FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

DOCTORAL THESIS

Erfan Khaniki

(Im)possibilty results in Proof Complexity and Arithmetic

Department of Algebra

Supervisor of the doctoral thesis:	Prof. RNDr. Pavel Pudlák, DrSc
Study programme:	Mathematics
Study branch:	Algebra, Number Theory and Mathematical Logic

Prague 2023

I declare that I carried out this doctoral thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....

Author's signature

Acknowledgment. First and foremost, I would like to thank Pavel Pudlák to whom I am incredibly indebted, for his guidance, his support, the discussions that we have had, and all the things I have learned from him.

I also wish to thank Mohammad Ardeshir, Jan Krajíček, and Rasoul Ramezanian from whom I learned a lot.

I am grateful to Amirhossein Akbar Tabatabai, Sam Buss, Jan Bydžovský, Susanna de Rezende, Lukáš Folwarczný, Svyatoslav Gryaznov, Pavel Hrubeš, Pavel Hubácek, Farzad Jafarrahmani, Emil Jeřábek, Fedor Part, Fedor Pakhomov, Jan Pich, Ahmadreza Rahimi, Rahul Santhanam, Mohsen Shahriari, Navid Talebanfard, Neil Thapen, and Albert Visser for their help and also for interesting discussions that we have had about various fun and serious topics.

I want to express my gratitude to my friends who made my Ph.D. journey enjoyable: Susanna de Rezende, Lukáš Folwarczný, Babak Ghanbari, Farzad Jafarrahmani, Mohammad Latifian, Jan Pich, Ahmadreza Rahimi, and Mohsen Shahriari.

Last but not least, I would like to thank my parents for their unconditional love and support throughout my whole life.

My research was supported by the GACR grant 19-27871X, the institute grant RVO: 67985840, and the Specific university research projects SVV-2020-260589 and SVV-2023-260721.

Title: (Im)possibilty results in Proof Complexity and Arithmetic

Author: Erfan Khaniki

Department: Department of Algebra

Supervisor: Prof. RNDr. Pavel Pudlák, DrSc, Institute of Mathematics, Academy of Sciences of the Czech Republic

Abstract: We study various problems in proof complexity, bounded arithmetic, and intuitionistic arithmetic. We focus on topics such as lower bounds for different proof systems, connections between proof complexity generators and models of arithmetic, jump operators in proof complexity, and the non-locality of certain Kripke models of Heyting arithmetic.

Keywords: Proof complexity, Lower bounds, Bounded arithmetic, Independence, Heyting arithmetic, Kripke models

Contents

Part I: Thesis

1 Introduction

This thesis consists of the following articles:

A. E. Khaniki.
On Proof Complexity of Resolution over Polynomial Calculus.
ACM Trans. Comput. Logic, 23(3), 2022.

B. E. Khaniki.
Nisan-Wigderson Generators in Proof Complexity: New Lower Bounds.
In *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*, volume 234 of LIPIcs, pages 17:1–17:15, 2022.

C. E. Khaniki.
Jump operators, Interactive Proofs and Proof Complexity Generators.
Preprint, 2023.

D. E. Khaniki.
Not all Kripke models of HA are locally PA.
Advances in Mathematics, 397:22, 2022.

This thesis focuses on different problems in proof complexity, bounded arithmetic, and intuitionistic arithmetic. In the rest of this chapter, we briefly explain the main contributions of the above articles. In the Included Papers Chapter of the thesis, the aforementioned papers have been attached.

1.1 Paper A: On Proof Complexity of Resolution over Polynomial Calculus

A long-standing open problem in propositional proof complexity is proving super polynomial lower bounds for $\mathsf{AC}^0(\oplus)$-Frege. This problem remained unsolved despite many efforts by experts and even a nontrivial polynomial lower bound is not known for this proof system. As proving lower bounds for $\mathsf{AC}^0(\oplus)$-Frege seemed out of reach of the current techniques, different subsystems of $\mathsf{AC}^0(\oplus)$-Frege (or in general weak proof systems that can do limited counting) were considered in the literature. One of these systems is Resolution over parities ($\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$) [IS20]. Several lower bounds for the tree-like version of this proof system and more generally for the tree-like versions of Resolution over linear equalities over fields ($\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$) have been proved [IS20, GK18, Kra18, PT20, Gry19], but no super-polynomial lower bound is known for the dag-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$ when $\mathbb{F}$ is a finite field for a family of CNFs. In [Kha22c], we investigated $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$ proof system and in general $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$ proof system (Resolution over polynomial equalities). We proved a size-width relation for these proof systems and using that we proved several lower bounds for tree-like $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}_p})$ (d can be larger than 1) and moreover, we proved the only known nontrivial lower bounds ($n^{2-o(1)}$) for dag-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_p})$ proof system for any prime p.

1.2 Paper B: Nisan–Wigderson generators in Proof Complexity: New lower bounds

Proof complexity generators were defined independently by Alekhnovich *et al.* [ABRW04] and Krajíček [Kra01] with different motivations. Let g be a stretching map (for any n, $g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$ and moreover, $m(n) > n$) that can be computed in a low complexity class. The mapping g is called a hard proof complexity generator for a proof system P if and only if for any large enough n, for any b outside of the range of g_n, P requires super-polynomial P-proofs for propositional formulas $\tau_b(g_n) :=$ "b is not in the range of g_n". A well-studied generator in the context of proof complexity generators is the Nisan-Wigderson generator [NW94]. It is known that Nisan-Wigderson generators are hard for some proof systems (for example see [ABRW04, Raz15]) and more interestingly Razborov conjectured that under certain assumptions, Nisan-Wigderson generators should be hard for some strong proof systems.

Conjecture 1.1. *(Razborov [Raz15]) Any Nisan–Wigderson generator based on suitable matrices and any function in* $\mathsf{NP} \cap \mathsf{CoNP}$ *that is hard on average for* $\mathsf{P/poly}$*, is hard for Extended Frege.*

In [Kha22a], we proved a form of Razborov's conjecture for AC^0-Frege. In more detail, we proved that for any symmetric $f \in \mathsf{NP} \cap \mathsf{CoNP}$ that requires $2^{n^{\Omega(1)}}$ depth two AC^0 circuits, for any $\Sigma_1^1 \cap \Pi_1^1$ pair (ϕ_0, ϕ_1) that defines f, any suitable matrix A, $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for AC^0-Frege when the Paris-Wilkie translation of (ϕ_0, ϕ_1) is used to form the formula $\tau_b(\mathsf{NW}_{f,A})$. Moreover, we discussed some applications of this lower bound to some other questions about the power of AC^0-Frege.

1.3 Paper C: Jump operators, Interactive Proofs and Proof Complexity Generators

Krajíček and Pudlák [KP89] proved that if there is no optimal proof system, then for any proof system P, there is another proof system Q such that P requires super-polynomial size proofs to prove the finite reflection principle formulas for Q which we denote by $\{Rfn_Q\}$. This is quite interesting as for any proof system, we get a uniform family of hard tautologies. So the natural next step is to try and prove lower bounds for a strong proof system such as Frege (unconditionally or conditionally based on some other hardness assumptions) for the family $\{Rfn_Q\}$ for a proof system Q. The problem is that the result of [KP89] does not imply any explicit construction of Q based on P. We call such constructions, jump operators where given a proof system P, it outputs another proof system Q such that $\{Rfn_Q\}$ is a hard sequence for P. Some candidates for effectively computable jump operators were proposed by Krajíček and Pudlák [KP89] and Krajíček [Kra04], but it is open whether a computable jump operator exists or not. In the first part of [Kha23], we introduced a new candidate jump operator based on the power of interactive proofs. Given a proof system P, IP-randomized implicit proof system based on P, which is denoted by $[\![\mathsf{IP}, P]\!]$, is a Merlin-Arthur proof system (MA). This jump operator can be seen as a version of Krajíček's implicit proof system [Kra04] and in a sense, it is related to the Ideal proof system of Grochow and Pitassi [GP18]. We investigated this jump operator and proved several results. We proved that for any proof system P, if the strong proof system of $\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP}$ proves exponential hard-on-average circuit lower bounds for a Boolean function f, then the strong proof system of $\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP}$ simulates $[\![\mathsf{IP}, P]\!]$. This is similar to the conditional simulation of the Ideal proof system by Extended Frege [GP18].

The second result is a hardness magnification theorem for strong proof systems. We proved that for any strong enough proof system P and any proof system Q that contains tree-like Resolution, if truth-table generators for polynomial-size circuits are hard proof complexity generators for P, then for any tautology ϕ, P requires exponential size proofs to prove the propositional formulas $LB_Q(\phi)$:="There is no polynomial-size $[\![\mathsf{IP}, P]\!]$-proof of ϕ". Following this result, we proved that under plausible hardness assumption for proof complexity generators, both PV_1 and S^1_2 are consistent with the arithmetical sentence "$[\![\mathsf{IP}, \mathsf{Res}^*]\!]$ is a sound and polynomially bounded MA proof system for true DNFs" where Res^* is tree-like Resolution. What makes this consistency result interesting is that a reasonable fraction of complexity theory can be formalized in PV_1, which means that complexity theory from the point of view of PV_1 is close to our knowledge about complexity theory (for a survey, see [Pic15, MP20]).

It is well known that EF is not automatable under cryptographic hardness assumptions [KP98], but it is not known whether this nonautomatability can be based on a structural complexity hardness assumption like the nonautomatability result for Resolution [AM20]. Moreover, nothing is known about whether EF has the feasible disjunction property or not. We observed that it is possible to apply the core idea of [AM20] on $LB_Q(\phi)$ formulas (under some extra assumption) to get nonautomatbility of EF under a structural complexity hardness assumption. Moreover, we proved that (under the same extra assumption as before) EF does not have the feasible disjunction property under another structural complexity hardness assumption. In more detail, assume that intuitionistic S^1_2 proves the strong soundness of $[\![\mathsf{IP}, \mathsf{Res}^*]\!]$. Then the following statements hold:

1. If EF is automatable, for infinitely many n there is a $\mathsf{P/poly}$ natural property useful against $\mathsf{P/poly}$.

2. If EF has the feasible disjunction property, for infinitely many n there is a $\mathsf{NP/poly}$ natural property useful against $\mathsf{P/poly}$.

One ingredient of our proofs is a formalization of the sum-check protocol [LFKN92] in $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ which might be of independent interest.

Motivated by the hardness properties that enabled us to prove the consistency result for PV_1 and S^1_2, we defined a new hardness property for proof complexity generators and investigated its properties. A stretching map $g \in \mathsf{FP}$ is P-provably hard for P for a proof system P if and only if P has short proofs for the propositional formulas "For any b, there is no polynomial-size P-proof for $\tau_b(g_n)$". We gave a model-theoretic characterization of this property and investigated its relationship with previously defined hardness properties for proof complexity generators.

In the second part of [Kha23], we looked at the general theory of jump operators and considered an old open problem by Krajíček and Pudlák [KP89] which asks whether finite consistency formulas for an arithmetical theory T' have polynomial size proofs in an arithmetical theory T when T' proves the consistency of T. In this regard, we proved that certain statements are equivalent, in particular, the following two are equivalent:

- There exists a partial recursive jump operator in proof complexity.
- For any strong enough finitely axiomatizable arithmetical theory S, S does not have polynomial size proofs for $Con_{S+Con_S}(\bar{n})$ in n.

1.4 Paper D: Not all Kripke models of HA are locally PA

Let $\mathbf{K}$ be a Kripke model Heyting arithmetic (HA). $\mathbf{K}$ is locally T where T is an arithmetical theory, if and only if for any $k \in \mathbf{K}$, $\mathcal{M}_k$, which is the classical structure associated with k, believes in T. An old open problem originated from the work of van Dalen *et al.* [vMKV86] was whether every Kripke model of Heyting arithmetic is locally Peano arithmetic. Several positive results for this problem were proved by posing different restrictions on Kripke frames [vMKV86, Weh96, AH02, Mon02, Poł06, Moj18], but the original problem had remained open. In [Kha22b], we gave a negative answer to this problem. We introduced two new Kripke model constructions which can be used to give a negative answer to the mentioned problem. The first model construction only works for HA, but the second model construction is a general method that can be used to construct new Kripke models for any reasonable intuitionistic arithmetical theory, which might be of independent interest.

Bibliography

[ABRW04] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, 2004.

[AH02] M. Ardeshir and B. Hesaam. Every Rooted Narrow Tree Kripke Model of HA is Locally PA. *Mathematical Logic Quarterly*, 48(3):391–395, 2002.

[AM20] A. Atserias and M. Müller. Automating resolution is NP-hard. *Journal of the ACM*, 67(5):17, 2020.

[GK18] M. Garlík and L. A. Kołodziejczyk. Some Subsystems of Constant-Depth Frege with Parity. *ACM Trans. Comput. Logic*, 19(4), November 2018.

[GP18] J. A. Grochow and T. Pitassi. Circuit complexity, proof complexity, and polynomial identity testing. The ideal proof system. *Journal of the ACM*, 65(6):59, 2018.

[Gry19] S. Gryaznov. Notes on Resolution over Linear Equations. In *Computer Science – Theory and Applications (CSR '19)*, pages 168—179, 2019.

[IS20] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Annals of Pure and Applied Logic*, 171(1), 2020. Preliminary version in *MFCS '14*.

[Kha22a] E. Khaniki. Nisan-Wigderson Generators in Proof Complexity: New Lower Bounds. In *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*, volume 234 of *LIPIcs*, pages 17:1–17:15, 2022.

[Kha22b] E. Khaniki. Not all Kripke models of HA are locally PA. *Advances in Mathematics*, 397:22, 2022.

[Kha22c] E. Khaniki. On Proof Complexity of Resolution over Polynomial Calculus. *ACM Trans. Comput. Logic*, 23(3), 2022.

[Kha23] E. Khaniki. Jump operators, Interactive Proofs and Proof Complexity Generators. *Preprint*, 2023.

[KP89] J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[KP98] J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S_2^1 and EF. *Information and Computation*, 140(1):82–94, 1998.

[Kra01] J. Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1-2):123–140, 2001.

[Kra04] J. Krajíček. Implicit proofs. *The Journal of Symbolic Logic*, 69(2):387–397, 2004.

[Kra18] J. Krajíček. Randomized feasible interpolation and monotone circuits with a local oracle. *Journal of Mathematical Logic*, 18(2), 2018.

[LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, oct 1992.

[Moj18] M. Mojtahedi. Localizing finite-depth Kripke models. *Logic Journal of the IGPL*, 27(3):239–251, 2018.

[Mon02] M. Moniri. H-theories, fragments of HA and PA-normality. *Archive for Mathematical Logic*, 41(1):101–105, 2002.

[MP20] M. Müller and J. Pich. Feasibly constructive proofs of succinct weak circuit lower bounds. *Annals of Pure and Applied Logic*, 171(2):45, 2020.

[NW94] N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.

[Pic15] J. Pich. Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic. *Logical Methods in Computer Science*, 11(2):38, 2015.

[Poł06] T. Połacik. Partially-Elementary Extension Kripke Models: A Characterization and Applications. *Logic Journal of the IGPL*, 14(1):73–86, 2006.

[PT20] F. Part and I. Tzameret. Resolution with Counting: Dag-Like Lower Bounds and Different Moduli. In *11th Innovations in Theoretical Computer Science Conference (ITCS '20)*, volume 151, pages 1–37, 2020.

[Raz15] A. A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics. Second Series*, 181(2):415–472, 2015.

[vMKV86] D. van Dalen, H. Mulder, E. C. W. Krabbe, and A. Visser. Finite Kripke models of HA are locally PA. *Notre Dame Journal of Formal Logic*, 27(4):528–532, 1986.

[Weh96] K. F. Wehmeier. Classical and intuitionistic models of arithmetic. *Notre Dame Journal of Formal Logic*, 37(3):452–461, 1996.

Part II: Included Papers

Paper A

On Proof Complexity of Resolution over Polynomial Calculus

Erfan Khaniki[1,2]
[1]Faculty of Mathematics and Physics, Charles University
[2]Institute of Mathematics, Czech Academy of Sciences

Abstract

The proof system $\mathsf{Res}(\mathsf{PC}_{d,R})$ is a natural extension of the Resolution proof system that instead of disjunctions of literals operates with disjunctions of degree d multivariate polynomials over a ring R with Boolean variables. Proving super-polynomial lower bounds for the size of $\mathsf{Res}(\mathsf{PC}_{1,R})$-refutations of CNFs is one of the important problems in propositional proof complexity. The existence of such lower bounds is even open for $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$ when $\mathbb{F}$ is a finite field such as $\mathbb{F}_2$. In this paper, we investigate $\mathsf{Res}(\mathsf{PC}_{d,R})$ and tree-like $\mathsf{Res}(\mathsf{PC}_{d,R})$ and prove size-width relations for them when R is a finite ring. As an application, we prove new lower bounds and also reprove some known lower bounds for every finite field $\mathbb{F}$ as follows:

1. We prove almost quadratic lower bounds for $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$-refutations for every fixed d. The new lower bounds are for the following CNFs:
   (a) Mod q Tseitin formulas ($char(\mathbb{F}) \neq q$) and Flow formulas,
   (b) Random k-CNFs with linearly many clauses.
2. We also prove super-polynomial (more than n^k for any fixed k) and also exponential (2^{n^ϵ} for an $\epsilon > 0$) lower bounds for tree-like $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$-refutations based on how big d is with respect to n for the following CNFs:
   (a) Mod q Tseitin formulas ($char(\mathbb{F}) \neq q$) and Flow formulas,
   (b) Random k-CNFs of suitable densities,
   (c) Pigeonhole principle and Counting mod q principle.

The lower bounds for the dag-like systems are the first nontrivial lower bounds for these systems including the case $d = 1$. The lower bounds for the tree-like systems were known for the case $d = 1$ (except for the Counting mod q principle which lower bounds for the case $d > 1$ were known too). Our lower bounds extend those results to the case where $d > 1$ and also give new proofs for the case $d = 1$.

2 Introduction

Resolution is perhaps the most studied proof system in propositional proof complexity. This system works with clauses of literals. Given an unsatisfiable CNF formula F, a Resolution refutation of F starts with this formula and derives the empty clause with several applications of its rules. Resolution is important in several ways. For example, it is closely related to SAT solvers, so studying Resolution leads to a better understanding of the limits of Resolution based SAT solvers. Moreover, Resolution is a starting point for defining stronger proof systems. Understanding stronger proof systems in terms of the size of proofs is important in the following ways:

1. From the mathematical logic point of view, the existence of super-polynomial lower bounds for strong enough proof systems implies independence results for first-order theories.

2. From the computational complexity point of view, proving lower bounds for proof systems is related to the $\mathsf{NP} \neq \mathsf{CoNP}$ question. Indeed, $\mathsf{NP} \neq \mathsf{CoNP}$ is equivalent to the existence of super-polynomial lower bounds for every propositional proof system.

One way of introducing a proof system that is stronger than Resolution is to define it in a way that it can work with functions that are stronger than the disjunction of literals (in terms of definability) in lines of the proof. As examples of such proof systems we can list the following ones:

Proof system	**Proof lines**
Cutting Planes	Linear inequalities
Polynomial Calculus	Multivariate polynomials
AC^0-Frege	Constant depth formulas
Frege	Formulas

Table 1

We know lower bounds for the first three systems in the above list, but there are no known super-polynomial lower bounds for the Frege proof system. Since the known lower bounds for the AC^0-Frege proof system were proved by adapting the techniques which had been used to prove super-polynomial and exponential lower bounds for AC^0 circuits (see [Ajt94a, KPW95, PBI93]), the natural next step seemed to be to prove lower bounds for the $\mathsf{AC}^0[p]$-Frege proof system by adapting the Razborov–Smolensky approximation method that was used to prove $\mathsf{AC}^0[p]$ circuit lower bounds. However, this problem has remained open to this day, and it is one of the frontier problems in propositional proof complexity. Since proving super-polynomial lower bounds for the $\mathsf{AC}^0[p]$-Frege proof system seems to be hard, reasonable subsystems of $\mathsf{AC}^0[p]$-Frege and similar proof systems that can work with some kind of limited counting were investigated in the literature. We briefly review the known results about these systems.

One of the first such systems is the AC^0-Frege proof system with the Count_p^n principle when p is a prime number. Super-polynomial lower bounds were proved on the size of proofs of the Count_q^n principle when $q \neq p$ is a prime number for this system in [Ajt94b, BIK$^+$94, Rii97].

Two other well-studied proof systems are Nullstellensatz and Polynomial Calculus. Here we mention only some of the first results that were proved for them. The Nullstellensatz proof system was defined by Beame *et al.* in [BIK$^+$94] and they proved the first degree lower bound for it which was for the Count_q^n principle. Later the Polynomial Calculus proof system was defined by Clegg *et al.* in [CEI96] and a degree separation between the Nullstellensatz proof system and Polynomial Calculus proof system was proved there. Razborov in [Raz98] proved the first nontrivial degree lower bound for Polynomial Calculus and showed that every Polynomial Calculus refutation of the Pigeonhole principle has degree at least $n/2 + 1$.

Krajíček in [Kra97] defined the subsystem $\mathsf{F}_d^c(\mathsf{MOD}_p)$ of $\mathsf{AC}^0[p]$-Frege proof system and proved that $\mathsf{F}_d^c(\mathsf{MOD}_p)$ needs super-polynomial size for the Count_q^n principle (where $q \neq p$ is a prime number) and tree-like $\mathsf{F}_d^c(\mathsf{MOD}_p)$ needs exponential size for proving the Pigeonhole principle.

To have a uniform notation for the Resolution based systems, we use Table 2 for the rest of the paper.

Our notation	**Aliases**
$\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Z}})$	$\mathsf{R}(\mathsf{lin})$ [RT08]
$\mathsf{Res}(\mathsf{PC}_{2,\mathbb{Z}})$	$\mathsf{R}(\mathsf{quad})$ [Tza14]
$\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$	$\mathsf{Res}(\oplus)$ [IS20], $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$ [Kra18]
$\mathsf{Res}(\mathsf{PC}_{1,R})$	$\mathsf{Res}(\mathsf{lin}_R)$ [PT20]
$\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}_2})$	$\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$ [Kra18]

Table 2

Raz and Tzameret in [RT08] defined the proof system $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Z}})$ and showed that $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Z}})$ is very strong by proving that this system has polynomial size refutations of the Pigeonhole principle, Mod q Tseitin formulas, and the Clique-Coloring principle. They also proved an exponential lower bound for a fairly strong fragment of $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Z}})$ using monotone feasible interpolation. Later Tzameret in [Tza14] investigated the proof system $\mathsf{Res}(\mathsf{PC}_{2,\mathbb{Z}})$ and proved that if it has the feasible interpolation property, then there is an efficient deterministic refutation algorithm for random 3SAT with n variables and $\Omega(n^{1.4})$ clauses.

Itsykson and Sokolov in [IS20] introduced the proof system $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$. They investigated the power of this system from different perspectives and proved that tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ needs exponential size for refuting the Pigeonhole principle (FPHP_n^m), lifted versions of Tseitin formulas (lifted $\mathsf{TS}_2(G,\sigma)$) and Pebbling formulas (lifted Peb_G). They proved these lower bounds by generalizing the well-known prover-delayer games of [PI00] and also by using the known communication complexity lower bounds. Moreover, they proved that $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Z}})$ polynomially simulates $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$.

In [Kra18] Krajíček defined randomized dag-like communication games for Karchmer–Wigderson relations. He proved that $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ has the randomized feasible interpolation property which means that from a $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$-refutation of the non-disjointness of two NP sets U and V, we can construct such a game for computing the Karchmer–Wigderson relation associated with U and V. Furthermore, he proved that such protocols correspond to monotone circuits with local oracles (CLO) in the case when U is upward closed or V is downward closed. Therefore, if we prove lower bounds for any CLO separating a monotone disjoint NP-pair, this will lead to a lower bound for $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$. Using the randomized feasible interpolation, he proved that every tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$-refutation of the Hall principle (Hall_n) has exponential size (see Theorem 18.6.4 in [Kra19]). He also introduced the proof system $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}_2})$ which is a natural generalization of $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ and discussed the possibility of proving the randomized feasible interpolation property for it. Krajíček and Oliveira in [KO18] proved lower bounds for a subclass of CLOs (containing the class of the usual monotone circuits) separating k-cliques and the set of complete $(k-1)$-partite graphs, but it is not known whether a lower bound for this subclass is enough for getting a super-polynomial lower bound on the size of $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$-refutations of the Clique-Coloring principle.

Following [Kra97], Garlík and Kołodziejczyk in [GK18] defined the subsystem $\mathsf{PK}^c_d(\oplus)$ of $\mathsf{AC}^0[2]$-Frege proof system. In this system, every line of a proof is a disjunction such that disjuncts have depth at most d, and parities can only appear as the outermost connectives of disjuncts, and all but c disjuncts contain no parity connective at all. Then they investigated the relation between $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$, tree-like $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$ and the AC^0-Frege proof systems with the Count^n_2 principle and proved several lower bounds for them. They also proved that an extension of tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ is polynomially simulated by a system related to $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$, and hence they obtained an exponential lower bound for the Count^n_3 principle for tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$. Although they did not mention it in their paper, their lower bound also works for tree-like $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}_2})$ when $d = n^\epsilon$ and $\epsilon > 0$ is a small enough constant[1]. So they implicitly proved the first super-polynomial lower bound for tree-like $\mathsf{Res}(\mathsf{PC}_{n^\epsilon,\mathbb{F}_2})$.

Part and Tzameret in [PT20] defined the proof system $\mathsf{Res}(\mathsf{PC}_{1,R})$ for every ring R, and proved several lower bounds for dag-like and tree-like $\mathsf{Res}(\mathsf{PC}_{1,R})$ for different rings. In particular, for finite fields they proved that tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$ ($char(\mathbb{F}) \neq q$) requires exponential size to refute the Pigeonhole principle, Mod q Tseitin formulas ($\mathsf{TS}_q(G,\sigma)$) and random k-CNFs. They used two main tools for proving these lower bounds. First, they generalized the prover-delayer game of [IS20] to an arbitrary ring R. Second they proved a size-width relation for tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$ for any field $\mathbb{F}$. They also proved the first super-polynomial lower bound for dag-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Q}})$-refutations. This lower bound was proved for the Subset-sum principle which is not a CNF, so the lower bound problem for CNFs remained open. It is worth noting that a size-width relation for tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ was proved by Garlík and Kołodziejczyk in an unpublished manuscript before [PT20].

Following the prover-delayer method that was used in [IS20, PT20], Gryaznov proved in [Gry19] exponential lower bounds for the Ordering and Dense Linear Ordering principles ($\mathsf{Ordering}_n$ and DLO_n) in tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$, and hence separated tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ and Res. Regarding the separation between tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ and Res, [IS20] strengthened Gryaznov's result by proving that a lifted version of Pebbling formulas is hard for tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$, but it is easy for regular Resolution.

Table 3 summarizes the mentioned lower bounds for (tree-like) $\mathsf{Res}(\mathsf{PC}_1, \mathbb{F})$.

In this paper we continue investigating the power of $\mathsf{Res}(\mathsf{PC}_{1,R})$, tree-like $\mathsf{Res}(\mathsf{PC}_{1,R})$ and also their generalization $\mathsf{Res}(\mathsf{PC}_{d,R})$ and tree-like $\mathsf{Res}(\mathsf{PC}_{d,R})$ when $d > 1$. Our main theorem is the following new size-width relation. Here $\mathsf{S}_{d,R}(F)$ and $\mathsf{S}^*_{d,R}(F)$ are the least number of steps to refute F in $\mathsf{Res}(\mathsf{PC}_{d,R})$ and tree-like $\mathsf{Res}(\mathsf{PC}_{d,R})$ respectively, $\mathsf{w}_{d,R}(F)$ is the least width required to refute F in $\mathsf{Res}(\mathsf{PC}_{d,R})$, and $\mathsf{w}(F)$ is the width of the CNF F.

Theorem 2.1. *(Size-Width relation, a simplified version) Let R be a finite ring and F be an unsatisfiable CNF in n variables, then the following inequalities hold:*

1. $\mathsf{w}_{d,R}(F) \leq \mathsf{w}(F) + O\left(\log(\mathsf{S}^*_{d,R}(F))\right)$.

[1] Private communication with Leszek Kołodziejczyk.

2. $\mathsf{w}_{d,R}(F) \leq \mathsf{w}(F) + O\left(\sqrt{\big(n + \mathsf{S}_{d,R}(F)\big)\log(\mathsf{S}_{d,R}(F))}\right)$.

This theorem has two advantages over the size-width relation of [PT20]. First, it works for dag-like systems such as $\mathsf{Res}(\mathsf{PC}_{1,R})$ and hence we can prove nontrivial lower bounds in the dag-like setting. Second, it is not limited to linear forms, and we can prove lower bounds for Resolution over multivariate polynomials. We would also like to point out that the proof of this theorem uses the same strategy for both the tree-like and the dag-like proofs, and that all of the lower bounds that are stated in this paper are proved using this theorem.

Contents of this paper. As we stated earlier, the main theorem of this paper is a new size-width relation that works for (tree-like) $\mathsf{Res}(\mathsf{PC}_{d,R})$ proof system when R is a finite ring. The novel idea that is used to prove these size-width relations is a combination of the usage of extension variables and the size-width relation of Ben-Sasson and Wigderson for Resolution [BW99]. In more detail, the main idea is to use the extension variables to translate refutations in $\mathsf{Res}(\mathsf{PC}_{d,R})$ and tree-like $\mathsf{Res}(\mathsf{PC}_{d,R})$ to Resolution refutations of some new clauses formed by these new extension variables, then use the size-width relation of Ben-Sasson and Wigderson for Resolution [BW99], and finally translate back to $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutations. To prove the lower bounds, we show that if a CNF formula F has a low width $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$-refutation, then it also has a low degree refutation in Polynomial Calculus over $\mathbb{F}$ when $\mathbb{F}$ is a finite field. This strategy was first used in [PT20] to relate the width of $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$-refutations of F to the degree of Polynomial Calculus refutations of it. This enables us to combine the known degree lower bounds for Polynomial Calculus with the new size-width relation to prove our lower bounds.

We prove the first nontrivial lower bounds ($n^{2-o(1)}$) for $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}})$ and in general for $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$ (for every fixed d) over finite fields. These new lower bounds for the dag-like systems are proved for different principles. For the tree-like case over finite fields, we prove the first super-polynomial and exponential lower bounds for tree-like $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$ where d is limited by some sub-linear function of n and moreover reprove some of the known lower bounds for the case $d = 1$.

Proof system	**Formula**	**Reference**
Tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$	FPHP^m_n Lifted $\mathsf{TS}_2(G,\sigma)$ Lifted Peb_G	[IS20]
	Hall_n	[Kra18]
	Count^n_3	[GK18]
	$\mathsf{Ordering}_n$ DLO_n	[Gry19]
Tree-like $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_{p^k}})$	FPHP^m_n $\mathsf{TS}_q(G,\sigma)$ Random k'-CNF	[PT20]
$\mathsf{Res}(\mathsf{PC}_{1,\mathbb{Q}})$	Subset-sum principle	[PT20]

Table 3: All of the lower bounds in this table are exponential in the number of variables except the lower bounds for FPHP^m_n which are exponential in n

The organization of the paper is as follows. In Section 3, we explain definitions and notations. In Section 4, we state the main results and prove the lower bounds. In Section 5, we prove the main results.

3 Preliminaries

3.1 Proof systems

3.2 Resolution

Resolution (Res) is a proof system that works with clauses of literals. Every clause in a Resolution derivation is a disjunction of variables or negation of variables without repetition (it is a set of literals). Resolution proof system has the following rules:

1. Resolution rule:

$$\frac{C \vee p \qquad D \vee \neg p}{C \vee D}$$

2. Weakening rule:

$$\frac{C}{C \vee D}$$

where $p \in \{p_1, ..., p_n\}$ (the set of variables appearing in the initial clauses) and C and D are arbitrary clauses. We need Resolution to be an implicationally complete system. This is the reason for including the weakening rule.

A CNF formula is a set of clauses.

Definition 3.1. *A Resolution derivation of a clause D from the CNF formula $F = \{C_1, ..., C_k\}$ is a sequence of clauses ($\pi = D_1, ..., D_l$) such that:*

1. *$D_l = D$,*
2. *for every $i \leq l$, D_i is in F or D_i was derived by the resolution rule or the weakening from $\{D_j | j < i\}$ in one step.*

A Resolution refutation of a CNF F is a Resolution derivation of $\emptyset$ from F.

3.2.1 Polynomial Calculus

Let R be a ring. Then Polynomial Calculus over the ring R, PC_R is a proof system that works with multivariate polynomials with coefficients in R. A multivariate polynomial $f \in R[x_1, ..., x_n]$ is true under the Boolean assignment $a \in \{0,1\}^n$ iff $f(a) = 0$. PC_R has the following rules:

1. Addition:

$$\frac{f \qquad g}{af + bg}$$

for every $a, b \in R$,

2. Multiplication:

$$\frac{f}{g \cdot f}$$

where f, g are multivariate polynomials with coefficients in R. Moreover, PC_R has $x^2 - x$ for every $x \in \{x_1, ..., x_n\}$ as an axiom.

Definition 3.2. *A PC_R-derivation of a multivariate polynomial $f \in R[x_1, ..., x_n]$ from a set of multivariate polynomials $F \subseteq R[x_1, ..., x_n]$, is a sequence of multivariate polynomials ($\pi = f_1, ..., f_l$) such that:*

1. *$f_l = f$,*
2. *for every $i \leq l$, f_i is in F, or f_i is a PC_R axiom, or f_i was derived by the rules of PC_R from $\{f_j | j < i\}$ in one step.*

A PC_R-refutation of a set $F \subseteq R[x_1, ..., x_n]$ is a PC_R-derivation of 1 from F.

One of the important measures for Polynomial calculus derivations is the degree measure.

Definition 3.3. *For a multivariate polynomial $f \in R[x_1, ..., x_n]$ let $\mathsf{deg}(f)$ be the degree of f. For a set $F \subseteq R[x_1, ..., x_n]$ (not necessarily nonempty) and a multivariate polynomial $f \in R[x_1, ..., x_n]$, the notation*

$$F \mathrel{\Big|\!\!\frac{\;\mathsf{PC}_R\;}{d}} f$$

means there exists a PC_R-derivation π for f from F such that the degree of each multivariate polynomial in π is at most d.

To prove the relation between $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$ and $\mathsf{PC}_{\mathbb{F}}$ we need the following lemma when R is a ring of prime characteristic.

Lemma 3.1. *Let $\mathbb{F}$ be a finite field such that char$(\mathbb{F}) = p$ for a prime p and $f \in \mathbb{F}[x_1, ..., x_n]$ be a multivariate polynomial. Then*

$$\{f^2\} \mathrel{\Big|\!\!\frac{\;\mathsf{PC}_{\mathbb{F}}\;}{p\cdot\mathsf{deg}(f)}} f.$$

Proof. Let $f = \sum_{(a,M)\in A} a \cdot M$ in which for every $(a, M) \in A$, M is a monomial and a is its coefficient. For every $i \geq 1$, define

$$g_i := \sum_{(a,M)\in A} a^{p^i} \cdot M.$$

We want to show that for every $i \geq 1$, $\{g_i\} \mathrel{\Big|\!\!\frac{\;\mathsf{PC}_{\mathbb{F}}\;}{p\cdot\mathsf{deg}(f)}} g_{i+1}$. It is known that the identity $(x+y)^p = x^p + y^p$ is true in every field of characteristic p when p is prime. Therefore

$$g_i^p = \sum_{(a,M)\in A} a^{p^{i+1}} \cdot M^p$$

which implies

$$\{g_i\} \mathrel{\Big|\!\!\frac{\;\mathsf{PC}_{\mathbb{F}}\;}{p\cdot\mathsf{deg}(f)}} \sum_{(a,M)\in A} a^{p^{i+1}} \cdot M^p$$

by the multiplication rule. Moreover, it is easy to prove that for every monomial $M = \prod_{i=1}^{n} x_i^{d_i}$ and every $k \geq 1$, $\varnothing \left|\frac{\mathsf{PC}_{\mathbb{F}}}{k \cdot \mathsf{deg}(M)}\right. M^k - M$. This can be proved by induction on $\mathsf{deg}(M)$ and using the fact that $x^2 - x$ is an axiom for every $x \in \{x_1, ..., x_n\}$. This implies that by applications of the addition rule we get

$$\{g_i\} \left|\frac{\mathsf{PC}_{\mathbb{F}}}{p \cdot \mathsf{deg}(f)}\right. \sum_{(a,M) \in A} a^{p^{i+1}} \cdot M^p - a^{p^{i+1}} \cdot (M^p - M)$$

which means

$$\{g_i\} \left|\frac{\mathsf{PC}_{\mathbb{F}}}{p \cdot \mathsf{deg}(f)}\right. g_{i+1}.$$

Following the same argument, we have $\{f^2\} \left|\frac{\mathsf{PC}_{\mathbb{F}}}{p \cdot \mathsf{deg}(f)}\right. g_1$ by multiplying f^{p-2} and do the rest of the argument as before. Therefore we get $\{f^2\} \left|\frac{\mathsf{PC}_{\mathbb{F}}}{p \cdot \mathsf{deg}(f)}\right. g_{k'}$ where $p^{k'}$ is the order of $\mathbb{F}$. As $\mathbb{F}$ is a finite field, for every $a \in \mathbb{F}$, $a^{p^{k'}} = a$ which implies that $g_{k'} = f$. □

3.2.2 Resolution over Polynomial Calculus

For a ring R, we define Resolution over Polynomial Calculus (over R), denoted by $\mathsf{Res}(\mathsf{PC}_R)$, as a proof system like Res, except that instead of disjunctions of literals, it works with disjunctions of multivariate polynomials of Boolean variables (no negative variables) with coefficients in R. Moreover, there is no repetition of multivariate polynomials in a disjunction (each disjunction in a derivation is treated as a set).

Definition 3.4. *A disjunction $C = \bigvee_{i<l} f_i$ where every $f_i \in R[x_1, ..., x_n]$ is a clause if every f_i appears in C exactly once.*

A clause $C = \bigvee_{i<l} f_i$ is true under a Boolean assignment $a \in \{0,1\}^n$ iff there exists an i such that $f_i(a) = 0$.

Definition 3.5. *A CNF_d formula F is a set of clauses of multivariate polynomials such that every multivariate polynomial f in a clause of F has degree at most d. So a CNF can be written as a CNF_1 formula by translating x to $x - 1$ and $\neg x$ to x.*

Following [PT20], we use a similar set of rules for defining $\mathsf{Res}(\mathsf{PC}_R)$:

1. Resolution rule:

$$\frac{C \vee f \qquad D \vee g}{C \vee D \vee (af + bg)}$$

   for every $a, b \in R$,

2. Weakening rule:

$$\frac{C}{C \vee f}$$

3. Simplification rule:

$$\frac{C \vee a}{C}$$

for every $a \in R \setminus \{0\}$,

4. Multiplication rule:

$$\frac{C \vee f}{C \vee (g \cdot f)}$$

where f, g are multivariate polynomials with coefficients in R and C, D are arbitrary clauses. We note that after an application of the resolution, the weakening or the multiplication rule, contraction of duplicates disjuncts is done to make sure that the resulted disjunction is a clause. Furthermore, $\mathsf{Res}(\mathsf{PC}_R)$ has the following axioms:

1. Zero axiom which is the polynomial 0.

2. Boolean axioms which are $x \vee (x-1)$ for every $x \in \{x_1, ..., x_n\}$.

Definition 3.6. *A $\mathsf{Res}(\mathsf{PC}_R)$-derivation of a clause D from the CNF$_d$ formula $F = \{C_1, ..., C_k\}$ is a sequence of clauses of multivariate polynomials ($\pi = D_1, ..., D_l$) such that:*

1. *$D_l = D$,*

2. *for every $i \leq l$, D_i is in F, or D_i is a $\mathsf{Res}(\mathsf{PC}_R)$ axiom, or D_i was derived by the rules of $\mathsf{Res}(\mathsf{PC}_R)$ from $\{D_j | j < i\}$ in one step.*

A $\mathsf{Res}(\mathsf{PC}_R)$-refutation of a CNF$_d$ F is a $\mathsf{Res}(\mathsf{PC}_R)$-derivation of $\emptyset$ from F.

$\mathsf{Res}(\mathsf{PC}_{d,R})$ is a proof system using $\mathsf{Res}(\mathsf{PC}_R)$ rules and axioms, with the restriction that every multivariate polynomial appearing in a derivation should have degree at most d.

It is easy to see that (tree-like) $\mathsf{Res}(\mathsf{PC}_{1,\mathbb{F}_2})$ is p-equivalent to (tree-like) $\mathsf{Res}(\oplus)$ of [IS20] and (tree-like) $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}_2})$ is p-equivalent to (tree-like) $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$ of [Kra18].

3.2.3 Additional notations and definitions

In this part, we define complementary notations and definitions for the rest of the paper.

Definition 3.7. *Let $\pi = D_1, .., D_l$ be a derivation in one of the defined proof systems. The graph G_π associated with π is a DAG with D_is as nodes, and for every derivation step, directed edges are added from the assumptions to the consequence. π is called tree-like iff G_π is a tree. Moreover, the size of π is l and it is denoted by $|\pi|$.*

In general, it is possible to make any derivation tree-like by making copies of the initial clauses. If P is one of the defined proof systems, then P^* denotes tree-like P.

Definition 3.8. *Let $C = \bigvee_{i<l} f_i$ be a clause of multivariate polynomials over the ring R. Then the arithmetization of C is the multivariate polynomial $h_C = \prod_{f \in C} f$ $(h_\emptyset = 1)$ expanded as sum of monomials.*

Definition 3.9. *The set of variables appearing in a clause C and a CNF or CNF$_d$ formula F are denoted by $V(C)$ and $V(F)$ respectively.*

Definition 3.10. *The width of a clause C is the number of literals (multivariate polynomials) in it and it is denoted by $\mathsf{w}(C)$.*

Definition 3.11. *For a CNF$_d$ formula $F = \{C_1, ..., C_k\}$, $\mathsf{w}(F) = \max_{C \in F} \mathsf{w}(C)$. For a derivation π in one of the defined Resolution based proof systems, $\mathsf{w}(\pi) = \max_{D \in \pi} \mathsf{w}(D)$.*

Definition 3.12. *For a proof system P, a set of clauses F (not necessarily nonempty) and a clause D, the notation*

$$F \left|\frac{P}{w}\right. D$$

means that there exists a P-derivation π for D from F such that $\mathsf{w}(\pi) \leq w$.

If F is an unsatisfiable CNF$_d$ and R is a ring, then the refutation size and the width corresponding to F in $\mathsf{Res}(\mathsf{PC}_{d,R})$ are respectively:

1. $\mathsf{S}_{d,R}(F)$ is the minimum $|\pi|$ among all $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutations π of F.

2. $\mathsf{w}_{d,R}(F)$ is the minimum $\mathsf{w}(\pi)$ among all $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutations π of F,

$\mathsf{S}^*_{d,R}(F)$ is the refutation size corresponding to F in $\mathsf{Res}^*(\mathsf{PC}_{d,R})$. If F is a CNF formula, then Res-refutation width and size corresponding to F are denoted by $\mathsf{w}_{\mathsf{Res}}(F)$ and $\mathsf{S}_{\mathsf{Res}}(F)$. For Res^*, the refutation size of F is denoted by $\mathsf{S}_{\mathsf{Res}^*}(F)$.

An important result in proof complexity that we use in this paper is the size-width relation of Ben-Sasson and Wigderson for Resolution that were proved in the seminal paper [BW99].

Theorem 3.2. *([BW99]) For every unsatisfiable CNF formula F in n variables, the following inequalities hold:*

1. $\mathsf{w}_{\mathsf{Res}}(F) \leq \mathsf{w}(F) + \log(\mathsf{S}_{\mathsf{Res}^*}(F))$.

