Independence of the MIN principle from the PHP principle

Mykyta Narusevych

September 14, 2024

Charles University, Prague

Bounded Arithmetic

Σ_i^b-formulas

- L_{S_2} is a finite language containing
  - constants $0, 1$
  - unary $\lfloor \frac{x}{2} \rfloor, |x| (:= \lfloor \log_2 x \rfloor + 1 \text{ in } \mathbb{N})$
  - binary $x + y, x \cdot y, x \# y (:= 2^{|x| \cdot |y|} \text{ in } \mathbb{N})$
  - binary $x \leq y$
- (occurrence of) quantifier $Qx \leq t(\bar{y})$ is called bounded, $Qx \leq |t(\bar{y})|$ is called sharply bounded
- $\Sigma_0^b = \Pi_0^b$ is the class of sharply bounded formulas
- Σ_{i+1}^b is a closure of Π_i^b over $\wedge, \vee, Qx \leq |t(\bar{y})|$ and $\exists x \leq t(\bar{y})$
- Π_{i+1}^b is a closure of Σ_i^b over $\wedge, \vee, Qx \leq |t(\bar{y})|$ and $\forall x \leq t(\bar{y})$

Theories T_2^i

- The base theory BASIC consists of 32 axioms describing basic properties of L_{S_2}

1. $a \leq b \rightarrow a \leq b + 1$
2. $a \neq a + 1$
3. $0 \leq a$
4. $(a \leq b \wedge a \neq b) \rightarrow a + 1 \leq b$
5. $a \neq 0 \rightarrow 2a \neq 0$
6. $a \leq b \vee b \leq a$
7. $(a \leq b \wedge b \leq a) \rightarrow a = b$
8. $(a \leq b \wedge b \leq c) \rightarrow a \leq c$
9. $|0| = 0$
10. $a \neq 0 \rightarrow (|2a| = |a| + 1 \wedge |2a + 1| = |a| + 1)$
11. $|1| = 1$
12. $a \leq b \rightarrow |a| \leq |b|$
13. $|a\#b| = |a| \cdot |b| + 1$
14. $0\#a = 1$
15. $a \neq 0 \rightarrow (1\#(2a) = 2(1\#a) \wedge 1\#(2a + 1) = 2(1\#a))$
16. $a\#b = b\#a$
17. $|a| = |b| \rightarrow a\#c = b\#c$
18. $|a| = |b| + |c| \rightarrow a\#d = (b\#d) \cdot (c\#d)$
19. $a \leq a + b$
20. $(a \leq b \wedge a \neq b) \rightarrow (2a + 1 \leq 2b \wedge 2a + 1 \neq 2b)$
21. $a + b = b + a$
22. $a + 0 = a$
23. $a + (b + 1) = (a + b) + 1$
24. $(a + b) + c = a + (b + c)$
25. $a + b \leq a + c \rightarrow b \leq c$
26. $a \cdot 0 = 0$
27. $a \cdot (b + 1) = a \cdot b + a$
28. $a \cdot b = b \cdot a$
29. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
30. $1 \leq a \rightarrow ((a \cdot b \leq a \cdot c) \equiv (b \leq c))$
31. $a \neq 0 \rightarrow |a| = |\lfloor (a/2) \rfloor| + 1$
32. $a = \lfloor (b/2) \rfloor \equiv (2a = b \vee 2a + 1 = b)$

- T_2^i is BASIC augmeneted by induction scheme for Σ_i^b-formulas

Relativized theories $T^i_2(R)$

- $L_{S_2}(R)$ is an extension of L_{S_2} by a symbol R
- Classes $\Sigma^b_i(R)$ and $\Pi^b_i(R)$ are defined analogously to the unrelativized case
- Theory $T^i_2(R)$ is BASIC augmented by induction scheme for $\Sigma^b_i(R)$-formulas (no specific axioms for R)

Combinatorial principles

ontoPHP and injPHP principles

For binary R, injPHP(R) is

$$\exists a \neq b < p \, \exists c < h \, (R(a,b) \wedge R(a,c))$$

$$\vee$$

$$\exists a < p \, \exists b \neq c < h \, (R(a,b) \wedge R(a,c))$$

$$\vee$$

$$\exists a < p \, \forall b < h \, (\neg R(a,b)),$$

and ontoPHP(R) is

$$\text{injPHP}(R)$$

$$\vee$$

$$\exists b < h \, \forall a < p \, (\neg R(a,b)),$$

where p and h are free variables in both formulas above.

