsetneq \mathcal{E}_4$-sets

Some notation

Let C be a class of formulas

$\Delta_{0,k}(C)$ – a formula of form

$$Q y_1 \le t_1 \cdots Q y_n \le t_n \, \varphi$$

$\exists$ or $\forall$

where $t_i \in L_k$, $\varphi \in C$.

$E_{1,k}(C)$ – a formula of form

$$\exists y_1 \le t_1 \, \varphi \qquad t_1 \in L_k, \ \varphi \in C.$$

$U_{1,k}(C)$ – a formula of form

$$\forall y_1 \le t_1 \, \varphi \qquad t_1 \in L_k, \ \varphi \in C.$$

Note add $=$ for L_4.
i.e. $\Delta_{0,4}(C)$.

By G-D know $I\Delta_{0,4} \vdash MRDP$

But consider

$I\mathcal{E}_{3,4}$ which is BASIC open ax together with

allowed in L_4 term

$$\frac{A(a,\vec{a}';\vec{b}),\Gamma \to \Delta, A(Sa,\vec{a}',\vec{b})}{A(0,\vec{a}';\vec{b}),\Gamma \to \Delta, A(t,\vec{a}',\vec{b})}$$

A, Γ, Δ in $\Delta_{0,3}(\mathrm{open}_4)$, $t \in L_3$

Cut is restricted to $\Delta_{0,3}(\text{open}_4)$ formulas.

$$(\text{cut}) \quad \frac{\Gamma \to \Delta, A \quad A, \Gamma \to \Delta}{\Gamma \to \Delta}$$

Def^n^ A predicate is $\nabla_{1,4}[\vec{b}]$ in $I\mathcal{E}_{3,4}$ if its provably equivalent in $I\mathcal{E}_{3,4}$ to a $E_{1,4}(\Delta_{0,3}(\text{open}_4))[\vec{b}]$-formula and to a $U_{1,4}(\Delta_{0,3}(\text{open}_4))[\vec{b}]$ formula. Here $\vec{b}$ are the free variables which appear in $L_4 \setminus L_3$ -terms.

Thm ⊛ The $\nabla_{1,4}[\vec{b}]$ predicates of $I\mathcal{E}_{3,4}$ are precisely the $\Delta_{0,3}(\text{open}_4)[\vec{b}]$ predicates. When $[\vec{b}]$ empty set the $\Delta_{0,3}$ (hence $\mathcal{E}_3$) predicates.

pf By a Buss style witnessing argument

Lemma

If $I\mathcal{E}_{3,4} \vdash$ MRDP then
$I\mathcal{E}_{3,4} \vdash E_{1,4} = U_{1,4} = \Delta_{0,4}$

<u>pf</u> Suppose $I\mathcal{E}_{3,4} \vdash$ MRDP.
Let $A \in U_{1,4}$. By MRDP,
$I\mathcal{E}_{3,4} \vdash A \equiv \exists \vec{y}\ p = q$ where
p, q polynomials over $\mathbb{N}$.

Since pairing in language
$I\mathcal{E}_{3,4} \vdash A \equiv \exists y'\ t_1 = t_2$
In particular,
$I\mathcal{E}_{3,4} \vdash A \Rightarrow \exists y'\ t_1 = t_2$
Can rewrite apply Parikh's Thm
to get
$I\mathcal{E}_{3,4} \vdash A \rightarrow \exists y' \leq t\ t_1 = t_2$
But $\exists y' \leq t\ t_1 = t_2 \Rightarrow \exists y'\ t_1 = t_2$
So $I\Delta_0 \vdash A \equiv \exists y' \leq t\ t_1 = t_2$
$\in E_{1,4}$

Thm $I\mathcal{E}_{3,4} \nvdash$ MRDP

pf Thm (*) $\Rightarrow \nabla^{[\,]}_{1,4}$-sets of $I\mathcal{E}_{3,4}$ are $\mathcal{E}_3 = \Delta_{0,3}$-sets.

Lemma (**) $\Rightarrow \nabla^{[\,]}_{1,4}$-sets of $I\mathcal{E}_{3,4}$ are $\mathcal{E}_4 = \Delta_{0,4}$-sets.

Know $\mathcal{E}_3 \subsetneq \mathcal{E}_4$.

Another application . . .

Lemma: For any $E_{1,4}$-formula $A(a)$, there is an $E^-_{1,4}$-formula $U_A(a,z)$ such that there is an L_4^--term for which

$$I\mathcal{E}_{3,4} \vdash A(a) \equiv U_A(a, t_A(a))$$

pf sketch.

Let $K_\neg(x) := 1 \dot- x$, $K_\vee(x,y) := x+y$

$K_\le(x,y) := K_\neg(y \dot- x)$.

Rewrite A in form $\exists y \le t_1\ t_2(x,y) = 0$

Consider

$$\exists w \le z\ \exists y_1 \le z \bigwedge_{j=e}^{|e|} \varphi(e_j, x, y_1)$$

$\leftarrow$ w codes step j or $\le$ on x, y

w/ pairing $E_{1,4}$ $\langle \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

Can verify

$\beta_{|k|}(j, \ulcorner t_m \urcorner) = \ulcorner z^x \urcorner \supset$

$|\beta_{|k|}(j,w)| = s(\beta_{|k|}(j-1,w))$

notice did not use z^x $\wedge$ no other bits on

similar for z_x.

$\boxed{/}$

<u>Thm</u> $I\Sigma_{3,4} \nvdash NP = coNP$ (almost)

<u>pf</u> Suffices to show

$I\Sigma_{3,4} \vdash E^-_{1,4} = U^-_{1,4} \Rightarrow E_{1,4} = U^-_{1,4} = \Delta_{0,3}$ "$= \mathcal{E}_3$"

As said before these NP-sets,

And by Thm ⓢ, $\nabla^{[\,]}_{4,4}$-sets of $I\Sigma_{3,4}$ are the $\Delta_{0,3}$-sets $= \mathcal{E}_3$

Let $A \in E_{1,4}$. So $I\Sigma_{3,4}$ proves

$U_A(x,z) \equiv U'_A(x,z)$

$E^-_{3,1}$ $\quad$ $U^-_{1,4}$

So $I\Sigma_{3,4} \vdash A \equiv U'_A(x, t_A(x))$

$E_{1,4}$ $\quad$ $U_{1,4}$

$\boxed{/}$

Conclusion

Technique seems to generalize to finite levels of Grzegorczyk Hierarchy. After that don't know.

Thm (***) says something about non-uniform a proof $NP \neq coNP$ must be in theories weaker than $I\mathcal{E}_{3,4}$