Bounded Versions of HTP
\[ \frac{1}{3} \]
\[ NP = co-NP \]
Outline

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

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

Work in weak arithmetics.

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

Ex? (Folklore) if $S_2 \vdash MRDP$
then $S_2 \vdash NP = coNP$
Gaifman & Dimitricopoulos '12

Showed $\Delta_0 (2^x) \vdash_{\text{MRDP}}$

$\Delta_0 (2^x) \vdash_{\text{MRDP}}$

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

Seems to imply if $T \equiv \Delta_0 (2^x) \text{ cons}$ then $T \vdash \text{MRDP}$.

Not entirely...

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

$\exists y \; \text{bad formula is equivalent to a formula}$

$\exists y \; p(x, y) = q(x, y)$

But...

-3-
The terms bounding the bounded quantifiers always exponential in size.

Parikh's Thm (holds any theory considered today)

\[ \mathcal{A}_0(z^x) \vdash \exists z A(a, y) \]

than \[ I \mathcal{A}_0(z^x) \vdash \exists y \text{st} A(a, g) \]

+ term in language.

So \[ I \mathcal{A}_0(z^x) \] cannot reason about superexponential growth funs!

If expand language to include such a \( \mathcal{L} \) but keep induction somehow restricted so can't reason about it; maybe can't eliminate the bounded quantifiers in proof of MRDP

---

4
System $I^E_{3,4}$

Let
\[ L_4^+ = \{ 0, \delta, \delta^2, +, \cdot \}, \]
\[ L_4^- = \{ 0, \delta, \delta^2, - \}, \]
\[ L_5 = \{ \lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^5 \}. \]

Observations

1. Pairing and projection of blocks of bits $\beta_{x_0}(i, \omega)$ can be defined as terms.

2. $L_4^- = L_4 \setminus \{ z \in \mathbb{Z}^x, z \neq 5 \}$, p-computable operations $E_{i, \omega}$, $\omega$-sets $\in$ NP

3. $L_3 = L_4 \setminus \{ z \in \mathbb{Z}^x \}$, $\exists x$ open in $L_4$

$\Delta_0, \delta$ language

$\Delta_0, \delta$ - sets = $E_\delta$ - sets

$\Delta_0, \gamma$ - sets = $E_\gamma$ - sets

Known $E_\delta$ - sets $\subseteq E_\gamma$ - sets

(Grzegoreczyk Hierarchy)
Some notation

Let $C$ be a class of formulas

$\Delta_{0,1}(C)$ - a formula of form

$Qy_1 \leq t_1 \ldots Qy_n \leq t_n \; \forall \; \varphi \in C.$

$E_{1,1}(C)$ - a formula of form

$\exists y_1 \leq t \; \forall \; \varphi \in C.$

$U_{1,1}(C)$ - a formula of form

$\forall y_1 \leq t \; \forall \; \varphi \in C.$

Note: add $\exists$ for $\Sigma_1^0,
\forall$ for $\Pi_1^0,
\exists$ for $\Sigma_2^0,
\forall$ for $\Pi_2^0.
\forall$ for $\Sigma_3^0,
\exists$ for $\Pi_3^0.

By G-D know $I\Delta_{0,1}$ MRDP

But consider

$I\Sigma_3^0$ which is basic openax

together with

$A(c, z, y, B), \; \Gamma \Rightarrow \Delta, A(s, c, z, w)$

in $\Gamma$ form

$A(c, z, y, B), \; \Gamma \Rightarrow \Delta, A(t, z, w),
A, \Gamma, \Delta \in \Delta_{0,3}(\text{open}), \; t \in \mathbb{L}.$
Cut is restricted to $\Delta_{0,3}(\text{open}_4)$
formulas.

\[ \Gamma \Rightarrow \Delta, \alpha \quad \alpha, \pi \Rightarrow \Delta \]

\[ \Rightarrow \]

**Def** A predicate $\varphi$ in $\forall, \exists^2$ is $\text{IE}_{3,4}$-equivalent to a $E_{1,4}(\Delta_{0,3}(\text{open}_4)) [\beta]$-formula and to a $U_{1,4}(\Delta_{0,3}(\text{open}_4)) [\beta]$-formula. Here $\beta$ are the free variables which appear in $\beta_4 \setminus \beta_3$-terms.