2. $\mathsf{w}_{\mathsf{Res}}(F) \leq \mathsf{w}(F) + O\left(\sqrt{n \log(\mathsf{S}_{\mathsf{Res}}(F))}\right)$.

where log *is the binary logarithm.*

3.3 Hard formulas

In this part, we define the CNFs that are hard for (tree-like) $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$ when $\mathbb{F}$ is a finite field. Moreover, we state the known $\mathsf{PC}_{\mathbb{F}}$ degree lower bounds for them as they are one of the ingredients in the proofs of the lower bounds.

3.3.1 Mod q Tseitin formulas and Flow formulas

Definition 3.13. *(Mod q Tseitin formulas) Let $G = (V, E)$ be a directed d-regular graph (G is a d-regular undirected graph whose edges are then oriented). For every $(v, u) \in E$, we have a fixed variable $x_{v,u}$. Let $\sigma : V \to \mathbb{F}_q$ (q is a prime number). Then Mod q Tseitin formula $\mathsf{TS}_q(G, \sigma)$ is a CNF encoding of the following equations for every $v \in V$:*

$$(\sum_{(v,u)\in E} x_{v,u} - \sum_{(u,v)\in E} x_{u,v}) \equiv \sigma(v) \pmod{q}.$$

Note that $\mathsf{TS}_q(G, \sigma)$ is unsatisfiable iff $\sum_{v\in V} \sigma(v) \not\equiv 0 \pmod{q}$. This formula has $O(2^d|V|)$ clauses and each clause has width d. So in particular, the number of clauses of this formula is linear in the number of variables when d is a fixed constant. This is important as it shows that our dag-like lower bound is nontrivial.

The following theorem states the existence of strong $\mathsf{PC}_{\mathbb{F}}$ degree lower bounds for $\mathsf{TS}_q(G, \sigma)$.

Theorem 3.3. *([AR01]) For any field $\mathbb{F}$ and for any fixed prime q such that $char(\mathbb{F}) \neq q$, there exists a constant d_q such that the following holds. If $d \geq d_q$ and G is a d-regular Ramanujan graph on n vertices (augmented with arbitrary orientation of its edges), then for every function σ such that $\mathsf{TS}_q(G, \sigma)$ is unsatisfiable, every $\mathsf{PC}_{\mathbb{F}}$-refutation of $\mathsf{TS}_q(G, \sigma)$ has degree $\Omega(dn)$.*

Actually, the above theorem holds for any good enough expander graph (see [AR01] for the required parameters). It is well-known that for every fixed d, there exists an infinite family of d-regular Ramanujan graphs (see [LPS88]), hence for every fixed d, there exists an infinite family of d_q-regular Ramanujan graphs $\mathcal{G}$ such that lower bound of Theorem 3.3 works on Mod q Tseitin formulas defined based on members of $\mathcal{G}$.

Definition 3.14. *(Flow formulas) Let $G = (V, E)$ be a directed d-regular graph (G is a d-regular undirected graph whose edges are then oriented). For every $(v, u) \in E$, we have a fixed variable $x_{v,u}$. For every $v \in V$ denote by $\mathsf{PosFlow}(G, v)$ the following Boolean predicate:*

$$\sum_{\{w|(w,v)\in E\}} (1 - 2x_{(w,v)}) > \sum_{\{w|(v,w)\in E\}} (1 - 2x_{(v,w)}).$$

Then Flow formula $\mathsf{Fl}(G)$ is a CNF encoding of $\mathsf{PosFlow}(G, v)$ for every $v \in V$.

It is easy to see that $\mathsf{Fl}(G)$ is unsatisfiable. Moreover, similar to the $\mathsf{TS}_q(G, \sigma)$ formula, $\mathsf{Fl}(G)$ has $O(2^d|V|)$ clauses and each clause has width d. So again, if G is a constant degree graph, then the number of clauses in this formula is linear in the number of variables which is important for the dag-like lower bound. Finally, we have the following theorem for Flow formulas.

Theorem 3.4. *([AR01]) For any field $\mathbb{F}$ and for any $d \geq 255$, if G is a d-regular Ramanujan graph on n vertices (augmented with arbitrary orientation of its edges), then every $\mathsf{PC}_{\mathbb{F}}$-refutation of $\mathsf{Fl}(G)$ has degree $\Omega(dn)$.*

Again, the above theorem holds for good enough expander graphs (see [AR01] for the required parameters).

3.3.2 Random k-CNF

Definition 3.15. *A random k-CNF is a formula $F \sim \mathcal{F}_k^{n,\Delta}$ with n variables that is generated by picking randomly and independently $\Delta \cdot n$ clauses from the set of all $2^k \binom{n}{k}$ clauses of width k.*

The following theorem explains the known degree lower bounds for random k-CNFs in $\mathsf{PC}_{\mathbb{F}}$.

Theorem 3.5. *([AR01]) Let $F \sim \mathcal{F}_k^{n,\Delta}$, $k \geq 3$ and $\Delta = \Delta(n)$ is such that $\Delta = o(n^{\frac{k-2}{2}})$. Then every $\mathsf{PC}_{\mathbb{F}}$-refutation of F has degree $\Omega(\frac{n}{\Delta^{2/(k-2)} \cdot \log \Delta})$ with probability $1 - o(1)$ for any field $\mathbb{F}$.*

It is not hard to show that if $F \sim \mathcal{F}_k^{n,\Delta}$ and Δ satisfies the assumption of the theorem, then with probability $1 - o(1)$ F is unsatisfiable (see [CS88]).

3.3.3 Pigeonhole principle and Counting mod q principle

Definition 3.16. *(Pigeonhole principle) The CNF formula FPHP_n^m ($m > n$) is the set of the following clauses over the variables $\{p_{i,j} : 1 \leq i \leq m, 1 \leq j \leq n\}$:*

1. *For every $1 \leq i \leq m$:*
$$P_i := \bigvee_{1 \leq j \leq n} p_{i,j}.$$

2. *For every $1 \leq i, j \leq m, i \neq j, 1 \leq k \leq n$:*
$$P_{i,j \to k} := \neg p_{i,k} \vee \neg p_{j,k}.$$

3. *For every $1 \leq i, j \leq n, i \neq j, 1 \leq k \leq m$:*
$$P_{k \to i,j} := \neg p_{k,i} \vee \neg p_{k,j}.$$

As the algebraization of P_i has degree n, we cannot get a meaningful $\mathsf{PC}_{\mathbb{F}}$ degree lower bound for it. To solve this matter we use the algebraic Pigeonhole principle ($a\mathsf{PHP}_n^m$) which has the set of the clauses of FPHP_n^m except that each P_i clause is replaced by the linear form $-1 + \sum_{j=1}^n p_{i,j}$. We have the following degree lower bound for $a\mathsf{PHP}_n^m$.

Theorem 3.6. *([Raz98]) For any $m > n$ and any field $\mathbb{F}$, every $\mathsf{PC}_{\mathbb{F}}$-refutation of $a\mathsf{PHP}_n^m$ has degree at least $n/2 + 1$.*

Definition 3.17. *(Counting mod q principle) The CNF formula Count_q^n ($n \equiv 1 \pmod q$) is the set of following clauses over the variables x_e where e ranges over all q elements subset of $\{1, ..., n\}$ (we denote this set as U):*

1. *For every $1 \leq i \leq n$:*
$$Q_i := \bigvee_{\{e \in U | i \in e\}} x_e.$$

2. *For every different $e, e' \in U$ such that $e \cap e' \neq \varnothing$:*
$$Q_{e,e'} := \neg x_e \vee \neg x_{e'}.$$

Again to have a meaningful $\mathsf{PC}_{\mathbb{F}}$ degree lower bound, we define the algebraic Counting mod q principle ($a\mathsf{Count}_q^n$) which has the same clauses as Count_q^n except that each Q_i is replaced by the linear form $-1+\sum_{\{e\in U|i\in e\}} x_e$. We have the following $\mathsf{PC}_{\mathbb{F}}$ degree lower bound for $a\mathsf{Count}_q^n$.

Theorem 3.7. *([BGIP01]) Let $p \geq 2$ be a prime such that $p \not| q$ and let $\mathbb{F}$ be a field of characteristic p. Then any $\mathsf{PC}_{\mathbb{F}}$-refutation of $a\mathsf{Count}_q^n$ requires degree δn, for a constant $\delta > 0$.*

We need the following lemma which relates $\mathsf{S}^*_{d,R}(F)$ to $\mathsf{S}^*_{d,R}(aF)$ where $F \in \{\mathsf{FPHP}_n^m, \mathsf{Count}_q^n\}$.

Lemma 3.8. *Let $\{x_1, ..., x_n\}$ be a set of variables and $C := \bigvee_{1\leq i\leq n} x_i$. Then there exists a $\mathsf{Res}^*(\mathsf{PC}_{d,R})$-derivation of C from $-1+\sum_{j=1}^n x_i$ of size $2n-1$.*

Proof. Let π be the following sequence of clauses:

1. $\pi_1 := -1+\sum_{j=1}^n x_i$.
2. For $1 \leq k \leq n-1$,
$$\pi_{k+1} := x_k \vee (x_k - 1).$$
3. For $1 \leq k \leq n-1$,
$$\pi_{n+k} := (-1+\sum_{j=k+1}^{n} x_j) \vee \bigvee_{u=1}^{k} (x_u - 1).$$

It is easy to see that π satisfies the desired properties.

□

4 Main results

In this section, we mention the main results of this paper. The main theorem is a size-width relation for (tree-like) $\mathsf{Res}(\mathsf{PC}_{d,R})$ when R is a finite ring (for the proof see Section 4).

Theorem 4.1. *(Size-Width relation) Let R be a finite ring and F be an unsatisfiable CNF_d in n variables, then the following inequalities hold:*

1. $\frac{\mathsf{w}_{d,R}(F)}{|R|} - 1 \leq \max\{3, \mathsf{w}(F)\} + \log(3\mathsf{S}^*_{d,R}(F))$.
2. *If F is a CNF formula, then*
$$\frac{\mathsf{w}_{d,R}(F)}{|R|} \leq \max\{3, \mathsf{w}(F)\} + O\left(\sqrt{\left(n + \mathsf{S}_{d,R}(F)\right)\log(\mathsf{S}_{d,R}(F))}\right).$$

where log *is the binary logarithm.*

Another statement which we need to prove the lower bounds is the following lemma. This lemma shows that Theorem 45 in [PT20] holds for the general proof system $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$ when $\mathbb{F}$ is a finite field (for the proof see Section 4).

Lemma 4.2. *Let F be a CNF$_d$ and $H_F = \{h_C | C \in F\}$. Then for every finite field $\mathbb{F}$ such that char$(\mathbb{F}) = p$ and every clause C', if $F \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{w} C'$, then $H_F \vdash^{\mathsf{PC}_{\mathbb{F}}}_{pwd} h_{C'}$.*

An easy and direct consequence of Theorem 4.1 and Lemma 4.3 is the following corollary which is the main tool for proving our lower bounds.

Corollary 4.3. *Let $\mathbb{F}$ be a finite field such that char$(\mathbb{F}) = p$ and F be an unsatisfiable CNF$_d$ in n variables such that every $\mathsf{PC}_{\mathbb{F}}$-refutation of F requires degree d'. Then the following inequalities hold:*

1. $\log(\mathsf{S}^*_{d,\mathbb{F}}(F)) \geq \Omega\left(\frac{d'}{|\mathbb{F}|pd} - \mathsf{w}(F)\right)$.
2. *If F is a CNF formula, then*

$$\sqrt{(n + \mathsf{S}_{d,\mathbb{F}}(F)) \log\left(\mathsf{S}_{d,\mathbb{F}}(F)\right)} \geq \Omega\left(\frac{d'}{|\mathbb{F}|pd} - \mathsf{w}(F)\right).$$

4.1 Lower bounds for the hard formulas

The following corollaries explain the new lower bounds. The general strategy to prove these lower bounds is to combine Corollary 4.3 with suitable PC degree lower bounds. It is worth mentioning that Corollaries 4.4, 4.5, and 4.6 use the same proof pattern and Corollaries 4.7 and 4.8 use a second proof pattern. Therefore, we just state the proofs of Corollaries 4.4 and 4.7.

Corollary 4.4. *(Mod q Tseitin formula) Let $\mathbb{F}$ be a finite field and q be a fixed prime such that char$(\mathbb{F}) \neq q$, then there exists a constant d_q such that the following holds. If $c \geq d_q$, then for every large enough n and every c-regular Ramanujan graph G on n nodes (augmented with arbitrary orientation of its edges) and for every function σ such that $\mathsf{TS}_q(G, \sigma)$ is unsatisfiable,*

1. *If d is a fixed constant, then $\mathsf{S}_{d,\mathbb{F}}(\mathsf{TS}_q(G, \sigma)) \geq n^{2-\frac{(\log\log n)^2}{\log n}}$.*
2. $\mathsf{S}^*_{d,\mathbb{F}}(\mathsf{TS}_q(G, \sigma)) = 2^{\Omega(\frac{n}{|\mathbb{F}|pd})}$ *(here d can be a function of n).*

Proof. Here we prove the first part as the proof of the second part is similar. Suppose for a large enough n, $\mathsf{S}_{d,\mathbb{F}}(\mathsf{TS}_q(G, \sigma)) < n^{2-\frac{(\log\log n)^2}{\log n}}$. Then by Theorem 3.3 and Corollary 4.3 there exists an $\epsilon > 0$ such that

$$\left(n + n^{2-\frac{(\log\log n)^2}{\log n}}\right) \log(n^{2-\frac{(\log\log n)^2}{\log n}}) \geq \Omega\left(\left(\frac{\epsilon c n}{|\mathbb{F}|pd} - c\right)^2\right),$$

but this is not true because $n^{2-\frac{(\log\log n)^2}{\log n}} \log(n^{2-\frac{(\log\log n)^2}{\log n}}) = o(n^2)$, hence we get a contradiction and this completes the proof. □

Corollary 4.5. *(Flow formula) Let $\mathbb{F}$ be a finite field. If $c \geq 255$, then for every large enough n and every c-regular Ramanujan graph G on n nodes (augmented with arbitrary orientation of its edges),*

1. *If d is a fixed constant, then $\mathsf{S}_{d,\mathbb{F}}(\mathsf{Fl}(G)) \geq n^{2-\frac{(\log\log n)^2}{\log n}}$.*

2. $\mathsf{S}^*_{d,\mathbb{F}}(\mathsf{FI}(G)) = 2^{\Omega(\frac{n}{pd|\mathbb{F}|})}$ *(here d can be a function of n).*

Corollary 4.6. *(Random k-CNF) Let $\mathbb{F}$ be a finite field, $F \sim \mathcal{F}_k^{n,\Delta}$, $k \geq 3$ and $\Delta = \Delta(n)$ is such that $\Delta = o(n^{\frac{k-2}{2}})$. Then with probability $1 - o(1)$:*

1. *If d is a fixed constant and $\Delta = c$ for a constant such that $c2^{-k} \geq 0.7$, then $\mathsf{S}_{d,\mathbb{F}}(F) \geq n^{2-\frac{(\log\log n)^2}{\log n}}$.*

2. $\mathsf{S}^*_{d,\mathbb{F}}(F) = 2^{\Omega\left(\frac{n}{|\mathbb{F}|pd\Delta^{2/(k-2)}\log\Delta}\right)}$ *(here d can be a function of n).*

Corollary 4.7. *(Pigeonhole principle) Let $\mathbb{F}$ be a finite field of characteristic p. Then for every m, n $(m > n)$ and every d, $\mathsf{S}^*_{d,\mathbb{F}}(\mathsf{FPHP}^m_n) = \frac{2^{\Omega\left(\frac{n}{|\mathbb{F}|pd}\right)}}{n}$.*

Proof. First, we show that $\mathsf{S}^*_{d,\mathbb{F}}(a\mathsf{PHP}^m_n) = 2^{\Omega\left(\frac{n}{|\mathbb{F}|pd}\right)}$. Note that by Theorem 3.6 and Corollary 4.3

$$\log(\mathsf{S}^*_{d,\mathbb{F}}(a\mathsf{PHP}^m_n)) \geq \Omega\left(\frac{n}{|\mathbb{F}|pd} - 2\right).$$

This implies that $\mathsf{S}^*_{d,\mathbb{F}}(a\mathsf{PHP}^m_n) = 2^{\Omega\left(\frac{n}{|\mathbb{F}|pd}\right)}$. To complete the proof we show that a $\mathsf{Res}^*(\mathsf{PC}_{d,\mathbb{F}})$-refutation of FPHP^m_n of size s can be transformed into a $\mathsf{Res}^*(\mathsf{PC}_{d,\mathbb{F}})$-refutation of $a\mathsf{PHP}^m_n$ of size at most $2ns$ and this gives the desired lower bound. Let π be a minimal size $\mathsf{Res}^*(\mathsf{PC}_{d,\mathbb{F}})$-refutation of FPHP^m_n ($|\pi| = \mathsf{S}^*_{d,\mathbb{F}}(\mathsf{FPHP}^m_n)$). To transform π to a refutation of $a\mathsf{PHP}^m_n$ which we call it π', it is sufficient to derive every P_i clause that is used in π from $a\mathsf{PHP}^m_n$ and then concatenate these derivations to the beginning of π. Note that there are at most $|\pi|$ many times usage of the P_i clauses in π. So by Lemma 9.3

$$|\pi'| \leq (2n-1)|\pi| + |\pi| = 2n|\pi|.$$

Therefore $\mathsf{S}^*_{d,\mathbb{F}}(\mathsf{FPHP}^m_n) = \frac{2^{\Omega\left(\frac{n}{|\mathbb{F}|pd}\right)}}{n}$. □

Corollary 4.8. *(Counting mod q principle) Let $\mathbb{F}$ be a finite field of characteristic p where $p \not| q$. Then for every n and every d, $\mathsf{S}^*_{d,\mathbb{F}}(\mathsf{Count}^n_q) = \frac{2^{\Omega\left(\frac{n}{|\mathbb{F}|pd}\right)}}{\binom{n-1}{q-1}}$.*

It is worth mentioning that the lower bound for FPHP^m_n when $d = 1$ was proved using the generalized prover-delayer games in the previous works [IS20, PT20], but here we prove it using the application of the size-width relation. Moreover, our lower bound for FPHP^m_n matches the previous lower bounds in [IS20, PT20] up to a multiplicative constant in the exponent. Regarding $d > 1$ (even non-constant ones), it implies strong lower bounds (at least super-polynomial for even big values of m and d) for tree-like $\mathsf{R}(\mathsf{PC}_{d,\mathbb{F}_2})$ system of Krajíček [Kra18] for FPHP^m_n. Moreover, the last corollary gives a new proof of the same result in [GK18].

5 Size, width, degree and their relations

This section is dedicated to the proofs of Theorem 4.1 and Lemma 4.3.

Proposition 5.1. *For every ring R, and every monomial $M = \prod_{i=1}^{n} x_i^{d_i}$ of degree d,*

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{2}\, M \vee (M-1).$$

Proof. We prove this proposition by induction on d. The statement is true when $d \leq 1$ as $\mathsf{Res}(\mathsf{PC}_{d,R})$ has Boolean axioms for every variable and also 0 is an axiom. Let $M = x'M'$ with degree $d = k+1$. By induction hypothesis

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{k,R})}{2}\, M' \vee (M'-1).$$

So by two times using of the multiplication rule we get

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{k+1,R})}{2}\, x'M' \vee (x'M'-x').$$

Note that $x' \vee x'-1$ is an axiom in $\mathsf{Res}(\mathsf{PC}_{k+1,R})$, and hence by k times using the multiplication rule we get

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{k+1,R})}{2}\, x'M' \vee (x'-1).$$

By applying the resolution rule on $x'M' \vee (x'M'-x')$ and $x'M' \vee (x'-1)$, we get

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{k+1,R})}{2}\, x'M' \vee (x'M'-1).$$

□

The following proposition shows that something similar to Proposition 10 in [PT20] holds for multivariate polynomials when we are working with $\mathsf{Res}(\mathsf{PC}_{d,R})$.

Proposition 5.2. *Let R be a finite ring. Then for every multivariate polynomial $f \in R[x_1, ..., x_n]$ of degree d,*

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|+1} \bigvee_{a\in R} (f-a).$$

Proof. We prove the proposition by induction on the number of non-zero degree monomials in f. The statement is true for multivariate polynomial $f = b$, $(b \in R)$, because 0 is an axiom and we can use the weakening rule on 0 to derive the desired clause. Let $f = bM + g$ such that $M = \prod_{i=1}^{n} x_i^{d_i}$ is a non-zero degree monomial and $b \in R \setminus \{0\}$. g has one less non-zero degree monomial than f, hence by induction hypothesis,

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|+1} \bigvee_{a\in R} (g-a).$$

By Proposition 11,

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{2}\, M \vee (M-1).$$

So by using $|R|$ times resolution rule we get

$$\varnothing \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|+1} (M-1) \vee \bigvee_{a\in R} (bM+g-a).$$

By the same argument, we get

$$\varnothing \Big|\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|+1}\; M \vee \bigvee_{a\in R}(bM+g-a-b).$$

Therefore by the resolution rule on $M \vee \bigvee_{a\in R}(bM+g-a-b)$ and $(M-1)\vee \bigvee_{a\in R}(bM+g-a)$ and a simplification rule we have

$$\varnothing \Big|\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|+1}\; \bigvee_{a\in R}(f-a).$$

□

For every multivariate polynomial $f \in R[x_1, ..., x_n]$, fix an atomic variable q_f. These atomic variables are going to be the translation of multivariate polynomials. For every CNF$_d$ formula F and every $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutation π of F, we use the following simple mapping to translate the multivariate polynomials that appear in clauses of π to atomic variables:

$$Q(f) = q_f.$$

For a clause C, $Q(C)$ is $\bigvee_{r\in C} Q(r)$ $(Q(\emptyset) = \emptyset)$ and for a CNF$_d$ formula $F = \{C_1, ..C_k\}$, $Q(F)$ is $\{Q(C_1), ..., Q(C_k)\}$.

The general plan is to translate an arbitrary $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutation to a Resolution refutation using the $\{q_f\}_{f\in R[x_1,...,x_n]}$ variables. To this end, we define the CNF formula $\mathsf{Ex}(\pi)$ which contains the following clauses:

1. If the simplification rule is used on a non-zero constant multivariate polynomial a in π, then $\neg q_a \in \mathsf{Ex}(\pi)$.

2. $q_{x_i} \vee q_{x_i - 1} \in \mathsf{Ex}(\pi)$, if the axiom $x_i \vee (x_i - 1)$ is used in π.

3. $q_0 \in \mathsf{Ex}(\pi)$, if the axiom 0 is used in π.

4. If the resolution rule is used in π to derive $af + bg$ from f and g, then

$$\neg q_f \vee \neg q_g \vee q_{af+bg} \in \mathsf{Ex}(\pi).$$

5. If the multiplication rule is used to derive $g \cdot f$ from f, then

$$\neg q_f \vee q_{g\cdot f} \in \mathsf{Ex}(\pi).$$

We need another translation from clauses definable in $V(\mathsf{Ex}(\pi)\cup Q(F))$ to clauses of multivariate polynomials of degree at most d over $V(F)$. For this, we define a mapping from these variables to multivariate polynomials and hence, clauses of these literals automatically translate to clauses of multivariate polynomials. This mapping is defined as follows:

$$Q'(r) = \begin{cases} f & r = q_f \\ \bigvee_{a\in R\setminus\{0\}}(f-a) & r = \neg q_f \end{cases}$$

For a clause C, $Q'(C)$ is $\bigvee_{r\in C} Q'(r)$ $(Q'(\emptyset) = \emptyset)$. Let C be a clause of literals or multivariate polynomials, then $\mathsf{m}[C]$ is the set of disjuncts of C, so $\mathsf{w}(C) = |\mathsf{m}[C]|$. The following lemma is the core for proving the size-width relation.

Lemma 5.3. *For a finite ring R and every CNF_d formula F, let π be a $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutation of F, then the following statements are true:*

1. *There exists a Res-refutation π' of $\mathsf{Ex}(\pi) \cup Q(F)$ such that $|\pi'| \leq 3|\pi|$. Moreover, if π is tree-like, then π' is also tree-like.*

2. *If F is a CNF, then $|V(\mathsf{Ex}(\pi) \cup Q(F))| \leq 2n + 3|\pi|$.*

3. *For every clause C' in variables of $\mathsf{Ex}(\pi) \cup Q(F)$, if*

$$\mathsf{Ex}(\pi) \cup Q(F) \mid\!\frac{\mathsf{Res}}{w}\, C',$$

then

$$F \mid\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|(w+1)}\, Q'(C').$$

Proof. To prove item 1 we do as follows. Let π_s be a sub-sequence of π such that a clause C in π is in π_s iff there exists a directed path from C to the empty clause in G_π. Note that π is a $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutation of F, hence π_s becomes a $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutation of F too. The important property of π_s is the following claim.

Claim 5.1. *Let $f \in R[x_1, ..., x_n]$ be a multivariate polynomial, then if the step*

$$\frac{C}{C \vee f}$$

exists in π_s for some clause C, then $q_f \in V(\mathsf{Ex}(\pi))$.

Proof. Suppose such a step exists in π_s for f and a clause C. Note that according to the definition of π_s, there exists a directed path P from $C \vee f$ to the empty clause in G_π and moreover, P also exists in G_{π_s}. P starts from $C \vee f$ to $\emptyset$, hence there should be a step in P such that either one of the resolution rule, or the multiplication rule, or the simplification rule is used on f. This implies that q_f or its negation is appeared in one of the clauses of $\mathsf{Ex}(\pi)$ and hence $q_f \in V(\mathsf{Ex}(\pi))$. □

Now we are ready to prove the statement of the lemma. Let $\pi_s = D_1, ..., D_l$. We want to construct a sequence $\pi'_1 \sqsubseteq \pi'_2 \sqsubseteq ...\pi'_l$ from π_s by iterating the following process on D_is starting from D_1. Suppose we have constructed $\pi'_{i-1} = D'_1, ..., D'_u$ (for some u) from π'_{i-2} and D_{i-1} and now we want to construct π'_i:

1. If D_i is a clause of F, then $Q(D_i)$ is a clause of $Q(F)$ and $\pi'_i = \pi'_{i-1}, Q(D_i)$.

2. If $D_i := x_j \vee (x_j - 1)$ for some j, then $q_{x_j} \vee q_{x_j-1}$ is a clause of $\mathsf{Ex}(\pi)$ and $\pi'_i = \pi'_{i-1}, q_{x_j} \vee q_{x_j-1}$.

3. If $D_i := 0$, then q_0 is a clause of $\mathsf{Ex}(\pi)$ and $\pi'_i = \pi'_{i-1}, q_0$.

4. If $D_i = C \vee C' \vee (af + bg)$ and it is derived from $D_j = C \vee f$ and $D_k = C' \vee g$ by the resolution rule, then if

   (a) $f \neq g$:
   Then $\neg q_f \vee \neg q_g \vee q_{af+bg}$ is a clause of $\mathsf{Ex}(\pi)$ and moreover, $Q(C) \vee q_f$ and $Q(C') \vee q_g$ are the last clauses of π'_j and π'_k respectively. So π'_i is π'_{i-1} appended by the following clauses:

i. $\neg q_f \vee \neg q_g \vee q_{af+bg}$,

ii. $Q(C) \vee \neg q_g \vee q_{af+bg}$,

iii. $Q(C) \vee Q(C') \vee q_{af+bg}$.

So the appended derivation is the following:

$$\dfrac{\dfrac{\overline{Q(C) \vee q_f} \qquad \neg q_f \vee \neg q_g \vee q_{af+bg}}{Q(C) \vee \neg q_g \vee q_{af+bg}} \qquad \overline{Q(C') \vee q_g}}{Q(C) \vee Q(C') \vee q_{af+bg}}$$

(b) $f = g$:

Then $\neg q_f \vee q_{af+bf}$ is a clause of $\mathsf{Ex}(\pi)$ and moreover, $Q(C) \vee q_f$ is the last clause of π'_j. So π'_i is π'_{i-1} appended by the following clauses:

i. $\neg q_f \vee q_{af+bf}$,

ii. $Q(C) \vee q_{af+bf}$,

iii. $Q(C) \vee Q(C') \vee q_{af+bf}$.

So the appended derivation is the following:

$$\dfrac{\dfrac{\overline{Q(C) \vee q_f} \qquad \neg q_f \vee q_{af+bf}}{Q(C) \vee q_{af+bf}}}{Q(C) \vee Q(C') \vee q_{af+bf}}$$

5. If $D_i = C \vee f$ and it is derived from $D_j = C$ by the weakening rule, then by Claim 5.1 $q_f \in V(\mathsf{Ex}(\pi))$. Moreover, $Q(C)$ is the last clause of π'_j. So $\pi'_i = \pi'_{i-1}, Q(C) \vee q_f$. So the appended derivation is the following:

$$\dfrac{\overline{Q(C)}}{Q(C) \vee q_f}$$

6. If $D_i = C$ and it is derived from $D_j = C \vee a$ ($a \in R \setminus \{0\}$) by the simplification rule, then $\neg q_a$ is a clause of $\mathsf{Ex}(\pi)$. Moreover, $Q(C) \vee q_a$ is the last clause of π'_j. So $\pi'_i = \pi'_{i-1}, \neg q_a, Q(C)$. So the appended derivation is the following:

$$\dfrac{\overline{Q(C) \vee q_a} \qquad \neg q_a}{Q(C)}$$

7. If $D_i = C \vee g \cdot f$ and it is derived from $D_j = C \vee f$ by the multiplication rule, then $\neg q_f \vee q_{g \cdot f}$ is a clause of $\mathsf{Ex}(\pi)$. Moreover, $Q(C) \vee q_f$ is the last clause of π'_j. So $\pi'_i = \pi'_{i-1}, \neg q_f \vee q_{g \cdot f}, Q(C) \vee q_{g \cdot f}$. So the appended derivation is the following:

$$\dfrac{\overline{Q(C) \vee q_f} \qquad \neg q_f \vee q_{g \cdot f}}{Q(C) \vee q_{g \cdot f}}$$

It is easy to verify that $\pi' := \pi'_l$ is a Res-refutation of $\mathsf{Ex}(\pi) \cup Q(F)$. The reason is that for the cases (a), (b), and (c), the appended clauses are in $\mathsf{Ex}(\pi) \cup Q(F)$. For case (e), the weakening rule of Resolution is used. For the remaining cases, the resolution rule is used. The initial clauses are the clauses of $\mathsf{Ex}(\pi) \cup Q(F)$ and the last clause in π' is the empty clause, hence π' is a Res-refutation of $\mathsf{Ex}(\pi) \cup Q(F)$. It is apparent from the explanations that if π is tree-like, then π' is also tree-like. Note that for every i the inequality $|\pi'_i| \leq |\pi'_{i-1}| + 3$ holds, hence $|\pi'| \leq 3|\pi|$.

To prove item 2, note that F is a CNF, so as a CNF_1, every disjunct in a clause of it is of the form of x or $x - 1$ where $x \in V(F)$. By the fact that F has n variables, we can deduce that $|V(Q(F))| \leq 2n$. Moreover, if we look at the way $\mathsf{Ex}(\pi)$ was constructed, we can see that for every step in π, we add a clause with at most three new variables to $\mathsf{Ex}(\pi)$, so this implies $|V(\mathsf{Ex}(\pi))| \leq 3|\pi|$.

We prove item 3 by induction on the number of steps of deriving C'. For the base step, we argue as follows. If the number of steps in deriving C' is one, then C' is one of the initial clauses of $\mathsf{Ex}(\pi) \cup Q(F)$. Therefore we have the following cases:

1. $C' \in Q(F)$:

   In this case $Q'(C')$ is a clause of F, so
   $$F \mid\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{w} Q'(C').$$

2. $C' = q_0$:

   0 is an axiom of $\mathsf{Res}(\mathsf{PC}_{d,R})$, so
   $$\varnothing \mid\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{1} 0.$$

3. $C' = \neg q_a$ for some $a \in R \setminus \{0\}$:

   Note that $Q'(\neg q_a) = \bigvee_{b \in R \setminus \{0\}} (a - b)$ which is $\bigvee_{b \in R \setminus \{a\}} b$. 0 is an axiom of $\mathsf{Res}(\mathsf{PC}_{d,R})$, so by $|R| - 1$ times use of the weakening rule we get
   $$\varnothing \mid\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|-1} \bigvee_{b \in R \setminus \{a\}} b.$$

4. $C' = q_{x_i} \vee q_{x_i - 1}$:

   $Q'(q_{x_i} \vee q_{x_i - 1})$ is $x_i \vee (x_i - 1)$ which is an axiom of $\mathsf{Res}(\mathsf{PC}_{d,R})$, so
   $$\varnothing \mid\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{2} x_i \vee (x_i - 1).$$

5. $C' = \neg q_f \vee \neg q_g \vee q_{af+bg}$:

   (a) $f \neq g$:

   Note that
   $$\mathsf{Ex}(\pi) \cup Q(F) \mid\frac{\mathsf{Res}}{3} C'.$$

   By Proposition 12,
   $$\varnothing \mid\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|+1} \bigvee_{c \in R} (f - c)$$

and

$$\varnothing \mathrel{\vdash^{\mathsf{Res}(\mathsf{PC}_{d,R})}_{|R|+1}} \bigvee_{c\in R} (g-c),$$

hence by the resolution rule we get

$$\varnothing \mathrel{\vdash^{\mathsf{Res}(\mathsf{PC}_{d,R})}_{2|R|-1}} (af+bg) \vee \bigvee_{c\in R\setminus\{0\}} (f-c) \vee \bigvee_{c\in R\setminus\{0\}} (g-c).$$

(b) $f = g$:

Note that

$$\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\vdash^{\mathsf{Res}}_{2}} C'$$

because $C' = \neg q_f \vee q_{af+bf}$. By Proposition 12,

$$\varnothing \mathrel{\vdash^{\mathsf{Res}(\mathsf{PC}_{d,R})}_{|R|+1}} \bigvee_{c\in R} (f-c),$$

hence by the multiplication rule we get

$$\varnothing \mathrel{\vdash^{\mathsf{Res}(\mathsf{PC}_{d,R})}_{|R|+1}} (a+b)f \vee \bigvee_{c\in R\setminus\{0\}} (f-c).$$

6. $C' = \neg q_f \vee q_{g\cdot f}$:

Note that

$$\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\vdash^{\mathsf{Res}}_{2}} C'.$$

By Proposition 12,

$$\varnothing \mathrel{\vdash^{\mathsf{Res}(\mathsf{PC}_{d,R})}_{|R|+1}} \bigvee_{c\in R} (f-c),$$

hence by the multiplication rule we get

$$\varnothing \mathrel{\vdash^{\mathsf{Res}(\mathsf{PC}_{d,R})}_{|R|+1}} g\cdot f \vee \bigvee_{c\in R\setminus\{0\}} (f-c).$$

For the induction step, the argument goes as follows:

1. Resolution rule:

   Suppose C and D are clauses in variables of $\mathsf{Ex}(\pi) \cup Q(F)$ such that

   $$\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\vdash^{\mathsf{Res}}_{w}} C \vee D$$

   in $k+1$ steps. Moreover, assume the last rule is an application of the resolution rule on $C \vee q_f$ and $D \vee \neg q_f$ such that $q_f \in V(\mathsf{Ex}(\pi) \cup Q(F))$. Therefore

   (a) $\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\vdash^{\mathsf{Res}}_{w_1}} C \vee q_f$ in at most k steps.

   (b) $\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\vdash^{\mathsf{Res}}_{w_2}} D \vee \neg q_f$ in at most k steps.

   So $w = \max\{w_1, w_2, \mathsf{w}(C \vee D)\}$. Moreover, by induction hypothesis

(a) $F \mathrel{\Big|}\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|(w_1+1)} Q'(C \vee q_f)$.

(b) $F \mathrel{\Big|}\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|(w_2+1)} Q'(D \vee \neg q_f)$.

Note that $Q'(q_f) = f$ and $Q'(\neg q_f) = \bigvee_{c \in R \setminus \{0\}} (f - c)$. Let

$$H := \{f - c | c \in R\},$$

then by applying the resolution and simplification rules $|R| - 1$ times, we can derive

$$E := \bigvee_{g \in \mathsf{m}[Q'(C \vee D)] \setminus H} g$$

from $Q'(C \vee q_f)$ and $Q'(D \vee \neg q_f)$. Note that $\mathsf{m}[E] \subseteq \mathsf{m}[Q'(C \vee D)]$. The width of deriving E is at most

$$\max \{(w_1 + 1)|R|, (w_2 + 1)|R|, \mathsf{w}(Q'(C \vee D)) + |R| - 1\}$$

which is less than or equal to

$$\max \{(w_1 + 1)|R|, (w_2 + 1)|R|, (\mathsf{w}(C \vee D) + 1)(|R| - 1)\},$$

which is less than or equal to

$$|R|(\max \{w_1, w_2, \mathsf{w}(C \vee D)\} + 1).$$

If $\mathsf{m}[Q'(C \vee D)] \cap H = \varnothing$, then we are done, otherwise $\mathsf{m}[Q'(C \vee D)] \setminus H \subsetneq \mathsf{m}[Q'(C \vee D)]$. In this case, $\{E\} \mathrel{\Big|}\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{\mathsf{w}(Q'(C \vee D))} Q'(C \vee D)$ by applications of the weakening rule, so the width of deriving $Q'(C \vee D)$ is at most

$$\max\{Q'(C \vee D), |R|(\max \{w_1, w_2, \mathsf{w}(C \vee D)\} + 1)\}$$

which is less than or equal to

$$|R|(\max \{w_1, w_2, \mathsf{w}(C \vee D)\} + 1).$$

2. Weakening rule:

Suppose C and D are clauses in variables of $\mathsf{Ex}(\pi) \cup Q(F)$ such that

$$\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\Big|}\!\frac{\mathsf{Res}}{w} C \vee D$$

in $k + 1$ steps. Moreover, assume that the last rule is an application of the weakening rule on C. Therefore

(a) $\mathsf{Ex}(\pi) \cup Q(F) \mathrel{\Big|}\!\frac{\mathsf{Res}}{w_1} C$ in at most k steps.

So $w = \max\{w_1, \mathsf{w}(C \vee D)\}$. Moreover, by induction hypothesis

(a) $F \mathrel{\Big|}\!\frac{\mathsf{Res}(\mathsf{PC}_{d,R})}{|R|(w_1+1)} Q'(C)$.

If $D = \bigvee_{q_f \in A} q_f \vee \bigvee_{q_g \in B} \neg q_g$ where $A, B \subseteq V(\mathsf{Ex}(\pi) \cup Q(F))$, then

$$\mathsf{m}[Q'(D)] \subseteq \{f | q_f \in A\} \cup \{g - c | c \in R \setminus \{0\}, q_g \in B\},$$

so by applying the weakening rule at most $|A| + |B|(|R| - 1)$ times on $Q'(C)$, we can derive $Q'(C \vee D)$. The width of deriving $Q'(C \vee D)$ is at most

$$\max\{(w_1 + 1)|R|, \mathsf{w}(Q'(C \vee D))\}$$

which is less than or equal to

$$\max\{(w_1 + 1)|R|, \mathsf{w}(C \vee D)(|R| - 1)\},$$

which is less than or equal to

$$|R|(\max\{w_1, \mathsf{w}(C \vee D)\} + 1).$$

□

5.1 Proof of Theorem 4.1

1. Let π be a minimal size $\mathsf{Res}^*(\mathsf{PC}_{d,R})$-refutation of F ($|\pi| = \mathsf{S}^*_{d,R}(F)$). By the first part of Lemma 9.1,

$$\mathsf{S}_{\mathsf{Res}^*}(\mathsf{Ex}(\pi) \cup Q(F)) \leq 3\mathsf{S}^*_{d,R}(F).$$

   On the other hand, by the third part of Lemma 9.1,

$$\frac{\mathsf{w}_{d,R}(F)}{|R|} - 1 \leq \mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)).$$

   Furthermore, $\mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) \leq \max\{3, \mathsf{w}(F)\}$, because $\mathsf{w}(\mathsf{Ex}(\pi)) \leq 3$ by the way we constructed it. Note that by the first inequality of Theorem 19.2

$$\mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)) \leq \mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) + \log\left(\mathsf{S}_{\mathsf{Res}^*}(\mathsf{Ex}(\pi) \cup Q(F))\right).$$

   So putting these inequalities together we get

$$\frac{\mathsf{w}_{d,R}(F)}{|R|} - 1 \leq \max\{3, \mathsf{w}(F)\} + \log(3\mathsf{S}^*_{d,R}(F)).$$

2. The proof of this part is similar to the proof of the previous part with some extra changes. Let π be a minimal size $\mathsf{Res}(\mathsf{PC}_{d,R})$-refutation of F ($|\pi| = \mathsf{S}_{d,R}(F)$). By the first part of Lemma 9.1,

$$\mathsf{S}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)) \leq 3\mathsf{S}_{d,R}(F).$$

   On the other hand, by the third part of Lemma 9.1,

$$\frac{\mathsf{w}_{d,R}(F)}{|R|} - 1 \leq \mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)).$$

Furthermore, $\mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) \leq \max\{3, \mathsf{w}(F)\}$, because $\mathsf{w}(\mathsf{Ex}(\pi)) \leq 3$ by the way we have constructed it. Note that by the second inequality of Theorem 19.2

$$\mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)) \leq \mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) +$$

$$O\left(\sqrt{|V\left(\mathsf{Ex}(\pi) \cup Q(F)\right)| \log(\mathsf{S}_{\mathsf{Res}}\left(\mathsf{Ex}(\pi) \cup Q(F)\right))}\right).$$

so putting these inequalities together we get

$$\frac{\mathsf{w}_{d,R}(F)}{|R|} \leq \max\{3, \mathsf{w}(F)\} + O\left(\sqrt{|V\left(\mathsf{Ex}(\pi) \cup Q(F)\right)| \log(\mathsf{S}_{d,R}(F))}\right).$$

To complete the proof, it is sufficient to bound the value of $|V(\mathsf{Ex}(\pi) \cup Q(F))|$ and by the second part of Lemma 9.1 we know

$$|V(\mathsf{Ex}(\pi) \cup Q(F))| \leq 2n + 3\mathsf{S}_{d,R}(F),$$

so we get the desired inequality which is

$$\frac{\mathsf{w}_{d,R}(F)}{|R|} \leq \max\{3, \mathsf{w}(F)\} + O\left(\sqrt{(n + \mathsf{S}_{d,R}(F)) \log(\mathsf{S}_{d,R}(F))}\right).$$

□

5.2 Proof of Lemma 4.2

The proof of this lemma is similar to the proof of Theorem 45 in [PT20] using induction on the number of the steps in a derivation of C' from F. For the base step, we argue as follows. If the number of steps in deriving C' is one, then C' is one of the initial clauses of F or an axiom. Therefore we have the following cases:

1. $C' \in F$:

   In this case

   $$C' \left|\frac{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}{\mathsf{w}(C')}\right. C',$$

   so

   $$\{h_{C'}\} \left|\frac{\mathsf{PC}_{\mathbb{F}}}{d\mathsf{w}(C')}\right. h_{C'}.$$

2. 0:

   0 is an axiom of $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$, so

   $$\varnothing \left|\frac{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}{1}\right. 0.$$

   Note that $x_i^2 - x_i$ is an axiom in $\mathsf{PC}_{\mathbb{F}}$. So we can derive 0 by using the addition rule on $x_i^2 - x_i$, therefore

   $$\varnothing \left|\frac{\mathsf{PC}_{\mathbb{F}}}{2}\right. 0.$$

3. $x_i \vee (x_i - 1)$:

   $x_i \vee (x_i - 1)$ is an axiom of $\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})$, so
   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{2} x_i \vee (x_i - 1).$$
   Furthermore, $h_{x_i \vee (x_i - 1)}$ is $x_i^2 - x_i$ which is an axiom of $\mathsf{PC}_{\mathbb{F}}$. So
   $$\varnothing \vdash^{\mathsf{PC}_{\mathbb{F}}}_{2} x_i^2 - x_i.$$

For the induction step, the argument goes as follows:

1. Resolution rule:

   Suppose C and D are clauses in variables of F and $f, g \in \mathbb{F}[x_1, ..., x_n]$ such that
   $$F \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{w} C \vee D \vee (af + bg)$$
   in $k + 1$ steps. Moreover, assume the last rule is an application of the resolution rule on $C \vee f$ and $D \vee g$. Therefore

   (a) $F \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{w_1} C \vee f$ in at most k steps.