Ajtai's theorem

The crucial classical result concerning independence in bounded arithmetic is the following statement, originally established by Ajtai, and later improved by Krajíček, Pudlák, Woods and Pitassi, Beame, Impagliazzo

$$T_2(R) \nvdash \mathrm{ontoPHP}(R)$$

MIN principle

For binary $\prec$, MIN($\prec$) is

$$\exists a < n\,(a \prec a)$$
$$\vee$$
$$\exists a \neq b < n\,(a \not\prec b \wedge b \not\prec a)$$
$$\vee$$
$$\exists a, b, c < n\,(a \prec b \wedge b \prec c \wedge a \not\prec c)$$
$$\vee$$
$$\exists a < n\,\forall b \neq a < n\,(a \prec b),$$

where n is a free variable in the above formula.

Application of Theorem of Riis

Applying Theorem of Riis one can immediately derive

$$T_2^1(\prec) \nvdash \mathsf{MIN}(\prec),$$

although this time it holds that

$$T_2^2(\prec) \vdash \mathsf{MIN}(\prec)$$

Our results

MIN vs. PHP

Theorem

$$T^1_2(\prec) + injPHP(\Delta^b_1(\prec)) \nvdash MIN(\prec)$$

- $\Delta^b_1(\prec)$ stands for the class of binary formulas naturally corresponding to p-time
- proof is model theoretic, we start with a countable non-standard model of true arithmetic and then expand it by suitably interpreting $\prec$ relation
- The construction can be viewed in terms of simple pebble game, or as forcing

Proof sketch

- Start with non-standard model $\mathbb{M}$ and pick non-standard number n
- Consider a game between Alice, Bob and Cecile which take turn in building a chain on $[0, \cdots, n)$, each extending the previous by at most $|n|^C$-elements for some standard C
- Alice tries to make sure that the resulting $\prec$ is a total ordering on $[0, \cdots, n)$ with no minimal element
- Bob tries to make sure that the resulting expansion satisfies $T^1_2(\prec)$
- Cecile tries to make sure that the resulting expansion satisfies $\mathrm{injPHP}(\Delta^b_1(\prec))$

Forcing

- The proof can be naturally cast as a forcing argument in the framework of partially definable forcing of Atserias and Müller
- In fact, the poset is exactly the one used by argument of Riis (i.e. poset of small conditions)
- The biggest difference is that we provide additional combinatorial analysis of the construction

Extensions

The same argument can be used to give additional independence results

- $T^1_2(\prec) + \mathrm{injPHP}(\Delta^b_1(\prec)) \nvdash \mathrm{DLO}(\prec)$
- $T^1_2(\prec) + \mathrm{injPHP}(\Delta^b_1(\prec)) \nvdash \mathrm{DiscLO}(\prec)$
- $T^1_2(E) + \mathrm{injPHP}(\Delta^b_1(E)) \nvdash \mathrm{TOUR}(E)$
- $T^1_2(f) + \mathrm{injPHP}(\Delta^b_1(f)) \nvdash \mathrm{dWPHP}(f)$

What's next

- Undestand the difference between ontoPHP(R) and injPHP(R), in particualr is it possible to prove $T^1_2(R) + \text{ontoPHP}(\Delta^b_1(R)) \nvdash \text{injPHP}(R)$ using techniques developed in the current work
- Extract natural Riis-like criterion for $T^1_2(R) + \text{injPHP}(\Delta^b_1(R))$
- Derive unreducibility between corresponding TFNP and TFΣ^p_2 classes using the framework of typical forcing of Müller
- Adapt methods to the following version of the pigeonhole principle

$$\exists a \neq b < p\, \exists c < h\, (R(a,b) \wedge R(a,c))$$
$$\vee$$
$$\exists a < p\, \forall b < h\, (\neg R(a,b))$$