**Thm** The $\forall, \exists^2 [\beta]$ predicates of $\text{IE}_{3,4}$ are precisely the $\Delta_{0,3}(\text{open}_4)[\beta]$ predicates. When $[\beta]$ empty set the $\Delta_{0,3}$ (hence $E_3$) predicates.

**PF** By a Buss style witnessing argument
Lemma 0

\begin{align*}
&\text{If } IE_{3,4} \vdash \text{MRDP then} \\
&IE_{3,4} \vdash E_{1,4} = U_{1,4} = \Delta_{0,4} \\
&\text{Suppose } IE_{3,4} \vdash \text{MRDP.}
\end{align*}

Let \( A \in U_{1,4} \). By MRDP,

\[ IE_{3,4} \vdash A = \exists y \rho = q \text{ where } p, q \text{ polynomials over } \mathbb{N}. \]

Since pairing in language

\[ IE_{3,4} \vdash A = \exists y' t_1 = t_2 \]

In particular,

\[ IE_{3,4} \vdash A \Rightarrow \exists y' t_1 = t_2 \]

Can rewrite apply Parikh's Thm. to get

\[ IE_{3,4} \vdash A \Rightarrow \exists y' \leq t_1 = t_2 \]

But \( \exists y' \leq t_1 = t_2 \Rightarrow \exists y' t_1 = t_2 \)

So \[ IE_{3,4} \vdash A \Rightarrow \exists y' \leq t_1 = t_2 \]

\[ IE_{3,4} \vdash A \Rightarrow \exists y' t_1 = t_2 \]

\[ E_{1,4} \]

\[ \Delta_{0,4} \]

\[ \rho = q \]

\[ p, q \text{ polynomials over } \mathbb{N}. \]
Thm $I_{E_3,4} \vdash \text{MRDP}$

pf. Thm $\Theta \Rightarrow \exists \cup_i, \exists^i$-sets of $I_{E_3,4}$ are $E_3 = \Delta_{0,3}$-sets.

Lemma $\Theta \Rightarrow \exists \cup_i, \exists^i$-sets of $I_{E_3,4}$

are $E_4 = \Delta_{0,4}$-sets.

Know $E_3 \subseteq E_4$.

Another application...  

Lemma: For any $E_{1,1}$-formula $A(a)$, there is an $E_{1,4}$-formula $U_A(a,x)$ such that for which $I_{E_{3,4}} \vdash A(a) \equiv U_A(a, t_1(a))$

Proof sketch:

Let $K_0(x) := 1-x$, $K_r(x,y) := x+y$, $K_E(x,y) := K_0(y-x)$.

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

Consider $

\exists \bar{w} \leq 2 \exists \bar{x}, \bar{y}, \bar{z} \exists x, y, z$
Let \( \Pi \in \text{NP} \), so \( \Pi \Rightarrow \text{A} \). We wish to show

\[
\text{A} \in \text{NP} \Rightarrow \text{NP} = \text{coNP}.
\]

As said before, by Theorem 4.19, there are \( \Pi \in \text{A} \) s.t.

\[
\forall x \in \text{NP} \Rightarrow \text{NP} = \text{coNP}.
\]

Similarly for \( \text{coNP} \), notice that.

Can verify that \( \Pi \in \text{NP} \) for \( \text{NP} \).
Conclusion

Technique seems to generalize to finite levels of Grzegorzyck hierarchy. After that don't know.

Thm says something about non-uniform a proof NPs coNP must be in theories weaker than I<3,4