   (b) $F \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{w_2} D \vee g$ in at most k steps.

   So $w = \max\{w_1, w_2, \mathsf{w}(C \vee D \vee (af + bg))\}$. Moreover, by induction hypothesis

   (a) $H_F \vdash^{\mathsf{PC}_{\mathbb{F}}}_{pw_1 d} h_{C \vee f}$.

   (b) $H_F \vdash^{\mathsf{PC}_{\mathbb{F}}}_{pw_2 d} h_{D \vee g}$.

   Let $E := \mathsf{m}[C \vee D]$. Then by the multiplication rule

   (a) $\{h_{C \vee f}\} \vdash^{\mathsf{PC}_{\mathbb{F}}}_{\mathsf{deg}(h_E) + \mathsf{deg}(f)} h_E \cdot f$.

   (b) $\{h_{D \vee g}\} \vdash^{\mathsf{PC}_{\mathbb{F}}}_{\mathsf{deg}(h_E) + \mathsf{deg}(g)} h_E \cdot g$.

   Hence by application of the addition rule we get
   $$h_E(af + bg)$$
   and the degree of deriving this multivariate polynomial is at most
   $$\max\{pw_1 d, pw_2 d, \mathsf{deg}(h_E(af + bg))\}.$$
   To prove an upper bound for the above quantity we should consider the following cases:

   (a) $af + bg \notin E$:

   In this case,
   $$h_E(af + bg) = h_{C \vee D \vee (af + bg)}.$$
   Therefore
   $$\mathsf{deg}(h_E(af + bg)) \leq d\mathsf{w}(C \vee D \vee (af + bg)),$$
   so the degree of deriving $h_{C \vee D \vee (af + bg)}$ is at most
   $$pd \max\{w_1, w_2, \mathsf{w}(C \vee D \vee (af + bg))\}.$$

(b) $af + bg \in E$:
Let $E' := E \setminus \{af + bg\}$. Then

$$h_E(af + bg) = h_{E'}(af + bg)^2.$$

By Lemma 3.1 we have

$$\{(af + bg)^2\} \vdash^{\mathsf{PC}_{\mathbb{F}}}_{p\mathsf{deg}(af+bg)} af + bg.$$

Hence the degree of deriving $h_{C\vee D\vee(af+bg)} = h_{E'}(af + bg)$ is at most

$$\max\{pw_1 d, pw_2 d, \mathsf{deg}(h_E(af + bg)), \mathsf{deg}(h_{E'}) + p\mathsf{deg}(af + bg)\}.$$

Note that $h_E = h_{C\vee D\vee(af+bg)}$, so

$$\mathsf{deg}(h_E(af + bg)) \leq d(\mathsf{w}(C \vee D \vee (af + bg)) + 1),$$

$\mathsf{deg}(h_{E'}) \leq d(\mathsf{w}(C \vee D) - 1)$, and also $\mathsf{deg}(af + bg) \leq d$, hence the degree upper bound is

$$\max\{pw_1 d, pw_2 d, d(\mathsf{w}(C \vee D \vee (af + bg)) + 1), d(\mathsf{w}(C \vee D) - 1) + pd\}$$

which is less than or equal to

$$pd \max\{w_1, w_2, \mathsf{w}(C \vee D \vee (af + bg))\}.$$

2. Weakening rule: Suppose C is a clause in variables of F and $f \in \mathbb{F}[x_1, ..., x_n]$ such that

$$F \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{w} C \vee f$$

in $k + 1$ steps. Moreover, assume the last rule is an application of the weakening rule on C. Therefore

(a) $F \vdash^{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}_{w_1} C$ in at most k steps.

So $w = \max\{w_1, \mathsf{w}(C \vee f)\}$. Moreover, by induction hypothesis

(a) $H_F \vdash^{\mathsf{PC}_{\mathbb{F}}}_{pw_1 d} h_C$.

Note that $h_{C\vee f} = h_C \cdot f$, hence by the first part of Lemma 3.1

(a) $\{h_C\} \vdash^{\mathsf{PC}_{\mathbb{F}}}_{\mathsf{deg}(h_C)+\mathsf{deg}(f)} h_{C\vee f}$.

Therefore the degree of deriving $h_{C\vee f}$ is at most

$$\max\{pw_1 d, \mathsf{deg}(h_{C\vee f})\}$$

and by the fact that $\mathsf{deg}(h_{C\vee f}) \leq d\mathsf{w}(C \vee f)$, it is at most

$$pd \max\{w_1, \mathsf{w}(C \vee f)\}.$$

3. Simplification rule:

   Suppose C is a clause in variables of F and $a \in \mathbb{F} \setminus \{0\}$ such that

$$F \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}{w}} C$$

   in $k+1$ steps. Moreover, assume the last rule is an application of the simplification rule on $C \vee a$. Therefore

   (a) $F \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}{w_1}} C \vee a$ in at most k steps.

   So $w = w_1$. Moreover, by induction hypothesis

   (a) $H_F \mathrel{\Big|\!\!\frac{\mathsf{PC}_{\mathbb{F}}}{pw_1 d}} h_{C\vee a}$.

   Note that $h_{C\vee a} = ah_C$, hence by applying the addition rule on $x_1^2 - x_1$ and ah_C ($h_C = a^{-1}h_{C\vee a} + 0(x_1^2 - x_1)$) we can derive h_C. The degree of this derivation is at most

$$\max\{pw_1 d, \mathsf{deg}(h_C)\} \leq pw_1 d.$$

4. Multiplication rule:

   Suppose C is a clause in variables of F and $f, g \in \mathbb{F}[x_1, ..., x_n]$ such that

$$F \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}{w}} C \vee g \cdot f$$

   in $k+1$ steps. Moreover, assume the last rule is an application of the multiplication rule on $C \vee f$. Therefore

   (a) $F \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_{d,\mathbb{F}})}{w_1}} C \vee f$ in at most k steps.

   So $w = w_1$. Moreover, by induction hypothesis

   (a) $H_F \mathrel{\Big|\!\!\frac{\mathsf{PC}_{\mathbb{F}}}{pw_1 d}} h_{C\vee f}$.

   Note that by the multiplication rule

$$\{h_{C\vee f}\} \mathrel{\Big|\!\!\frac{\mathsf{PC}_{\mathbb{F}}}{\mathsf{deg}(h_{C\vee f})+\mathsf{deg}(g)}} g \cdot h_{C\vee f}.$$

   So the degree of deriving $g \cdot h_{C\vee f}$ from H_F is at most

$$\max\{pw_1 d, \mathsf{deg}(h_{C\vee f}) + \mathsf{deg}(g)\} \leq pw_1 d.$$

   Now to conclude the induction step, we should consider the following cases:

   (a) $h_{C\vee g\cdot f} = g \cdot h_{C\vee f}$:
   In this case we know

$$\mathsf{deg}(h_{C\vee g\cdot f}) \leq w_1 d$$

   which means the degree of deriving $h_{C\vee g\cdot f}$ is at most $pw_1 d$.

(b) $h_{C \vee g \cdot f} \neq g \cdot h_{C \vee f}$:
In this case

$$g \cdot h_{C \vee f} = h_E \cdot (g \cdot f)^2.$$

where $E := \mathsf{m}[C] \setminus \{g \cdot f\}$. Note that by Lemma 3.1

$$\{(g \cdot f)^2\} \mid\frac{\mathsf{PC}_{\mathbb{F}}}{p \cdot \mathsf{deg}(g \cdot f)} g \cdot f.$$

Hence the degree of deriving $h_{C \vee g \cdot f}$ is at most

$$\max\{pw_1 d, \mathsf{deg}(h_E) + p\mathsf{deg}(g \cdot f)\}.$$

Note that $\mathsf{deg}(h_E) \leq d(\mathsf{w}(C) - 1)$ and $\mathsf{deg}(g \cdot f) \leq d$, hence the degree of deriving $h_{C \vee g \cdot f}$ is at most

$$\max\{pw_1 d, d(\mathsf{w}(C) - 1) + pd\} \leq pw_1 d.$$

□

Bibliography

[Ajt94a] M. Ajtai. The Complexity of the Pigeonhole Principle. *Combinatorica*, 14(4):417–433, 1994. Preliminary version in *FOCS '88*.

[Ajt94b] M. Ajtai. The Independence of the modulo p Counting Principles. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC '94)*, pages 402—411, 1994.

[AR01] M. Alekhnovich and A. A. Razborov. Lower Bounds for Polynomial Calculus: Non-Binomial Case. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS '01)*, pages 190–199, October 2001.

[BGIP01] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi. Linear Gaps between Degrees for the Polynomial Calculus Modulo Distinct Primes. *Journal of Computer and System Sciences*, 62(2):267–289, 2001.

[BIK$^+$94] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower Bounds on Hilbert's Nullstellensatz and Propositional Proofs. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science (FOCS '94)*, pages 794–806, November 1994.

[BW99] E. Ben-Sasson and A. Wigderson. Short Proofs are Narrow—Resolution Made Simple. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99)*, pages 517–526, May 1999.

[CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 174–183, May 1996.

[CS88] V. Chvátal and E. Szemerédi. Many Hard Examples for Resolution. *Journal of the ACM*, 35(4):759–768, October 1988.

[GK18] M. Garlík and L. A. Kołodziejczyk. Some Subsystems of Constant-Depth Frege with Parity. *ACM Trans. Comput. Logic*, 19(4), November 2018.

[Gry19] S. Gryaznov. Notes on Resolution over Linear Equations. In *Computer Science – Theory and Applications (CSR '19)*, pages 168—179, 2019.

[IS20] D. Itsykson and D. Sokolov. Resolution over linear equations modulo two. *Annals of Pure and Applied Logic*, 171(1), 2020. Preliminary version in *MFCS '14*.

[KO18] J. Krajícek and I. C. Oliveira. On monotone circuits with local oracles and clique lower bounds. *Chic. J. Theor. Comput. Sci.*, 2018.

[KPW95] J. Krajíček, P. Pudlák, and A. R. Woods. An Exponential Lower Bound to the Size of Bounded Depth Frege Proofs of the Pigeonhole Principle. *Random Structures and Algorithms*, 7(1):15–40, 1995. Preliminary version in *STOC '92*.

[Kra97] J. Krajíček. Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over Polynomial Calculus. In *Mathematical Foundations of Computer Science (MFCS '97)*, pages 85—90, 1997.

[Kra18] J. Krajíček. Randomized feasible interpolation and monotone circuits with a local oracle. *Journal of Mathematical Logic*, 18(2), 2018.

[Kra19] J. Krajíček. *Proof Complexity*, volume 170 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, March 2019.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[PBI93] T. Pitassi, P. Beame, and R. Impagliazzo. Exponential Lower Bounds for the Pigeonhole Principle. *Computational Complexity*, 3:97–140, 1993. Preliminary version in *STOC '92*.

[PI00] P. Pudlák and R. Impagliazzo. A Lower Bound for DLL Algorithms for k-SAT (Preliminary Version). In *Proceedings of the 11th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '00)*, pages 128–136, January 2000.

[PT20] F. Part and I. Tzameret. Resolution with Counting: Dag-Like Lower Bounds and Different Moduli. In *11th Innovations in Theoretical Computer Science Conference (ITCS '20)*, volume 151, pages 1–37, 2020.

[Raz98] A. A. Razborov. Lower Bounds for the Polynomial Calculus. *Computational Complexity*, 7(4):291–324, December 1998.

[Rii97] S. Riis. Count(q) does not imply Count(p). *Annals of Pure and Applied Logic*, 90(1):1–56, 1997.

[RT08] R. Raz and I. Tzameret. Resolution over linear equations and multilinear proofs. *Annals of Pure and Applied Logic*, 155(3):194–224, 2008.

[Tza14] I. Tzameret. Sparser Random 3-SAT Refutation Algorithms and the Interpolation Problem - (Extended Abstract). In *Proceedings of the 41st International Colloquium on Automata, Languages and Programming (ICALP '14)*, pages 1015–1026, 2014.

Paper B

Nisan–Wigderson generators in Proof Complexity: New lower bounds

Erfan Khaniki[1,2]
[1]Faculty of Mathematics and Physics, Charles University
[2]Institute of Mathematics, Czech Academy of Sciences

Abstract

A map $g : \{0,1\}^n \to \{0,1\}^m$ $(m > n)$ is a hard proof complexity generator for a proof system P iff for every string $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, formula $\tau_b(g)$ naturally expressing $b \notin \mathsf{Rng}(g)$ requires super-polynomial size P-proofs. One of the well-studied maps in the theory of proof complexity generators is Nisan–Wigderson generator. Razborov [Raz15] conjectured that if A is a suitable matrix and f is a $\mathsf{NP} \cap \mathsf{CoNP}$ function hard-on-average for $\mathsf{P/poly}$, then $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for Extended Frege. In this paper, we prove a form of Razborov's conjecture for AC^0-Frege. We show that for any symmetric $\mathsf{NP} \cap \mathsf{CoNP}$ function f that is exponentially hard for depth two AC^0 circuits, $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for AC^0-Frege in a natural setting. As direct applications of this theorem, we show that:

1. For any f with the specified properties, $\tau_b(\mathsf{NW}_{f,A})$ based on a random b and a random matrix A with probability $1 - o(1)$ is a tautology and requires super-polynomial (or even exponential) AC^0-Frege proofs.
2. Certain formalizations of the principle $f_n \notin (\mathsf{NP} \cap \mathsf{CoNP})/\mathsf{poly}$ requires super-polynomial AC^0-Frege proofs.

These applications relate to two questions that were asked by Krajíček [Kra19].

6 Introduction

Proving super-polynomial lower bounds for every proof system is one of the ultimate goals in proof complexity. For this matter, we need to prove that for every proof system P, there exists an infinite family of tautologies $\{\phi_n\}_{n\in\mathbb{N}}$ such that P does not have polynomial size proofs for $\{\phi_n\}_{n\in\mathbb{N}}$. It is known that some weak proof systems require super-polynomial (or even exponential) size proofs for some families of tautologies (see [Kra19] for more information). No super-polynomial lower bounds are known for strong proof systems such as Frege or Extended Frege. We do not even know super-polynomial lower bounds for $\mathsf{AC}^0(\oplus)$-Frege. It seems that one of the main issues in proving lower bounds is the lack of good candidate hard formulas. There are three prominent candidates of formulas that are believed to be hard for any proof system. The first candidate of these formulas is random CNFs. Some experts believe that these formulas should be hard for any proof system (see [Kra19]). Another family of conjectured hard formulas is finite consistency statements. These formulas have tight connections to important conjectures in proof complexity and experts believed that they are hard for any proof system (For a detailed discussion, see [KP89, Pud17]). The third candidate is proof complexity generators.

6.1 Proof complexity generators

Let $g : \{0,1\}^n \to \{0,1\}^m$ $(m > n)$ be a function which is computable in a *reasonable low complexity class* such as $\mathsf{FP/poly}$. As $m > n$, $\{0,1\}^m \setminus \mathsf{Rng}(g)$ is nonempty. Let $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, then as g is computable in $\mathsf{FP/poly}$, we can naturally express the true statement $b \notin \mathsf{Rng}(g)$ as a propositional formula which is denoted by $\tau_b(g)$. If for a proof system P, $\tau_b(g)$ requires super-polynomial size P-proofs for every $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, then g is a hard proof complexity generator for P. The concept of proof complexity generators were defined independently by Alekhnovich *et. al.* [ABRW04] and Krajíček [Kra01a].

As pseudorandom generators are an important topic in computational complexity, Alekhnovich *et al.* [ABRW04] asked the following natural question: *which mappings $g : \{0,1\}^n \to \{0,1\}^m$ should be considered hard from the point of view of proof complexity?* To understand this concept, different mappings were investigated from different aspects in [ABRW04]. In particular, they investigated conditions that make a Nisan–Wigderson generator hard for proof systems such as Resolution and Polynomial Calculus.

Krajíček [Kra01a] investigated the hardness of different variants of the Pigeonhole principle in proof systems and their provability in related theories of bounded arithmetic. One of these variants is the dual weak Pigeonhole principle (dWPHP^n_{2n}) which says that for every function $g : [n] \to [2n]$, g cannot be onto. An interesting theory of bounded arithmetic is $\mathsf{BT} := \mathsf{S}^1_2 + \mathsf{dWPHP}(\mathsf{PV})$ which has several nice properties (see [Jeř04, Jeř07]). Here S^1_2 is the base bounded arithmetic theory in the Buss's Bounded arithmetic hierarchy which is related to the polynomial-time reasoning (see [Bus86]) and $\mathsf{dWPHP}(\mathsf{PV})$ consists of $\mathsf{dWPHP}^n_{2n}(f)$ for every polynomial-time computable function f. A natural question is whether S^1_2 and BT are actually the same theory. Krajíček introduced the concept of proof complexity generators as functions which violate $\mathsf{dWPHP}(\mathsf{PV})$ and formulated a conjecture about them in the setting of model theory of arithmetic that implies $\mathsf{S}^1_2 \neq \mathsf{BT}$ (see [Kra21] for a proof of separation of PV and $\mathsf{PV} + \mathsf{dWPHP}(\mathsf{PV})$ under a different assumption). Moreover, this conjecture implies that proof complexity generators are hard for Extended Frege.

Later, Krajíček [Kra01b, Kra04a, Kra04b, Kra05, Kra09, Kra11a, Kra11b] investigated proof complexity generators from different aspects, developed the theory of proof complexity generators in great length and proposed some conjectures. In particular, Krajíček [Kra11a] defined the generator $\mathsf{nw}_{n,c}$ based on the gadget generators of [Kra09] and conjectured that $\mathsf{nw}_{n,c}$ is a hard proof complexity generator for any proof system.

Razborov [Raz15] made a significant contribution to the lower bound problem for proof complexity generators. He proved that Nisan–Wigderson generators based on suitable matrices and suitable functions are hard not only for Resolution but also for k-DNF Resolution, which improved the previous lower bounds in terms of the stretch of the generator and the strength of the proof system in [ABRW04, Kra04b]. Moreover, he formulated the following intriguing conjecture:

Conjecture 6.1. *(Razborov [Raz15]) Any Nisan–Wigderson generator based on suitable matrices and any function in* $\mathsf{NP} \cap \mathsf{CoNP}$ *that is hard on average for* $\mathsf{P/poly}$*, is hard for Extended Frege.*

Conjecture 6.1 initiated new investigations in the theory of proof complexity generators from different aspects. We refer the reader for comprehensive dissections of the conjectures about the proof complexity generators to read Chapter 30 of [Kra11a] and Section 19.4 of [Kra19].

Regarding Razborov's conjecture, Pich [Pic11] proved that this conjecture is true for proof systems that enjoy different forms of the feasible interpolation property.

The strongest argument that supports Conjecture 6.1 was done by Krajíček in [Kra11b]. He proved that assuming the existence of a function $f \in \mathsf{NP} \cap \mathsf{CoNP}$ which is hard on average for $\mathsf{P/poly}$; it is consistent with the universal theory PV that any Nisan–Wigderson generator based on f (or for a function closely related to f) and suitable matrices is hard not only for Extended Frege but also for any proof system. Note that PV is a fairly strong theory as it proves a reasonable fragment of computational complexity theorems (see [Pic15b] for more information). It is worth mentioning those investigations of the Nisan–Wigderson generators in proof complexity led to advancements in other areas as well, such as [Pic15a, PS21] which proved unprovability of circuit lower bounds in bounded arithmetic and [Pic20] which proved the existence of learning algorithms from circuit lower bounds.

Razborov's conjecture is inherently different from other conjectures in proof complexity that imply that strong proof systems are not p-bounded. The reason is that this conjecture describes a situation where *the hardness of computation implies the hardness of proof* for strong proof systems. For weak proof systems, such a relation exists, which is called *feasible interpolation property*. Krajíček defined this property in [Kra97] and proved that several proof systems such as Resolution have the feasible interpolation property, which implied lower bounds for new formulas. Proving lower bounds using feasible interpolation proved to be very fruitful and led to several lower bounds for different proof systems such as Cutting Planes [Pud97]. Unfortunately, this property does not hold for strong proof systems such as Extended Frege [KP98], and even AC^0-Frege [BDG$^+$04] assuming cryptographic hardness assumptions (for more information, see chapter 17 of [Kra19]). To overcome the barrier against the feasible interpolation property, different attempts were made to prove *hardness of computation implies hardness of proof* theorems for strong proof systems. Krajíček [Kra10] proved a form of feasible interpolation for AC^0-Frege that is different from the original definition of the feasible interpolation property. Moreover, he developed the method of *Forcing with random variables* in [Kra11a] intending to prove *hardness of computation to hardness of proofs* theorems for strong proof systems (bounded arithmetics) and proved types of this theorem for AC^0-Frege and $\mathsf{AC}^0(\oplus)$-Frege (for a finitary proof of the theorem for $\mathsf{AC}^0(\oplus)$-Frege see [Kra15]). Pudlák [Pud21] characterized the canonical disjoint NP-pairs of AC^0-Frege and proved a generalized feasible interpolation theorem for them.

6.2 Our results

This paper aims to find sufficient conditions that make a Nisan–Wigderson generator hard for proof systems such as AC^0-Frege. Our main contribution is the proof of Razborov's conjecture for AC^0-Frege in a natural setting which was not known before.

Theorem 6.1. *(Main theorem, informal version) Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function that requires $2^{n^{\Omega(1)}}$ depth two AC^0 circuits. Then for any $\Sigma_1^1 \cap \Pi_1^1$ pair (ϕ_0, ϕ_1) that defines f, any suitable matrix A, and any $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, $\tau_b(\mathsf{NW}_{f,A})$ requires super-polynomial (exponential) AC^0-Frege proofs when the Paris-Wilkie translation of (ϕ_0, ϕ_1) is used to form the formula $\tau_b(\mathsf{NW}_{f,A})$.*

Theorem 6.1 unconditionally implies that $\mathsf{NW}_{f,A}$ for suitable functions f (such as Parity or Majority) and suitable matrices A are hard proof complexity generators for AC^0-Frege even when the stretch is exponential. No lower bounds for Nisan–Wigderson generators were known for this system. It is worth noting that before this work, the only known hard proof complexity generators for AC^0-Frege, were the PHP-generator of [Kra09] and the more general generator $\mathsf{nw}_{n,c}$ of [Kra11a]. Moreover, Theorem 6.1 implies the following results:

1. For any f that satisfies the conditions of Theorem 6.1 such as Parity, the formula $\tau_b(\mathsf{NW}_{f,A})$ based on a random b and a random matrix A is a tautology with probability $1 - o(1)$ and requires super-polynomial (exponential) AC^0-Frege proofs.

2. Certain formalizations of the principle

$$f_n \notin (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$$

requires super-polynomial AC^0-Frege proofs.

These results relate to two questions asked by Krajíček [Kra19] (problems 19.4.5 and 19.6.1). The first problem asks whether random linear generators (random systems of linear equations over $\mathbb{F}_2$) are hard for AC^0-Frege or not. The second problem asks whether linear generators are iterable for AC^0-Frege or not, which relates to the question of the hardness of proving the principle $f_n \notin \mathsf{SIZE}(n^k)$ in AC^0-Frege.

7 Preliminaries

7.1 Nisan–Wigderson generators

For the rest of the paper for any two real numbers $r_1 \leq r_2$, define $[r_1, r_2) := \{i \in \mathbb{N} : \lfloor r_1 \rfloor \leq i < \lceil r_2 \rceil\}$ and $[r_1, r_2] := \{i \in \mathbb{N} : \lfloor r_1 \rfloor \leq i \leq \lceil r_2 \rceil\}$.

Let $f : \{0,1\}^* \to \{0,1\}$ be a Boolean function. For a natural number n, f_n denotes the function f restricted to $\{0,1\}^n$. Let A be an $m \times n$ $0-1$ matrix such that each row of A has exactly l ones. Such a matrix is called an l-sparse matrix. For such a $m \times n$ l-sparse matrix A, $J_i(A) := \{j \in [0, n) : A_{i,j} = 1\}$.

For every pair (f, A) where f is a Boolean function and A is a $m \times n$ l-sparse matrix, Nisan and Wigderson [NW94] defined the generator $\mathsf{NW}_{f,A} : \{0,1\}^l \to \{0,1\}^m$ as follows:

- For every input $a \in \{0,1\}^l$, the i'th bit of the output of $\mathsf{NW}_{f,A}(a)$ is $f(a|J_i(A))$.

It was proved in the seminal paper [NW94] that if f is a hard function (depending on the application) and A satisfies specific combinatorial properties, then $\mathsf{NW}_{f,A}$ is a *good* pseudorandom generator (depending on the parameters).

Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$. A pair of propositional formulas $(\sigma_0(\mathbf{p}, \mathbf{q}), \sigma_1(\mathbf{p}, \mathbf{r}))$ is a representation of f_n for a natural number n iff:

1. $|\mathbf{p}| = n$ and moreover $\mathbf{p}$, $\mathbf{q}$, and $\mathbf{r}$ variables are disjoint.
2. (σ_0, σ_1) defines the function f_n which means:
   (a) $\neg\sigma_0 \vee \neg\sigma_1$ is a tautology.
   (b) For every $a \in \{0,1\}^n$, $f(a) = i$ iff $\sigma_i(a, \mathbf{t})$ is satisfiable where $i \in [0, 2)$.

Note that as $f \in \mathsf{NP} \cap \mathsf{CoNP}$, for every n, f_n has a representation.

Suppose $f \in \mathsf{NP} \cap \mathsf{CoNP}$, (σ_0, σ_1) is a representation for f_l, and A is a $m \times n$ l-sparse matrix. Then for any $b \in \{0,1\}^m$, $\tau_b(\mathsf{NW}_{f,A})$ based on (σ_0, σ_1) is the following propositional formula:

$$\bigvee_{b_i=1} \neg\sigma_1(\mathbf{p}|J_i(A), \mathbf{q}_i) \vee \bigvee_{b_i=0} \neg\sigma_0(\mathbf{p}|J_i(A), \mathbf{q}_i)$$

where $\mathbf{q}_i$'s are disjoint variables. Note that if $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, then $\tau_b(\mathsf{NW}_{f,A})$ is tautology.

As it was discussed in previous works [ABRW04, Kra05, Raz15, Kra11b], $\mathsf{NW}_{f,A}$ can be a hard proof complexity generator for a proof system P for the following four reasons:

- The complexity of f.
- The properties that A satisfies.
- The representation of f that is used in the formula $\tau_b(\mathsf{NW}_{f,A})$.
- The string $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$.

As we will see, our main result also imposes different conditions on $\tau_b(\mathsf{NW}_{f,A})$ to make sure that it requires long proofs.

The following parts explain the properties that we need for the matrices and representations to prove our theorems.

7.1.1 Representations

The hardness of $\tau_b(\mathsf{NW}_{f,A})$ can depend on the pair (σ_0, σ_1) that is used in it. This matter has been investigated in [ABRW04] and they examined different representations. Recently, Sokolov [Sok21] answered one of the open problems that was stated about a representation of $\tau_b(\mathsf{NW}_{f,A})$ in [ABRW04].

$\Sigma_1^1 \cap \Pi_1^1$ representation

Let $\mathcal{L}$ be a finite relational language and X be a unary relational symbol which is not in $\mathcal{L}$. A Σ_1^1 formula $\psi(X)$ in the language $\mathcal{L} \cup \{X\}$ with equality defines a function $f \in \mathsf{NP}$ iff:

1. $\psi := \exists \bar{Y} \phi(X, \bar{Y})$ where $\phi(X, \bar{Y})$ is a first order formula in the language $\mathcal{L} \cup \{X\}$ with equality.

2. X is not in $\bar{Y}$.

3. For every n, every $a \in \{0,1\}^n$, $f_n(a) = 1$ iff $([0,n), a) \models \psi(X)$ when X is interpreted by a.

Fagin's theorem [Fag74] directly implies that for every symmetric $f \in \mathsf{NP}$, a Σ_1^1 formula $\psi_f(X)$ exists in a language $\mathcal{L} \cup \{X\}$ that defines f. Therefore, the set of functions that are Σ_1^1 definable is exactly symmetric NP and hence this set is quite rich. As an example, we explain how the negation of Parity function can be defined as a Σ_1^1 formula. Let $\mathcal{L} = \{Y\}$ where Y is a binary relation symbol. Then $\bar{\oplus}(X, Y)$ denotes

$$\forall i\, (X(i) \rightarrow \exists j(j \neq i \wedge X(j) \wedge Y(i,j) \wedge Y(j,i) \wedge \forall k(k = i \vee \neg Y(i,k) \vee j = k))\,.$$

Then $\psi_{\bar{\oplus}}(X) := \exists Y \bar{\oplus}(X, Y)$ defines the negation of Parity function (parity of $a \in \{0,1\}^n$ is 0 iff the number of 1's in a is even).

The class of Σ_1^1 formulas is a natural and important class in finite model theory and descriptive complexity. Moreover, this class has appeared in different places in proof complexity, too (for example, see [Kra10]).

To prove Theorem 6.1, the following lemma is needed. If A is a set and Q is a relation on it, i.e. $Q \subseteq A^k$ for some k, and $h : A \rightarrow A$ is a function, then $h(Q) := \{(h(a_1), ..., h(a_k)) : (a_1, ..., a_k) \in A^k\}$.

Lemma 7.1. *Let $\mathcal{L} = \{Y_0, ..., Y_k\}$ be a finite relational language and $\mathcal{A}_0 = (A, \{Q_0^0, ..., Q_k^0\})$ be an $\mathcal{L}$-structure. Let h be a bijective function from A onto A. Consider the $\mathcal{L}$-structure $\mathcal{A}_1 := (A, \{Q_0^1, ..., Q_k^1\})$ where $Q_i^1 = h(Q_i^0)$, for every $i \in [0,k]$. Then for every first-order formula $\phi(x_0, ..., x_p)$ in $\mathcal{L}$ with equality, every $(a_0, ..., a_p) \in A^p$:*

$$\mathcal{A}_0 \models \phi(a_0, ..., a_p) \Leftrightarrow \mathcal{A}_1 \models \phi(h(a_0), ..., h(a_p)).$$

Proof. This lemma can be proved by induction on the complexity of ϕ. □

Let $\exists \bar{Y} \phi(X, \bar{Y})$ be a Σ_1^1 formula. Then for any n, the Paris–Wilkie translation [PW85] (see also Section 8.2 of [Kra19]) of $\phi^{<n}(X, \bar{Y})$ ($\phi^{<n}$ is ϕ when every first order quantifier is bounded by n) is denoted by $\langle \phi \rangle_n (\mathbf{p}, \mathbf{q})$ which is a constant depth formula (without loss of generality we can assume that it is a CNF using extension variables). The number n indicates the size of the universe in which $\phi(X, Y)$ has been considered. For example the Paris-Wilkie translation of $\bar{\oplus}(X, Y)$ in the universe of size n is

$$\langle \bar{\oplus}(X, Y) \rangle_n := \bigwedge_{i=0}^{n-1} \left(\neg p_i \vee \bigvee_{j=0, j \neq i}^{n-1} \left(p_j \wedge q_{i,j} \wedge q_{j,i} \wedge \bigwedge_{k=0, k \neq i, k \neq j}^{n-1} \neg q_{i,k} \right) \right).$$

Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function. Then a pair of Σ_1^1 formulas $(\exists \bar{Y} \phi_0(X, \bar{Y}), \exists \bar{Z} \phi_1(X, \bar{Z}))$ defines f iff:

1. $\exists \bar{Y} \phi_1(X, \bar{Y})$ defines f.
2. $\exists \bar{Z} \phi_0(X, \bar{Z})$ defines $\neg f$.

Such a pair is called a $\Sigma_1^1 \cap \Pi_1^1$ definition of f. Moreover, for any n, $(\langle \phi_0 \rangle_n, \langle \phi_1 \rangle_n)$ is a representation of f_n. For the sake of easiness, by $\langle \psi \rangle_n$ we mean $\langle \phi \rangle_n$ where $\psi(X) := \exists \bar{Y} \phi(X, \bar{Y})$ is a Σ_1^1 formula.

7.2 Proof systems

We assume the reader knows the basic facts about proof complexity, proof systems, and bounded arithmetics (for a detailed discussion, see [Kra19, Kra95]). Here we state some useful facts about AC^0-Frege, which will be used in the results.

7.2.1 AC^0-Frege

AC^0-Frege is the name for a family of proof systems that work with constant-depth de morgan formulas. For each $d \geq 1$, F_d denotes AC^0-Frege proof system of depth d.

To prove Theorem 6.1, we need some known relations between AC^0-Frege and V_1^0, which is a two-sorted bounded arithmetic (see [Bus86, Kra95]). These relations are related to the model theory of V_1^0.

Let $\mathcal{M}$ be an arbitrary nonstandard model of true arithmetic and $n \in \mathcal{M} \setminus \mathbb{N}$. Then

$$\mathcal{M}_n := \{a \in \mathcal{M} : \text{There exists a } b \in \mathcal{M} \setminus \mathbb{N} \text{ such that } a < 2^{n^{1/b}}\}.$$

The following theorems explain the relationship between AC^0-Frege and V_1^0 from the point of view of proof complexity.

For a set A, $\mathcal{P}(A)$ denotes the power set of A.

Theorem 7.2. *([Kra95]) Let $(\mathcal{M}, \chi) \models \mathsf{V}_1^0$ and $\sigma \in \chi$ be a constant depth propositional formula (depth of σ is standard). If $\neg\sigma$ is satisfiable by an assignment in χ, then for every standard d, there is no F_d-proof of σ in $(\mathcal{M}, \chi)$.*

Note that Theorem 7.2 also holds in the case where σ is the Paris-Wilkie translation of a bounded arithmetical formula such as $\phi(x, \bar{R})$ $(\sigma = \left\langle \phi(n, \bar{R}) \right\rangle_n$ for some $n \in \mathcal{M}$), i.e. if there is an $\bar{\alpha} \in \chi$ such that $(\mathcal{M}, \chi) \models \neg\phi(n, \bar{\alpha})$, then $\neg\sigma$ is satisfiable by an assignment from χ and therefore it does not have any F_d-proof in $\mathcal{M}$.

Theorem 7.3. *([Kra95]) Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic and $\phi(x, R)$ be a bounded arithmetical formula such that for every d, the family $\{\langle \phi(n, R) \rangle_n\}_{n \in \mathbb{N}}$ requires exponential F_d-proofs. Then for every $m \in \mathcal{M} \setminus \mathbb{N}$, there exists a $\chi \subseteq \mathcal{P}(\mathcal{M}_m)$ such that:*

1. *Every bounded subset of $\mathcal{M}_m$ which is definable in $\mathcal{M}$ is in χ.*
2. *$(\mathcal{M}_m, \chi) \models \mathsf{V}_1^0$.*
3. *There is an $\alpha \in \chi$ such that $(\mathcal{M}_m, \chi) \models \neg\phi(m, \alpha)$.*

8 Razborov's conjecture for AC^0-Frege

In this section, we estate the main result of the paper. Let $\mathsf{S}_{\mathsf{AC}^0_2}$ denote the depth two AC^0 circuit complexity of functions, then:

Theorem 8.1. *Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function such that $\mathsf{S}_{\mathsf{AC}^0_2}(f) = 2^{n^{\Omega(1)}}$ and (ϕ_0, ϕ_1) be a $\Sigma^1_1 \cap \Pi^1_1$ definition of f. Then for every d:*

1. *For every positive $c \in \mathbb{N}$, every $0 < \epsilon < 1$, every large enough n, every $n^c \times n$ $\lfloor n^\epsilon \rfloor$-sparse matrix A, any $b \notin \mathsf{Rng}$, $\tau_b(\mathsf{NW}_{f,A})$ based on $(\langle\phi_0\rangle_{\lfloor n^\epsilon \rfloor}, \langle\phi_1\rangle_{\lfloor n^\epsilon \rfloor})$ does not have sub-exponential F_d-proofs.*

2. *For every positive $r \in \mathbb{N}$, every large enough s, every $t \in [s/r, s]$, every large enough n, every $2^n \times n^s$ n^t-sparse matrix A, $\tau_b(\mathsf{NW}_{f,A})$ based on $(\langle\phi_0\rangle_{n^t}, \langle\phi_1\rangle_{n^t})$ does not have polynomial size F_d-proofs.*

We prove this theorem in Section 9. This theorem is proved by a model-theoretic argument based on the relations explained in Preliminaries in combination with the hardness of the Pigeonhole principle in AC^0-Frege. Model theoretic arguments have been used previously in proof complexity and they were very fruitful (for example see [Ajt94, Kra01a, Kra10] and [Kra95] for a detailed explanation). See [Woo97, Kra01b] for discussions about the importance and benefits of the model-theoretic arguments (and in general, the logical point of view) in proof complexity.

Note that an immediate consequence of Theorem 8.1 is that $\mathsf{NW}_{f,A}$ based on a hard enough function f with suitable parameters is a hard proof complexity generator for AC^0-Frege. As the Parity function or the Majority function satisfies the required assumptions of Theorem 8.1, we get that NW-generators based on these functions are hard proof complexity generators for AC^0-Frege.

9 Proof of Theorem 8.1

In this section, we prove Theorem 8.1. We state the proof as a series of lemmas for more clarity. We prove the second part of this theorem. The first part can be proved in the same way. For the rest of the paper, $[n] := [0, n)$.

Lemma 9.1. *Let $f : \{0,1\}^* \to \{0,1\}$ be a symmetric Boolean function such that $\mathsf{S}_{\mathsf{AC}^0_2}(f_n) = \Omega(2^{n^\epsilon})$ for an $\epsilon > 0$. Then there is a natural m such that for every $n \geq m$ there is natural number $u \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that*

$$f_n(1^u 0^{n-u}) \neq f_n(1^{u+1} 0^{n-u-1}).$$

Proof. Let $g : \{0,1\}^n \to \{0,1\}$ be a symmetric function. If there exists a $r \leq n/2$ such that for every $r \leq k \leq n - r$, $g(1^k 0^{n-k}) = 0$, then

$$\mathsf{S}_{\mathsf{DNF}}(g) \leq 2n \cdot \sum_{i=0}^{r} \binom{n}{i} \leq 2n(\frac{en}{r})^r$$

where $\mathsf{S}_{\mathsf{DNF}}$ denotes the DNF complexity of functions. Writing this inequality (1) for f_n, we get $c2^{n^\epsilon} \leq 2n(\frac{en}{r})^r$ for a $c > 0$. So if we put $r = n^\delta$ and rewriting this inequality we have

$$c2^{n^\epsilon} \leq 2n(en^{1-\delta})^{n^\delta} \leq 2e^{n^\delta} n^{1+n^\delta} \leq 2n^{1+2n^\delta} = 2^{(2n^\delta+1)\log n+1}.$$

So assuming $\delta = \epsilon/2$, we have $(2n^\delta+1)\log n+1 = o(n^\epsilon)$. Therefore for every large enough n, there exists a $v \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that $f_n(1^v0^{n-v}) = 1$. Following the same argument for $\neg f_n$, we can deduce that for every large enough n, there exists a $v' \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that $\neg f_n(1^{v'}0^{n-v'}) = 1$. So we have found $v, v' \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that $f_n(1^v0^{n-v}) \neq f_n(1^{v'}0^{n-v'})$, hence there exists a $u \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that

$$f_n(1^u0^{n-u}) \neq f_n(1^{u+1}0^{n-u-1}).$$

□

Now let $\mathcal{M}$ be a countable nonstandard model of true arithmetic. Let n, s, t, A, b be arbitrary elements of $\mathcal{M}$ such that:

1. $n, t \in \mathcal{M} \setminus \mathbb{N}$.
2. $A \in \mathcal{M} \setminus \mathbb{N}$ encodes a $2^n \times n^s$ n^t-sparse matrix where $t \in [s/r, s]$, $n^s < 2^n$, and $n^s2^n \leq 2^{n^{t/u}}$ for a nonstandard u.
3. $b \in \mathcal{M} \setminus \mathbb{N}$ is a binary string of length 2^n such that $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$.

Let χ be the set of all bounded subset of $\mathcal{M}_{n^t}$ encoded in $\mathcal{M}$. So in particular $A, b \in \chi$.

As $\mathsf{S}_{\mathsf{AC}^0_2}(f_m) = 2^{m^{\Omega(1)}}$, there is a standard rational $\epsilon > 0$ such that $\mathsf{S}_{\mathsf{AC}^0_2}(f_m) = \Omega(2^{m^\epsilon})$. Let $\delta := \epsilon/2$, then there exists $u \in [n^{\delta t}, n^t - n^{\delta t}]$ that is guaranteed to exist by Lemma 9.1 for f_{n^t}. Let $v := \min\{u, n^t - u\}$, then

Lemma 9.2. *There exists a binary string $\alpha \in \chi$ of length n^s such that for every $i \in [2^n]$,*

$$\#_1(\alpha|J_i(A)) \in [v(1 - \frac{1}{\sqrt[3]{v}}), v(1 + \frac{1}{\sqrt[3]{v}})]$$

where $\#_s(w)$ is the number of occurrences of symbol s in the string w.

Proof. Let $X_0, ..., X_{n^s-1}$ be independent random variables taking values in $\{0, 1\}$ such that for every i, $Pr[X_i = 1] = \frac{v}{n^t}$. For every $i \in [2^n]$, let $Y_i = \sum_{j \in J_i(A)} X_j$ and hence $\mathbb{E}[Y_i] = v$. By the Chernoff bound we have the following inequalities for every $i \in [2^n]$:

1. $Pr[Y_i \leq v(1 - \frac{1}{\sqrt[3]{v}})] \leq e^{\frac{-\sqrt[3]{v}}{2}}$.
2. $Pr[Y_i \geq v(1 + \frac{1}{\sqrt[3]{v}})] \leq e^{\frac{-\sqrt[3]{v}}{3}}$.

Let X' be the concatenation of $X_0, ..., X_{n^s-1}$, hence it is a random string of length of n^s. Now combining the above inequalities with the union bound we get:

$$\mathbf{P} = Pr\left[\bigvee_{i=0}^{2^n-1} \#_1(X'|J_i(A)) \notin [v(1 - \frac{1}{\sqrt[3]{v}}), v(1 + \frac{1}{\sqrt[3]{v}})]\right] \leq$$
$$\sum_{i=0}^{2^n-1} Pr\left[\#_1(X'|J_i(A)) \notin [v(1 - \frac{1}{\sqrt[3]{v}}), v(1 + \frac{1}{\sqrt[3]{v}})]\right] \leq$$
$$\sum_{i=0}^{2^n-1} \left(Pr[Y_i \leq v(1 - \frac{1}{\sqrt[3]{v}})] + Pr[Y_i \geq v(1 + \frac{1}{\sqrt[3]{v}})]\right) \leq$$
$$2^n \cdot 2e^{\frac{-\sqrt[3]{v}}{3}}.$$

We know that $v \geq n^{\delta t}$, t is a nonstandard number, and δ is a standard rational, so

$$n + 1 < \frac{n^{\delta t/3}}{3} \leq \frac{\sqrt[3]{v}}{3}$$

which implies $2^n \cdot 2e^{\frac{-\sqrt[3]{v}}{3}} < 1$, and hence $\mathbf{P} < 1$. This implies that there exists a string $\alpha \in \chi$ that satisfies the desired property. □

Lemma 9.3. *The following functions exist in χ:*

1. $\gamma : [2^n] \to [n^t + 1]$ *such that for every* $i \in [2^n]$, $\gamma(i) = \#_1(\alpha | J_i(A))$.
2. $\omega : [2^n] \times [n^t] \to [n^t]$ *such that for every* $i \in [2^n]$, $\omega(i, .)$ *defines a permutation over* $[n^t]$ *and moreover* $\beta_j = \big(\alpha | J_i(A)\big)_{\omega(i,j)}$ *where* $\beta = 1^{\gamma(i)} 0^{n^t - \gamma(i)}$.

Proof.

1. The function γ exists in $\mathcal{M}$. To prove that γ is in χ, we observe that encoding of γ as a binary string requires at most $c2^n \cdot \log n^t$ (for some $c \in \mathbb{N}$) which is less than $2^{n^{\sqrt{t}}}$, hence $\gamma \in \chi$.
2. Like the previous part, ω exists in $\mathcal{M}$, and its bit representation requires at most $c2^n \cdot n^t \log n^t$ (for some $c \in \mathbb{N}$) which is again less than $2^{n^{\sqrt{t}}}$, and therefore $\omega \in \chi$.

□

To continue the proof, we need the celebrated result about the hardness of the Pigeonhole principle for AC^0-Frege.

Theorem 9.4. *([Ajt94, KPW95, PBI93]) For any natural number d, there exists an $\epsilon_d > 0$ such that for large values of n, any F_d-proof of PHP_n^{n+1} has size at least $2^{\Omega(n^{\epsilon_d})}$.*

Now let $l = \lfloor \sqrt[4]{v} \rfloor$, then we have the following lemma.

Lemma 9.5. *There exists $\chi' \subseteq \mathcal{P}(\mathcal{M}_{n^t})$ such that:*

1. $\chi \subseteq \chi'$.
2. *There exists a function $\sigma \in \chi'$ such that σ is a bijection from $[l]$ onto $[l-1]$.*
3. $(\mathcal{M}_{n^t}, \chi') \models \mathsf{V}_1^0$.

Proof. By Theorem 9.4 we know that PHP_{m-1}^m requires exponential size F_d-proofs for every d. Therefore by Theorem 7.3, there exists a $\chi' \subseteq \mathcal{P}(\mathcal{M}_l)$ such that every bounded subset of $\mathcal{M}_l$ is in χ', $(\mathcal{M}_l, \chi') \models \mathsf{V}_1^0$ and there exists a $\sigma \in \chi'$ such that it is bijection from $[l]$ onto $[l-1]$. Note that if $a \in \mathcal{M}_{n^t}$, then there exists a $b \in \mathcal{M} \setminus \mathbb{N}$ such that $a < 2^{n^{t/b}}$. Let $b' = \lfloor \frac{\delta b}{4} \rfloor$, then $a < 2^{l^{1/b'}}$ as we know $l \geq n^{\delta t/4}$. This implies that $\mathcal{M}_l = \mathcal{M}_{n^t}$, and moreover $\chi \subseteq \chi'$ which completes the proof. □

The following lemma shows that we can simultaneously falsify some weak Pigeonhole principle instances.

Lemma 9.6. *There exists a function $F : [2^n] \times \{-1, 0, 1\} \times [n^t] \to [n^t]$ in χ' such that for every $i \in [2^n]$*

1. *$F(i,a,.)$ restricted to $[v+a]$, is a bijection from $[v+a]$ onto $[\gamma(i)]$.*
2. *$F(i,a,.)$ restricted to $[v+a,n^t)$, is a bijection from $[v+a,n^t)$ onto $[\gamma(i),n^t)$.*

Proof. Let $g \in \chi'$ be the function that Lemma 9.5 provides. Let

1. $w_{i,a} = |\gamma(i) - v - a|$.
2. $M_{i,a} = \max\{v+a, \gamma(i)\}$.
3. $m_{i,a} = \min\{v+a, \gamma(i)\}$.

Then we define the function $G_0(i,a,b)$ as follows:

$$G_0(i,a,b) := \begin{cases} \sigma(b-lk) + (l-1)k & b \in [lk, l(k+1)) \wedge k \in [w_{i,a}] \\ b - w_{i,a} & b \in [lw_{i,a}, M_{i,a}) \end{cases}$$

where $i \in [2^n]$, $a \in \{-1,0,1\}$, and $b \in [M_{i,a}]$.

Note that $v - 1 \leq M_{i,a}$, hence

$$w_{i,a} \leq \frac{v-1}{\sqrt[4]{v}} \leq \frac{v-1}{l} \leq \frac{M_{i,a}}{l}$$

as $w_{i,a} \leq \sqrt[3]{v^2} + 1$ by Lemma 9.2. So $G_0(i,a,.)$ is a bijection from $[lw_{i,a}]$ onto $[(l-1)w_{i,a}]$ and moreover is a bijection from $[lw_{i,a}, M_{i,a})$ onto $[(l-1)w_{i,a}, m_{i,a})$ as

$$M_{i,a} - lw_{i,a} = m_{i,a} - (l-1)w_{i,a}.$$

Therefore the conclusion is that $G(i,a,.)$ is a bijection from $[M_{i,a}]$ onto $[m_{i,a}]$ for every $i \in [2^n]$ and $a \in \{-1,0,1\}$. Now, we define the function $G_1(i,a,b)$ as the inverse of G_0 which means that

$$G_1(i,a,G_0(i,a,b)) = b$$

where $i \in [2^n]$, $a \in \{-1,0,1\}$, and $b \in [M_{i,a}]$. So $G_1(i,a,.)$ is a bijection from $[m_{i,a}]$ onto $[M_{i,a}]$.

Using G_0 and G_1, we can fulfill (1) from the lemma. Now we want to construct two other functions H_0 and H_1 to fulfill (2).

The task is to define $H_0(i,a,.)$ as a function that defines a bijection from $[\max\{n^t - v - a, n^t - \gamma(i)\}]$ onto $[\min\{n^t - v - a, n^t - \gamma(i)\}]$ where $i \in [2^n]$ and $a \in \{-1,0,1\}$ and moreover H_1 would be the inverse of H_0. Let

1. $M'_{i,a} = \max\{n^t - v - a, n^t - \gamma(i)\}$.
2. $m'_{i,a} = \min\{n^t - v - a, n^t - \gamma(i)\}$.

Then we define $H_0(i,a,b)$ as follows:

$$H_0(i,a,b) := \begin{cases} \sigma(b-lk) + (l-1)k & b \in [lk, l(k+1)) \wedge k \in [w_{i,a}] \\ b - w_{i,a} & b \in [lw_{i,a}, M'_{i,a}) \end{cases}$$

where $i \in [2^n]$, $a \in \{-1,0,1\}$, and $b \in [M'_{i,a}]$.

Note that $n^t - v - 1 \leq M'_{i,a}$ and moreover $v \leq n^t/2$, therefore $n^t/2 - 1 \leq M'_{i,a}$. This implies that

$$w_{i,a} \leq \sqrt[3]{v^2} + 1 \leq \sqrt[3]{(n^t/2)^2} + 1 \leq \sqrt[4]{(n^t/2)^3} - 1$$
$$\leq \frac{n^t/2 - 1}{\sqrt[4]{n^t/2}} \leq \frac{n^t/2 - 1}{\sqrt[4]{v}} \leq \frac{n^t/2 - 1}{l} \leq \frac{M'_{i,a}}{l}.$$

Therefore $H_0(i, a, .)$ is a bijection from $[lw_{i,a}]$ onto $[(l-1)w_{i,a}]$ and moreover is a bijection $[lw_{i,a}, M'_{i,a})$ onto $[(l-1)w_{i,a}, m'_{i,a})$. Hence $H_0(i, a, .)$ is a bijection from $[M'_{i,a}]$ onto $[m'_{i,a}]$ for every $i \in [2^n]$ and $a \in \{-1, 0, 1\}$. Now we define the function $H_1(i, a, b)$ as the inverse again as follows:

$$H_1(i, a, H_0(i, a, b)) = b$$

where $i \in [2^n]$, $a \in \{-1, 0, 1\}$, and $b \in [M'_{i,a}]$. Hence $H_1(i, a, .)$ is a bijection from $[m'_{i,a}]$ onto $[M'_{i,a}]$.

Now $F(i, a, b)$ is:

$$F(i,a,b) := \begin{cases} G_0(i,a,b) & b \in [v+a] \wedge v + a = M_{i,a} \\ G_1(i,a,b) & b \in [v+a] \wedge v + a = m_{i,a} \\ H_0(i,a,b-v-a) & b \in [v+a, n^t) \wedge n^t - v - a = M'_{i,a} \\ H_1(i,a,b-v-a) & b \in [v+a, n^t) \wedge n^t - v - a = m'_{i,a} \end{cases}$$

As G_0, G_1, H_0, H_1 are definable by a bounded arithmetical formula based on γ and σ, therefore F is also definable by a bounded arithmetical formula based on γ and σ and this implies that $F \in \chi'$ as $(\mathcal{M}_{n^t}, \chi') \models \mathsf{V}^0_1$. □

Without the loss of generality we can assume $f_{n^t}(1^u 0^{n^t - u}) = 0$. Consider the following relations in χ:

1. $\theta_0 = 1^u 0^{n^t - u}$.
2. $\theta'_0 = 0^{n^t - u} 1^u$.
3. $\theta_1 = 1^{u+1} 0^{n^t - u - 1}$.
4. $\theta'_1 = 0^{n^t - u - 1} 1^{u+1}$.
5. $\bar{\lambda}_0$ such that $\phi_0(\theta_0, \bar{\lambda}_0)$ holds in $(\mathcal{M}_{n^t}, \chi)$.
6. $\bar{\lambda}'_0$ such that $\phi_0(\theta'_0, \bar{\lambda}'_0)$ holds in $(\mathcal{M}_{n^t}, \chi)$.
7. $\bar{\lambda}_1$ such that $\phi_1(\theta_1, \bar{\lambda}_1)$ holds in $(\mathcal{M}_{n^t}, \chi)$.
8. $\bar{\lambda}'_1$ such that $\phi_1(\theta'_1, \bar{\lambda}'_1)$ holds in $(\mathcal{M}_{n^t}, \chi)$.

Now we are ready to describe the assignments $\mathcal{X}$, $\{\bar{\mathcal{Y}}_i\}_{i \in [2^n]}$, and $\{\bar{\mathcal{Z}}_i\}_{i \in [2^n]}$ such that

$$(\mathcal{M}_{n^t}, \chi') \models \forall i < 2^n \left(b_i = 0 \rightarrow \phi_0(\mathcal{X}|J_i(A), \bar{\mathcal{Y}}_i)\right) \wedge \left(b_i = 1 \rightarrow \phi_1(\mathcal{X}|J_i(A), \bar{\mathcal{Z}}_i)\right)$$

which implies that $\tau_b(\mathsf{NW}_{f,A})$ based on $(\langle\phi_0\rangle_{n^t}, \langle\phi_1\rangle_{n^t})$ fails under an assignment in $(\mathcal{M}_{n^t}, \chi')$. We define these assignments as follows:

1. If $u = v$:
   (a) $\mathcal{X} = \alpha$.
   (b) $\bar{\mathcal{Y}}_i = \omega(i, F(i, 0, \bar{\lambda}_0))$.
   (c) $\bar{\mathcal{Z}}_i = \omega(i, F(i, 1, \bar{\lambda}_1))$.
2. If $u = n^t - v$:
   (a) $\mathcal{X}$ is the complement of α, i.e., $\mathcal{X}_j = 1 - \alpha_j \; j \in [n^s]$.
   (b) $\bar{\mathcal{Y}}_i = \omega(i, F(i, 0, \bar{\lambda'_0}))$.
   (c) $\bar{\mathcal{Z}}_i = \omega(i, F(i, -1, \bar{\lambda'_1}))$.

Without loss of generality assume $v = u$. Then for an arbitrary $i \in [2^n]$, we know that

$$\mathcal{X}|J_i(A) = \omega(i, F(i, 0, \theta_0)),$$

hence $\sigma_0(\mathcal{X}|J_i(A), \bar{\mathcal{Y}}_i)$ holds by Lemma 7.1 as $\omega(i, F(i, 0, .))$ is a bijection from $[n^t]$ onto itself and the fact that $\sigma_0(\theta_0, \bar{\lambda}_0)$ holds. The same argument works for $\sigma_1(\mathcal{X}|J_i(A), \bar{\mathcal{Z}}_i)$. Moreover if $v = n^t - u$, the same argument works by using $\theta'_0, \theta'_1, \bar{\lambda'_0}, \bar{\lambda'_1}$.

To complete the proof, we argue as follows. Suppose the statement of the theorem is not true. This means that there exist standard d and r such that the following arithmetical sentence is true in $\mathbb{N}$:

- $\mathbf{H} := \forall s_1 \exists s \geq s_1, \exists t \in [s/r, s], \exists c > 0, \forall m, \exists n > m \exists \; 2^n \times n^s \; n^t$-sparse matrix A, $\exists b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, $\exists$ F_d-proof π for $\tau_b(\mathsf{NW}_{f,A})$ such that $|\pi| \leq |\tau_b(\mathsf{NW}_{f,A})|^c$.

Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic. This means that $\mathcal{M} \models \mathbf{H}$. To simplify the presentation let

$$\mathbf{H} := \forall s_1 \exists s, t, c \forall m \exists n, A, b, \pi \Phi(s_1, s, t, c, m, n, A, b, \pi).$$

Let $s_1 \in \mathcal{M} \setminus \mathbb{N}$, then there exist $s, t \in \mathcal{M} \setminus \mathbb{N}$ and $c \in \mathcal{M}$ such that

$$\mathcal{M} \models \forall m \exists n, A, b, \pi \Phi(s_1, s, t, c, m, n, A, b, \pi).$$

We choose an $m \in \mathcal{M} \setminus \mathbb{N}$ such that for all $m_1 \geq m$, $m_1^{ct} 2^{cm_1} \leq 2^{m_1^{\sqrt{t}/2}}$, hence there exist an $n > m$, a $2^n \times n^s$ n^t-sparse matrix $A \in \mathcal{M} \setminus \mathbb{N}$, a $b \in \mathcal{M} \setminus \mathbb{N}$ such that $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, and an F_d-proof $\pi \in \mathcal{M}$ for $\tau_b(\mathsf{NW}_{f,A})$ such that $|\pi| \leq |\tau_b(\mathsf{NW}_{f,A})|^c$. Now we consider $\mathcal{M}_{n^t}$ and by the argument in this section, there exists a $\chi' \subseteq \mathcal{P}(\mathcal{M}_{n^t})$ such that it has every bounded $\mathcal{M}$-definable subset of $\mathcal{M}_{n^t}$ and moreover

1. $(\mathcal{M}_{n^t}, \chi') \models \mathsf{V}^0_1$.
2. There exists an $\alpha \in \chi'$ which falsifies $\tau_b(\mathsf{NW}_{f,A})$.

Then by Theorem 7.2 there is no F_d-proof of $\tau_b(\mathsf{NW}_{f,A})$ in $(\mathcal{M}_{n^t}, \chi')$. Note that there is a standard number e such that

$$|\pi| \leq |\tau_b(\mathsf{NW}_{f,A})|^c \leq (n^{ct} 2^{cn})^e \leq 2^{en^{\sqrt{t}/2}}$$

which implies that $\pi \in \chi$, but this leads to a contradiction and completes the proof.

10 What are the implications of the hardness of NW-generators for a proof system?

Some experts believe that random DNFs with suitable parameters give hard formulas to prove in any proof system. The hardness of random DNFs has been proved for several proof systems. One way of proving the hardness of these formulas is by proving the harness of certain NW-generators. Let A be a $m \times n$ l-sparse matrix such that $m \geq 2n$ and l is a constant or it is at most $O(\log n)$. Let the base function be the Parity function $\oplus$. Then if we choose a random $b \in \{0,1\}^m$ uniformly, with probability $1 - o(1)$, $b \notin \mathsf{Rng}(\mathsf{NW}_{\oplus,A})$. Now, if we choose a random A and a random b uniformly, then with probability $1 - o(1)$ $\tau_b(\mathsf{NW}_{\oplus,A})$ is a tautology (here we use DNF representation of the Parity function in the definition of the τ formula). The interesting point about these formulas is that if $\tau_b(\mathsf{NW}_{\oplus,A})$ is hard with probability $1 - o(1)$ for a proof system P, then random l-DNFs are hard with probability $1 - o(1)$ for P. This strategy was used to prove the hardness of random DNFs for some proof systems (for example, see [Kra04b, BI10]). For more information, see Section 13.4 of [Kra19]. In this regard, Krajíček [Kra19] asked whether random systems of linear equations over $\mathbb{F}_2$ are hard for AC^0-Frege or not (problem 19.4.5). We note that Theorem 8.1 partially answers this question as follows.

Let (ϕ_0, ϕ_1) be a $\Sigma^1_1 \cap \Pi^1_1$ definition of a function $f \in \mathsf{NP} \cap \mathsf{CoNP}$ (for example we can take f as the Parity function). Then a random formula $F \sim \mathcal{F}(\phi_0, \phi_1, m, n, l)$ is generated as follows:

1. we choose m subsets $J_0, ..., J_{m-1}$ independently uniformly randomly such that $J_i \subseteq [n]$ and $|J_i| = l$ for every $i \in [m]$. These subsets specify a random $m \times n$ l-sparse matrix A.

2. We choose a random $b \in \{0,1\}^m$ uniformly randomly.

3. Then $F := \tau_b(\mathsf{NW}_{f,A})$ based on $(\langle\phi_0\rangle_l, \langle\phi_1\rangle_l)$.

The following corollary partially answers Krajíček's question.

Corollary 10.1. *Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function such that $\mathsf{S}_{\mathsf{AC}^0_2}(f_n) = 2^{n^{\Omega(1)}}$. Let (ϕ_0, ϕ_1) be a $\Sigma^1_1 \cap \Pi^1_1$ definition of f. Then for every d, for every $c > 1$ and every $0 < \epsilon < 1$, if n is large enough, then $F \sim \mathcal{F}(\phi_0, \phi_1, n^c, n, \lfloor n^\epsilon \rfloor)$ is a tautology with probability $1 - o(1)$ and it requires exponential F_d-proofs.*

Another implication of the hardness of NW-generators for a proof system P is that it implies that it is hard for P to prove circuit lower bounds effectively. Razborov [Raz15] pointed out that if the base function is in $\mathsf{P/poly}$ and the $2^n \times n^{O(1)}$ matrix A is *efficiently constructibe* (an example of such matrices was constructed in [NW94]), and moreover $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for a proof system P, the P cannot prove circuit lower bounds effectively. Moreover, this implies that $\mathsf{NP} \not\subseteq \mathsf{P/poly}$ does not have efficient proofs in P. Razborov proved such a result for k-DNF Resolution in [Raz15]. In this regard, our results imply a partial answer for the question of the hardness of circuit lower bounds for proof systems. A related question about AC^0-Frege was asked by

Krajíček [Kra19] (problem 19.6.1). Let $f \in \mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k)$ and A be a $2^n \times n^s$ n^t-sparse matrix which is *effectively constructible*. Then for any fixed $w \in \{0,1\}^{n^c}$, $\mathsf{NW}_{f,A}(w)$ defines a function $C_w \in (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$ as follows:

- For every $i \in \{0,1\}^n$, $C_w(i) = f\left(w|J_{n(i)}(A)\right)$ where $n(i)$ is the number with the binary representation i.

This means that if $\tau_b(\mathsf{NW}_{f,A})$ is a tautology (for a fixed representation of f), then the function with the truth-table b does not have a C_w circuit for any $w \in \{0,1\}^{n^s}$. As Theorem 8.1 (part 2) implies that NW-generators based on suitable $\mathsf{NP} \cap \mathsf{CoNP}$ functions, suitable matrices, and suitable representations are hard proof complexity generators AC^0-Frege, we get the fact that proving certain $(\mathsf{NP} \cap \mathsf{CoNP})/\mathsf{poly}$ lower bounds (b does not have C_w circuits) for Boolean functions are hard for AC^0-Frege. Note that in contrast with with the principle $f_n \notin \mathsf{SIZE}(n^k)$ which can be written as a propositional formula, it is not clear how the principle $f_n \notin (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$ can be written as a propositional formula. So one way of considering this principle in proof complexity is to consider $\tau_{f_n}(\mathsf{NW}_{f,A})$ for any $g \in \mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k)$, any representation of g and any effectively constructible A. In this regard, Theorem 8.1 includes a lot of possible natural formalizations (but not all) of $f_n \notin (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$.

Bibliography

[ABRW04] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, 2004.

[Ajt94] M. Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994.

[BDG$^+$04] M. L. Bonet, C. Domingo, R. Gavaldà, A. Maciel, and T. Pitassi. Non-automatizability of bounded-depth Frege proofs. *Computational Complexity*, 13(1-2):47–68, 2004.

[BI10] E. Ben-Sasson and R. Impagliazzo. Random CNF's are hard for the polynomial calculus. *Computational Complexity*, 19(4):501–519, 2010.

[Bus86] S. R. Buss. Bounded arithmetic. Studies in Proof Theory. Lecture Notes, 3. Napoli: Bibliopolis. VII, 221 p. (1986)., 1986.

[Fag74] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. Complexity of Comput., Proc. Symp. appl. Math., New York City 1973, 43-73 (1974)., 1974.

[Jeř04] E. Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Annals of Pure and Applied Logic*, 129(1-3):1–37, 2004.

[Jeř07] E. Jeřábek. Approximate counting in bounded arithmetic. *The Journal of Symbolic Logic*, 72(3):959–993, 2007.

[KP89] J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[KP98] J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S^1_2 and EF. *Information and Computation*, 140(1):82–94, 1998.

[KPW95] J. Krajíček, P. Pudlák, and A. Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures & Algorithms*, 7(1):15–39, 1995.

[Kra95] J. Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60. Cambridge: Cambridge Univ. Press, 1995.

[Kra97] J. Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[Kra01a] J. Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1-2):123–140, 2001.

[Kra01b] J. Krajíček. Tautologies from pseudo-random generators. *The Bulletin of Symbolic Logic*, 7(2):197–212, 2001.

[Kra04a] J. Krajíček. Diagonalization in proof complexity. *Fundamenta Mathematicae*, 182(2):181–192, 2004.

[Kra04b] J. Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *The Journal of Symbolic Logic*, 69(1):265–286, 2004.

[Kra05] J. Krajíček. Structured pigeonhole principle, search problems and hard tautologies. *The Journal of Symbolic Logic*, 70(2):616–630, 2005.

[Kra09] J. Krajíček. A proof complexity generator. In *Logic, methodology and philosophy of science. Proceedings of the 13th international congress, Beijing, China, August 2007*, pages 185–190. London: College Publications, 2009.

[Kra10] J. Krajíček. A form of feasible interpolation for constant depth Frege systems. *The Journal of Symbolic Logic*, 75(2):774–784, 2010.

[Kra11a] J. Krajíček. *Forcing with random variables and proof complexity*, volume 382. Cambridge: Cambridge University Press, 2011.

[Kra11b] J. Krajíček. On the proof complexity of the Nisan-Wigderson generator based on a hard NP $\cap$ coNP function. *Journal of Mathematical Logic*, 11(1):11–27, 2011.

[Kra15] J. Krajíček. A reduction of proof complexity to computational complexity for $\mathrm{AC}^0[p]$ Frege systems. *Proceedings of the American Mathematical Society*, 143(11):4951–4965, 2015.

[Kra19] J. Krajíček. *Proof complexity*, volume 170. Cambridge: Cambridge University Press, 2019.

[Kra21] J. Krajíček. Small Circuits and Dual Weak PHP in the Universal Theory of P-Time Algorithms. *ACM Transactions on Computational Logic*, 22(2), 2021.

[NW94] N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.

[PBI93] T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3(2):97–140, 1993.

[Pic11] J. Pich. Nisan-Wigderson generators in proof systems with forms of interpolation. *Mathematical Logic Quarterly (MLQ)*, 57(4):379–383, 2011.

[Pic15a] J. Pich. Circuit lower bounds in bounded arithmetics. *Annals of Pure and Applied Logic*, 166(1):29–45, 2015.

[Pic15b] J. Pich. Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic. *Logical Methods in Computer Science*, 11(2):38, 2015.

[Pic20] J. Pich. Learning algorithms from circuit lower bounds . *arXiv*, (2012.14095), 2020.

[PS21] J. Pich and R. Santhanam. Strong Co-Nondeterministic Lower Bounds for NP Cannot Be Proved Feasibly. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, page 223–233, 2021.

[Pud97] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

[Pud17] P. Pudlák. Incompleteness in the finite domain. *The Bulletin of Symbolic Logic*, 23(4):405–441, 2017.

[Pud21] P. Pudlák. The canonical pairs of bounded depth Frege systems. *Annals of Pure and Applied Logic*, 172(2):42, 2021. Id/No 102892.

[PW85] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. Methods in mathematical logic, Proc. 6th Latin Amer. Symp., Caracas/Venez. 1983, Lect. Notes Math. 1130, 317-340 (1985)., 1985.

[Raz15] A. A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics. Second Series*, 181(2):415–472, 2015.

[Sok21] D. Sokolov. Pseudorandom Generators, Resolution and Heavy Width . *ECCC*, (TR21-076), 2021.

[Woo97] A. R. Woods. Approximating the structures accepted by a constant depth circuit or satisfying a sentence – a nonstandard approach. In *Logic and random structures. DIMACS workshop, November 5–7, 1995*, pages 109–130. 1997.

Paper C

Jump operators, Interactive Proofs and Proof Complexity Generators

Erfan Khaniki[1,2]

[1]Faculty of Mathematics and Physics, Charles University

[2]Institute of Mathematics, Czech Academy of Sciences

Abstract

A jump operator J in proof complexity is a function such that for any proof system P, $J(P)$ is a proof system such that P cannot simulate $J(P)$. Some candidate jump operators were proposed by Krajíček and Pudlák [KP89] and Krajíček [Kra04c], but it is an open problem whether computable jump operators exist or not. In the first part of this paper, we introduce a new candidate jump operator based on the power of interactive proofs which given a proof system P, $[\![\mathsf{IP}, P]\!]$ is a MA proof system. This jump operator can be seen as a version of Krajíček's implicit proof system [Kra04c] and in a sense, it is related to the Ideal proof system of Grochow and Pitassi [GP18]. We investigate the properties of this operator and we show its tight relationship with proof complexity generators:

1. Simulation: We prove that for any proof system P, $[\![\mathsf{IP}, P]\!]$ polynomially simulates P and moreover if there exists a Boolean function f such that the strong proof system associated with $\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP}$ efficiently proves exponential size hard on average circuit lower bounds for f, then the strong proof system associated with $\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP}$ simulates $[\![\mathsf{IP}, P]\!]$.
2. Hardness magnification: We prove that for any strong enough proof system P, if truth-table formulas are hard for P, then for any proof system Q that contains tree-like Resolution and any tautology ϕ, P requires exponential size proofs (in the size of the following formula) to prove the formula "$[\![\mathsf{IP}, Q]\!]$ does not have polynomial size proofs for ϕ".
3. Meta-mathematics of complexity theory: For any strong enough proof system P, $T + Rfn_P + 1\text{-}\mathsf{subEXP}$ is consistent with the statement "$[\![\mathsf{IP}, \mathsf{Res}^*]\!]$ is a sound proof system and it has polynomial size proofs for any true DNF" assuming different hardness property for proof complexity generators, where T is PV_1 or S^1_2 depending on the assumption about the hardness of proof complexity generators.
4. Automatability and feasible disjunction property for Extended Frege: We show that assuming intuitionistic S^1_2 proves the strong soundness of
$[\![\mathsf{IP}, \mathsf{Res}^*]\!]$, then if EF is automatable, then for infinitely many n, P/poly natural properties useful against P/poly exist, and if EF has the feasible disjunction property, then for infinitely many n, $\mathsf{NP}/\mathsf{poly}$ natural properties useful against P/poly exist.

Motivated by the hardness assumptions that enable us to prove the above consistency result, we introduce a new hardness property for proof complexity generators. We give a model-theoretic characterization of this property and investigate its relationship with previously known hardness properties. One ingredient of our proofs is a formalization of the sum-check protocol [LFKN92] in $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ which might be of independent interest.

In the second part of the paper, we consider an old open problem by Krajíček and Pudlák [KP89] which asks whether finite consistency formulas for an arithmetical theory T' have polynomial size proofs in an arithmetical theory T when T' proves the consistency of T. In this regard, we prove that certain statements are equivalent, in particular the following two are equivalent:

- There exists a partial recursive jump operator in proof complexity.
- For any strong enough finitely axiomatizable arithmetical theory S, S does not have polynomial size proofs for $Con_{S+Con_S}(\bar{n})$ in n.

11 Introduction

A long-standing problem in complexity theory is to prove super-polynomial size lower bounds for any proof system for propositional tautologies. This is closely related to the well-known question NP vs. CoNP (see [CR79]). Although there is a huge amount of work understanding the power of proof systems (see [Kra19]), the current techniques are not strong enough to help us to prove lower bounds for strong proof systems such as Extended Frege (EF). Apart from the problem regarding the lack of good techniques to prove lower bounds, there is also a lack of families of tautologies that are believed to be hard for a proof system such as EF. There are three main candidate hard tautologies for strong proof systems. The first one is random DNFs with suitable densities. Some experts believe that random DNFs are hard for any proof system. The second one is proof complexity generators which were defined independently by Alekhnovich *et al.* [ABRW04] and Krajíček [Kra01b] (for more information about these formulas, see [Kra11, Raz15, Kra19, Kra22]). The last families of tautologies are finite consistency formulas or finite reflection principles that were suggested by Krajíček and Pudlák [KP89]. In [KP89], they conjectured that there is no optimal proof system which in fact, implies that for any proof system P, there is another proof system Q such that finite reflection principles for Q requires super-polynomial size P-proofs. Although this conjecture gives us a reasonably well-behaved family of hard tautologies, it does not indicate what Q should be. So what seems to become important here is to be able to describe Q, given P. Two such procedures were suggested by Krajíček and Pudlák [KP89] and Krajíček [Kra04c]. We call such a procedure that given a proof system P, generates a stronger proof system Q such that P does not have polynomial size proofs for finite reflection principle of Q (or equivalently P cannot simulate Q), a jump operator. The focus of this paper is to understand efficient jump operators that hopefully can be used to prove lower bounds for strong proof systems such as Extended Frege. In the first part of the paper, we define a new candidate jump operator based on the sum-check protocol of Lund *et al.* [LFKN92] and implicit proof systems of Krajíček [Kra04c]. Let P be a proof system. Following [Kra04c], a proof of ϕ in IP-randomized implicit proof system based on P, which is denoted by $[\![\mathsf{IP}, P]\!]$, is a pair (C, C') such that:

1. the truth-table of C' is a P-proof of ϕ, and
2. the truth-table of C encodes the movement of the prover in the sum-check protocol when the input of the sum-check protocol is the 3DNF $Correct_P^{C'}(\phi)$:="truth-table of C' is a P-proof of ϕ".

Looking at the definition of $[\![\mathsf{IP}, P]\!]$, it is similar to Krajíček implicit proof system $[P', P]$ (P' is an arbitrary proof system) where P' is replaced by the prover in the sum-check protocol. It is clear from the definition that $[\![\mathsf{IP}, P]\!]$ is a Merlin-Arthur proof system (MA proof system) which is actually a Cook-Reckhow proof system under standard hardness assumptions (see [IW99]). Looking at the definition of IP-randomized implicit proof systems, we are trying to build stronger proof systems based on the power of compression by circuits. The role of compression is heavily studied in computational complexity (see for example [IKW02, FS11]). However, only a few works investigated the role of compression in proof complexity (see [Kra04a, Kra04c, Kra05, GP18]). In this regard, the research into randomized implicit proof systems can be seen as having a better understanding of the role of compression in proof complexity. The first result is about the relationship between IP-randomized proof systems and Cook-Reckhow proof systems (similar to the case of Extended Frege and Ideal proof system [GP18]).

Theorem 11.1. *(Informal) For any proof system P, if the strong proof system associated with $\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP}$ proves exponential size hard-on-average circuit lower bounds for a Boolean function f, then the strong proof system associated with $\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP}$ simulates $[\![\mathsf{IP}, P]\!]$.*

The strong proof of a suitable arithmetical theory T is defined as follows. π is a proof of a tautology ϕ in the strong proof system of T iff π is a T-proof for the first-order sentence $Taut(\ulcorner\phi\urcorner)$ (ϕ is a tautology iff $Taut(\ulcorner\phi\urcorner)$ is a true sentence).

A well-studied concept in computational complexity is hardness magnification. Informally speaking, hardness magnification means that if we have a weak computational lower bound for some problem, we can get a strong computational lower bound for possibly another problem (see [CHO$^+$22] for a survey). As hardness magnification is well-studied in computational complexity, it is natural to try to prove similar results in proof complexity. For weak proof systems, several works based on lifting theorems or relativization can be seen as hardness magnification in proof complexity (for example see [DR03, GGKS20]). Another example of hardness magnification for weak proof systems started from the seminal work of Atserias and Müller [AM20]. They proved that the CNF Ref_ϕ where it says that there is a short Resolution refutation for ϕ does not have short Resolution refutations. Such results for different formulations of the Ref_ϕ were proved for different weak proof systems (see [Gar19, Gar20, GKMP20, dRGN$^+$21, dR21, IR22]). In contrast with the several results regarding hardness magnification for weak proof systems, almost nothing is known for strong proof systems (see [MP20]). In this regard, we show that the propositional formula which says that "ϕ does not have polynomial size $[\![\mathsf{IP}, Q]\!]$-proofs" actually plays the role of Ref_ϕ for any strong enough proof system P and therefore we get a hardness magnification result (assuming the truth-table generator is hard for P).

Theorem 11.2. *(Informal) Let P be a strong enough proof system and Q be a proof system that contains tree-like Resolution. If truth-table generator for polynomial size circuit is hard for P, then for any tautology ϕ, the formula*

$$LB_Q(\phi) := \text{“ There is no polynomial size } [\![\mathsf{IP}, P]\!]\text{-proof of } \phi\text{”}$$

requires $2^{\Omega(|\phi|)}$ size P-proofs.

In the above theorem $|LB_Q(\phi)| = |\phi|^{O(1)}$ which means that assuming a polynomial size lower bound for P (the truth-table generator is hard), we get exponential size lower bounds for P.

An important line of research in the area of bounded arithmetic is proving independence and consistency results. In this direction, we prove the following theorem.

Theorem 11.3. *(Informal) Let P be a strong enough proof system, $T(T') := T' + Rfn_P + 1\text{-}\mathsf{subEXP}$, and θ denotes the following formula:*

" $[\![\mathsf{IP}, \mathsf{Res}^*]\!]$ is a sound and polynomially bounded proof system for true DNFs".

Then the following statements are true:

1. *If there is a stretching generator g which is exponentially pseudo-surjective for P, then $T(\mathsf{S}^1_2) + \theta$ is consistent.*

2. *If the truth-table generator is for polynomial size circuits is free for P, then $T(\mathsf{PV}_1) + \theta$ is consistent.*

It is worth mentioning that some experts believe that the assumptions that are used in the above theorem are true (for example see [Kra01b, Kra04b]). Moreover, the above consistency theorem is actually quite strong as PV_1 and S^1_2 can prove a reasonable amount of results of complexity theory which makes them powerful from the point of view of reverse mathematics of complexity theory (see [Pic15, MP20] for a survey).

It is well-known that EF is not automatable under some cryptographic hardness assumptions (see [KP98]). However, it is not known whether we can prove the nonautomatability of EF under structural hardness assumption in complexity theory like the nonautomatability results for weak proof systems (see [AM20, Gar20, GKMP20, Bel20, dRGN$^+$21, dR21, IR22]). We observed that under some extra assumption, it is possible to prove nonautomatability of EF under structural hardness assumptions applying the core idea of [AM20] to the formula $LB_{\mathsf{Res}^*}(\phi)$ where Res denotes Resolution and Res^* denotes tree-like Resolution (for another attempt for proving nonautomatability of strong proof systems under structural hardness assumptions see [PS22]). Another concept that is related to automatability is the feasible disjunction property (see [Pud03]). It is known that weak proof systems such as Resolution and Cutting Planes [Pud97], Polynomial Calculus over the reals and Sum-of-Squares [Hak20] have the feasible disjunction property and k-DNF Resolution for $k > 1$ does not have the feasible disjunction property [Gar20] (see also [Rud97] for a discussion). Apart from the results mentioned for weak proof systems, it is unknown whether strong proof systems such as Frege and Extended Frege have the feasible disjunction property. Under the same extra assumption for the nonautomatbility result for EF, we show that EF does not have the feasible disjunction property under another structural hardness assumption.

Theorem 11.4. *(Informal) Suppose intuitionistic S^1_2 proves the strong soundness of $[\![\mathsf{IP}, \mathsf{Res}^*]\!]$. Then the following statements hold:*

1. *If EF is automatable, then for infinitely many n, there is a $\mathsf{P/poly}$ natural property useful against $\mathsf{P/poly}$.*

2. *If* EF *has the feasible disjunction property, then for infinitely many* n*, there is a* $\mathsf{NP/poly}$ *natural property useful against* $\mathsf{P/poly}$*.*

Motivated by the assumptions that enable us to prove Theorem 11.3, we consider a new hardness property for proof complexity generators. Let P be a proof system and g be a polynomial time computable stretching map (for any n, $g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$ where $m(n) > n$). Then g is P-provably hard for P iff P has short proofs for the propositional formulas $IsHard_{P,g}$:="For every $b \in \{0,1\}^{m(n)}$ P does not have polynomial size proofs (in $m(n)$) for the propositional formula "b is not in the range of g_n"" (see [ST21] for a related formula). The reader might think that this property is too strong to be true for a proof system as for example, something similar to Gödel's incompleteness theorems should be true for proof systems. In contrast to the first-order provability, the situation about proof systems is completely different as strong proof systems such as EF, PA, and ZFC have short proofs for their own finite consistency (see [Coo75, Pud86, Pud87] and [Pud17] for a discussion about finite incompleteness). Also, regardless of whether this property holds or not, it is a win-win situation. Let us consider the truth-table generator for polynomial size circuits ($tt_{n^k,n}$) and EF. If $tt_{n^k,n}$ is EF-provably hard for EF, then we get that EF is not polynomially bounded. No supper polynomial lower bound is known for EF and moreover, it is even open whether the $tt_{n^k,n}$ is hard for $\mathsf{Res}(\log)$ or not (see [Raz15]). If $tt_{n^k,n}$ is not EF-provably hard for EF, then two possibilities can happen. The first possibility is that formulas $\{IsHard_{\mathsf{EF},tt_{n^k,n}}\}$ are tautologies which implies that EF is not an optimal proof system. The other possibility is that formulas $\{IsHard_{\mathsf{EF},tt_{n^k,n}}\}$ are not tautologies which implies that there is a Boolean function f such that for infinity many n, EF has short proofs of the fact that $f_n \not\in \mathsf{Size}(n^k)$. All of the discussed possibilities are breakthrough results in complexity theory, and it seems that the current techniques are not strong enough to rule out which one is true. To better understand this property, we give a model-theoretic characterization of the property "g is P-provably hard for P" and compare it to other known hardness properties for proof complexity generators. Moreover, we propose two hardness hypotheses about this property.

In the second part of the paper, we look at the general theory of efficient jump operators (for a discussion about a closely related concept see [Kra14]). Motivated by the results and conjectures of [KP89, Pud17], we give several statements that are equivalent to the existence of an efficient jump operator including the following ones:

- There exists a partial recursive jump operator in proof complexity.
- For any strong enough finitely axiomatizable arithmetical theory S, S does not have polynomial size proofs for $Con_{S+Con_S}(\bar{n})$ in n.

As it is conjectured that consistency is a jump operator [KP89, Pud17], we propose a weaker conjecture which is equivalent to a weaker form of the conjecture in [KP89, Pud17] (see the above statements). This conjecture states that there is a partial recursive jump operator.

Apart from the above results, we also discuss a possible definition of randomized implicit proof systems based on the PCP theorem of [BFLS91, BFL91]. Also, we discuss new types of TFNP problems based on breaking Nisan-Wigderson generators [NW94] which are motivated by the definition of the soundness for IP-randomized proof systems.

The organization of the paper is as follows. In Section 2, we explain definitions and notations. In Section 3, we define the notion of jump operators. In Section 4, we define IP-randomized implicit proof systems. In Section 5, we state the main results of the paper. In Section 6, we prove the main results of the paper. In Section 7, we state concluding remarks and some open problems.

12 Preliminaries

We assume the reader knows the basic facts about bounded arithmetic, proof complexity, proof systems, and computational complexity (for a detailed discussion of these topics, see [Bus86, HP93, Kra95, Kra19, AB09]). Here we state the required facts which will be used in the results.

12.1 Bounded arithmetics

The basic theory that we work with in this paper is Buss's bounded arithmetic S^1_2 [Bus86], which is axiomatized in the language $\mathcal{L}_{BA} = \{0, S, +, \cdot, |x|, \lfloor x/2 \rfloor, x\#y\}$. The intended meaning of the $\lfloor x/2 \rfloor$ is clear. The meaning of the $|x|$ is $\lceil \log_2(x+1) \rceil$. $x\#y$ is interpreted as $2^{|x|\cdot|y|}$.

A sharply bounded quantifier is of the form $Qx < |t|, Q \in \{\forall, \exists\}$. The class of bounded formulas Σ^b_n, Π^b_n, $n \geq 1$ is defined by counting alternations of bounded quantifiers while ignoring sharply bounded quantifiers (see [Bus86]). The class of Δ^b_n formulas is the class of Σ^b_n formulas with an equivalent Π^b_n definition. Then for any $i \geq 0$, $\mathsf{S}^{\mathsf{i}}_2$ consists of basic axioms defining the usual properties of the function symbols and p-induction axioms

$$\phi(0) \wedge \forall x(\phi(\lfloor x/2 \rfloor) \rightarrow \phi(x)) \rightarrow \forall x \phi(x)$$

for every Σ^b_i formula $\phi(x)$. Moreover, for any $i \geq 0$, $\mathsf{T}^{\mathsf{i}}_2$ consists of basic axioms defining the usual properties of the function symbols and induction axioms

$$\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(S(x))) \rightarrow \forall x \phi(x)$$

for every Σ^b_i formula $\phi(x)$.

A closely related theory to S^1_2 is PV. PV is a purely equational theory that was defined by Cook [Coo75]. Its language contains a few basic function symbols, and it is inductively expanded by symbols for functions defined from previously introduced functions by composition, and limited recursion on notation. Then PV is axiomatized by equations defining the function symbols and a derivation rule similar to open induction. It is important to know that under the standard interpretation of PV in $\mathbb{N}$, PV function symbols define exactly computable functions in polynomial time (FP). The first-order version of PV is called PV_1 [KPT91, Bus95, Coo98]. It is important to know that by Buss's witnessing theorem [Bus86], PV_1 can be seen as the theory $\forall\Sigma^b_1(\mathsf{S}^1_2)$. So without loss of generality when we work in S^1_2, we assume that we have access to PV function symbols and their definition (in more detail, we work in $\mathsf{S}^1_2(\mathsf{PV})$ which is S^1_2 in the language of PV with the basic axioms of PV_1 and p-induction for $\Sigma^b_1(\mathsf{PV})$ formulas). A useful fact about S^1_2 is that it proves normal induction for Δ^b_1 formulas as follows:

Theorem 12.1. *Let $\phi(x), \psi(x) \in \Sigma_1^b$. Then S_2^1 proves:*

$$\forall x(\phi(x) \leftrightarrow \neg\psi(x)) \to (\phi(0) \wedge \forall x(\phi(x) \to \phi(x+1)) \to \forall x \phi(x)).$$

Another theory that we need is intuitionistic S_2^1 ($i\mathsf{S}_2^1$). This theory is the intuitionistic version of S_2^1. Namely, it has non-logical axioms that the theory becomes exactly S_2^1 over the classical logic, but to reason in iS_2^1, the logical framework is the intuitionistic first-order logic. Here we consider iS_2^1 as the theory that Cook and Urquhart defined [CU93]. An important property of iS_2^1 is its strong witnessing theorem.

Theorem 12.2. *([CU93]). Let $\phi(x, y) \in \Sigma_\infty^b$. If $\mathsf{iS}_2^1 \vdash_i \forall x \exists y \phi(x, y)$, then there exists a PV-function f such that $\mathsf{iS}_2^1 \vdash_i \forall x \phi(x, f(x))$ where $\vdash_i$ denotes the provability using axioms and rules of intuitionistic first-order logic.*

An important statement about theories of bounded arithmetic is Parikh's theorem.

Theorem 12.3. *([Par71]) Let T be a $\forall\Sigma_\infty^b$- axiomatizable theory and let $\phi(x, y) \in \Sigma_\infty^b$. Then if $T \vdash \forall x \exists y \phi(x, y)$, then there exists an $\mathcal{L}_{BA}$ term t such that $T \vdash \forall x \exists y \leq t(x) \phi(x, y)$.*

12.2 Formalization in bounded arithmetics

The main objects of theories of arithmetic are natural numbers. So to talk about other concepts such as circuits, algorithms, and generally finite mathematical objects, we need to encode these objects in natural numbers meaningfully so that the theory can reason about them. As natural numbers can be seen as binary strings in a natural way, we can encode finite mathematical objects as natural numbers in the real world. Fortunately, PV_1 is strong enough to talk about these concepts and naturally work with them. Here we do not need to know how PV_1 does the encoding and how it works with these finite objects. The important thing is that such a thing is possible. In particular, $\ulcorner . \urcorner$ denotes the number or the string associated with a mathematical object depending on the context. Also, for any $n \in \mathbb{N}$, there are several ways to find a closed term t such that the interpretation of t in $\mathbb{N}$ becomes n. We use the following representation:

$$\bar{n} := \begin{cases} SS0 \cdot \bar{k} & n = 2k \\ SS0 \cdot \bar{k} + S0 & n = 2k+1 \end{cases}$$

where $\bar{0} = 0$. The main property of this representation is that for any $n \in \mathbb{N}$, $\bar{n}$ has size $O(\log n)$. For more information, see [Bus86, HP93, Kra95].

12.3 Exact counting and approximate counting

Counting is an important tool for proving mathematical theorems. In particular, counting is an important topic in complexity theory, so it is natural to know under which circumstances we can do a counting argument in a bounded arithmetic.

We usually work with bounded definable sets which are collections of numbers of the form

$$X = \{x < a : \phi(x)\}$$

where $\phi \in \Sigma^b_\infty$. When used in a context that asks for a set, a natural number a represents the integer interval $[0, a)$.

By $n \in \mathit{Log}$ we mean that $\exists x(|x| = n)$. Let $C : 2^k \to 2$ be an arbitrary circuit and let $X_C := \{x < 2^k : C(x) = 1\}$. There is a PV-function Count such that $\mathit{Count}(C, y) = |X_C \cap y|$. So in particular, if we know that $2^k \in \mathit{Log}$, then we can exactly count the size of X_C in PV_1. As we have Count, we can talk about probabilities. Let C be as before. Then by the following notation

$$\Pr_{x<y}[C(x) = 1] \leq \frac{z}{w},$$

we mean $w \times \mathit{Count}(C, y) \leq y \times z$ which is a PV_1-relation.

It is not clear how one can count exactly $|X_C|$ when $2^k \notin \mathit{Log}$ in bounded arithmetics, but Jeřábek [Jeř05, Jeř07] developed a framework to approximately counting big sets (when $2^k \notin \mathit{Log}$) in bounded arithmetics. For the rest of this part, we follow the notations of [Jeř07] and explain the relevant results from there.

For any function f we define the *dual (or surjective) weak pigeonhole principle* for f, written as $\mathsf{dWPHP}(f)$ is the universal closure of the following formula

$$x > 0 \to \exists v < x(|y| + 1)\forall u < x|y| f(u) \neq v$$

where f may involve other parameters not explicitly shown. For a set of functions Γ, $\mathsf{dWPHP}(\Gamma)$ denotes $\{\mathsf{dWPHP}(f) : f \in \Gamma\}$. The next theorem shows that $\mathsf{dWPHP}(\mathsf{PV})$ is provable in T_2.

Theorem 12.4. *([PWW88, Kra95, MPW02])* $\mathsf{T}^2_2 \vdash \mathsf{dWPHP}(\mathsf{PV})$.

Let $\mathsf{APC}_1 := \mathsf{PV}_1 + \mathsf{dWPHP}(\mathsf{PV})$. As it was shown in [Jeř05, Jeř07] APC_1 is the right fragment of Buss's bounded arithmetic to develop approximate counting for sets that are definable by polynomial size circuits (note that by Theorem 12.4 $\mathsf{T}^2_2 \vdash \mathsf{APC}_1$).

Definition 12.1. *(in PV_1) Let $C : 2^n \to 2^m$ be a circuit, X and Y are definable sets. Then*

1. *we say that C computes a function from X to Y, written as $C : X \to Y$, iff $X \subseteq 2^n, Y \subseteq 2^m$, and $C[X] \subseteq Y$.*
2. *We write $C : X \hookrightarrow Y$ if, in addition, the function computed by C is injective on X.*
3. *We write $C : X \twoheadrightarrow Y$ if $X \subseteq 2^n$, $Y \subseteq 2^m$, and $Y \subseteq C[X]$.*

Definition 12.2. *Let $X \subseteq a$ and $Y \subseteq b$ where $a, b \in \mathbb{N}$. Then*

1. *$X \times Y := \{bx + y : x \in X, y \in Y\} \subseteq ab$.*
2. *$X \dot\cup Y := X \cup \{y + a : y \in Y\} \subseteq a + b$.*

Now we can state the main theorem of [Jeř07] related to approximate counting.

Theorem 12.5. *(in APC_1) Let $C : 2^n \to 2$ be a Boolean circuit and $\epsilon^{-1} \in \mathit{Log}$. Then there exists $s \leq 2^n$, $v \leq poly(n\epsilon^{-1}|C|)$, and circuits G_0, G_1, H_0, H_1 of size $poly(n\epsilon^{-1}|C|)$ such that:*

1. $G_0 : v(s + \epsilon 2^n) \twoheadrightarrow v \times X_C$,

2. $G_1 : v \times (x_C \mathbin{\dot\cup} \epsilon 2^n) \twoheadrightarrow vs$,

3. $H_0 : v \times X_C \hookrightarrow v(s + \epsilon 2^n)$,

4. and $H_1 : vs \hookrightarrow v \times (X \mathbin{\dot\cup} \epsilon 2^n)$.

such that $G_i \circ H_i = id$ on their respective domains.

Definition 12.3. *(in APC_1) Let $X, Y \subseteq 2^n$ be definable sets by circuits and $\epsilon < 1$. We say that the size of X is approximately less than the size of Y with error ϵ, written as $X \preceq_\epsilon Y$, if there exists a circuit G and $v > 0$ such that*

$$G : v \times (Y \mathbin{\dot\cup} \epsilon 2^n) \twoheadrightarrow v \times X.$$

Moreover, by $X \approx_\epsilon Y$ we mean $X \preceq_\epsilon \wedge Y \preceq_\epsilon X$.

As before, we can talk about probabilities using the notion of approximate counting. Let $C : 2^n \to 2$. Then by the following notation

$$\Pr_{x<y}[C(x) = 1] \circ_\epsilon \frac{z}{w}$$

we mean $w \times (X_C \cap y) \Box_\epsilon yz$ where $\Box \in \{\preceq, \approx\}$.

The definition of $\preceq_\epsilon$ is problematic because it is a $\exists\Pi^b_2$ formula; therefore, we cannot use it in an induction argument in APC_1. To overcome this problem, Jeřábek [Jeř07, Jeř05] worked in a suitable conservative extension of APC_1. Here we explain the relevant definitions and notations.

Definition 12.4. *(in PV_1) Let $f : 2^k \to 2$ be truth-table of a Boolean function (f is encoded as string of 2^k bits, hence $2^k \in Log$). We say f is (wrost-case) ϵ-hard, written as $Hard_\epsilon(f)$, if there is no circuit C of size at most $2^{\epsilon k}$ that computes f. f is average-case ϵ-hard, written as $Hard^A_\epsilon(f)$, if there is no circuit C of size at most $2^{\epsilon k}$ such that*

$$|\{u < 2^k : C(u) = f(u)\} \geq (\frac{1}{2} + 2^{-\epsilon k})2^k.$$

Note that both $Hard_\epsilon(f)$ and $Hard^A_\epsilon(f)$ are Π^b_1-definable.

Lemma 12.6. *([Jeř04]) For every fixed $\epsilon < \frac{1}{3}$ there is a fixed constant c such that APC_1 proves: for every $k \geq c$ such that $2^k \in Log$, there exists an average-case ϵ-hard function $f : 2^k \to 2$.*

Definition 12.5. *Let $\alpha(.)$ be a new uninterpreted function symbol. Then the theory $\mathsf{sHARD}^\mathsf{A}$ is the extension of $\mathsf{S}^1_2(\alpha)$ by the axioms*

1. $\alpha(x)$ is the truth-table of a Boolean function in $||x||$ variables,

2. $x \geq c \to Hard^A_{\frac{1}{4}}(\alpha(x))$,

3. $||x|| = ||y|| \to \alpha(x) = \alpha(y)$,

where c is the constant from Lemma 12.6.

Then, as explained in [Jeř07], we have the following version of the approximate counting.

Theorem 12.7. *There is a* $\mathsf{PV}(\alpha)$*-function Size such that* $\mathsf{sHARD}^{\mathsf{A}}$ *proves: if* $X \subseteq 2^n$ *is definable by a circuit* C*, then*

$$X \approx_\epsilon Size(\alpha, C, 2^n, e),$$

where $\epsilon = |e|^{-1}$*. Moreover, the witnessing functions* H_i, G_i *for* $i \in \{0,1\}$ *from Theorem 12.5 are constructible by* $\mathsf{PV}(\alpha)$*-functions.*

Note that using the above theorem, we can define approximate probabilities in Definition 12.3 using $\mathsf{PV}(\alpha)$ relations. Let $C : 2^n \to 2$. Then by the following notation

$$\Pr_{x<y}[C(x) = 1] \preceq^\alpha_\epsilon \frac{z}{w}$$

we mean $w \times Size(\alpha, C, 2^n, e) \le yz$ where $\epsilon = |e|^{-1}$.

12.4 On the theory $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$

In this part, we introduce a powerful first-order theory of arithmetic which we use in different places to formalize complexity-theoretic concepts.

Definition 12.6. *Let* ϕ *be an arithmetical formula and* ψ *be an arithmetical sentence. Then* $\mathsf{S}^1_2 + \psi + 1\text{-}\mathsf{EXP} \vdash \forall x \phi(x)$ *means that there is a term* t *such that*

$$\mathsf{S}^1_2 + \psi \vdash \forall x, y(t(x) \le |y| \to \phi(x)).$$

As we already said, $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ is powerful. Here we state some of the known results about this theory to show this fact.

Theorem 12.8. *([Kra90]) Let* $\phi \in \forall\Sigma^b_\infty$ *such that* $\mathsf{T}_2 \vdash \phi$*, then* $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP} \vdash \phi$*.*

Let $Prime(x)$ (which says that x is a prime number) be the following Π^b_1 formula

$$x > 1 \wedge \forall y, z < x(y \cdot z \ne x).$$

Then we have the following corollary by Theorem 12.8, the main result of [PWW88] and Parikh's theorem.

Corollary 12.9. *There exists a term* t *such that*

$$\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP} \vdash \forall x \exists y (y > x \wedge t(x) > y \wedge Prime(y)).$$

The last property that we need is that $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ is strong enough to talk about Pratt primality certificate [Pra75].

Definition 12.7. *Let* $Pratt(x, y)$ *be a* PV *formula that formalizes the following definition:* $Pratt(x, y) = 1$ *iff the following conditions hold:*

1. $y = \langle \langle q_i : i < k\rangle, \langle c_i : i < k\rangle, g\rangle$ *for some* k*,*
2. $x - 1 = \prod_{i<k} q_i$*,*

3. *for every $i < k$, $Pratt(q_i, c_i) = 1$,*

4. *$g < x$, $g^{x-1} \equiv 1 \pmod{x}$ and $g^{\frac{x-1}{q_i}} \not\equiv 1 \pmod{x}$ for all $i < k$.*

Then it is easy to see that the following proposition holds.

Proposition 12.10. $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP} \vdash \forall x(Prime(x) \leftrightarrow \exists y Pratt(x,y) = 1)$.

Actually, the base theory to prove the above proposition can be weakened to $\mathsf{S}^1_2 + \mathsf{iWPHP(PV)}$[1].

12.5 Proof systems

Following the work of Cook and Reckhow [CR79], we have the following definition.

Definition 12.8. *Let $\mathcal{L} \subseteq \{0,1\}^*$. Then a function $P \in \mathsf{FP}$ is a proof system for $\mathcal{L}$ iff the range of P is exactly $\mathcal{L}$. Moreover, the size of a P-proof π is $|\pi|$ (length of π if π is a string or the length of the binary representation of π if it is a number).*

Let P be a proof system for $\mathcal{L} \subseteq \{0,1\}^*$. For a $x \in \mathcal{L}$, π is a P-proof of x iff $P(\pi) = x$.

Definition 12.9. *Let P and Q be two proof systems for a set $\mathcal{L} \subseteq \{0,1\}^*$. Then P simulates Q iff there is a polynomial p such that for any $x \in \mathcal{L}$ and any Q-proof π of x, there is a P-proof of size $\leq p(|\pi|)$.*

P and Q are polynomially equivalent iff P simulates Q and also Q simulates P.

Definition 12.10. *A propositional proof system is a proof system for the set of propositional tautologies (*TAUT*).*

In the rest of the paper, when we talk about proof systems, we mean propositional proof systems (otherwise, we emphasize what the associates set to the proof system we are discussing).

Next, we need the definition of Merlin-Arthur proof systems (MA for short).

Definition 12.11. *([Bab85]) Let $\mathcal{L} \subseteq \{0,1\}^*$. Then a function $P \in \mathsf{FP}$ is a MA proof system for $\mathcal{L}$ iff there exists a polynomial p such that for any $x \in \{0,1\}^*$ the following conditions hold:*

1. *if $x \in \mathcal{L}$, then there is a $\pi \in \{0,1\}^*$ such that*

$$\Pr_{r \in \{0,1\}^{p(x,\pi)}}[P(x,\pi,r) = 1] = 1,$$

2. *if $x \notin \mathcal{L}$, then for any $\pi \in \{0,1\}^*$*

$$\Pr_{r \in \{0,1\}^{p(x,\pi)}}[P(x,\pi,r) = 1] < \frac{1}{3}.$$

It is well-known that under standard hardness assumptions such as $\mathsf{E} \not\subseteq_{i.o.} \mathsf{Size}(2^{\Omega(n)})$, MA proof systems are actually Cook-Reckhow proof systems ([IW99]). It is also important to note that the concept of simulation can be defined in the same manner as Definition 12.9 for MA proof systems.

[1] Personal communication with Emil Jeřábek.

12.6 Automatability and feasible disjunction property

An important concept in proof complexity is the notion of proof search. The next definition formalizes this notion.

Definition 12.12. *([BPR00]) A proof system P is automatable iff there exists a deterministic algorithm A such that for any tautology ϕ, $A(P)$ outputs a P-proof of ϕ in time polynomial in the size of the shortest P-proof of ϕ.*

A somewhat related notion to automatability is the concept of the following definition (see subsection 3.2 of [Pud03]).

Definition 12.13. *([Pud03]) A proof system P has feasible disjunction property iff there exists a polynomial p such that for any two propositional formulas ϕ and ψ, in which ϕ and ψ do not share variables, if π is a P-proof for $\phi \vee \psi$, then there exists a P-proof for ϕ of size $\leq p(|\pi|)$ or there exists a P-proof for ψ of size $\leq p(|\pi|)$.*

12.7 Translation of first-order formulas and weak proof systems of theories

Let $\phi(x_1, ..., x_n)$ be a PV relation (or a Δ_1^b formula). Then given $m_1, ..., m_n \in \mathbb{N}$, there is a canonical way to construct the circuit

$$[[\phi]]_{m_1,...,m_n}(y_1^1, ..., y_{m_1}^1, ..., y_1^n, ..., y_{m_n}^n)$$

in polynomial time in $m_1, ..., m_n$ such that for any $a_1, ..., a_n \in \mathbb{N}$ where $|a_i| = m_i$, $\phi(a_1, ..., a_m) = 1$ iff $[[\phi]]_{m_1,...,m_n}(a_1, ..., a_n) = 1$ and moreover this correspondence can be proved in S_2^1 (for more information see [Coo75, Bus95]). As we want to work with proof systems, by $[[\phi]]_{\vec{m}}^c$ we mean the DNF translation of $[[\phi]]_{\vec{m}}$ using some extension variables and again this correspondence can be proved in S_2^1.

Let P be a proof system for tautologies (P is a PV function). Then the reflection principle for P is

$$Rfn_P := \forall x, \phi(P(x) = \phi \rightarrow Taut(\phi))$$

where $Taut(\phi)$ is a Π_1^b formula that checks whether ϕ is a tautology or not.

Now for the key definitions of this part, we follow [Pud20].

Definition 12.14. *A proof system P is the weak proof system of an arithmetical theory T iff the following conditions hold:*

1. *For any PV relation $\phi(x)$, if $T \vdash \forall x \phi(x)$, then there is a polynomial p such that for any n, $[[\phi]]_n^c$ has a P-proof of size at most $p(n)$.*

2. *$T \vdash Rfn_P$.*

The weak proof systems of many arithmetical theories are known. For example, the weak proof system of S_2^1 and PV_1 is EF. For more information, see [Coo75, Bus95, KP89, KP90b, Kra04c, Kra19, Pud20]. There is another way to associate a propositional proof system with a theory.

Definition 12.15. *Let T be a theory that extends S^1_2 with a polynomial time decidable set of axioms and $Proof_T(x,y)$ is the provability predicate of T (it is a* PV *relation). Then the strong proof system of T, which is denoted by P_T, works as follows:*

$$P_T(\pi) := \begin{cases} \phi & \pi = \langle \pi', \phi \rangle \wedge Proof_T(\pi', \ulcorner Taut(\ulcorner \phi \urcorner) \urcorner) \\ x \vee \neg x & o.w. \end{cases}$$

where x is a fixed variable.

Let $\forall x \phi(x)$ be a true $\forall \Pi^b_1$ sentence. Then $\mathsf{EF} + \{[[\phi]]^c\}$ is EF augmented with any substitution instance of $[[\phi]]^c_n$ for some n.

Definition 12.16. *A proof system P is well-behaved iff there is a true $\forall \Pi^b_1$ sentence $\forall x \phi(x)$ such that P is polynomially equivalent to $\mathsf{EF} + \{[[\phi]]^c\}$.*

Many well-known proof systems such as $\mathsf{G_i}$'s, iEF and even strong proof systems associated with PA and ZFC are well-behaved (see [KP90b, Kra04c, Pud86, Pud87]). From the above definition, we get the following theorem.

Theorem 12.11. *([Pud20]) If P is a well-behaved proof system, then P is the weak proof system of $\mathsf{S}^1_2 + Rfn_P$.*

12.8 Feasible soundness and completeness for proof systems

It is possible to prove a form of soundness and completeness for tautologies with short proofs in a proof system. This relation was discovered by Paris and Wilkie [PW85] and Ajtai [Ajt94] for AC^0-Frege and $\mathsf{I}\Delta_0(f)$. Here we state two theorems about this relationship (for more information, see [Kra95]).

Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic ($\mathcal{M} \models Th(\mathbb{N})$). Let $n \in \mathcal{M} \setminus \mathbb{N}$. Then

$$\mathcal{M}_n := \{x \in \mathcal{M} : \exists k \in \mathbb{N}(|x| \leq n^k)\}.$$

Theorem 12.12. *(Soundness) Let P be a proof system and $\mathcal{M} \models \mathsf{PV}_1 + Rfn_P$. If there is a P-proof of ϕ inside $\mathcal{M}$, then $\mathcal{M} \models Taut(\phi)$.*

Theorem 12.13. *Let P be a well-behaved proof system, $\mathcal{M}$ be a countable nonstandard model of true arithmetic, $n \in \mathcal{M} \setminus \mathbb{N}$, and ϕ be a propositional formula in $\mathcal{M}_n$. If there is no P-proof of ϕ in $\mathcal{M}_n$, then there is a cofinal extension $\mathcal{M}^* \supseteq \mathcal{M}_n$ such that:*

1. *$\mathcal{M}^* \models \mathsf{S}^1_2 + Rfn_P$.*
2. *There is a falsifying assignment for ϕ in $\mathcal{M}^*$.*

12.9 Krajíček's implicit proof systems

In this part, we follow the main definition of [Kra04c].

Definition 12.17. *Let P be a proof system for $\mathcal{L} \subseteq \{0,1\}^*$. Let P' be a proof system for tautologies. Then $[P', P]$ is a proof system for $\mathcal{L}$ as follows:*

- *Let $x \in \mathcal{L}$. Then a pair $\langle \pi, C \rangle$ is a $[P', P]$-proof for $x \in \mathcal{L}$ iff the following conditions hold:*

  π is a P'-proof for the canonical 3DNF $Correct_P^C(x)$ where $Correct_P^C(x)$ is a tautology iff the truth-table of C as a circuit is a P-proof of $x \in \mathcal{L}$.

Using this definition, we can define new proof systems as it was done in [Kra04c].

12.10 Proof complexity generators

Let $g \in \mathsf{FP}$ be a stretching function which means that for any n, $g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$ where $m(n) > n$. Let $b \in \{0,1\}^{m(n)}$. Then as $g \in \mathsf{FP}$, we can write a propositional formula $\tau_b(g_n)$ which is a tautology iff b is not in the range of g_n. Note that as $m(n) > n$, there are strings outside of the range of g_n hence for some b's, $\tau_b(g_n)$ is a tautology and we can talk about their proof complexity. These tautologies were defined independently by Alekhnovich *et al.* [ABRW04] and Krajíček [Kra01b] with different motivations. For more information about these tautologies, see [Kra01b, ABRW04, Kra11, Raz15, Kra19, Kra22].

Here we mention several notions of hardness for proof complexity generators.

Definition 12.18. *A stretching map $g \in \mathsf{FP}$ is a hard proof complexity generator for a proof system P iff for any k there is a c_k such that for any $n > c_k$ and any $b \in \{0,1\}^{m(n)}$, $\tau_b(g_n)$ requires $(m(n))^k + k$ size P-proofs.*

For the next definition, we do not explicitly show all variables of the τ formulas. Namely, the notation $\tau_b(C)(x_1, ..., x_n)$ means that $x_1, ..., x_n$ are the variables of $\tau_b(C)$ corresponding to the bits of an $x \in \{0,1\}^n$. The symbol $CircVar(\vec{y})$ denotes the set of circuits using variables from $\vec{y}$.

Definition 12.19. *([Kra01a, Kra04b]) Let $g \in \mathsf{FP}$ be a stretching map and P be a proof system. Then:*

1. *let $s \geq 1$. Then g_n is s-pseudo-surjective for a proof system P iff all disjunctions of the form*

   $$\tau_{B_1}(g_n)(\vec{y}_1) \vee ... \vee \tau_{B_k}(g_n)(\vec{y}_1, ..., \vec{y}_k)$$

   require P-proofs of size at least s. Here $k \geq 1$ is arbitrary (it can be a function of n), and $B_1, ..., B_k$ are circuits such that

   $$B_1 \in CircVar(\emptyset), B_2 \in CircVar(\vec{y}_1), ..., B_k \in CircVar(\vec{y}_1, ..., \vec{y}_{k-1}), \vec{y}_i$$

   disjoint $m(n)$-tuples of atoms.

2. *Let $s(n) \geq 1$ be a function. Then g is $s(n)$-pseudo-surjective for P iff for all but finitely many $n \geq 1$ g_n is $s(n)$-pseudo-surjective for P.*

3. *g is (exponentially) pseudo-surjective for P iff it is $s(n)$-pseudo-surjective for some $s(n) \geq n^{\omega(1)}$ (resp. for $s(n) \geq 2^{n^{\Omega(1)}}$).*

4. *g is free for P if it obeys the property in the previous item but with any constant k only.*

The next theorem gives a model-theoretic characterization of the above definition.

Theorem 12.14. *([Kra01a, Kra04b]) Let P be a well-behaved proof system, $g \in \mathsf{FP}$ be a stretching map, and $\mathcal{M}$ be a countable nonstandard model of arithmetic. Then the following statements hold:*

1. *g is free for P iff for any $n \in \mathcal{M} \setminus \mathbb{N}$, there is an extension $\mathcal{M}^* \supseteq \mathcal{M}_{m(n)}$ such that $\mathcal{M}^* \models \mathsf{PV}_1 + Rfn_P$ and moreover g_n is onto in $\mathcal{M}^*$.*

2. *g is pseudo-surjective for P iff for any $n \in \mathcal{M} \setminus \mathbb{N}$, there is an extension $\mathcal{M}^* \supseteq \mathcal{M}_{m(n)}$ such that $\mathcal{M}^* \models \mathsf{S}^1_2 + Rfn_P$ and moreover g_n is onto in $\mathcal{M}^*$.*

Truth-table generators are important in the theory of proof complexity generators.

Definition 12.20. *Let $s \geq n \geq 1$. then the truth-table function $tt_{s,n}$ (as a PV function) takes as input $10s\log(s)$ (for some fixed constant c_0) bits describing a size $\leq s$ circuit C with n inputs, and out puts 2^n bits: the truth-table of the function computed by C. By definition, $tt_{s,n}$ outputs zero at inputs that do not encode a size $\leq s$ circuit with n inputs.*

It is clear from the above definition that the τ formula based on $tt_{2^{\epsilon n},n}$ and f is the same as $[[Hard_\epsilon(f)]]^c$.

Now we have the following theorem.

Theorem 12.15. *([Kra04b]) Let P be a proof system that simulates EF. Then the following statements are equivalent:*

1. *There is a stretching map $g \in \mathsf{FP}$ which is exponentially pseudo-surjective for P.*

2. *There is a $k \geq 1$ such that $tt_{n^k,n}$ is exponentially pseudo-surjective for P.*

Another closely related formulas to $\tau_b(tt_{s,n})$ are formulas that express a function is hard on average.

Definition 12.21. *Let $s \geq n \geq 1$ and $0 < \delta < 1$. Then $tt^\delta(s, n, C, f)$ is a PV function such that if*

1. *f is a string of length 2^n and $(f : 2^n \to 2)$,*

2. *$C : 2^n \to 2$ is a circuit of size $\leq s$ and,*

3. *$|\{u < 2^n : C(u) = f(u)\}| \geq (\frac{1}{2} + 2^{-\delta n})2^n$,*

it outputs 1, and otherwise, it outputs 0.

From the above definition, we get that $Hard^A_\epsilon(f)$ is equivalent to

$$\forall |C| \leq c_0 2^{\epsilon n} \log(2^{\epsilon n})(tt^\epsilon(2^{\epsilon n}, n, C, f) = 0).$$

For the sake of simplicity, we denote $[[Hard^A_\epsilon(f)]]^c$ by $LB_\epsilon(2^{\epsilon n}, n, f)$.

12.11 Natural properties

An important and well-studied in computational complexity is the notion of Razborov and Rudich's natural properties [RR97]. Here is the definition. Let $s : \mathbb{N} \to \mathbb{N}$. Then for any $n \in \mathbb{N}$, $\mathsf{Size}(s(n))$ denotes the set of all Boolean function $f : \{0,1\}^n \to \{0,1\}$ such that there is a Boolean circuit of size $\leq s(n)$ that computes f.

Definition 12.22. *Let $\mathcal{C} = \{C_n\}_{n \in \mathbb{N}}$ be a family of circuits such that for every n, C_n is a circuit on 2^n many input bits. $\mathcal{C}$ is a $\mathsf{P/poly}$ natural property iff the following conditions hold:*

1. *Constructivity: There is a $c \in \mathbb{N}$ such that for any n, $|C_n| \leq 2^{cn} + c$.*
2. *Largeness: There is a $d > 0$ such that for any large enough n,*

$$\Pr_{f \in \{0,1\}^{2^n}}[C_n(f) = 1] \geq 2^{-dn}.$$

Let $s : \mathbb{N} \to \mathbb{N}$. Then $\mathcal{C}$ is useful against $\mathsf{Size}(s)$ iff for every large enough n, for any Boolean function $f : \{0,1\}^n \to \{0,1\}$, if $C_n(f) = 1$, then $f \notin \mathsf{Size}(s(n))$.

A $\mathsf{NP/poly}$ natural property useful against $\mathsf{Size}(s)$ is defined as the same as the last definition with this difference that $\mathcal{C}$ should be a family of nondeterministic circuits. Actually, we need a weaker notion of usefulness for our results, which is explained in the next definition.

Definition 12.23. *Let $s : \mathbb{N} \to \mathbb{N}$. Then for infinitely many n, there is a $(\mathsf{N})\mathsf{P/poly}$ natural property useful against $\mathsf{Size}(s)$ means that there is a $\mathcal{C} = \{C_n\}_{n \in \mathbb{N}}$ such that $\mathcal{C}$ has the constructivity property and for infinitely many n $\mathcal{C}$ has both the largeness property and the usefulness property for the Boolean functions of input length n.*

To finish this subsection, it is important to know that experts believe that infinitely often $(\mathsf{N})\mathsf{P/poly}$ natural properties useful against $\mathsf{P/poly}$ do not exist (see [RR97, Rud97]).

13 Jump operators in proof complexity

In this part, we define the notion of jump operators in proof complexity.

Definition 13.1. *A jump operator is a function $J : \{0,1\}^* \to \{0,1\}^*$ such that on an input a, if a is code of a Turing machine that computes a propositional proof system P, then $J(a)$ is code of a Turing machine that computes a propositional proof system P' such that P cannot simulate P'.*

In the rest of the paper, we abuse the notation and for a proof system P, we write $J(P)$, and the intended meaning is what is written in the previous definition.

Another concept that is closely related to jump operators is the following definition.

Definition 13.2. *A hard tautology generator is a function $H : \{0,1\}^* \to \{0,1\}^*$ such that on an input a, if a is code of a Turing machine that computes a propositional proof system P, then $H(a)$ is the code of a $\forall\Pi_1^b$ sentence ϕ such that the family $\{[[\phi]]^c\}$ requires super-polynomial size P-proofs.*

One of the main conjectures in proof complexity is the following one.

Conjecture 13.1. *([KP89]) There is no optimal proof system.*

So by the main result of [KP89] and Theorem 15.10 Conjecture 13.1 is equivalent to the existence of a jump operator which is equivalent to the existence of a hard tautology generator. It is open whether Conjecture 13.1 implies the existence of an efficient jump operator or equivalently an efficient hard tautology generator. As for the conjecture, we have the following conjecture about the existence of efficient jump operators. Let T be a theory that extends S_2^1 with a polynomial decidable set of axioms and let $Proof_T$ be the probability predicate of T. Then the finite consistency of T is the Π_1^b formula

$$Con_T(x) := \forall |y| \leq |x| \neg Proof_T(y, \ulcorner \perp \urcorner)$$

and the consistency statement of T is $Con_T := \forall x Con_T(x)$.

Conjecture 13.2. *([KP89, Pud17]) Let T_1 and T_2 be finite axiomatizable true extensions of S_2^1. Then if $T_1 \vdash Con_{T_2}$, T_2 does not have polynomial size proofs of $Con_{T_1}(\bar{n})$ in n.*

14 A jump operator based on interactive proof systems

In this section, we define a new candidate jump operator based on the sum-check protocol [LFKN92]. The sum-check protocol for deciding the unsatisfiability of a 3CNF $\phi(x_1, ..., x_n)$ works as follows: the protocol consists of messages exchanges between a powerful prover $\mathcal{P}$ and a randomized polynomial time verifier $\mathcal{V}$.

1. Both $\mathcal{P}$ and $\mathcal{V}$ receives $\phi(x_1, ..., x_n)$.

2. $\mathcal{P}$ generates a prime number $2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$ (c_p is the constant from the upper bound term t in Corollary 12.9) and a Pratt certificate u such that $Pratt(p, u) = 1$ and sends $\langle p, u \rangle$ to $\mathcal{V}$. $\mathcal{V}$ checks whether $Pratt(p, u) = 1$ or not, and if it u was not a Pratt certificate for p, then it terminates the protocol; otherwise the protocol continues.

3. $\mathcal{V}$ initializes $v_0 := 0$.

4. Both $\mathcal{P}$ and $\mathcal{V}$ arithmetize ϕ to obtain a polynomial $\Phi(x_1, ..., x_n)$. Then the following interaction is repeated for all $i = 1$ to n:

   (a) Leaving x_i free, $\mathcal{P}$ computes the coefficients of the following polynomial (computations are over $\mathbb{F}_p$):

   $$Q_i(x_i) := \sum_{x_{i+1} \in \{0,1\}} \dots \sum_{x_n \in \{0,1\}} \Phi(r_1, ..., r_{i-1}, x_i, x_{i+1}, ..., x_n).$$

   Then $\mathcal{P}$ sends Q_i as its list of coefficients to $\mathcal{V}$.

(b) $\mathcal{V}$ checked whether $Q_i(0) + Q_i(1) = v_{i-1}$. If so, it samples a random $r_i\mathbb{F}_p$, computes $v_i := Q_i(r_i)$, and sends r_i to $\mathcal{P}$.

5. In the final round, instead of sending r_n to $\mathcal{P}$, $\mathcal{V}$ checks that $\Phi(r_1, ..., r_n) = v_n$ or not and based on that accepts or rejects.

It can be proved that the above protocol has a soundness and completeness property (see Theorem 14.1). Let $V(p, u, \phi, \pi, r)$ be the PV-function that works as follows:

- On a 3CNF $\phi(x_1, ..., x_n)$, it outputs 0 if at least one of the following conditions does not hold:

  1. $2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$,
  2. $Pratt(p, u) = 1$,
  3. $|r| = n^{c_r} + c_r$,
  4. the input length of π interpreted as a Boolean circuit is $n^{c_r} + c_r$,

  where c_p is the constant from the upper bound term t in Corollary 12.9 and c_r is a constant from the definition of the sum-check protocol for the length of a required random string so that the protocol can be executed correctly. If all of the previous conditions hold, V interprets the truth-table of π as the transcript of the prover and based on r, it queries different places of the truth-table of π using π to simulate the sum-check protocol and outputs 1 iff the sum-check protocol passes, and otherwise it outputs 0.

Note that there is a constant c such that if $\phi \in \overline{\mathsf{3SAT}}$ ($\overline{\mathsf{3SAT}}$ is the set of unsatisfiable 3CNFs), then there is a π of size $\leq p^{c(3n^3|p|+(n-1)|p|)} \leq 2^{n^{c_r}+c_r}$. The important property of the sum-check protocol is the following soundness and completeness theorem.

Theorem 14.1. *Let ϕ be a 3CNF in n variables. then the following statements hold:*

1. *Soundness: if ϕ is satisfiable, then for any π of size $\leq 2^{n^{c_r}+c_r}$, p and u,*

$$\Pr_{r\in\{0,1\}^{n^{c_r}+c_r}}[V(p, u, \phi, \pi, r) = 1] \leq \frac{n\binom{2n}{3}}{2^{(2n^3+n)}}.$$

2. *Completeness: if ϕ is unsatisfiable, then there is a π of size $\leq 2^{n^{c_r}+c_r}$, p and u such that*

$$\Pr_{r\in\{0,1\}^{n^{c_r}+c_r}}[V(p, u, \phi, \pi, r) = 1] = 1.$$

Definition 14.1. *Let P be a proof system for a set $\mathcal{L} \subseteq \{0, 1\}^*$. Then $[\![\mathsf{IP}, P]\!]$ denotes the IP-randomized implicit proof system based on P. The verifier for $[\![\mathsf{IP}, P]\!]$ is the PV function $V_P(x, p, u, C, C', r)$ which works as follows:*

- *First, V_P checks whether $P(C) = x$ or not. If this was the case, then it outputs 1; otherwise, it outputs the output of $V(p, u, Correct_P^{C'}(x), C, r)$.*

It is clear from the above definition and the statement of Theorem 14.1 that $[\![\mathsf{IP}, P]\!]$ is a MA proof system.

15 Main results

In this section, we explain the main results of the paper.

15.1 On properties of IP-randomized implicit proof systems

The first theorem that we explain is the relationship between IP-randomized implicit proof systems and Cook-Reckhow proof systems, similar to the relationship between EF and the Ideal proof system of [GP18].

Theorem 15.1. *Let P be a proof system. Then $[\![\mathsf{IP}, P]\!]$ simulates P. Moreover, if there exists a Boolean function $f : \{0,1\}^* \to \{0,1\}$ and a constant c such that for any large enough n, there are 2^{cn} size $P_{\mathsf{S}^1_2+Rfn_P+1\text{-}\mathsf{EXP}}$-proofs of $LB_{\frac{1}{4}}(2^{\frac{n}{4}}, n, f_n)$, then $P_{\mathsf{S}^1_2+Rfn_P+1\text{-}\mathsf{EXP}}$ simulates $[\![\mathsf{IP}, P]\!]$.*

To prove the above theorem, we need to prove the soundness of $[\![\mathsf{IP}, P]\!]$ in a suitable arithmetical theory.

Definition 15.1. *Let P be a proof system and $c > 0$. Then the soundness of $[\![\mathsf{IP}, P]\!]$, which is denoted by $Sound_c([\![\mathsf{IP}, P]\!])$, is the following $\forall\Sigma^b_1$ sentence: for all ϕ, a, p, u, C, C', f where $|\phi| > c$, there is a circuit D of size $\leq \lceil |f|^{\frac{1}{4}} \rceil$ such that one of the following conditions hold:*

1. *$|f| \neq |Var(C)|^{k_a} + k_a$ or,*
2. *$tt^{\frac{1}{4}}(\lceil |f|^{\frac{1}{4}} \rceil, |\lceil |f|^{\frac{1}{4}} \rceil|, D, f) = 1$ or,*
3. *$\phi(a) = 1$, or*
4. $$\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\phi, p, u, C, C', r) = 1] \preceq^f_\epsilon \frac{1}{2},$$

where k_a is the constant that we get from Theorem 12.7 to make sure that Size function works properly, $\epsilon = \frac{1}{4}$, and $n := |Var(Correct^{C'}_P(\phi))|$.

The following theorem is one of the main ingredients of the proof of Theorem 15.1.

Theorem 15.2. *Let P be a proof system. Then there is a constant $c > 0$ such that*

$$\mathsf{S}^1_2 + Rfn_P + 1\text{-}\mathsf{EXP} \vdash Sound_c([\![\mathsf{IP}, P]\!]).$$

Theorem 15.3 is the consequence of a formalization of the soundness and completeness of the sum-check protocol in $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$.

Theorem 15.3. *(Soundness) There is a constant c such that $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ proves: for every n, ϕ, a, p, u, π; if*

1. *ϕ is a 3CNF in n variables where $n \geq c$ and,*
2. *$\phi(a) = 1$ and,*

3. *$Pratt(p, u) = 1$ and,*

4. *$2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$ and,*

5. *the input length of π interpreted as a circuit is $n^{c_r} + c_r$,*

then

$$\Pr_{r \in \mathbb{F}_p^n}\Big[V(p, u, \phi, \pi, r) = 1\Big] \leq \frac{n\binom{2n}{3}}{p}.$$

Theorem 15.4. *(Completeness) There exists a function F that is Δ_1^b-definable in S_2^1 such that $\mathsf{S}_2^1 + 1\text{-}\mathsf{EXP}$ proves: for every n, ϕ, p, u; if*

1. *ϕ is a 3CNF in n variables and,*

2. *$\forall a < 2^n \phi(a) = 0$ and,*

3. *$Pratt(p, u) = 1$ and,*

4. *$2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$,*

then

$$\Pr_{r \in \mathbb{F}_p^n}\Big[V(p, u, \phi, F(p, \phi), r) = 1\Big] = 1.$$

Let P be a proof system. Then for a sequence of numbers

$$l := \langle n_\phi, n_p, n_u, n_C, n_{C'}, n_r \rangle,$$

we define the propositional formula $LB_P^l(\vec{x_\phi}, \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, \vec{x_f})$ as:

$$\left[\!\!\left[\Pr_{r < 2^{|Var(Correct_Q^{C'}(\phi))|^{c_r} + c_r}} [V_P(\phi, p, u, C, C', r) = 1] \preceq_\epsilon^f \frac{1}{2} \right]\!\!\right]_l^c (\vec{x_\phi}, \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, \vec{x_f})$$

where $\epsilon = \frac{1}{4}$. Let ϕ be a propositional formula of size $\leq n_\phi$ and f be a string of length $\leq n_f$. Then if $LB_P^l(\ulcorner \phi \urcorner, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, f)$ is a tautology, then there is no $[\![\mathsf{IP}, P]\!]$-proof $\pi = (p, u, C, C')$ such that $|p| \leq n_p, |u| \leq n_u, |C| \leq n_C$, and $|C'| \leq n_{C'}$. The interesting property of the LB_P^l formula is the next theorem. To state the next theorem, we need the following definition.

Definition 15.2. *A proof system P is compressible if there is a constant d_P such that for any propositional tautology ϕ such that $|\phi|$ is big enough, there is a circuit C of size $|\phi|^{d_P}$ such that $P(tt(C)) = \phi$.*

It is important to note that proof systems such as Frege and Extended Frege are compressible. In particular, any proof system that contains tree-like Resolution is compressible (see Lemma 4.1 of [Kra04c]).

Theorem 15.5. *Let P be a well-behaved proof system and Q be a compressible proof system. Then if there is a k such that $tt_{n^k,n}$ is a hard proof complexity generator for P, then for any constant $c > 0$, there is m such that for any*

$n \geq m$, for any propositional tautology ϕ such that $|\phi| = n$, and for any f, $LB^l_Q(\ulcorner \phi \urcorner, \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, f)$ does not have P-proofs of size $< 2^{cn^{d \cdot d_Q \cdot c_r}}$ where

$$l(n) := \left\langle n, (2n^3+n)^{c_p}, (2n^3+n)^{c_p \cdot c_{cert}}, (n^{d \cdot d_Q \cdot c_r} + c_r)^k, n^{d_Q}, n^{d_Q \cdot k_a} + k_a \right\rangle,$$

$d > 0$ is a constant such that for any big enough D and any big enough ψ, $|Var(Correct^D_Q(\psi))| \leq (|D| + |\psi|)^d$, and $c_{cert} > 0$ is a constant such that for any large enough prime q, there is a Pratt certificate of size $\leq |q|^{c_{cert}}$.

Moreover, if additionally $\mathsf{CoNP} \not\subseteq \mathsf{MA}$, then there is an infinite family of propositional tautologies $\{\phi_n\}_{n \in \mathbb{N}}$ such that $LB^l_Q(\ulcorner \phi_n \urcorner, \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, f)$ is a tautology for almost every f for the parameter size $l(|\phi_n|)$.

By Combining the previous results, we get the following consistency statement.

Theorem 15.6. *Let P be a well-behaved proof system. Then the following statements are true:*

1. *If there is a stretching map $g \in \mathsf{FP}$ which is exponentially pseudo-surjective for P, then there exists a nonstandard model $\mathcal{M}^* \models \mathsf{S}^1_2 + Rfn_P$ and a $n \in \mathcal{M}^* \setminus \mathbb{N}$ such that:*

   (a) there is a constant $c > 0$ such that $\mathcal{M} \models 2^{n^c} \in Log$.

   (b) There is a constant $c' \in \mathbb{N}$ such that for any DNF $\phi \in \mathcal{M}^*$ such that $|\phi| = n$, if $\mathcal{M}^* \models \exists a \phi(a) = 0$, then

   $$\mathcal{M}^* \models \text{“}\phi \text{ does not have any } [\![\mathsf{IP}, \mathsf{Res}^*]\!]\text{-proofs”}$$

   and if $\mathcal{M}^* \models \forall a \phi(a) = 1$, then

   $$\mathcal{M}^* \models \text{“There is a } [\![\mathsf{IP}, \mathsf{Res}^*]\!]\text{-proof of size} \leq n^{c'} \text{ for } \phi\text{”.}$$

2. *If there is a constant k such that $tt_{n^k,k}$ is free for P, then there exists a nonstandard model $\mathcal{M}^* \models \mathsf{PV}_1 + Rfn_P$ and a $n \in \mathcal{M}^* \setminus \mathbb{N}$ such that:*

   (a) there is a constant $c > 0$ such that $\mathcal{M} \models 2^{n^c} \in Log$.

   (b) There is a constant $c' \in \mathbb{N}$ such that for any DNF $\phi \in \mathcal{M}^*$ such that $|\phi| = n$, if $\mathcal{M}^* \models \exists a \phi(a) = 0$, then

   $$\mathcal{M}^* \models \text{“}\phi \text{ does not have any } [\![\mathsf{IP}, \mathsf{Res}^*]\!]\text{-proofs”}$$

   and if $\mathcal{M}^* \models \forall a \phi(a) = 1$, then

   $$\mathcal{M}^* \models \text{“There is a } [\![\mathsf{IP}, \mathsf{Res}^*]\!]\text{-proof of size} \leq n^{c'} \text{ for } \phi\text{”.}$$

The next definition is a another version of Definition 15.1.

Definition 15.3. *Let P be a proof system. Then the strong soundness of $[\![\mathsf{IP}, P]\!]$, which is denoted by $sSound_c([\![\mathsf{IP}, P]\!])$, is the following $\forall \Sigma^b_2$ sentence: for all ϕ, a, p, u, f where $|\phi| > c$, there is a circuit D of size $\leq \lceil |f|^{\frac{1}{4}} \rceil$ such that for all C, C', one of the following conditions hold:*

1. $|f| \neq |Var(C)|^{k_a} + k_a$ *or,*
2. $tt^{\frac{1}{4}}(\lceil |f|^{\frac{1}{4}} \rceil, |\lceil |f|^{\frac{1}{4}} \rceil|, D, f) = 1$ *or,*
3. $\phi(a) = 1$, *or*
4. $$\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\phi, p, u, C, C', r) = 1] \preceq^f_\epsilon \frac{1}{2},$$

where k_a is the constant that we get from Theorem 12.7 to make sure that Size function works properly, $\epsilon = \frac{1}{4}$, and and $n := |Var(Correct^{C'}_P(\phi))|$.

It is easy to see that for any proof system P, there is a constant $c > 0$ such that $sSound_c([\![\mathsf{IP}, P]\!])$ is a true sentence. It should be mentioned that $Sound_c([\![\mathsf{IP}, P]\!])$ and $sSound_c([\![\mathsf{IP}, P]\!])$ are equivalent over PV_1, but it is not clear whether the same equivalence holds over iS^1_2. Using the above definition, we have the following statement.

Theorem 15.7. *If $\mathsf{iS}^1_2 \vdash_i sSound_c([\![\mathsf{IP}, \mathsf{Res}^*]\!])$ for a constant $c \in \mathbb{N}$, then the following statements are true:*

1. *If EF is automatable, then for any constant $k > 0$, for infinitely many n there is a $\mathsf{P/poly}$ natural property useful against $\mathsf{Size}(n^k)$.*
2. *If EF has the feasible disjunction property, then for any constant $k > 0$, for infinitely many n there is a $\mathsf{NP/poly}$ natural property useful against $\mathsf{Size}(n^k)$.*

15.2 A new hardness property for proof complexity generators

Motivated by hardness assumptions that enable us to prove Theorem 15.6, we define the following new property.

Definition 15.4. *Let P a proof system and $g \in \mathsf{FP}$ be a stretching map ($g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$). Then g is P-provably hard for P iff for every $k \in \mathbb{N}$, there are $c, c' \in \mathbb{N}$ such that for any $n > c$, there are P-proofs of size at most $(m(n))^{c'} + c'$ for the propositional formulas*

$$IsHard^{n,k}_{P,g}(\vec{x}_\pi, \vec{x}_b) := [[\neg Proof_P(\pi, \tau_b(g_n))]]^c_{(m(n))^k, m(n)}(\vec{x}_\pi, \vec{x}_b)$$

(the Π^b_1 version is $\forall |\pi| \leq (m(n)^k), \forall |b| = m(n) \neg Proof_P(\pi, \tau_b(g_n))$).

The following theorem gives a model-theoretic characterization of this property.

Theorem 15.8. *Let P be a well-behaved proof system and $g \in \mathsf{FP}$ be a stretching map ($g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$). Then the following statements are equivalent:*

1. *g is P-provably hard for P.*

2. *Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic and $n \in \mathcal{M} \setminus \mathbb{N}$. Then for any countable cofinal extension $\mathcal{M}^*$ of $\mathcal{M}_{m(n)}$ such that $\mathcal{M}^* \models \mathsf{PV}_1 + Rfn_P$, there is a countable cofinal extension $\mathcal{M}^{**}$ of $\mathcal{M}^*$ such that:*
   - *(a) $\mathcal{M}^{**} \models \mathsf{PV}_1 + Rfn_P$.*
   - *(b) g_n is onto in $\mathcal{M}^{**}$.*

An immediate consequence of the above theorem is the following statement.

Corollary 15.9. *Let P be a well-behaved proof system and $g \in \mathsf{FP}$ be a stretching map. If g is P-provably hard for P, then g is free for P.*

Proof. By combining Theorem 12.14 and Theorem 15.8 □

So the last corollary implies that we can get item 2 of Theorem 15.6 under the assumption that $tt_{n^k,n}$ is P-provably hard for P.

The existence of proof complexity generators that are P-provably hard for a proof system P is consistent with the current knowledge of complexity theory and mathematical logic. Therefore we propose the following new hypotheses about proof complexity generators.

Hypothesis 15.1. *For any well-behaved proof system P, there is a stretching map $g \in \mathsf{FP}$ such that g is P-provably hard for P.*

Hypothesis 15.2. *For any well-behaved proof system P, there is a constant $0 < \epsilon < 1$ such that $tt_{2^{\epsilon n},n}$ is P-provably hard for P.*

15.3 On the existence of an efficient jump operator

In this part, we explain the main theorem which describes several equivalent statements to the existence of an efficient jump operator.

Definition 15.5. *$\mathcal{T}$ is the set of all consistent finitely axiomatizable first-order theory $\mathsf{S}^1_2 \subseteq T$ in the language of S^1_2.*

Theorem 15.10. *The following statements are equivalent:*

1. *There exists a polynomial time computable/recursive/partial recursive jump operator.*
2. *There exists a polynomial time computable/recursive/partial recursive hard tautology generator.*
3. *There exists a true $T \in \mathcal{T}$ such that for every $S \in \mathcal{T}$, S does not have polynomial size proofs of $Con_{T+Con_S}(\bar{n})$ in n.*
4. *There exists a true $T \in \mathcal{T}$ such that for every proof system P, P does not simulate $P_{T+Con_{\mathsf{S}^1_2+Con_P}}$.*
5. *There exists a true theory $T \in \mathcal{T}$ such that for every $S \in \mathcal{T}$, if $S \vdash T$, then S does not have polynomial size proofs of $Con_{S+Con_S}(\bar{n})$ in n.*

Motivated by Conjecture 13.2 and Theorem 15.10, we propose the following conjecture.

Conjecture 15.1. *There is a partial recursive jump operator.*

16 Proofs of the main results

16.1 Proof of Theorem 15.3

In this part, we prove Theorem 15.3. As we argue in $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$, we freely assume the existence of objects of exponential length ($2^{n^{O(1)}}$) with properties that can be checked in polynomial time with respect to the length of the object (so the property can be checked in $2^{n^{O(1)}}$).

We need the following lemma in the proof.

Lemma 16.1. *(Lemma 4.3.6 of [Jeř05]) PV_1 proves: For every prime number $p \in Log$, every nonzero $f \in \mathbb{F}_p[x]$, f has at most $deg(f)$ many roots.*

Suppose conditions 1-5 of the statement of Theorem 15.3 hold for n, ϕ, a, p, u, π. Let $\phi(x_0, ..., x_{n-1}) = \bigwedge_{i<m} C_i$ where for every $i < m$, $C_i = l^i_0 \vee l^i_1 \vee l^i_2$ such that for every $j < 3$, l^i_j is x_k or $\neg x_k$ for some $k < n$. Define the arithmetization of ϕ as

$$\Phi(x_0, ..., x_{n-1}) := \prod_{i<m} (v(l^i_0) + v(l^i_1) + v(l^i_2))$$

where $v(l) := \begin{cases} x & l = x \\ 1 - x & l = \neg x \end{cases}$. From now on, suppose we look at polynomials as polynomials with coefficients in $\mathbb{F}_p$. The first observation is that for every $|b| < n$, $\Phi(b) \neq 0$ iff $\phi(b) = 1$. Moreover, as $p \in LogLog$ and Φ has at most 3^m many monomials when written as the sum of monomials and the fact that $3^m \in Log$ using the Δ^b_1-induction we can show that:

1. there exists a $M \subseteq \mathbb{F}_p \times 2^n$ such that $\Phi = \sum_{(a,m)\in M} a \cdot \prod_{i\in m} x_i$.

2. Total degree of Φ is at most m.

Let $r = \langle r_1, ..., r_i\rangle$ be a sequence of i elements of $\mathbb{F}_p$ for some i. Fix the following notations for any number i:

1. $P_r(x) := \sum_{j\leq m} a_j x^j$ where $\pi(r) = \langle a_0, ..., a_m\rangle$.

2. $\Phi_r(x_{i+1}, ..., x_n) := \Phi((r)_1, ..., (r)_i, x_{i+1}, ..., x_n)$.

Consider the the formula $\psi(k)$ as follows:

- For every $v \in \mathbb{F}_p$, for every sequence of i elements of $\mathbb{F}_p$ r, if

  $$v \neq \sum_{x_{i+1}<2} ... \sum_{x_n<2} \Phi_r(x_{i+1}, ..., x_n),$$

  then

  $$\Pr[\pi \text{ can persuade the verifier}] \leq \frac{km}{p}$$

  where $i = n - k + 1$.

As $p \in Log$ and with the power of 1-EXP we have exact counting, ψ is a Δ^b_1-formula. Now, using the Δ^b_1-induction on k, we want to show that $\forall k < n\, \psi(k)$.

- Base step:

  Let $k = 1$, r be a $n-1$ element sequence of $\mathbb{F}_p$ and $v \in \mathbb{F}_p$ such that $v \neq \sum_{x_n<2} \Phi_r(x_n)$. Then there are two cases. If $P_r = \Phi_r$, then with probability 0 the verifier accepts as $P_r(0) + P_r(1) \neq v$. Otherwise, $P_r \neq \Phi_r$ which means that by Lemma 16.1, P_r and Φ_r are equal on at most m points which implies that the verifier accepts with probability at most $\frac{m}{p}$.

- Inductive step:

  Suppose the claim is true when $k = j$. Let $v \in \mathbb{F}_p$ and r be a n element sequence of $\mathbb{F}_p$ such that

  $$v \neq \sum_{x_i<2} \dots \sum_{x_n<2} \Phi_r(x_i, \dots, x_n)$$

  where $i = n - j$. Let

  $$P(x) := \sum_{x_{i+1}<2} \dots \sum_{x_n<2} \Phi_r(x, x_{i+1}, \dots, x_n).$$

  Consider the following possibilities. If $P_r(x) = P(x)$, then verifier accepts with probability 0 as $P_r(0) + P_r(1) \neq v$. Otherwise, $P_r \neq P$ and therefore P_r and P are equal on at most m points. Let $S := \{a \in \mathbb{F}_p : P(a) = P_r(a)\}$. If the verifier chooses a point from S, then it will accept it by the end of the protocol with probability at most $\frac{m}{p}$. If the verifier chooses a point outside of S like a, then as $\psi(j)$ is true, it should be true for $v' := P_r(a)$ and $r' := \langle (r)_1, \dots, (r)_i, a \rangle$, hence the verifier accepts with probability at most $\frac{jm}{p}$. So overall the probability that the verifier accepts is $\frac{m}{p} + \frac{jm}{p} = \frac{(j+1)m}{p}$.

Note that as $\psi(n-1)$ is true and the fact that $m \leq \binom{2n}{3}$, we get

$$\Pr_{v \in \mathbb{F}_p^n} \left[V(p, u, \phi, \pi, v) = 1 \right] \leq \frac{n\binom{2n}{3}}{p}.$$

16.2 Proof of Theorem 15.4

The proof of this theorem uses some of the arguments that we used in the proof of Theorem 15.3, so we do not go into detail. Suppose conditions 1-4 hold for n, ϕ, p, u. Let Φ be the polynomial from the proof of Theorem 15.3. Define the function $F'_{p,\phi}(r)$ as follows:

- On the input r where r is an i element sequence of $\mathbb{F}_p$ for some $i < n$, it computes the coefficients of

  $$Q_r(x) := \sum_{x_{i+2}<2} \dots \sum_{x_n<2} \Phi_r(x, x_{i+2}, \dots, x_n)$$

  and outputs the sequence of coefficients. Namely, if $Q_r(x) = \sum_{j<m+1} a_j x^j$, then $F(r) = \langle a_0, \dots, a_m \rangle$ where m is the number of clauses of ϕ.

As we have the power of 1-EXP, F' is Δ_1^b definable, and moreover, as we have exact counting and F' always outputs the right answer for the sum-check protocol. Now, let $F(p,\phi)$ be the function that outputs the trivial circuit that its truth-table encodes the graph of $F'_{p,\phi}$ (so F is Δ_1^b-definable in S_2^1). Then using the Δ_1^b induction we get

$$\Pr_{v\in\mathbb{F}_p^n}\left[V(p,u,\phi,F(p,\phi),v)=1\right]=1.$$

16.3 Proof of Theorem 15.2

The contact c can be computed by looking at the proof. To simplify the proof, we assume that $|\phi|$ is big enough. Arguing in $\mathsf{S}_2^1+Rfn_P+1$-EXP, let ϕ,a,p,u,C,C',f be in such a way that:

1. there is no circuit D of size $\le\lceil|f|^{\frac{1}{4}}\rceil$ such that $tt^{\frac{1}{4}}(\lceil|f|^{\frac{1}{4}}\rceil,|\lceil|f|^{\frac{1}{4}}\rceil|,D,f)=1$ and,
2. $|f|=|Var(C)|^{k_a}+k_a$ and,
3. $\phi(a)=0$ and,
4. $2^{2n^3+n}<p\le 2^{(2n^3+n)^{c_P}}$ and,
5. $Pratt(p,u)=1$ and,
6. $|Var(C)|=n^{c_r}+c_r$

where $n=|Var(Correct_P^{C'}(\phi))|$. We can do exact counting as we have the power of 1-EXP. For the sake of contradiction suppose

$$\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\phi,p,u,C,C',r)=1]>\frac{1}{4}.$$

This means that

$$\Pr_{v\in\mathbb{F}_p^n}\left[V(p,u,Correct_P^{C'}(\phi),C,v)=1\right]>\frac{1}{4}.$$

As $|\phi|$ is big enough, this implies that $|Correct_P^{C'}(\phi)|$ is also big enough, so what we actually get is that

$$\Pr_{v\in\mathbb{F}_p^n}\left[V(p,u,Correct_P^{C'}(\phi),C,v)=1\right]>\frac{n\binom{2n}{3}}{p}.$$

This implies that $Correct_P^{C'}(\phi)$ does not have any falsifying assignment by Theorem 15.3. Therefore, the truth-table of C' is actually a valid P-proof for ϕ which means $P(tt(C'))=\phi$. As we have Rfn_P as one of the axioms, we get that ϕ is actually a tautology, but this leads to a contradiction by the fact that $\phi(a)=0$, hence we have

$$\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\phi,p,u,C,C',r)=1]\le\frac{1}{4}.$$

It is clear from the proof of Theorem 12.7 (see Lemma 2.14 in [Jeř07]) that knowing $Hard_{\frac{1}{4}}^A(f)$ is sufficient to do approximate counting. Namely, we have access to f as a string so we can do arguments using p-induction on Σ_1^b formulas that use f as a parameter and moreover, we know $Hard^A_{\frac{1}{4}}(f)$ holds, so we can approximately compute the probability $\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\phi, p, u, C, C', r) = 1]$. So by Theorem 12.7 and Theorem 12.5 that there is a circuit G_1 and a $v \leq poly((n^{c_r}+c_r)\epsilon^{-1}|C^*|)$ such that

$$G_1 : v \times (X_{C^*} \dot{\cup} \ \epsilon 2^{n^{c_r}+c_r}) \twoheadrightarrow vSize(f, C^*, 2^{n^{c_r}+c_r}, e)$$

where $|e|^{-1} = \frac{1}{4}$ and for any $r < 2^{n^{c_r}+c_r}$, $C^*(r) := V_P(\phi, p, u, C, C', r)$. As we have the power 1-EXP, we can do exact counting and we get

$$Size(f, C^*, 2^{n^{c_r}+c_r}, e) \leq |X_{C^*}| + \epsilon 2^{n^{c_r}+c_r}.$$

As we showed $|X_{C^*}| \leq \frac{2^{n^{c_r}+c_r}}{4}$ and as $\epsilon = \frac{1}{4}$, we get

$$Size(f, C^*, 2^{n^{c_r}+c_r}, e) \leq \frac{2^{n^{c_r}+c_r}}{2}$$

which means

$$\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\phi, p, u, C, C', r) = 1] \preceq^f_\epsilon \frac{1}{2}.$$

16.4 Proof of Theorem 15.1

By the definition of $[\![\mathsf{IP}, P]\!]$ it is trivial that $[\![\mathsf{IP}, P]\!]$ simulates P. To prove the rest of the statement, suppose ϕ is a propositional tautology such that $|\phi|$ is big enough. Let $\langle p, u, C, C'\rangle$ be a $[\![\mathsf{IP}, P]\!]$-proof of ϕ which means that

$$\mathbb{N} \models \Pr_{v \in \mathbb{F}_p^n}[V_P(\ulcorner \phi \urcorner, p, u, C, C', v) = 1] = 1$$

where $n = |Var(Correct_P^{C'}(\phi))|$. Let $m := ||Var(C)|^{k_a} + k_a|$ and $T := \mathsf{S}_2^1 + Rfn_P +$ 1-EXP. As P_T has short proofs for $LB_{\frac{1}{4}}(2^{\frac{n'}{4}}, n', f_{n'})$ for every $n' \in \mathbb{N}$ (polynomial in the size of the formula), then there is a short P_T-proof of $LB_{\frac{1}{4}}(2^{\frac{m}{4}}, m, f_m)$. By Theorem 15.2, there is a constant $c > 0$ such that $T \vdash Sound_c([\![\mathsf{IP}, P]\!])$. This means that $Sound_c([\![\mathsf{IP}, P]\!])$ has a constant size T-proof. By the fact that we know $LB_{\frac{1}{4}}(2^{\frac{m}{4}}, m, f_m)$, if we substitute f_m and $\langle p, u, C, C'\rangle$ in the corresponding variables in $Sound_c([\![\mathsf{IP}, P]\!])$, we get a short T-proof of

$$\forall a \left(\ulcorner \phi \urcorner(a) = 1 \vee \Pr_{r<2^{n^{c_r}+c_r}}[V_P(\ulcorner \phi \urcorner, p, u, C, C', r) = 1] \preceq^{f_m}_\epsilon \frac{1}{2} \right).$$

Note that

$$\mathbb{N} \models \Pr_{v \in \mathbb{F}_p^n}[V_P(\ulcorner \phi \urcorner, p, u, C, C', v) = 1] = 1$$

which implies that

$$\mathbb{N} \models \neg(\Pr_{r<2^{n^{c_r}+c_r}}[V_P(\ulcorner \phi \urcorner, p, u, C, C', r) = 1] \preceq^{f_m}_\epsilon \frac{1}{2})$$

is a true atomic sentence; hence it has a short S_2^1-proof which implies that $\forall a \ulcorner \phi \urcorner(a) = 1$ has a short T-proof which means that $Taut(\ulcorner \phi \urcorner)$ has a short T-proof.

16.5 Proof of Theorem 15.5

Suppose the statement of the theorem is not true. This means that there is a constant $c > 0$ such that for every m', there is a $n' > m'$ and a propositional tautology ϕ' ($|\phi'| = n'$) and a string f' with the right size such that there is a P-proof of size $< 2^{cn'^{d \cdot d_Q \cdot c_r}}$ for $LB^l_Q(\phi', \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, f')$. Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic. As the above assumption can be written as an arithmetical sentence and is true in $\mathbb{N}$, it should also be true in $\mathcal{M}$. Therefore, we can argue as follows. Let $m \in \mathcal{M} \backslash \mathbb{N}$. Then there is a n, a propositional formula ϕ, a string f, and a number π such that $\mathcal{M}$ believes the following statements:

1. $n > m$,
2. $|\phi| = n$,
3. f has the right size for the LB^l_P for ϕ,
4. $|\pi| < 2^{cn^{d \cdot d_Q \cdot c_r}}$, and
5. $P(\pi) = \ulcorner LB^l_Q(\phi, \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, f) \urcorner$.

As Q is compressible, there is a circuit $C \in \mathcal{M}$ of size $\leq n^{d_Q}$ such that $\mathcal{M} \models Q(tt(C)) = \phi$. Let $p, u \in \mathcal{M}$ be in such a way that $\mathcal{M}$ believe:

1. $Pratt(p, u) = 1$ and
2. $2^{2t^3+t} < p \leq 2^{(2t^3+t)^{c_p}}$

where $t = |Var(Correct^C_Q(\phi))|$. Note that by Theorem 15.4 there is a circuit

$$D : 2^{n^{d \cdot d_Q \cdot c_r} + c_r} \to 2$$

of size $\leq 2^{b(n^{d \cdot d_Q \cdot c_r} + c_r)}$ in $\mathcal{M}$ for some $b \in \mathbb{N}$ such that $\mathcal{M}$ believes

$$\Pr_{r < 2^{t^{c_r} + c_r}} [V_P(\phi, p, u, D, C, r) = 1] = 1.$$

As $tt_{n'^k, n'}$ is a hard proof complexity generator for P, then by Theorem 12.13, there is an extension $\mathcal{M}^* \supseteq \mathcal{M}_{2^{n^{d \cdot d_Q \cdot c_r}} + c_r}$ such that

1. $\mathcal{M}^* \models \mathsf{S}^1_2 + Rfn_P$ and
2. $\mathcal{M}^* \models \exists C^* (|C^*| \leq (n^{d \cdot d_Q \cdot c_r} + c_r)^k \wedge tt(C^*) = tt(D))$.

As $2^{t^{c_r} + c_r} \in Log$ in $\mathcal{M}^*$, $\mathcal{M}^*$ is an extension of $\mathcal{M}_{2^{n^{d \cdot d_Q \cdot c_r}} + c_r}$, and the fact that $\mathcal{M}^* \models \mathsf{S}^1_2$, we have exact counting and therefore $\mathcal{M}^*$ believes

$$\Pr_{r < 2^{t^{c_r} + c_r}} [V_P(\phi, p, u, C^*, C, r) = 1] = 1.$$

Now for the sake of contradiction suppose $\mathcal{M}^*$ believes

$$\Pr_{r < 2^{t^{c_r} + c_r}} [V_P(\phi, p, u, C^*, C, r) = 1] \preceq^f_\epsilon \frac{1}{2}$$

which means that $\mathcal{M}^*$ believes

$$Size(f, D^*, 2^{t^{c_r}+c_r}, e) \leq \frac{2^{t^{c_r}+c_r}}{2}$$

where $D^*(r) := V_P(\phi, p, u, C^*, C, r)$ for any $r < 2^{t^{c_r}+c_r}$ and $|e|^{-1} = \frac{1}{4}$. To complete the proof, we need to look at how the $Size$ function works (see proof of Theorem 2.7 in [Jeř07]). $Size(f, D^*, 2^{t^{c_r}+c_r}, e)$ works as follows: It constructs the circuit $H : 2^{c_{nw}|(t^{c_r}+c_r)|} \to 2^{t^{c_r}+c_r}$ in polynomial time using f (H is actually the Nisan–Wigderson generator based on f) where c_{nw} is a constant in $\mathbb{N}$. Then the output of $Size(f, D^*, 2^{t^{c_r}+c_r}, e)$ is

$$2^{t^{c_r}+c_r-c_{nw}|(t^{c_r}+c_r)|}|X_{D^*\circ H}|.$$

But as we argued before, $\Pr_{r<2^{t^{c_r}+c_r}}[D^*(r) = 1] = 1$ which implies $|X_{D^*\circ H}| = 2^{c_{nw}|(t^{c_r}+c_r)|}$ which means

$$Size(f, D^*, 2^{t^{c_r}+c_r}, e) = 2^{t^{c_r}+c_r}$$

and this leads to a contradiction and therefore the proof of this part is completed.

To prove the moreover part, if for any large enough n, and any propositional tautology ϕ where $|\phi| = n$, and for any f with the right size parameter such that $Hard^A_{\frac{1}{4}}(f)$ holds, $LB^l_Q(\phi, \vec{x_p}, \vec{x_u}, \vec{x_C}, \vec{x_{C'}}, f)$ is not a tautology, then $[\![\mathsf{IP}, Q]\!]$ is a MA proof system that has polynomial size proofs for any tautology (because by an easy counting argument, it can be shown that for almost every f, $Hard^A_{\frac{1}{4}}(f)$ holds) and therefore $\mathsf{CoNP} \subseteq \mathsf{MA}$ and this completes the proof of this part.

16.6 Proof of Theorem 15.6

In this part, we prove the first item of Theorem 15.6. The second part can be proved by applying the same argument using this fact that PV_1 and S^1_2 prove the same $\forall\Sigma^b_1$ sentences. The first thing to notice is that it is straightforward to show that $\mathsf{S}^1_2 + \text{1-}\mathsf{EXP}$ can prove that tree-like Res is compressible (see Lemma 4.1 of [Kra04c]). Let $c \in \mathbb{N}$ be the constant that S^1_2 proves that for any x, if $2^{|x|^c} \in Log$, then statements of Proposition 12.10, Theorem 15.2, Theorem 15.4 and the fact that tree-like Res is compressible are provable for the objects of size $\leq |x|$. Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic and $n \in \mathcal{M} \setminus \mathbb{N}$. Let $p, u \in \mathcal{M}$ be in such a way that $\mathcal{M}$ models:

1. $2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$,
2. $|u| \leq |p|^{c_{cert}}$, and
3. $Pratt(p, u) = 1$

where c_p, c_{cert} are the constants from Theorem 15.5. As g is exponentially pseudo-surjective for P, then by Theorem 12.15, there is a $k \geq 1$ such that $tt_{n'^k,n'}$ is exponentially pseudo-surjective for P. Then by Theorem 12.14 there is an extension $\mathcal{M}^*$ of $\mathcal{M}_{2^{(n^{d'}\cdot d_{\mathsf{Res}^*}\cdot c_r}+c_r)^c}$ such that

1. $\mathcal{M}^* \models \mathsf{S}^1_2 + Rfn_P$ and

2. $tt_{(n^{d'\cdot d_{\mathsf{Res}^*}\cdot c_r}+c_r)^{kc},(n^{d'\cdot d_{\mathsf{Res}^*}\cdot c_r}+c_r)^c}$ is onto in $\mathcal{M}^*$

where $d' \in \mathbb{N}$ is a constant such that for any big enough D and ψ,

$$|Var(Correct^{D}_{\mathsf{Res}^*}(\psi))| \leq (|D| + |\psi|)^{d'}.$$

To complete the proof note that $\mathcal{M} \models \mathsf{S}^1_2 + Rfn_P + 2^{n^c} \in Log$ which implies that by Theorem 15.2 for any DNF $\phi \in \mathcal{M}^*$ such that $|\phi| = n$, if $\mathcal{M}^* \models \exists a\phi(a) = 0$, we have

$$\mathcal{M}^* \models \forall C^*, D^* \Pr_{r<2^{tc_r+c_r}}[V_{\mathsf{Res}^*}(\phi, p, u, C^*, D^*, r) = 1] \leq \frac{1}{2}$$

where $t = |Var(Correct^{D^*}_{\mathsf{Res}^*}(\phi)|$. To prove the remaining part, note that if for a DNF $\phi \in \mathcal{M}^*$ such that $|\phi| = n$, $\mathcal{M}^* \models \forall a\phi(a) = 1$, then by the fact that $tt_{(n^{d'\cdot d_{\mathsf{Res}^*}\cdot c_r}+c_r)^{kc},(n^{d'\cdot d_{\mathsf{Res}^*}\cdot c_r}+c_r)^c}$ is onto in $\mathcal{M}^*$, Theorem 15.4, and the fact that $\mathcal{M}^*$ knows that Res^* is compressible following the same argument as in the proof of Theorem 15.5, we get that $\mathcal{M}^*$ believes

$$\exists |C^*| \leq (n^{d'\cdot d_{\mathsf{Res}^*}\cdot c_r} + c_r)^{kc}, |D^*| \leq n^{d_{\mathsf{Res}^*}} \Pr_{r<2^{tc_r+c_r}}[V_{\mathsf{Res}^*}(\phi, p, u, C^*, D^*, r) = 1] = 1.$$

16.7 Proof of Theorem 15.7

To prove this theorem, we need the following statement.

Theorem 16.2. *Suppose there is a $k \in \mathbb{N}$ such that $tt_{n^k,n}$ is not a hard proof complexity generator for* EF*. Then the following statements hold:*

1. *If* EF *is automatable, then for infinitely many n, there is a* P/poly *natural property useful against* Size$(\frac{n^k}{3})$*.*

2. *If* EF *has the feasible disjunction property, then for infinitely many n, there is a* NP/poly *natural property useful against* Size$(\frac{n^k}{3})$*.*

Proof. Both items can be proved following the argument of Theorem 29.2.3 of [Kra11]. □

To prove the first item, we argue as follows. If $tt_{n^k,n}$ is not a hard proof complexity generator for EF, then we get the desired conclusion by Theorem 16.2. So Suppose this is not the case and $tt_{n^k,n}$ is a hard proof complexity generator for EF. We want to apply the idea of [AM20] and show that for every large enough n, every DNF ϕ such that $|\phi| = n$, there are p, u, and f such that the following conditions hold:

1. if ϕ has a falsifying assignment, then there is a polynomial size EF-proof for

$$LB^{l}_{\mathsf{Res}^*}(\ulcorner\phi\urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$$

and

2. if ϕ is a tautology, then $LB^{l}_{\mathsf{Res}^*}(\ulcorner\phi\urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$ does not have subexponential size EF-proofs

where l is from Theorem 15.5. If we prove this, we can show that $\mathsf{NP} \subseteq \mathsf{P/poly}$ as follows. Let A be the algorithm that automates EF. Let n be large enough. Fix p, u, f such that the following properties hold:

1. $2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$.
2. $|u| \leq |p|^{c_{cert}}$.
3. $Pratt(p, u) = 1$.
4. $|f| = (n^{d' \cdot d_{\mathsf{Res}^*} \cdot c_r} + c_r)^{k_a} + k_a$.
5. $Hard^A_{\frac{1}{4}}(f)$.

Given a DNF ϕ where $|\phi| = n$, we run A on $LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$ polynomially many steps and let π be its output. Then if π is an EF-proof of $LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$ we output that ϕ has a falsifying assignment; otherwise we output ϕ is a tautology and as the set of true DNFs is CoNP-complete, we get that $\mathsf{NP} \subseteq \mathsf{P/poly}$.

To complete the proof, we just need to prove items 1 and 2. Note that item 2 is true by Theorem 15.5. To prove item 1, suppose a, p, u, f have the following properties:

1. $\phi(a) = 0$.
2. $2^{2n^3+n} < p \leq 2^{(2n^3+n)^{c_p}}$.
3. $|u| \leq |p|^{c_{cert}}$.
4. $Pratt(p, u) = 1$.
5. $|f| = (n^{d' \cdot d_{\mathsf{Res}^*} \cdot c_r} + c_r)^{k_a} + k_a$.
6. $Hard^A_{\frac{1}{4}}(f)$.

As $\mathsf{iS}^1_2 \vdash_i sSound_c([\![\mathsf{IP}, \mathsf{Res}^*]\!])$, by Theorem 12.2 there is a PV-function h such that S^1_2 proves: for all ϕ', a', p', u', f' where $|\phi'| > c$, for all C, C', one of the following conditions hold:

1. $|f'| \neq |Var(C)|^{k_a} + k_a$ or,
2. $h(\phi', a', p', u', f')$ outputs a circuit of size $\leq \lceil |f'|^{\frac{1}{4}} \rceil$ and
$$tt^{\frac{1}{4}}(\lceil |f'|^{\frac{1}{4}} \rceil, |\lceil |f|^{\frac{1}{4}} \rceil|, h(\phi', a', p', u', f'), f') = 1$$
or,
3. $\phi'(a') = 1$, or
4. $$\Pr_{r < 2^{t^{c_r} + c_r}} [V_{\mathsf{Res}^*}(\phi', p', u', C, C', r) = 1] \preceq^{f'}_{\epsilon} \frac{1}{2},$$

where $t = |Var(Correct^{C'}_{\mathsf{Res}^*}(\phi'))|$. To simplify things, we denote the first two disjuncts in the above formula by α and the last disjunct by β. So rewriting the above probability, we have

$$\mathsf{S}^1_2 \vdash \forall |\phi'| \geq c, a', p', u' \Big(\alpha(\phi', a', p', u', C, f') \vee \phi'(a') = 0 \vee \beta(\phi', p', u', C, C', f') \Big).$$

As EF is the weak proof system of S^1_2, we get that EF has polynomial size proofs for

$$\{[[\alpha(\phi', a', p', u', C, f') \vee \phi'(a') = 0 \vee \beta(\phi', p', u', C, C', f')]]^c\}.$$

Let π be an EF-proof of

$$\Phi := [[\alpha(\phi', a', p', u', C, f') \vee \phi'(a') = 0 \vee \beta(\phi', p', u', C, C', f')]]^c_{l'}$$

for the parameter size $|\phi'| = n$. Using π, there is a short EF-proof π' for $\Phi(\ulcorner \phi \urcorner, a, p, u, \vec{x}_C, \vec{x}_{C'}, f)$. As α only cares about $|C|$ and not C, $\phi(a) = 0$, and p, u, f have the right properties, the first two disjuncts in $\Phi(\ulcorner \phi \urcorner, a, p, u, \vec{x}_C, \vec{x}_{C'}, f)$ disappear which means π' is a short EF-proof of $LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$ and this completes the argument.

The proof of the second part of Theorem 15.7 is similar. Following a similar argument, we can show that for any DNF ϕ, EF has short proofs for the formula

$$\phi(\vec{x}) \vee LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f).$$

As $\phi(\vec{x})$ and $LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$ do not have common variables and moreover, EF has the feasible disjunction property, we get that either ϕ has a short EF-proof or

$$LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$$

has a short EF-proof. But note that if ϕ is a tautology, then

$$LB^l_{\mathsf{Res}^*}(\ulcorner \phi \urcorner, p, u, \vec{x}_C, \vec{x}_{C'}, f)$$

does not have short EF-proofs. Also, if ϕ has a falsifying assignment, then as EF is a proof system for tautologies, ϕ does not have any EF-proof at all. The conclusion is that for any DNF ϕ, ϕ has a short EF-proof iff ϕ is a tautology which implies that $\mathsf{CoNP} \subseteq \mathsf{NP/poly}$ and this completes the proof. It is worth noting that what we actually proved is something stronger. Looking at the proof of item 2, we actually proved that if $\mathsf{iS}^1_2 \vdash_i sSound_c([\![\mathsf{IP}, \mathsf{Res}^*]\!])$ and EF has the disjunction property, then for any k, $tt_{n^k,n}$ is not a hard proof complexity generator for EF.

16.8 Proof of Theorem 15.8

To prove this theorem, we need the following statement.

Theorem 16.3. *([KP90a]) Let P be a well-behaved proof system and $\mathcal{M}_0 \models \mathsf{PV}_1 + Rfn_P$ be a countable nonstandard model. Then there is a countable cofinal extension $\mathcal{M}^*_0 \supseteq \mathcal{M}_0$ such that the following conditions hold:*

1. *$\mathcal{M}^*_0 \models \mathsf{PV}_1 + Rfn_P$.*
2. *For any propositional formula $\phi \in \mathcal{M}^*_0$, if $\mathcal{M}^*_0 \models \forall a \phi(a) = 1$, then $\mathcal{M}^*_0 \models \exists \pi P(\pi) = \phi$.*

Now suppose g is P-provably hard for P. Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic and $n \in \mathcal{M} \setminus \mathbb{N}$ and let $\mathcal{M}^*$ be a countable cofinal extension of $\mathcal{M}_{m(n)}$ such that $\mathcal{M}^* \models \mathsf{PV}_1 + Rfn_P$. By applying Theorem 16.3 on $\mathcal{M}^*$ we get an extension $\mathcal{M}^{**} \supseteq \mathcal{M}^*$ such that the following conditions hold:

1. $\mathcal{M}^{**} \models \mathsf{PV}_1 + Rfn_P$.

2. For any propositional formula $\phi \in \mathcal{M}^{**}$, if $\mathcal{M}^{**} \models \forall a \phi(a) = 1$, then there is a $k_\phi \in \mathbb{N}$ such that $\mathcal{M}^{**} \models \exists \pi (|\pi| \leq (m(n))^{k_\phi} \wedge P(\pi) = \phi)$.

The second item is true as $\mathcal{M}^{**}$ is a cofinal extension of $\mathcal{M}_{m(n)}$. Now suppose for the sake of contradiction that g_n is not onto in $\mathcal{M}^{**}$. This means that there is a $b \in \mathcal{M}^{**}$ of length $|m(n)|$ such that b is not in the range of g_n which implies that $\mathcal{M}^{**}$ believes that $\tau_b(g_n)$ is a tautology. This implies that there is a $\pi' \in \mathcal{M}^{**}$ such that $\mathcal{M}^{**} \models |\pi'| \leq (m(n))^{k_{\tau_b(g_n)}} \wedge P(\pi') = \ulcorner \tau_b(g_n) \urcorner$. This means that $\mathcal{M}^{**} \models \ulcorner IsHard_{P,g}^{n,k_{\tau_b(g_n)}} \urcorner(\pi', b) = 0$. As $\mathcal{M}^{**} \models \mathsf{PV}_1 + Rfn_P$, then by Theorem 12.12 $IsHard_{P,g}^{n,k_{\tau_b(g_n)}}(\vec{x}_\pi, \vec{x}_b)$ does not have any P-proof in $\mathcal{M}^{**}$. As g is P-provably hard for P, there are $c, c' \in \mathbb{N}$ such that $\mathcal{M}$ believes: for any $n' > c$ there is a P-proof of $IsHard_{P,g}^{n',k_{\tau_b(g_n)}}(\vec{x}_\pi, \vec{x}_b)$ of size $\leq (m(n'))^{c'} + c'$. This implies that there is a $\pi'' \in \mathcal{M}_{m(n)}$ such that

$$\mathcal{M}_{m(n)} \models |\pi''| \leq (m(n))^{c'} + c' \wedge P(\pi'') = \ulcorner IsHard_{P,g}^{n',k_{\tau_b(g_n)}} \urcorner$$

which implies that $\mathcal{M}^{**} \models P(\pi'') = \ulcorner IsHard_{P,g}^{n',k_{\tau_b(g_n)}} \urcorner$. and this leads to a contradiction and completes the proof.

To prove the other direction, suppose item 2 holds, but g is not P-provably hard for P. This means that there is a k such that for any c, c' there is a $n' > c$ such that there is no P-proof of $IsHard_{P,g}^{n',k}(\vec{x}_\pi, \vec{x}_b)$ of size $\leq (m(n'))^{c'}$. As this statement can be written as an arithmetical sentence, it is true in a countable nonstandard model of true arithmetic $\mathcal{M}$. Let $c_0, c_1 \in \mathcal{M} \setminus \mathbb{N}$. Then there is a $n \in \mathcal{M}$ such that $n > c_0$ and there is no P-proof of $IsHard_{P,g}^{n,k}(\vec{x}_\pi, \vec{x}_b)$ of size $\leq (m(n))^{c_1}$ in $\mathcal{M}$ which means that there is no P-proof of $IsHard_{P,g}^{n,k}(\vec{x}_\pi, \vec{x}_b)$ in $\mathcal{M}_{m(n)}$ as c_1 is nonstandard. Then by Theorem 12.13, there is a cofinal countable extension $\mathcal{M}^* \supseteq \mathcal{M}_{m(n)}$ such that the following conditions hold:

1. $\mathcal{M}^* \models \mathsf{PV}_1 + Rfn_P$.

2. There are $\pi, b \in \mathcal{M}^*$ such that $\mathcal{M}^* \models \ulcorner IsHard_{P,g}^{n,k} \urcorner(\pi, b) = 0$.

By the assumption of the theorem, there is a cofinal countable extension $\mathcal{M}^{**} \supseteq \mathcal{M}^*$ such that:

1. $\mathcal{M}^{**} \models \mathsf{PV}_1 + Rfn_P$.

2. g_n is onto in $\mathcal{M}^{**}$.

As $\mathcal{M}^{**}$ is an extension of $\mathcal{M}^*$, $\mathcal{M}^{**} \models \ulcorner IsHard_{P,g}^{n,k} \urcorner(\pi, b) = 0$ which implies that $\mathcal{M}^{**} \models P(\pi) = \ulcorner \tau_b(g_n) \urcorner$. As $\mathcal{M}^{**} \models \mathsf{PV}_1 + Rfn_P$, this implies that $\tau_b(g_n)$ is a tautology in $\mathcal{M}^{**}$ which means that $\mathcal{M}^{**}$ believes that b is not in the range of g_n which leads to a contradiction as we already knew that g_n is onto in $\mathcal{M}^{**}$ and this completes the proof.

16.9 Proof of Theorem 15.10

We need the following statements to prove Theorem 15.10.

Lemma 16.4. *For every partial recursive function F, there exists a Σ_1 formula $\Phi_F(x, y)$ such that $\mathsf{S}^1_2 \vdash \forall x, y, z(\Phi_F(x, y) \wedge \Phi_F(x, z) \to y = z)$.*

Proof. F is a partial recursive function, so the graph of is Σ_1 definable by formula $\exists z \phi(x, y, z)$ where $\phi(x, y, z)$ is a bounded formula. Let $\langle ., . \rangle$ be a pairing function and π_1 and π_2 be the corresponding projection functions such that they are Δ^b_1 definable in S^1_2 and moreover S^1_2 proves the basic properties of them. Define

$$\psi(x, y) := \phi(x, \pi_1(y), \pi_2(y)) \wedge \forall z(z < y \to \neg\phi(x, \pi_1(z), \pi_2(z))).$$

So we can define $\Phi_F(x, y) := \exists z(\psi(x, z) \wedge \pi_1(z) = y)$. □

Theorem 16.5. *([Bus86]) For every $T \in \mathcal{T}$, every Σ^b_1 formula $\phi(\vec{x})$, there exists a polynomial $p(\vec{x})$ such that*

$$\mathsf{S}^1_2 \vdash \forall \vec{x}(\phi(\vec{x}) \to \exists y(|y| \leq p(|\vec{x}|) \wedge Proof_T(y, \ulcorner \phi(\dot{\vec{x}}) \urcorner)).$$

Theorem 16.6. *([Pud86]) For every $T \in \mathcal{T}$, P_T has polynomial size proofs of $\{[[Con_T]]^c\}$.*

Lemma 16.7. *([KP89]). For every proof system P, $P_{\mathsf{S}^1_2 + Con_P}$ simulates P.*

Lemma 16.8. *For every $T, S \in \mathcal{T}$, if T has polynomial size proofs of $Con_S(\bar{n})$ in n, then for every Π^b_1 formula $\phi(x)$, if S has polynomial size proofs of $\phi(\bar{n})$ in n, then T has polynomial size proofs of $\phi(\bar{n})$ in n.*

Proof. Let $\phi(x)$ be a Π^b_1 formula. Then by Theorem 16.5 there exists a polynomial p such that

$$\mathsf{S}^1_2 \vdash \forall x(\neg\phi(x) \to \exists y(|y| \leq p(|x|) \wedge Proof_S(y, \ulcorner \neg\phi(\dot{x}) \urcorner)). \qquad (1)$$

We know that S has polynomial size proofs of $\phi(\bar{n})$ in n, so by Theorem 16.5, there exists a polynomial q such that S^1_2 has polynomial size proofs of $\exists u(|u| \leq q(|\bar{n}|) \wedge Proof_S(u, \ulcorner \phi(\dot{n}) \urcorner))$ in n. Hence by Equation 1 there exists a polynomial h such that

$$\neg\phi(\bar{n}) \to \exists y(|y| \leq h(\bar{n}) \wedge Proof_S(y, \ulcorner \bot \urcorner))$$

has polynomial size S^1_2-proofs in n, hence by the fact that $\mathsf{S}^1_2 \subseteq T$ we get

$$Con_S(h(\bar{n})) \to \phi(\bar{n})$$

has polynomial size T-proofs in n. Note that $Con_S(\bar{n})$ has polynomial size T-proofs in n and moreover h is a polynomial, hence T has polynomial size proof of $\phi(\bar{n})$ in n. □

An important observation is that if J is a jump operator, then H which works as follows is a hard tautology generator: on the input P, it outputs the $\forall\Pi^b_1$ sentence $Rfn_{J(\mathsf{EF}+\{[[Rfn_P]]^c\})}$. Moreover, if H is a hard tautology generator, then J which works as follows is a jump operator: on the input P, it outputs the proof system $\mathsf{EF} + \{[[H(P)]]^c\}$. So to prove the theorem, it is sufficient to show equivalence between items 2, 3, 4, and 5.

(2 ⇒ 3). Let F be a partial recursive hard tautology generator. Let $Tr(x)$ be a Π_1 formula such that for every $\forall\Pi_1^b$ sentence ϕ, $\mathsf{S}_2^1 \vdash Tr(\ulcorner\phi\urcorner) \equiv \phi$. Then define:

$$\Delta_F := \forall x(Tr(x) \to \exists y(\Phi_F(\ulcorner P_{\mathsf{S}_2^1+x}\urcorner, y) \wedge Con_{\mathsf{S}_2^1+y})).$$

Let $T := \mathsf{S}_2^1 + \Delta_F$. Note that $\mathbb{N} \models T$, hence for every true $\forall\Pi_1^b$ sentence ϕ, $\{Con_{T+\phi}(\bar{n})\}_n$ are true sentences. Suppose ϕ is a $\forall\Pi_1^b$ sentence, then

$$T + \phi \vdash \exists y(\Phi_F(\ulcorner P_{\mathsf{S}_2^1+\phi}\urcorner, y) \wedge Con_{\mathsf{S}_2^1+y}). \tag{2}$$

If ϕ is a true sentence, then there exists a $\forall\Pi_1^b$ sentence ψ such that:

1. $\Phi_F(\ulcorner P_{\mathsf{S}_2^1+\phi}\urcorner, \ulcorner\psi\urcorner)$ is true.

2. $\mathsf{S}_2^1 + \psi$ is consistent.

3. $\mathsf{S}_2^1 + \phi$ does not have polynomial size proofs of $Con_{\mathsf{S}_2^1+\psi}(\bar{n})$ in n as $P_{\mathsf{S}_2^1+\phi}$ does not have polynomial size proofs of $\{[[\psi]]^c\}$ (by Lemma 16.8).

Note that T is a Σ_1 complete theory, hence $T \vdash \Phi_F(\ulcorner P_{\mathsf{S}_2^1+\phi}\urcorner, \ulcorner\psi\urcorner)$. Moreover by Lemma 16.4

$$T \vdash \forall z(\Phi_F(\ulcorner P_{\mathsf{S}_2^1+\phi}\urcorner, \ulcorner\psi\urcorner) \wedge \Phi_F(\ulcorner P_{\mathsf{S}_2^1+\phi}\urcorner, z) \to z = \ulcorner\psi\urcorner).$$

Hence by Equation 2

$$T + \phi \vdash \Phi_F(\ulcorner P_{\mathsf{S}_2^1+\phi}\urcorner, \ulcorner\psi\urcorner) \wedge Con_{\mathsf{S}_2^1+\psi}.$$

This implies that $T + \phi \vdash Con_{\mathsf{S}_2^1+\psi}$ (I). Let $S \in \mathcal{T}$. Following the same argument as before, there exists a $\forall\Pi_1^b$ sentence η such that:

i. $\mathsf{S}_2^1 + \eta$ is consistent.

ii. $\mathsf{S}_2^1 + Con_S$ does not have polynomial size proofs of $Con_{\mathsf{S}_2^1+\eta}(\bar{n})$ in n.

iii. $T + Con_S \vdash Con_{\mathsf{S}_2^1+\eta}$ (by (I)).

If S has polynomial size proofs of $Con_{T+Con_S}(\bar{n})$ in n, then by Lemma 16.8 S has polynomial size proofs of $Con_{\mathsf{S}_2^1+\eta}(\bar{n})$ in n. So again by Lemma 16.8 $\mathsf{S}_2^1 + Con_S$ has polynomial size proofs of $Con_{\mathsf{S}_2^1+\eta}(\bar{n})$ in n, but this leads to a contradiction because of (ii) and hence this completes the proof.

(3 ⇒ 4). Let $T \in \mathcal{T}$ be a theory that certifies (3) and let P be a proof system. Note that $\mathbb{N} \models T$, hence for every true $\forall\Pi_1^b$ sentence ϕ, $\{Con_{T+\phi}(\bar{n})\}_{n\in\mathbb{N}}$ are true sentences. By the assumption, we know that $\mathsf{S}_2^1 + Con_P$ does not have polynomial size proofs of $Con_{T+Con_{\mathsf{S}_2^1+Con_P}}(\bar{n})$ in n (I). Note that $T + Con_{\mathsf{S}_2^1+Con_P}$ is finitely axiomatizable, so by Theorem 16.6 $P_{T+Con_{\mathsf{S}_2^1+Con_P}}$ has polynomial size proofs of $\{[[Con_{T+Con_{\mathsf{S}_2^1+Con_P}}]]^c\}$. So if P simulates $P_{T+Con_{\mathsf{S}_2^1+Con_P}}$, then P has polynomial size proofs of $\{[[Con_{T+Con_{\mathsf{S}_2^1+Con_P}}]]^c\}$. Hence by Lemma 16.7, $\mathsf{S}_2^1 + Con_P$ has polynomial size proofs of $Con_{T+Con_{\mathsf{S}_2^1+Con_P}}(\bar{n})$ in n, but this leads to a contradiction by (I) and hence the proof is completed.

$(3 \Rightarrow 5)$. Let $T \in \mathcal{T}$ be a theory that certifies statement (3). Suppose $S \in \mathcal{T}$ and $S \vdash T$. First of all, by Gödel's second incompleteness Theorem, $S + Con_S$ is consistent, hence $\{Con_{S+Con_S}(\bar{n})\}_{n \in \mathbb{N}}$ are true sentences. By the assumption, we know that S does not have polynomial size proofs of $Con_{T+Con_S}(\bar{n})$ in n (I). Note that T is finitely axiomatizable and moreover $S \vdash T$, so

$$\mathsf{S}^1_2 \vdash \forall x (Con_{S+Con_S}(x) \to Con_{T+Con_S}(x)).$$

So if S has polynomial size proofs of $Con_{S+Con_S}(\bar{n})$ in n, then S has polynomial size proofs of $Con_{T+Con_S}(\bar{n})$ in n, but this leads to a contradiction by (I) and hence the proof is completed.

$(4 \Rightarrow 2)$. Let $T \in \mathcal{T}$ be a theory that certifies statement (4). Let ϕ be a true $\forall \Pi^b_1$ sentence, hence $P_{\mathsf{S}^1_2+\phi}$ is a propositional proof system. Because T is a true theory, we have $T + Con_{\mathsf{S}^1_2+\phi}$ is consistent. Therefore H which works as follows is a polynomial time computable hard tautology generator: on the input P, it outputs

$$Con_{P_{T+Con_{\mathsf{S}^1_2+Con_{P_{\mathsf{S}^1_2+Con_P}}}}}.$$

$(5 \Rightarrow 2)$. Let $T \in \mathcal{T}$ be a theory that certifies statement (5). Let ϕ be a true $\forall \Pi^b_1$ sentence, then because T is a true theory, we have $T + \phi$ is consistent. Therefore H which works as follows is a polynomial time computable hard tautology generator: on the input P, it outputs

$$Con_{T+Con_P+Con_{T+Con_P}}.$$

17 Concluding remarks and open problems

In Section 14, we defined the randomized implicit proof system based on interactive proofs. Another type of randomized implicit proof systems can be defined based on the PCP theorem for $\mathsf{NTIME}(T)$ [BFLS91, BFL91]. Let $R(x, y)$ be a polynomial time computable relation. Then there exists a PCP polynomial time computable verifier V^R with the following properties (see [BFLS91]):

1. Soundness: Let $x \in \{0,1\}^*$ and $t \in \mathbb{N}$ such that $|x| \le t$. If for every $|y| \le t$, $R(x, y) = 0$, then for every π of size $\le t$:
$$\Pr_{r \in \{0,1\}^{O(\log t)}}[V^R(x, \pi, r) = 1] \le \frac{1}{3}.$$

2. Completeness: Let $x, y \in \{0,1\}^*$ such that $R(x, y) = 1$, then there exists a π of size $\le |y|^{O(1)}$ such that:
$$\Pr_{r \in \{0,1\}^{O(\log |y|)}}[V^R(x, \pi, r) = 1] = 1.$$

Definition 17.1. *Let P be a proof system for $\mathcal{L} \subseteq \{0,1\}^*$. Then $[\![\mathsf{PCP}, P]\!]$ denotes the* PCP*-randomized implicit proof system based on P. The verifier for $[\![\mathsf{PCP}, P]\!]$ is the* PV *function $V'_P(x, C, r)$ which works as follows:*

- *It runs V^R on $(x, tt(C), r)$ in this way that whenever V^R needs to query the i'th bit of $tt(C)$, it computes $C(i)$ to find the answer and outputs the output of the verifier (here $R(x,y) = 1$ iff $P(y) = x$).*

Again it is clear from the above definition that PCP-randomized implicit proof systems are actually MA proof systems. It is worth mentioning that in Definition 17.1, we did not put the condition that checks whether $P(C) = \phi$. We had this condition in the definition of IP-randomized implicit proof systems to make sure that $[\![\mathsf{IP}, P]\!]$ can simulate P. But in the case of PCP-randomized proof system, we do not need this condition because of the efficient completeness of the PCP theorem. Theorems 15.5 and 15.7 can be proved for PCP-randomized implicit proof in the same way that they were proved for IP-randomized implicit proof systems (actually if we consider Theorem 15.5 for PCP-randomized implicit proof systems, then Q does not need to be compressible in the statement). To prove Theorems 15.1, 15.2, and 15.6, a formalization of the PCP theorem of [BFLS91] inside $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ is needed. If we have such a formalization, then those theorems can be proved for PCP-randomized implicit proof systems following the same proofs for IP-randomized implicit proof systems (a formalization of the PCP theorem [BFLS91] in $\mathsf{S}^1_2 + 1\text{-}\mathsf{EXP}$ is possible as we formalized the sum-check protocol, but we did not formalize it as it seems that it does not give anything more than what we proved for IP-randomized implicit proof systems). Looking at definitions of PCP-randomized implicit proof systems and IP-randomized implicit proof systems, it is natural to ask the following question:

Problem 1. *Let P be a proof system. What is the relationship between $[\![\mathsf{IP}, P]\!]$ and $[\![\mathsf{PCP}, P]\!]$?*

Let $f \in \mathsf{E}$ and P be a proof system for $\mathcal{L} \subseteq \{0,1\}^*$. Then we can define a proof system based on f as follows: a string π is a P-proof of x iff there exists a P-proof π' for x such that $\pi = \left\langle \pi', tt(f_{\lceil \log |\pi'| \rceil}) \right\rangle$. It is easy to see that for any proof system P and any $f \in \mathsf{E}$, P and P_f are polynomially equivalent, but as we will see in the next proposition knowing that P_0 and P_1 are polynomially equivalent does not imply that Krajíček's implicit proof systems based on P_0 and P_1 are polynomially equivalent.

Proposition 17.1. *Let $f \in \mathsf{E}$ but $f \notin_{i.o.} \mathsf{P/poly}$. Then $[\mathsf{Res}, \mathsf{Res}^*_f]$ does not simulate $[\mathsf{Res}, \mathsf{Res}^*]$.*

Proof. Suppose this is not the case. Therefore there is a polynomial p such that for any DNF ϕ, if π is a $[\mathsf{Res}, \mathsf{Res}^*]$-proof of ϕ, then there is a $[\mathsf{Res}, \mathsf{Res}^*_f]$-proof of ϕ of size $\leq p(|\pi|)$. As $[\mathsf{Res}, \mathsf{Res}^*]$ is polynomially equivalent to EF with respect to true DNFs [Wan13] and the fact that EF has polynomial size proofs for $\{\mathsf{PHP}^{n+1}_n\}_{n\in\mathbb{N}}$ [CR79], we get that $[\mathsf{Res}, \mathsf{Res}^*]$ has polynomial size proofs for $\{\mathsf{PHP}^{n+1}_n\}_{n\in\mathbb{N}}$. This implies that there is a polynomial q such that for any n, there is a $[\mathsf{Res}, \mathsf{Res}^*_f]$-proof of PHP^{n+1}_n of size $\leq q(n)$. Note that there is a $c \in \mathbb{N}$ and $\epsilon > 0$ such that for any $n > c$, any Res-proof of PHP^{n+1}_n has size at least $2^{\epsilon n}$ [Hak85]. Now let n be an arbitrarily big enough number and let (π, C) be a $[\mathsf{Res}, \mathsf{Res}^*_f]$-proof of PHP^{n+1}_n of size $\leq q(n)$. This means that $tt(C)$ is a Res^*_f-proof of PHP^{n+1}_n. So there is a Res^*-proof π' for PHP^{n+1}_n such that $tt(C) = \left\langle \pi', f_{\lceil \log |\pi'| \rceil} \right\rangle$. As we explained, $|\pi'| \geq 2^{\epsilon n}$ which means that $q(n)$ is polynomial in $\lceil \log |\pi'| \rceil$ and this shows that $f \in_{i.o.} \mathsf{P/poly}$ which contradicts the assumption. □

Knowing the above proposition, it is natural to ask the same question about randomized implicit proof systems.

Problem 2. *Let P and Q be proof systems such that P simulates Q. Does $[\![\mathsf{IP}, P]\!]$ ($[\![\mathsf{PCP}, P]\!]$) simulate $[\![\mathsf{IP}, Q]\!]$ ($[\![\mathsf{PCP}, P]\!]$)?*

Looking at the Definition 15.1, $Sound_c([\![\mathsf{IP}, P]\!])$ is a $\forall\Sigma_1^b$ sentence which means that it actually defines a total NP search problem (TFNP). The input of the search problem is ϕ, a, p, u, C, C', f and the output is a *small circuit* D such that the conditions in Definition 15.1. Moreover, we can define the soundness of any MA proof system Q, denoted by $Sound_c(Q)$, as the way we did it for IP-randomized implicit proof systems in 15.1 and again, they define TFNP problems. In general, we can define new TFNP problems that resemble Definition 15.1 as follows.

Definition 17.2. *Let A, B be PV functions such there are $k, k' \in \mathbb{N}$ that for any x either $A(x) = 1$ or*

$$\Pr_{r<2^{|x|^{k'}+k'}}[B(x,r) = 1] \leq 1 - \frac{1}{|x|^k + k}.$$

Then Small-Circuit(A, B) *is the* TFNP *problem associated with the following true $\forall\Sigma_1^b$ sentence: for any x, f where $|x| > c$, there is a circuit D of size $\lceil |f|^{\frac{1}{4}} \rceil$ such that one of the following conditions hold:*

1. $|f| \neq |x|^{k_a} + k_a$ *or,*
2. $tt^{\frac{1}{4}}(\lceil |f|^{\frac{1}{4}} \rceil, |\lceil |f|^{\frac{1}{4}} \rceil|, D, f) = 1$ *or,*
3. $A(x) = 1,$ *or*
4. $$\Pr_{r<2^{|x|^{k'}+k'}}[B(x,r) = 1] \preceq^{f}_{\frac{1}{|x|^{2k}}} 1 - \frac{1}{|x|^k + k},$$

where c is a big enough constant.

There are several pairs (A, B) that we can consider Small-Circuit(A, B) such as the soundness of randomized implicit proof systems and in general MA proof systems, Small-Circuit problem based on the density of the n bit prime numbers, and the Small-Circuit problem based on Schwartz–Zippel lemma, so one might think that there is a hierarchy of these problems in terms of reducibility, but as these problems are based on breaking Nisan–Wigderson generator, actually all of them belong to FZPP (see [IW99]). In contrast with the situation of these problems in computational complexity, the $\forall\Sigma_1^b$ sentence associated with Small-Circuit problems might actually be hard to be proved in certain bounded arithmetics. In particular, it is natural to ask the following question.

Problem 3. *Can T_2 prove $Sound_c([\![\mathsf{IP}, \mathsf{Res}^*]\!])$ for some c?*

Looking at Theorem 15.7, it is natural to ask whether its statement can be proved under weaker assumptions. It is well-known that if a proof system is automatable, then it has the feasible disjunction property (see [BPR00]), but the other direction seems not to be true as Resolution has the feasible interpolation property (see [Kra97]), but Resolution is not automatable unless P = NP (see [AM20]). So the first question in this regard is the following.

Problem 4. *Is it possible to prove item 1 of Theorem 15.7 if we just assume that* EF *has the feasible interpolation property?*

As PV_1 and S^1_2 prove the same $\forall\Sigma^b_1$ sentences and the fact that $\mathit{Sound}_c(\llbracket \mathsf{IP}, \mathsf{Res}^* \rrbracket)$ and $\mathit{sSound}_c(\llbracket \mathsf{IP}, \mathsf{Res}^* \rrbracket)$ are equivalent over PV_1, we have the following question.

Problem 5. *Is it possible to weaken the assumption of Theorem 15.7 to* $\mathsf{PV} \vdash \mathit{sSound}_c(\llbracket \mathsf{IP}, \mathsf{Res}^* \rrbracket)$*?*

Regarding proof complexity generators, we defined a new hardness property and investigated its properties. As we do not fully understand this concept, the following questions seem to be natural. For these problems, we assume that P is a well-behaved proof system and $g \in \mathsf{FP}$ is a stretching map.

Problem 6. *Is it true that if g is P-provably hard for P, then g is pseudo-surjective for P?*

Looking at Theorem 15.8 and Theorem 12.14, we expect that the following question has a negative answer.

Problem 7. *Is it true that if g is free or pseudo-surjective P, then g is P-provably hard for P?*

The next question concerns the hypotheses stated in Subsection 15.2.

Problem 8. *If g is P-provably hard for P, then is there a constant $\epsilon > 0$ such that $tt_{2^{\epsilon n},n}$ is P-provably hard for P?*

Looking at Conjecture 13.1, Conjecture 13.2, Conjecture 15.1, and Theorem 15.10, we have the following questions.

Problem 9. *Does Conjecture 15.1 imply Conjecture 13.2?*

Problem 10. *Does Conjecture 13.1 imply Conjecture 15.1?*

Bibliography

[AB09] S. Arora and B. Barak. *Computational complexity. A modern approach.* Cambridge: Cambridge University Press, 2009.

[ABRW04] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, 2004.

[Ajt94] M. Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994.

[AM20] A. Atserias and M. Müller. Automating resolution is NP-hard. *Journal of the ACM*, 67(5):17, 2020.

[Bab85] L Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, page 421–429, 1985.

[Bel20] Z. Bell. Automating regular or ordered resolution is np-hard. *Electron. Colloquium Comput. Complex.*, TR20-105, 2020.

[BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[BFLS91] L. Babai, L. Fortnow, L. A. Levin, and M. Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, page 21–32, 1991.

[BPR00] M. L. Bonet, T. Pitassi, and R. Raz. On interpolation and automatization for Frege systems. *SIAM Journal on Computing*, 29(6):1939–1967, 2000.

[Bus86] S. R. Buss. Bounded arithmetic. Studies in Proof Theory. Lecture Notes, 3. Napoli: Bibliopolis. VII, 221 p. (1986)., 1986.

[Bus95] S. R. Buss. Relating the bounded arithmetic and polynomial time hierarchies. *Annals of Pure and Applied Logic*, 75(1-2):67–77, 1995.

[CHO$^+$22] L. Chen, S. Hirahara, I. C. Oliveira, J. Pich, N. Rajgopal, and R. Santhanam. Beyond natural proofs: hardness magnification and locality. *Journal of the ACM*, 69(4):49, 2022.

[Coo75] S. A. Cook. Feasibly constructive proofs and the propositional calculus. Proc. 7th ann. ACM Symp. Theory Comput., Albuquerque 1975, 83-97 (1975)., 1975.

[Coo98] S. Cook. Relating the provable collapse of $\mathbf{P}$ to $\mathbf{NC}^1$ and the power of logical theories. In *Proof complexity and feasible arithmetics. Papers from the DIMACS workshop, Rutgers, NJ, USA, April 21–24, 1996*, pages 73–91. Providence, RI: American Mathematical Society, 1998.

[CR79] S. A. Cook and R. A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44:36–50, 1979.

[CU93] S. Cook and A. Urquhart. Functional interpretations of feasibly constructive arithmetic. *Annals of Pure and Applied Logic*, 63(2):103–200, 1993.

[DR03] S. Dantchev and S. Riis. On relativisation and complexity gap for resolution-based proof systems. In *Computer science logic. 17th international workshop CSL 2003, 12th annual conference of the EACSL, 8th Kurt Gödel colloquium KGC 2003, Vienna, Austria, August 25–30, 2003. Proceedings*, pages 142–154. 2003.

[dR21] S. F. de Rezende. Automating tree-like resolution in time $n^{o(\log n)}$ is eth-hard. In *Proceedings of the XI Latin and American Algorithms, Graphs and Optimization Symposium, LAGOS 2021, Online Event / São Paulo, Brazil, May 2021*, volume 195 of *Procedia Computer Science*, pages 152–162, 2021.

[dRGN$^+$21] S. F. de Rezende, M. Göös, J. Nordström, T. Pitassi, R. Robere, and D. Sokolov. Automating algebraic proof systems is np-hard. In *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 209–222, 2021.

[FS11] L. Fortnow and R. Santhanam. Infeasibility of instance compression and succinct PCPs for NP. *Journal of Computer and System Sciences*, 77(1):91–106, 2011.

[Gar19] M. Garlík. Resolution lower bounds for refutation statements. In *44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, August 26-30, 2019, Aachen, Germany*, volume 138 of *LIPIcs*, pages 37:1–37:13, 2019.

[Gar20] M. Garlík. Failure of feasible disjunction property for \$k\$-dnf resolution and np-hardness of automating it. *Electron. Colloquium Comput. Complex.*, TR20-037, 2020.

[GGKS20] A. Garg, M. Göös, P. Kamath, and D. Sokolov. Monotone circuit lower bounds from resolution. *Theory of Computing*, 16:30, 2020.

[GKMP20] M. Göös, S. Koroth, I. Mertz, and T. Pitassi. Automating cutting planes is NP-hard. In *Proceedings of the 52nd annual ACM SIGACT symposium on theory of computing, STOC '20, Chicago, IL, USA, June 22–26, 2020*, pages 68–77. 2020.

[GP18] J. A. Grochow and T. Pitassi. Circuit complexity, proof complexity, and polynomial identity testing. The ideal proof system. *Journal of the ACM*, 65(6):59, 2018.

[Hak85] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[Hak20] T. Hakoniemi. Feasible interpolation for polynomial calculus and sums-of-squares. In *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020, July 8-11, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 168 of *LIPIcs*, pages 63:1–63:14, 2020.

[HP93] P. Hájek and P. Pudlák. *Metamathematics of first-order arithmetic.* Perspectives in Mathematical Logic. Berlin: Springer-Verlag, 1993.

[IKW02] R. Impagliazzo, V. Kabanets, and A. Wigderson. In search of an easy witness: Exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002.

[IR22] D. Itsykson and A. Riazanov. Automating OBDD proofs is np-hard. In *47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria*, volume 241 of *LIPIcs*, pages 59:1–59:15, 2022.

[IW99] R. Impagliazzo and A. Wigderson. $P = BPP$ if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of the 29th annual ACM symposium on theory of computing, STOC '97. El Paso, TX, USA, May 4–6, 1997*, pages 220–229. 1999.

[Jeř04] E. Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Annals of Pure and Applied Logic*, 129(1-3):1–37, 2004.

[Jeř05] E. Jeřábek. Weak pigeonhole principle and randomized computation. *Ph.D. thesis, Charles University in Prague*, 2005.

[Jeř07] E. Jeřábek. Approximate counting in bounded arithmetic. *The Journal of Symbolic Logic*, 72(3):959–993, 2007.

[KP89] J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[KP90a] J Krajíček and P Pudlák. Propositional provability and models of weak arithmetic. In *CSL '89. 3rd workshop on computer science logic, Kaiserslautern, Germany, October 2–6, 1989. Proceedings*, pages 193–210. 1990.

[KP90b] J. Krajíček and P. Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 36(1):29–46, 1990.

[KP98] J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S^1_2 and EF. *Information and Computation*, 140(1):82–94, 1998.

[KPT91] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52(1-2):143–153, 1991.

[Kra90] J. Krajíček. Exponentiation and second-order bounded arithmetic. *Annals of Pure and Applied Logic*, 48(3):261–276, 1990.

[Kra95] J. Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge: Cambridge Univ. Press, 1995.

[Kra97] J. Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[Kra01a] J. Krajíček. Tautologies from pseudo-random generators. *The Bulletin of Symbolic Logic*, 7(2):197–212, 2001.

[Kra01b] J. Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1-2):123–140, 2001.

[Kra04a] J. Krajíček. Diagonalization in proof complexity. *Fundamenta Mathematicae*, 182(2):181–192, 2004.

[Kra04b] J. Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *The Journal of Symbolic Logic*, 69(1):265–286, 2004.

[Kra04c] J. Krajíček. Implicit proofs. *The Journal of Symbolic Logic*, 69(2):387–397, 2004.

[Kra05] J. Krajíček. Structured pigeonhole principle, search problems and hard tautologies. *The Journal of Symbolic Logic*, 70(2):616–630, 2005.

[Kra11] J. Krajíček. *Forcing with random variables and proof complexity*, volume 382. Cambridge: Cambridge University Press, 2011.

[Kra14] J Krajíček. On the computational complexity of finding hard tautologies. *Bulletin of the London Mathematical Society*, 46(1):111–125, 2014.

[Kra19] J. Krajíček. *Proof complexity*, volume 170. Cambridge: Cambridge University Press, 2019.

[Kra22] J. Krajíček. On the existence of strong proof complexity generators. *arXiv*, abs/2208.11642, 2022.

[LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, oct 1992.

[MP20] M. Müller and J. Pich. Feasibly constructive proofs of succinct weak circuit lower bounds. *Annals of Pure and Applied Logic*, 171(2):45, 2020.

[MPW02] A. Maciel, T. Pitassi, and A. R. Woods. A new proof of the weak pigeonhole principle. *Journal of Computer and System Sciences*, 64(4):843–872, 2002.

[NW94] N. Nisan and A. Wigderson. Hardness vs randomness. 49(2):149–167, 1994.

[Par71] R. Parikh. Existence and feasibility in arithmetic. *The Journal of Symbolic Logic*, 36:494–508, 1971.

[Pic15] J. Pich. Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic. *Logical Methods in Computer Science*, 11(2):38, 2015.

[Pra75] V. R. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4:214–220, 1975.

[PS22] J. Pich and R. Santhanam. Learning algorithms versus automatability of frege systems. In *49th International Colloquium on Automata, Languages, and Programming, ICALP 2022, July 4-8, 2022, Paris, France*, volume 229 of *LIPIcs*, pages 101:1–101:20, 2022.

[Pud86] P. Pudlák. On the length of proofs of finitistic consistency statements in first order theories. Logic colloq. '84, Proc. Colloq., Manchester/U.K. 1984, Stud. Logic Found. Math. 120, 165-196 (1986)., 1986.

[Pud87] P. Pudlák. Improved bounds to the length of proofs of finitistic consistency statements. Logic and combinatorics, Proc. AMS-IMS-SIAM Conf., Arcata/Calif. 1985, Contemp. Math. 65, 309-332 (1987)., 1987.

[Pud97] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

[Pud03] P. Pudlák. On reducibility and symmetry of disjoint NP pairs. *Theoretical Computer Science*, 295(1-3):323–339, 2003.

[Pud17] P. Pudlák. Incompleteness in the finite domain. *The Bulletin of Symbolic Logic*, 23(4):405–441, 2017.

[Pud20] P. Pudlák. Reflection principles, propositional proof systems, and theories. *arXiv*, (arXiv:2007.14835), 2020.

[PW85] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. Methods in mathematical logic, Proc. 6th Latin Amer. Symp., Caracas/Venez. 1983, Lect. Notes Math. 1130, 317-340 (1985)., 1985.

[PWW88] J. B. Paris, A. J. Wilkie, and A. R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *The Journal of Symbolic Logic*, 53(4):1235–1244, 1988.

[Raz15] A. A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics. Second Series*, 181(2):415–472, 2015.

[RR97] A. A. Razborov and S. Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[Rud97] S. Rudich. Super-bits, demi-bits, and np/qpoly-natural proofs. In *Proceedings of the International Workshop on Randomization and Approximation Techniques in Computer Science*, RANDOM '97, page 85–93, 1997.

[ST21] R. Santhanam and I. Tzameret. Iterated lower bound formulas: a diagonalization-based approach to proof complexity. In *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 234–247, 2021.

[Wan13] Z. Wang. Implicit resolution. *Logical Methods in Computer Science*, 9(4):10, 2013.

Paper D

Not all Kripke models of HA are locally PA

Erfan Khaniki[1,2]
[1]Faculty of Mathematics and Physics, Charles University
[2]Institute of Mathematics, Czech Academy of Sciences

Abstract

Let $\mathbf{K}$ be an arbitrary Kripke model of Heyting Arithmetic, HA. For every node k in $\mathbf{K}$, we can view the classical structure of k, $\mathcal{M}_k$ as a model of some classical theory of arithmetic. Let T be a classical theory in the language of arithmetic. We say $\mathbf{K}$ is locally T, iff for every k in $\mathbf{K}$, $\mathcal{M}_k \models T$. One of the most important problems in the model theory of HA is the following question: *Is every Kripke model of* HA *locally* PA*?* We answer this question negatively. We introduce two new Kripke model constructions to this end. The first construction actually characterizes the arithmetical structures that can be the root of a Kripke model $\mathbf{K} \Vdash \mathsf{HA} + \mathsf{ECT}_0$ (ECT_0 stands for Extended Church Thesis). The characterization says that for every arithmetical structure $\mathcal{M}$, there exists a rooted Kripke model $\mathbf{K} \Vdash \mathsf{HA} + \mathsf{ECT}_0$ with the root r such that $\mathcal{M}_r = \mathcal{M}$ iff $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$. One of the consequences of this characterization is that there is a rooted Kripke model $\mathbf{K} \Vdash \mathsf{HA} + \mathsf{ECT}_0$ with the root r such that $\mathcal{M}_r \not\models \mathbf{I}\Delta_1$ and hence $\mathbf{K}$ is not even locally $\mathbf{I}\Delta_1$. The second Kripke model construction is an implicit way of doing the first construction which works for any reasonable consistent intuitionistic arithmetical theory T with a recursively enumerable set of axioms that has the existence property. We get a sufficient condition from this construction that describes when for an arithmetical structure $\mathcal{M}$, there exists a rooted Kripke model $\mathbf{K} \Vdash T$ with the root r such that $\mathcal{M}_r = \mathcal{M}$. As applications of this sufficient condition, we construct two new Kripke models. The first one is a Kripke model $\mathbf{K} \Vdash \mathsf{HA} + \neg\theta + \mathsf{MP}$ (θ is an instance of ECT_0 and MP is Markov's principle) which is not locally $\mathbf{I}\Delta_1$. The second one is a Kripke model $\mathbf{K} \Vdash \mathsf{HA}$ such that $\mathbf{K}$ forces exactly the sentences that are provable from HA, but it is not locally $\mathbf{I}\Delta_1$. Also, we will prove that every countable Kripke model of intuitionistic first-order logic can be transformed into another Kripke model with the full infinite binary tree as the Kripke frame such that both Kripke models force the same sentences. So with the previous result, there is a binary Kripke model $\mathbf{K}$ of HA such that $\mathbf{K}$ is not locally $\mathbf{I}\Delta_1$.

18 Introduction

Heyting Arithmetic (HA) is the intuitionistic counterpart of Peano Arithmetic (PA). HA has the same non-logical axioms as PA with intuitionistic first-order logic as the underlying logic. This theory is one of the well-known and most studied theories of constructive mathematics, and it was investigated in many proof-theoretic and model-theoretic aspects in the literature (see [Tv88] for more information). This paper aims to answer a question about the model theory of HA. Let T be a classical theory in the language of arithmetic. A Kripke model of HA is called locally T, iff for every node $k \in \mathbf{K}$, the classical structure $\mathcal{M}_k$ associated with k, is a model of T. One of the most important problems in the model theory of HA is the following question:

Problem 11. *Is every Kripke model of* HA *locally* PA*?*

This problem was first asked and investigated in the seminal paper [vMKV86] by van Dalen *et al.* in 1986. They proved that every finite Kripke model of HA is locally PA. Furthermore, they proved that a Kripke model of HA with the Kripke frame $(\omega, \leq)$ as the underlying frame has infinitely many locally PA nodes. This work initiated a research line into Problem 11 and also about the following general question:

Problem 12. *For a Kripke model* $\mathbf{K}$ *of the theory* T *in a language* σ*, and a node* $k \in \mathbf{K}$*, what is the relationship between the sentences forced in* k *and the sentences satisfied in* $\mathcal{M}_k$*?*

There are several works that deal with these problems. We will review those works in the following paragraphs. Wehmeier in [Weh96], investigated Problem 11 and extended the results of [vMKV86] to a larger class of frames. In particular, he proved that every Kripke model of HA with $(\omega, \leq)$ as the Kripke frame is indeed locally PA. Moniri, in [Mon02], considered these problems and proved that every once-branching Kripke model of HA + MP (Markov's principle) is locally PA. Ardeshir and Hesaam in [AH02] generalized the results of [Weh96] to rooted narrow tree Kripke models of HA. Recently, Mojtahedi in [Moj18] considered Problem 12 and answered this problem in the case of finite depth Kripke models. As an application, he generalized the result of [AH02] to rooted semi-narrow tree Kripke models of HA.

Regarding Problem 11, the strongest positive result about the strength of induction axioms that are true in a node of a Kripke model of HA was proved by Marković in [Mar93]. He proved that every node of a Kripke model of HA satisfies induction for formulas that are provably Δ_1 in PA. Also, from Π_2 conservativity of PA over HA (see [Fri78]), we know that every Kripke model of HA is locally $\mathbf{Th}_{\Pi_2}(\mathsf{PA})$.

Buss studied another question related to these problems in [Bus93]. For every language σ and every classical theory T in it, he characterized the sentences that are true in every locally T Kripke model. As a result, he proved that HA is complete with respect to the locally PA Kripke models. In a similar direction, Ardeshir *et al.* in [ARS03] presented a set of axiom systems for the class of end-extension Kripke models. As an application, they proved that HA is strongly complete for its class of end-extension Kripke models. For the case of fragments of HA, Problem 11 was investigated and answered negatively by Połacik in [Poł06].

To best of our knowledge, the above theorems are all results relevant to Problem 11 in the literature. There are some other papers such as [AMZ18, AMZ19] that investigated Problem 12 in general and partially answered this question.

In this paper, we will present two new model construction to answer Problems 11 and 12. The main technical theorem of the first construction says that the theory $\mathsf{HA} + \mathsf{ECT}_0 + \mathsf{Diag}(\mathcal{M})$ for every $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$ has the existence and the disjunction properties (Theorem 20.5). This theorem provides the right tool for constructing rooted Kripke models of HA with control over the structure of the root (Theorem 20.6). This construction theorem moreover characterizes the necessary and sufficient conditions for an arithmetical structure $\mathcal{M}$ to be the root of a Kripke model of $\mathsf{HA} + \mathsf{ECT}_0$ (Corollary 20.7). Using this characterization we will construct a Kripke model of $\mathsf{HA} + \mathsf{ECT}_0$ that is not even locally $\mathbf{I}\Delta_1$.

This answers Problem 11 negatively. Moreover, this is optimal, because it is well-known that every node of a Kripke model of HA satisfies induction for formulas that are provably Δ_1 in PA ([Mar93]). The second construction is an implicit way of doing the first construction and it works for any reasonable consistent intuitionistic arithmetical theory with a recursively enumerable set of axioms that has the existence property (Theorem 20.14). This construction gives us a sufficient condition for an arithmetical structure $\mathcal{M}$ to be the root of a Kripke model of T. As applications of this sufficient condition, we will construct two new Kripke models. The first one is a Kripke model of $\mathsf{HA} + \neg\theta + \mathsf{MP}$ where θ is an instance of ECT_0 and MP is Markov's principle that is not locally $\mathbf{I}\Delta_1$ (Corollary 20.16). The second one is a Kripke model of HA that forces exactly all sentences that are provable in HA, but it is not locally $\mathbf{I}\Delta_1$ (Corollary 20.17).

The second construction is general and also works for $\mathsf{HA} + \mathsf{ECT}_0$, but some Kripke models can be constructed for $\mathsf{HA} + \mathsf{ECT}_0$ with the first construction, but not possible with the second one. We will discuss this matter in more detail at the end of Section 3. The new model constructions imply the existence of a large class of Kripke models of reasonable intuitionistic arithmetical theories including HA, which cannot be constructed by previous methods, so we think that these model constructions are interesting in their own rights.

We will also prove that every countable Kripke model of intuitionistic first-order logic can be transformed into another Kripke model with the full infinite binary tree as the Kripke frame (Lemma 21.1). Using this result, we will prove that there exists a Kripke model of HA with the full infinite binary tree as the Kripke frame that is not locally $\mathbf{I}\Delta_1$ (Corollary 21.2).

19 Preliminaries

19.1 Arithmetical Theories

Let $\mathcal{L}$ be the language of Primitive Recursive Arithmetic in which it has a function symbol for every primitive recursive function. HA is the intuitionistic theory with the following non-logical axioms:

1. Axioms of Robinson Arithmetic Q.
2. Axioms defining the primitive recursive functions.
3. For each formula $\phi(x, \vec{y}) \in \mathcal{L}$, the axiom $\forall \vec{y}\, \mathbf{I}_\phi$ in which

$$\mathbf{I}_\phi := \phi(\bar{0}) \wedge \forall x(\phi(x) \to \phi(Sx)) \to \forall x \phi(x).$$

PA is the classical theory that has the same non-logical axioms as HA. iPRA (intuitionistic Primitive Recursive Arithmetic) has axioms of Q, Axioms defining the primitive recursive functions, and induction for every atomic formula of $\mathcal{L}$. The underlying logic of iPRA is intuitionistic logic. PRA is the classical counter part of iPRA. $T \vdash_c \phi$ means that there exists a proof of ϕ from axioms of T using first-order classical logic Hilbert system. $\vdash_i$ denotes the same thing for intuitionistic proofs. An important set of intuitionistic arithmetical theories for the purpose of this paper is defined in the following definition.

Definition 19.1. *$\mathcal{I}$ is the set of all intuitionistic arithmetical theories T in $\mathcal{L}$ such that:*

1. *T is consistent.*
2. *$i\mathsf{PRA} \subseteq T$.*
3. *The set of axioms of T is recursively enumerable.*

Note that with the power of primitive recursive functions we can define finite sequences of numbers, so we can code finite objects such as formulas, proofs, and etc. as numbers. This is a standard technique and it is called Gödel numbering (see [Smo85]). With the help of this coding we can talk about proofs of theories in arithmetical theories (see [Smo85]). For every $\mathcal{L}$ sentence ϕ, $\ulcorner \phi \urcorner$ denotes the number associated with ϕ. If $\phi(x)$ is an $\mathcal{L}$ formula, then $\ulcorner \phi(\dot{c}) \urcorner$ denotes the number associated with $\psi(x)$ when we substitute the numeral with value c for x. Suppose $T \in \mathcal{I}$. Let $Axiom(x, y)$ be the primitive recursive function such that for every $\mathcal{L}$ sentence ϕ, ϕ is a T-axiom iff $\exists x Axiom(x, \ulcorner \phi \urcorner) = 0$ is true. Then it is possible to define the provability predicate of T, $Proof_T(x, y)$ as a primitive recursive predicate as follows. Let $\langle . \rangle$ be a natural primitive recursive coding function. Then $Proof_T(x, y)$ is true iff there exist a sequence of $\mathcal{L}$ sentences $\{\phi_i\}_{i \leq n}$ and a sequence of numbers $\{w_i\}_{i \leq n}$ for some n such that:

1. $x = \langle \langle w_1, \ulcorner \phi_1 \urcorner \rangle, ..., \langle w_n, \ulcorner \phi_n \urcorner \rangle \rangle$.
2. For every $i \leq n$:
   (a) If $w_i > 0$, then $Axiom(w_i - 1, \ulcorner \phi_i \urcorner)$ is true.
   (b) If $w_i = 0$, then ϕ_i can be derived from $\{\phi_j\}_{j<i}$ by one of the rules of standard Hilbert style deduction system for intuitionistic first-order logic.
3. $y = \ulcorner \phi_n \urcorner$.

The Σ_1 formula $Pr_T(y)$ is the abbreviation for $\exists x Proof_T(x, y)$. So consistency of T, Con_T, is $\neg Pr_T(\ulcorner \bot \urcorner)$. The following theorem states the useful facts about Pr_T.

Theorem 19.1. *For every $T \in \mathcal{I}$ the following statements are true:*

1. *For every $\mathcal{L}$ sentence ϕ, if $T \vdash_i \phi$, then $\mathsf{PRA} \vdash_c Pr_T(\ulcorner \phi \urcorner)$.*
2. *$\mathsf{PRA} \vdash_c \forall x, y(Pr_T(x) \wedge Pr_T(x \to y) \to Pr_T(y))$.*
3. *$\mathsf{PRA} \vdash_c \forall x, y(Pr_T(x) \wedge Pr_T(y) \to Pr_T(x \wedge y))$.*
4. *For every $\mathcal{L}$ formula $\phi(\vec{x})$ with $\vec{x}$ as the only free variables,*
$$\mathsf{PRA} \vdash_c Pr_T(\ulcorner \forall \vec{x} \phi(\vec{x}) \urcorner) \to \forall x Pr_T(\ulcorner \phi(\dot{x_1}, ..., \dot{x_n}) \urcorner).$$
5. *For every Σ_1 formula $\phi(\vec{x})$, $\mathsf{PRA} \vdash_c \forall \vec{x}(\phi(\vec{x}) \to Pr_T(\ulcorner \phi(\dot{x_1}, ..., \dot{x_n}) \urcorner))$.*
6. *For every Π_1 formula $\phi(\vec{x})$, $\mathsf{PRA} \vdash_c Con_T \to \forall \vec{x}(Pr_T(\ulcorner \phi(\dot{x_1}, ..., \dot{x_n}) \urcorner) \to \phi(\vec{x}))$.*

Proof. See [Smo85] for a detailed discussion of the first five items. For the last item see Theorem 4.1.4 of [Smo77]. □

19.2 Realizability

For proving the first model construction theorem, we need some definitions and theorems about Kleene's realizability.

Definition 19.2. *Let $T(x, y, z)$ be the primitive recursive function called Kleene's T-predicate and $U(x)$ be the primitive recursive function called result-extracting function. Note that*

$$\mathsf{HA} \vdash_i \forall x, y, z, z'(T(x, y, z) = 0 \wedge T(x, y, z') = 0 \to U(z) = U(z')).$$

We use $T(x, y, z)$ instead of $T(x, y, z) = 0$ for simplicity. For more information, see section 7 of the third chapter of [Tv88].

Let $j_1(x)$ and $j_2(x)$ be the primitive recursive projections of the pairing function $j(x, y) = 2^x \cdot (2y + 1) \dot{-} 1$. Kleene's realizability is defined as follows.

Definition 19.3. *$x \,\mathbf{r}\, \phi$ (x realizes ϕ) is defined by induction on the complexity of ϕ where $x \notin FV(\phi)$.*

1. $x \,\mathbf{r}\, p := p$ *for atomic* p,
2. $x \,\mathbf{r}\, (\psi \wedge \eta) := j_1(x) \,\mathbf{r}\, \psi \wedge j_2(x) \,\mathbf{r}\, \eta$,
3. $x \,\mathbf{r}\, (\psi \vee \eta) := (j_1(x) = 0 \wedge j_2(x) \,\mathbf{r}\, \psi) \vee (j_1(x) \neq 0 \wedge j_2(x) \,\mathbf{r}\, \eta)$,
4. $x \,\mathbf{r}\, (\psi \to \eta) := \forall y(y \,\mathbf{r}\, \psi \to \exists u(T(x, y, u) \wedge U(u) \,\mathbf{r}\, \eta)$, $u \notin FV(\eta)$,
5. $x \,\mathbf{r}\, \exists y \psi(y) := j_2(x) \,\mathbf{r}\, \psi(j_1(x))$,
6. $x \,\mathbf{r}\, \forall y \psi(y) := \forall y \exists u(T(x, y, u) \wedge U(u) \,\mathbf{r}\, \psi(y))$, $u \notin FV(\psi)$.

Definition 19.4. *A formula $\phi \in \mathcal{L}$ is almost negative iff ϕ does not contain $\vee$, and $\exists$ only immediately in front of atomic formulas.*

Definition 19.5. *The extended Church's thesis (ECT_0) is the following schema, where ϕ is almost negative:*

$$\forall \vec{v}\Big(\forall x(\phi(x, \vec{v}) \to \exists y \psi(x, y, \vec{v})) \to$$

$$\exists z \forall x(\phi(x, \vec{v}) \to \exists u(T(z, x, u) \wedge \psi(x, U(u), \vec{v})))\Big).$$

Next theorem explains the relationships between, HA, ECT_0 and Kleene's realizability.

Theorem 19.2. *For every formula $\phi \in \mathcal{L}$:*

1. $\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \phi \leftrightarrow \exists x(x \,\mathbf{r}\, \phi)$,
2. $\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \phi \Leftrightarrow \mathsf{HA} \vdash_i \exists x(x \,\mathbf{r}\, \phi)$.

Proof. See Theorem 4.10 in the fourth chapter of [Tv88]. □

Another important properties of HA are the existence and the disjunction properties. We will use notation $\bar{n}$ as the syntactic term corresponds to natural number n.

Theorem 19.3. *The following statements are true:*

1. *Disjunction property: For every sentences $\phi, \psi \in \mathcal{L}$, if $\mathsf{HA} \vdash_i \phi \vee \psi$, then $\mathsf{HA} \vdash_i \phi$ or $\mathsf{HA} \vdash_i \psi$,*

2. *Existence property: For every sentence $\exists x \phi(x) \in \mathcal{L}$, if $\mathsf{HA} \vdash_i \exists x \phi(x)$, then there exists a natural number n such that $\mathsf{HA} \vdash_i \phi(\bar{n})$.*

Proof. See Theorem 5.10 of the third chapter of [Tv88]. □

Although HA is an intuitionistic theory, it can prove some restricted class of formulas are discrete. The next theorem explains this fact.

Theorem 19.4. *([Tv88]) For every quantifier free formula $\phi \in \mathcal{L}$, $\mathsf{HA} \vdash_i \phi \vee \neg \phi$.*

19.3 Kripke models

A Kripke model for a language σ is a triple $\mathbf{K} = (K, \leq, \mathcal{M})$ such that:

1. $(K, \leq)$ is a nonempty partial order.

2. For every $k \in K$, $\mathcal{M}_k \in \mathcal{M}$ is a classical structure in the language $\sigma(\mathcal{M}_k) = \sigma \cup \{\underline{c} | c \in \mathcal{M}_k\}$.

3. For every $k, k' \in K$, if $k \leq k'$, then $\sigma(\mathcal{M}_k) \subseteq \sigma(\mathcal{M}_{k'})$ and also $\mathcal{M}_{k'} \models \mathsf{Diag}^+(\mathcal{M}_\mathsf{k})$ ($\mathcal{M}_k$ is a sub-structure of $\mathcal{M}_{k'}$).

For every Kripke model $\mathbf{K}$, there is a uniquely inductively defined relation $\Vdash \subseteq K \times (\bigcup_{k \in K} \sigma(\mathcal{M}_k))$ that is called forcing.

Definition 19.6. *For every $k \in K$, and every sentence $\phi \in \sigma(\mathcal{M}_k)$, the relation $k \Vdash \phi$ is defined by induction on complexity of ϕ:*

1. *$k \Vdash p$ iff $\mathcal{M}_k \models p$, for atomic p,*

2. *$k \Vdash \psi \wedge \eta$ iff $k \Vdash \psi$ and $k \Vdash \eta$,*

3. *$k \Vdash \psi \vee \eta$ iff $k \Vdash \psi$ or $k \Vdash \eta$,*

4. *$k \Vdash \neg \psi$ iff for no $k' \geq k$, $k' \Vdash \psi$,*

5. *$k \Vdash \psi \to \eta$ iff for every $k' \geq k$, if $k' \Vdash \psi$, then $k' \Vdash \eta$,*

6. *$k \Vdash \exists x \psi(x)$ iff there exists $\underline{c} \in \sigma_{\mathcal{M}_k}$ such that $k \Vdash \psi(\underline{c})$,*

7. *$k \Vdash \forall x \psi(x)$ iff for every $k' \geq k$ and every $\underline{c} \in \sigma(\mathcal{M}_{k'})$, $k' \Vdash \psi(\underline{c})$.*

We use the notation $\mathbf{K} \Vdash \phi$ ($\phi \in \bigcap_{k \in K} \sigma(\mathcal{M}_k)$ is a sentence) as an abbreviation that for every $k \in K$, $k \Vdash \phi$ which simply means that the Kripke model $\mathbf{K}$ forces ϕ. The important property of the forcing relation is its monotonicity. This means that for every $k' \geq k$ and every $\phi \in \sigma(\mathcal{M}_k)$, if $k \Vdash \phi$, then $k' \Vdash \phi$. Also, note that first-order intuitionistic logic is sound and is strongly complete with respect to the Kripke models. For more details see [Tv88].

As we mentioned in the introduction, every Kripke model of HA is locally $\mathbf{Th}_{\Pi_2}(\mathsf{PA})$. The following lemma states this fact.

Lemma 19.5. *Every Kripke model of* HA *is locally* $\mathbf{Th}_{\Pi_2}(\mathsf{PA})$*.*

Proof. Let $\mathbf{K}$ be a Kripke model of HA and k be an arbitrary node of $\mathbf{K}$. Let $\phi := \forall\vec{x}\exists\vec{y}\psi(\vec{x},\vec{y})$ be a Π_2 sentence such that $\mathsf{PA} \vdash_c \phi$. Then by Π_2 conservativity of HA over PA (see [Fri78]), we have $\mathsf{HA} \vdash_i \phi$, hence $\mathbf{K} \Vdash \phi$. This implies that $k \Vdash \forall\vec{x}\exists\vec{y}\psi(\vec{x},\vec{y})$. So for every $\vec{a} \in \mathcal{M}_k$:

1. $\Rightarrow k \Vdash \exists\vec{y}\psi(\underline{\vec{a}},\vec{y})$,

2. $\Rightarrow$ there exist $\vec{b} \in \mathcal{M}_k$ such that $k \Vdash \psi(\underline{\vec{a}},\underline{\vec{b}})$,

3. $\Rightarrow \mathcal{M}_k \models \psi(\underline{\vec{a}},\underline{\vec{b}})$.

Hence $\mathcal{M}_k \models \phi$. This implies that $\mathcal{M}_k \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$. □

20 Kripke model constructions for intuitionistic arithmetical theories

20.1 The first model construction

We will explain the first model construction in this subsection. This construction will be presented in a sequence of lemmas and theorems.

Lemma 20.1. *For every quantifier-free formula* $\phi \in \mathcal{L}$ *there exists an atomic formula* $p \in \mathcal{L}$ *with the same free variables such that* $\mathsf{HA} \vdash_i \phi \leftrightarrow p$*.*

Proof. By induction on the complexity of ϕ and using Theorem 19.4. □

Lemma 20.2. *Let* $\langle . \rangle$ *and* $(.)_x$ *be a primitive recursive coding and decoding functions, then for every formula* $Qx_1, ..., x_n\phi(\vec{x},\vec{y}) \in \mathcal{L}$ *where* $Q \in \{\forall, \exists\}$ *and* $n > 0$*,*

$$\mathsf{HA} \vdash_i Qx_1, ..., x_n\phi(\vec{x},\vec{y}) \leftrightarrow Qx\phi((x)_0, ..., (x)_n, \vec{y}).$$

Proof. Straightforward by properties of the coding and decoding functions. □

We use the notation $\phi([x],\vec{y})$ instead of $\phi((x)_0, ..., (x)_n, \vec{y})$ for simplicity.

Theorem 20.3. *For every* Π_2 *sentence* $\phi := \forall\vec{x}\exists\vec{y}\psi(\vec{x},\vec{y})$*, if* $\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \phi$*, then* $\mathsf{PA} \vdash_c \phi$*.*

Proof. Let ϕ be a Π_2 sentence and $\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \phi$. By Lemmas 20.2 and 20.1 there exists an atomic formula $p(x,y)$ such that $\mathsf{HA} \vdash_i \phi \leftrightarrow \forall x\exists yp(x,y)$ and therefore $\mathsf{HA}+\mathsf{ECT}_0 \vdash_i \forall x\exists yp(x,y)$. By Theorem 19.2 $\mathsf{HA} \vdash_i \exists n(n\,\mathbf{r}\,\forall x\exists yp(x,y))$. Because $\exists n(n\ \mathbf{r}\ \forall x\exists yp(x,y))$ is a sentence, by Theorem 19.3 there exists a natural number n such that $\mathsf{HA} \vdash_i \bar{n}\ \mathbf{r}\ \forall x\exists yp(x,y)$. Therefore by definition of the realizability:

1. $\Rightarrow \mathsf{HA} \vdash_i \forall x\exists u(T(\bar{n},x,u) \wedge U(u)\ \mathbf{r}\ \exists yp(x,y))$,

2. $\Rightarrow \mathsf{HA} \vdash_i \forall x\exists u(T(\bar{n},x,u) \wedge j_2(U(u))\ \mathbf{r}\ p(x, j_1(U(u))))$,

3. $\Rightarrow \mathsf{HA} \vdash_i \forall x\exists u(T(\bar{n},x,u) \wedge p(x, j_1(U(u))))$,

4. $\Rightarrow \mathsf{HA} \vdash_i \forall x \exists u p(x,u)$,

hence $\mathsf{PA} \vdash_c \phi$. □

In the rest of the paper, for every $\mathcal{L}$ structure $\mathcal{M}$,

$$\mathbf{T}_{\mathcal{M}} := \mathsf{HA} + \mathsf{ECT}_0 + \mathsf{Diag}(\mathcal{M}).$$

Theorem 20.4. *If $\mathcal{M} \models \mathbf{Th}_{\Pi_1}(\mathsf{PA})$, then $\mathbf{T}_{\mathcal{M}}$ is consistent.*

Proof. Suppose $\mathbf{T}_{\mathcal{M}}$ is inconsistent, so there exists a finite number of $\mathcal{L}(\mathcal{M})$ sentences $\{\phi_i(\vec{\underline{c_i}})\}_{i\leq n} \subseteq \mathsf{Diag}(\mathcal{M})$ such that $\mathsf{HA}+\mathsf{ECT}_0+\bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}}) \vdash_i \bot$, therefore $\mathsf{HA}+\mathsf{ECT}_0 \vdash_i \neg \bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}})$. Because $\vec{\underline{c_i}}$ are not used in the axioms of $\mathsf{HA}+\mathsf{ECT}_0$, we have $\mathsf{HA}+\mathsf{ECT}_0 \vdash_i \forall \vec{x_1}, ..., \vec{x_n}(\neg \bigwedge_{i=1}^n \phi_i(\vec{x_i}))$. Note that $\forall \vec{x_1}, ..., \vec{x_n}(\neg \bigwedge_{i=1}^n \phi_i(\vec{x_i}))$ is a Π_1 sentence and therefore by Theorem 20.3, $\mathsf{PA} \vdash_c \forall \vec{x_1}, ..., \vec{x_n}(\neg \bigwedge_{i=1}^n \phi_i(\vec{x_i}))$. This implies that $\mathcal{M} \models \forall \vec{x_1}, ..., \vec{x_n}(\neg \bigwedge_{i=1}^n \phi_i(\vec{x_i}))$ and especially $\mathcal{M} \models \neg \bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}})$, but by definition of $\mathsf{Diag}(\mathcal{M})$ we know $\mathcal{M} \models \bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}})$ and this leads to a contradiction, hence $\mathbf{T}_{\mathcal{M}}$ is consistent. □

If an $\mathcal{L}$ structure $\mathcal{M}$ satisfies a strong enough theory of arithmetic, then $\mathbf{T}_{\mathcal{M}}$ has actually the existence and the disjunction properties.

Theorem 20.5. *(Existence and disjunction properties). Suppose $\mathcal{M}$ is a model of $\mathbf{Th}_{\Pi_2}(\mathsf{PA})$, then the following statements are true:*

1. *For every $\mathcal{L}(\mathcal{M})$ sentence $\exists z \phi(z)$ such that $\mathbf{T}_{\mathcal{M}} \vdash_i \exists z \phi(z)$, there exists a constant symbol $\underline{c} \in \mathcal{L}(\mathcal{M})$ such that $\mathbf{T}_{\mathcal{M}} \vdash_i \phi(\underline{c})$.*

2. *For every $\mathcal{L}(\mathcal{M})$ sentence $\phi \vee \psi$ such that $\mathbf{T}_{\mathcal{M}} \vdash_i \phi \vee \psi$, $\mathbf{T}_{\mathcal{M}} \vdash_i \phi$ or $\mathbf{T}_{\mathcal{M}} \vdash_i \psi$.*

Proof. 1. Suppose $\phi(z)$ is $\psi(z, \vec{\underline{d}})$ such that $\psi(z, \vec{y})$ is an $\mathcal{L}$ formula. By assumption of the theorem there exists a finite number of $\mathcal{L}(\mathcal{M})$ sentences $\{\phi_i(\vec{\underline{c_i}})\}_{i\leq n} \subseteq \mathsf{Diag}(\mathcal{M})$ such that

$$\mathsf{HA} + \mathsf{ECT}_0 + \bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}}) \vdash_i \exists z \psi(z, \vec{\underline{d}}),$$

so $\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}}) \rightarrow \exists z \psi(z, \vec{\underline{d}})$. Because $\mathcal{L}(\mathcal{M})$ constants that appear in $\bigwedge_{i=1}^n \phi_i(\vec{\underline{c_i}}) \rightarrow \exists z \psi(z, \vec{\underline{d}})$ are not used in the axioms of $\mathsf{HA}+\mathsf{ECT}_0$, therefore

$$\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \forall \vec{y}, \vec{x_1}, ..., \vec{x_n}(\bigwedge_{i=1}^n \phi_i(\vec{x_i}, \vec{y}) \rightarrow \exists z \psi(z, \vec{y})).$$

Note that $\bigwedge_{i=1}^n \phi_i(\vec{x_i}, \vec{y})$ is a quantifier free formula, hence by Lemma 20.1 there exists an atomic formula p such that

$$\mathsf{HA} \vdash_i p(\vec{x}_1, ..., x_n, \vec{y}) \leftrightarrow \bigwedge_{i=1}^n \phi_i(\vec{x_i}, \vec{y}).$$

Also note that by Theorem 19.4 $\mathsf{HA} \vdash_i p \vee \neg p$, hence

$$\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \forall \vec{y}, \vec{x}_1, ..., \vec{x}_n \exists z (p(\vec{x}_1, ..., \vec{x}_n, \vec{y}) \rightarrow \psi(z, \vec{y})).$$

By Lemma 20.2 $\mathsf{HA} + \mathsf{ECT}_0 \vdash_i \forall x \exists z(p([x]) \to \psi(z, [x]))$. Note that

$$\forall x \exists z(p([x]) \to \psi(z, [x]))$$

is an $\mathcal{L}$ sentence and therefore by Theorems 19.2 and 19.3 there exists a natural number n such that

$$\mathsf{HA} \vdash_i \bar{n} \; \mathbf{r} \; \forall x \exists z(p([x]) \to \psi(z, [x])).$$

By definition of realizability we get

$$\mathsf{HA} \vdash_i \forall x \exists u(T(\bar{n}, x, u) \wedge U(u) \; \mathbf{r} \; \exists z(p([x]) \to \psi(z, [x]))).$$

Note that $\mathsf{HA} \vdash_i \forall x \exists u T(\bar{n}, x, u)$, hence $\mathsf{PA} \vdash_c \forall x \exists u T(\bar{n}, x, u)$ and therefore $\mathcal{M} \models \forall x \exists u T(\bar{n}, x, u)$. Let $\mathcal{M} \models \underline{e} = \left\langle \vec{\underline{c_1}}, ..., \vec{\underline{c_n}}, \vec{\underline{d}} \right\rangle$ and $\mathcal{M} \models T(\bar{n}, \underline{e}, \underline{f}) \wedge U(\underline{f}) = \underline{g}$ for some $e, f, g \in \mathcal{M}$. This implies $T(\bar{n}, \underline{e}, \underline{f}), U(\underline{f}) = \underline{g} \in \mathsf{Diag}(\mathcal{M})$ and therefore we get

$$\mathbf{T}_{\mathcal{M}} \vdash_i T(\bar{n}, \underline{e}, \underline{f}) \wedge \underline{g} \; \mathbf{r} \; \exists z(p([\underline{e}]) \to \psi(z, [\underline{e}]))$$

as

$$\mathsf{HA} \vdash_i \forall x, y, z, z'(T(x, y, z) \wedge T(x, y, z') \to U(z) = U(z')).$$

By applying the realizability definition we get $\mathbf{T}_{\mathcal{M}} \vdash_i j_2(\underline{g}) \; \mathbf{r} \; (p([\underline{e}]) \to \psi(j_1(\underline{g}), [\underline{e}]))$. Note that by Theorem 19.2,

$$\mathsf{HA} + \mathsf{ECT}_0 \vdash_i v \; \mathbf{r} \; (p[x] \to \psi(w, [x])) \to (p([x]) \to \psi(w, [x])),$$

so

$$\mathbf{T}_{\mathcal{M}} \vdash_i p([\underline{e}]) \to \psi(j_1(\underline{g}), [\underline{e}]).$$

Because $p([\underline{e}]) \in \mathsf{Diag}(\mathcal{M})$, we get $\mathbf{T}_{\mathcal{M}} \vdash_i \psi(j_1(\underline{g}), [\underline{e}])$ and this implies $\mathbf{T}_{\mathcal{M}} \vdash_i \psi(\underline{c}, [\underline{e}])$ for some $\underline{c} \in \mathcal{L}(\mathcal{M})$ such that $\mathcal{M} \models j_1(\underline{g}) = \underline{c}$.

2. Suppose $\mathbf{T}_{\mathcal{M}}$ proves $\phi \vee \psi$, therefore $\mathbf{T}_{\mathcal{M}} \vdash_i \exists x((x = 0 \to \phi) \wedge (x \neq 0 \to \psi))$. By the previous part there exists a constant symbol $\underline{c} \in \mathcal{L}(\mathcal{M})$ such that $\mathbf{T}_{\mathcal{M}} \vdash_i (\underline{c} = 0 \to \phi) \wedge (\underline{c} \neq 0 \to \psi)$. Note that $\underline{c} = 0$ is an atomic formula, hence $\underline{c} = 0 \in \mathsf{Diag}(\mathcal{M})$ or $\underline{c} \neq 0 \in \mathsf{Diag}(\mathcal{M})$ and this implies $\mathbf{T}_{\mathcal{M}} \vdash_i \phi$ or $\mathbf{T}_{\mathcal{M}} \vdash_i \psi$.

□

Definition 20.1. *Let $\mathcal{M}$ be an $\mathcal{L}$ structure and T be an intuitionistic theory in the language $\mathcal{L}(\mathcal{M})$. Then for every $\mathcal{L}(\mathcal{M})$ sentence ϕ such that $T \nvdash_i \phi$, fix a Kripke model $\mathbf{K}_T(\phi) \Vdash T$ such that $\mathbf{K}_T(\phi) \nVdash \phi$.*

The following definition is based on Smoryński collection operation in [Smo73].

Definition 20.2. *Let $\mathcal{M}$ be an $\mathcal{L}$ structure and T be an intuitionistic theory in the language $\mathcal{L}(\mathcal{M})$. Define*

$$\mathcal{S}(\mathcal{M}, T) := \{\phi \in \mathcal{L}(\mathcal{M}) | T \nvdash_i \phi, \phi \textit{ is a sentence}\}.$$

Define the universal model $\mathbf{K}(\mathcal{M}, T)$ as follows. Take the disjoint union

$$\{\mathbf{K}_T(\phi)\}_{\phi \in \mathcal{S}(\mathcal{M}, T)}$$

and then add a new root r with domain $\mathcal{M}_r = \mathcal{M}$.

Theorem 20.6. *If $\mathcal{M}$ is a model of $\mathbf{Th}_{\Pi_2}(\mathsf{PA})$, then $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$ is a well-defined Kripke model and for every $\mathcal{L}(\mathcal{M})$ sentence ϕ,*

$$\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \phi \Leftrightarrow \mathbf{T}_{\mathcal{M}} \vdash_i \phi.$$

Proof. First note that by Theorem 20.4 $\mathbf{T}_{\mathcal{M}} \nvdash \bot$, hence $\mathcal{S}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$ is not empty and therefore $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$ has other nodes except r. To make sure that $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$ is well-defined, we should check the three conditions in the definition of Kripke models. It is easy to see that the first two conditions hold for $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$. For the third condition, we need to show that for every node $k \neq r$, $\mathcal{L}(\mathcal{M}_r) \subseteq \mathcal{L}(\mathcal{M}_k)$ and $\mathcal{M}_k \models \mathsf{Diag}^+(\mathcal{M}_r)$. By definition of $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$, $\mathcal{L}(\mathcal{M}_r) \subseteq \mathcal{L}(\mathcal{M}_k)$ holds. For the condition $\mathcal{M}_k \models \mathsf{Diag}^+(\mathcal{M}_\mathsf{r})$, note that $\mathbf{T}_{\mathcal{M}} \vdash_i \mathsf{Diag}(\mathcal{M})$ which implies $\mathcal{M}_k \models \mathsf{Diag}(\mathcal{M}_\mathsf{r})$.

($\Rightarrow$). Let $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \phi$. If $\mathbf{T}_{\mathcal{M}} \nvdash_i \phi$, then $\mathbf{K}_{\mathbf{T}_{\mathcal{M}}}(\phi)$ exists and $\mathbf{K}_{\mathbf{T}_{\mathcal{M}}}(\phi) \subseteq \mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$. By the assumption we get $\mathbf{K}_{\mathbf{T}_{\mathcal{M}}}(\phi) \Vdash \phi$, but this leads to a contradiction by definition of $\mathbf{K}_{\mathbf{T}_{\mathcal{M}}}(\phi)$, hence $\mathbf{T}_{\mathcal{M}} \vdash_i \phi$.

($\Leftarrow$). We prove this part by induction on the complexity of ϕ:

1. $\phi = p$: Note that if $\mathbf{T}_{\mathcal{M}} \vdash_i p$, then $p \in \mathsf{Diag}(\mathcal{M})$. Because if $p \notin \mathsf{Diag}(\mathcal{M})$, then $\neg p \in \mathsf{Diag}(\mathcal{M})$, hence $\mathbf{T}_{\mathcal{M}} \vdash_i \bot$ which leads to a contradiction by Theorem 20.4. Therefore $p \in \mathsf{Diag}(\mathcal{M})$ and by the fact that $\mathcal{M} \models p$ we get $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash p$.
2. $\phi = \psi \wedge \eta$: By the assumption we get $\mathbf{T}_{\mathcal{M}} \vdash_i \psi$ and $\mathbf{T}_{\mathcal{M}} \vdash_i \eta$, therefore by the induction hypothesis $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi$ and $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \eta$, hence $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi \wedge \eta$.
3. $\phi = \psi \vee \eta$: By Theorem 20.5 $\mathbf{T}_{\mathcal{M}} \vdash_i \psi$ or $\mathbf{T}_{\mathcal{M}} \vdash_i \eta$, therefore by the induction hypothesis $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi$ or $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \eta$, hence $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi \vee \eta$.
4. $\phi = \psi \to \eta$: By the assumption for every $\theta \in \mathcal{S}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$, $\mathbf{K}_{\mathbf{T}_{\mathcal{M}}}(\theta) \Vdash \psi \to \eta$, so for proving $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi \to \eta$ we only need to show that if $r \Vdash \psi$, then $r \Vdash \eta$. Let $r \Vdash \psi$, therefore we have $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi$, hence by the previous part, $\mathbf{T}_{\mathcal{M}} \vdash_i \psi$. Note that By the assumption $\mathbf{T}_{\mathcal{M}} \vdash_i \psi \to \eta$, hence $\mathbf{T}_{\mathcal{M}} \vdash_i \eta$ and therefore by the induction hypothesis $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \eta$ which implies $r \Vdash \eta$.
5. $\phi = \exists x \psi(x)$: By Theorem 20.5 there exists a constant symbol $\underline{c} \in \mathcal{L}(\mathcal{M})$ such that $\mathbf{T}_{\mathcal{M}} \vdash_i \psi(\underline{c})$, therefore by the induction hypothesis $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi(\underline{c})$, hence $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \exists x \psi(x)$.
6. $\phi = \forall x \psi(x)$: By the assumption for every $\theta \in \mathcal{S}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$, $\mathbf{K}_{\mathbf{T}_{\mathcal{M}}}(\theta) \Vdash \forall x \psi(x)$, so for proving $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \forall x \psi(x)$ we only need to show that for every $c \in \mathcal{M}$, $r \Vdash \psi(\underline{c})$. Let $c \in \mathcal{M}$. By the assumption $\mathbf{T}_{\mathcal{M}} \vdash_i \forall x \psi(x)$, therefore $\mathbf{T}_{\mathcal{M}} \vdash_i \psi(\underline{c})$, hence by the induction hypothesis $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \psi(\underline{c})$. This implies that $r \Vdash \psi(\underline{c})$.

□

From the last theorem, we can get the characterization of the structure of the roots of Kripke models of $\mathsf{HA} + \mathsf{ECT}_0$.

Corollary 20.7. *For every $\mathcal{L}$ structure $\mathcal{M}$, there exists a rooted Kripke model* $\mathbf{K} \Vdash \mathsf{HA} + \mathsf{ECT}_0$ *with the root r such that $\mathcal{M}_r = \mathcal{M}$ iff $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$.*

Proof. The left to the right direction is true by Lemma 19.5. To prove the other direction, note that if $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$, then by Theorem 20.6 $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$ and moreover the classical structure attached to the root is $\mathcal{M}$. □

Now we have the right tool for constructing a counter example for Problem 11. In general we can get a lot of new models for every $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$. For our purpose, it is sufficient to know that $\mathbf{Th}_{\Pi_2}(\mathsf{PA}) \nvdash_c \mathsf{PA}$ to get the result. The next two theorems established the stronger fact which says $\mathbf{Th}_{\Pi_2}(\mathsf{PA}) \nvdash_c \mathbf{I}\Delta_1$. $\mathbf{I}\Delta_1$ is PRA plus Δ_1 induction:

$$\forall \vec{y}\, [\forall x(\phi(x, \vec{y}) \leftrightarrow \neg\psi(x, \vec{y})) \to \mathbf{I}_\phi]$$

for every Σ_1 formulas $\phi, \psi \in \mathcal{L}$.

For stating the theorems we also need another arithmetical theory that is called $\mathbf{B}\Sigma_1$. $\mathbf{B}\Sigma_1$ is PRA plus bounded Σ_1 collection:

$$\forall \vec{y}, x\, [\forall z(z < x \to \exists w \phi(z, w, \vec{y})) \to \exists r \forall z(z < x \to \exists w(w < r \wedge \phi(z, w, \vec{y}))]$$

for every Σ_1 formula $\phi \in \mathcal{L}$.

It is worth mentioning that these theories usually are defined over the language of Peano Arithmetic, and not over the language of Primitive Recursive Arithmetic, hence our definitions of $\mathbf{I}\Delta_1$ and $\mathbf{B}\Sigma_1$ are stronger than the usual definition, but for our use this does not cause a problem. Now we know the definitions, we state the theorems.

Theorem 20.8. $\mathbf{I}\Delta_1 \,{}_c\!\dashv\vdash_c \mathbf{B}\Sigma_1$.

Proof. As we explained before, this version of these theories are stronger that the original ones. Therefore by the result of [Sla04] these two theories are the same. □

Theorem 20.9. *There exists a model $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathbb{N})$ such that $\mathcal{M} \not\models \mathbf{I}\Delta_1$.*

Proof. By the result of [Par70] there exists a model $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathbb{N})$ such that $\mathcal{M} \not\models \mathbf{B}\Sigma_1$, hence by Theorem 20.8 $\mathcal{M} \not\models \mathbf{I}\Delta_1$ too. □

Corollary 20.10. *There exists a rooted Kripke model of* $\mathsf{HA} + \mathsf{ECT}_0$ *which is not locally* $\mathbf{I}\Delta_1$.

Proof. By Theorem 20.9 there exists a model $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathbb{N})$ such that $\mathcal{M} \not\models \mathbf{I}\Delta_1$. Note that by Theorem 20.6, $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$, and also $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}})$ is not locally $\mathbf{I}\Delta_1$. □

ECT_0 is a very powerful non-classical axiom schema, so a natural question is that: *Is it the case that for every Kripke model* $\mathbf{K} \Vdash \mathsf{HA} + \mathsf{ECT}_0$ *and every node k in* $\mathbf{K}$, $\mathcal{M}_k \not\models \mathsf{PA}$ *?* This question has a negative answer, because $\mathbf{K}(\mathbb{N}, \mathbf{T}_{\mathbb{N}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$, but $\mathcal{M}_r \models \mathsf{PA}$.

20.2 The second model construction

In this subsection, we will explain the generalized construction which works for any reasonable intuitionistic arithmetical theory. We will also mention an application of it at the end of this subsection.

For every $T \in \mathcal{I}$, the existence property of T is the following Π_2 sentence:

$$EP_T := \forall x(x = \ulcorner \exists y \phi(y) \urcorner \text{ for some formula } \phi(y) \wedge x \text{ is a sentence} \wedge$$

$$Pr_T(x) \to \exists y Pr_T(\ulcorner \phi(\dot{y}) \urcorner)).$$

For an $\mathcal{L}$ structure $\mathcal{M}$ and a theory $T \in \mathcal{I}$, let extension of T with respect to $\mathcal{M}$ be the following theory:

$$\mathsf{EXT}(\mathcal{M}, T) := \{\phi \in \mathcal{L}(\mathcal{M}) | \phi \text{ is a sentence}, \mathcal{M} \models Pr_T(\ulcorner \phi \urcorner)\}.$$

The following lemma states that $\mathsf{EXT}(\mathcal{M}, T)$ is closed under finite conjunctions.

Lemma 20.11. *Let $\mathcal{M} \models \mathsf{PRA}$ and $T \in \mathcal{I}$. Then for every $\mathcal{L}(\mathcal{M})$ sentences ϕ and ψ, if $\phi, \psi \in \mathsf{EXT}(\mathcal{M}, T)$, then $\phi \wedge \psi \in \mathsf{EXT}(\mathcal{M}, T)$.*

Proof. If $\phi, \psi \in \mathsf{EXT}(\mathcal{M}, T)$, then $\mathcal{M} \models Pr_T(\ulcorner \phi \urcorner) \wedge Pr_T(\ulcorner \psi \urcorner)$, so by Theorem 19.1 (item 3) $\mathcal{M} \models Pr_T(\ulcorner \phi \wedge \psi \urcorner)$. Hence $\phi \wedge \psi \in \mathsf{EXT}(\mathcal{M}, T)$. □

Define

$$\mathbf{C}_{\mathcal{M},T} := T + \mathsf{EXT}(\mathcal{M}, T).$$

The crucial property of $\mathbf{C}_{\mathcal{M},T}$ is the following lemma.

Lemma 20.12. *Suppose $\mathcal{M} \models \mathsf{PRA}$. Then for every $T \in \mathcal{I}$ and every $\mathcal{L}(\mathcal{M})$ sentence ψ, if $\mathbf{C}_{\mathcal{M},T} \vdash_i \psi$, then $\mathcal{M} \models Pr_T(\ulcorner \psi \urcorner)$.*

Proof. Let $\psi(\underline{d_1}, ..., \underline{d_n})$ be an $\mathcal{L}(\mathcal{M})$ sentence such that $\mathbf{C}_{\mathcal{M},T} \vdash_i \psi(\underline{d_1}, ..., \underline{d_n})$. So there exists a finite number of $\mathcal{L}(\mathcal{M})$ sentence $\{\phi_i(\underline{c^i_1}, ..., \underline{c^i_{n_i}})\}_{i \leq n'} \subseteq \mathsf{EXT}(\mathcal{M}, T)$ such that

$$T \vdash_i \bigwedge_{i=1}^{n} \phi_i(\underline{c^i_1}, ..., \underline{c^i_{n_i}}) \to \psi(\underline{d_1}, ..., \underline{d_n}).$$

Because $\mathcal{L}(\mathcal{M})$ constants that appear in $\bigwedge_{i=1}^{n} \phi_i(\underline{c^i_1}, ..., \underline{c^i_{n_i}}) \to \psi(\underline{d_1}, ..., \underline{d_n})$ are not used in the axioms of T, therefore

$$T \vdash_i \forall \vec{y}, \vec{x}_1, ..., \vec{x}_n (\bigwedge_{i=1}^{n} \phi_i(\vec{x}_i, \vec{y}) \to \psi(\vec{y})).$$

So by Theorem 19.1 (item 1)

$$\mathcal{M} \models Pr_T(\ulcorner \forall \vec{y}, \vec{x}_1, ..., \vec{x}_n (\bigwedge_{i=1}^{n} \phi_i(\vec{x}_i, \vec{y}) \to \psi(\vec{y})) \urcorner).$$

Hence by Theorem 19.1 (item 4)

$$\mathcal{M} \models Pr_T(\ulcorner \bigwedge_{i=1}^{n} \phi_i(\dot{\underline{c^i_1}}, ..., \dot{\underline{c^i_{n_i}}}) \to \psi(\dot{\underline{d_1}}, ..., \dot{\underline{d_n}}) \urcorner).$$

On the other hand by Lemma 20.12 $\mathsf{EXT}(\mathcal{M}, T)$ is closed under finite conjunctions, so $\bigwedge_{i=1}^{n} \phi_i(\underline{c_1^i}, ..., \underline{c_{n_i}^i}) \in \mathsf{EXT}(\mathcal{M}, T)$ which means

$$\mathcal{M} \models Pr_T(\ulcorner \bigwedge_{i=1}^{n} \phi_i(\underline{\dot{c}_1^i}, ..., \underline{\dot{c}_{n_i}^i}) \urcorner).$$

So by Theorem 19.1 (item 2) $\mathcal{M} \models Pr_T(\ulcorner \psi(\underline{\dot{d}_1}, ..., \underline{\dot{d}_n}) \urcorner)$. □

Theorem 20.13. *For every $T \in \mathcal{I}$ and every $\mathcal{M} \models \mathsf{PRA} + EP_T + Con_T$, the following statements are true:*

1. *$\mathbf{C}_{\mathcal{M},T}$ is consistent.*

2. *$\mathbf{C}_{\mathcal{M},T}$ has the existence and the disjunction properties.*

Proof.

1. Suppose $\mathbf{C}_{\mathcal{M},T} \vdash_i \bot$. Then by Lemma 20.12 $\mathcal{M} \models Pr_T(\ulcorner \bot \urcorner)$, but this is not possible because we assumed $\mathcal{M} \models Con_T$, hence $\mathbf{C}_{\mathcal{M},T}$ is consistent.

2. We will prove the existence property of $\mathbf{C}_{\mathcal{M},T}$. The disjunction property will follow from it by the same argument as in the proof of Theorem 20.5. Let $\psi(x)$ be a formula in $\mathcal{L}(\mathcal{M})$ with x as the only free variable. Suppose $\mathbf{C}_{\mathcal{M},T} \vdash_i \exists x \psi(x)$. Then by Lemma 20.12 $\mathcal{M} \models Pr_T(\ulcorner \exists x \psi(x) \urcorner)$. Note that $\mathcal{M} \models EP_T$, hence $\mathcal{M} \models \exists x Pr_T(\ulcorner \psi(\dot{x}) \urcorner)$. This means there exists a $c \in \mathcal{M}$ such that $\mathcal{M} \models Pr_T(\ulcorner \psi(\underline{\dot{c}}) \urcorner)$. This implies $\psi(\underline{c}) \in \mathsf{EXT}(\mathcal{M}, T)$, so $\mathbf{C}_{\mathcal{M},T} \vdash_i \psi(\underline{c})$.

□

This is the generalized version of Theorem 20.6 which gives us a sufficient condition.

Theorem 20.14. *Let $T \in \mathcal{I}$ and $\mathcal{M} \models \mathsf{PRA} + EP_T + Con_T$. Then $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},T})$ is a well-defined Kripke model and for every $\mathcal{L}(\mathcal{M})$ sentence ϕ,*

$$\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},T}) \Vdash \phi \Leftrightarrow \mathbf{C}_{\mathcal{M},T} \vdash_i \phi.$$

Proof. The proof of this theorem is essentially the same as the proof of Theorem 20.6 by using the Theorem 20.13. The only part that needs some extra work is the fact that $\mathbf{C}_{\mathcal{M},T} \vdash_i \mathsf{Diag}(\mathcal{M})$ and moreover if $\mathbf{C}_{\mathcal{M},T} \vdash_i p$ for atomic p, then $p \in \mathsf{Diag}(\mathcal{M})$.

Let $p \in \mathsf{Diag}(\mathcal{M})$. We know by Theorem 19.1 (item 5) $\mathcal{M} \models p \to Pr_T(\ulcorner p \urcorner)$. This implies $\mathcal{M} \models Pr_T(\ulcorner p \urcorner)$. So $p \in \mathsf{EXT}(\mathcal{M}, T)$ which implies $\mathbf{C}_{\mathcal{M},T} \vdash_i p$.

Now if we have $\mathbf{C}_{\mathcal{M},T} \vdash_i p$ for an atomic $\mathcal{L}(\mathcal{M})$ sentence p, then by Lemma 20.12 $\mathcal{M} \models Pr_T(\ulcorner p \urcorner)$. Note that $\mathcal{M} \models Con_T$, so by Theorem 19.1 (item 6) $\mathcal{M} \models p$ which means $p \in \mathsf{Diag}(\mathcal{M})$. □

As we already saw, using the first construction, we provide a Kripke model of $\mathsf{HA} + \mathsf{ECT}_0$ which is not locally $\mathbf{I}\Delta_1$. A natural conjecture would be that the existence of such a Kripke model was possible because the base theory has a very powerful non-classical schema ECT_0. As an application of Theorem 20.14

we will show this is not the case. Let $\mathsf{H}(x)$ be a Σ_1 formula that is a natural formalization of the statement ”The Turing machine with code x halts on input x”. Let θ be an instance of $\mathsf{ECT_0}$ in Definition 19.5 such that $\phi(x) := \top$ and $\psi(x, y) := (y = 0 \wedge \mathsf{H}(x)) \vee (y \neq 0 \wedge \neg\mathsf{H}(x))$. We also need the definition of Markov's principle.

Definition 20.3. *Markov's principle is the following schema:*

$$\mathsf{MP} := \forall \vec{y}(\forall x(\phi(x, \vec{y}) \vee \neg\phi(x, \vec{y})) \wedge \neg\neg\exists x\phi(x, \vec{y}) \to \exists x\phi(x, \vec{y})).$$

Lemma 20.15. *The following statements are true:*

1. $\mathsf{HA} + \neg\theta + \mathsf{MP}$ *is consistent.*
2. $\mathsf{HA} + \neg\theta + \mathsf{MP}$ *has the existence and disjunction properties.*

Proof.

1. It is easy to see that $\mathsf{PA} \vdash_c \neg\theta$ and also $\mathsf{PA} \vdash_c \mathsf{MP}$. So $\mathsf{HA} + \neg\theta + \mathsf{MP}$ is a sub-theory of PA and it is consistent.
2. We will prove the existence property of $\mathsf{HA} + \neg\theta + \mathsf{MP}$ here. The disjunction property will follow from it like before. This part is a standard application of Kripke models (see [Smo73]). Let $\exists x\psi(x)$ be an $\mathcal{L}$ sentence such that $\mathsf{HA} + \neg\theta + \mathsf{MP} \vdash_i \exists x\psi(x)$, but for every natural number n, $\mathsf{HA} + \neg\theta + \mathsf{MP} \nvdash_i \psi(\bar{n})$. It is well-know that $\mathbf{K}(\mathbb{N}, \mathsf{HA} + \neg\theta + \mathsf{MP})$ is a well-defined Kripke model and moreover $\mathbf{K}(\mathbb{N}, \mathsf{HA}{+}\neg\theta{+}\mathsf{MP}) \Vdash \mathsf{HA}$ (see Theorem 5.2.4 in [Smo73]). Moreover we can assume that $\mathbf{K}_{\mathsf{HA}+\neg\theta+\mathsf{MP}}(\bot)$ (Note that $\bot \in \mathcal{S}(\mathbb{N}, \mathsf{HA}{+}\neg\theta{+}\mathsf{MP})$) is a Kripke model with just one node with the classical structure $\mathbb{N}$. Note that $r \nVdash \theta$, because otherwise by the monotonicity of the forcing relation for every $\phi \in \mathcal{S}(\mathbb{N}, \mathsf{HA}{+}\neg\theta{+}\mathsf{MP})$, $\mathbf{K}_{\mathsf{HA}+\neg\theta+\mathsf{MP}}(\phi) \Vdash \theta$ which is not true. Moreover for every node $k \neq r$, $k \Vdash \neg\theta$, so with the last argument $r \Vdash \neg\theta$ which implies $\mathbf{K}(\mathbb{N}, \mathsf{HA}{+}\neg\theta{+}\mathsf{MP}) \Vdash \neg\theta$. Note that MP is forced in every node $k \neq r$. So we only need to show that $r \Vdash \mathsf{MP}$. For this matter suppose $r \Vdash \forall x(\phi(x, \bar{a_1}, ...\bar{a_n}) \vee \neg\phi(x, \bar{a_1}, ...\bar{a_n})) \wedge \neg\neg\exists x\phi(x, \bar{a_1}, ...\bar{a_n})$ where $\vec{a} \in \mathbb{N}$. If for every $n \in \mathbb{N}$, $r \nVdash \phi(\bar{n}, \bar{a_1}, ...\bar{a_n})$, then because $r \Vdash \phi(\bar{n}, \bar{a_1}, ...\bar{a_n}) \vee \neg\phi(\bar{n}, \bar{a_1}, ...\bar{a_n})$, for every $n \in \mathbb{N}$, $r \Vdash \neg\phi(\bar{n}, \bar{a_1}, ...\bar{a_n})$. This implies $\mathbf{K}_{\mathsf{HA}+\neg\theta+\mathsf{MP}}(\bot) \Vdash \forall x\neg\phi(x, \bar{a_1}, ...\bar{a_n})$. But this leads to a contradiction because $\mathbf{K}_{\mathsf{HA}+\neg\theta+\mathsf{MP}}(\bot) \Vdash \neg\neg\exists x\neg\phi(x, \bar{a_1}, ...\bar{a_n})$. This means that there exists a natural number n such that $r \Vdash \phi(\bar{n}, \bar{a_1}, ...\bar{a_n})$.

   By the above arguments, we have

   $$\mathbf{K}(\mathbb{N}, \mathsf{HA} + \neg\theta + \mathsf{MP}) \Vdash \mathsf{HA} + \neg\theta + \mathsf{MP}.$$

   So $\mathbf{K}(\mathbb{N}, \mathsf{HA} + \neg\theta + \mathsf{MP}) \Vdash \exists x\psi(x)$. This implies that there exists a natural number n such that $r \Vdash \psi(\bar{n})$. But this leads to a contradiction because we know $\mathbf{K}_{\mathsf{HA}+\neg\theta+\mathsf{MP}}(\psi(\bar{n})) \nVdash \psi(\bar{n})$. This implies that our assumption was false and there exists a natural number n such that $\mathsf{HA} + \neg\theta + \mathsf{MP} \vdash_i \psi(\bar{n})$.

□

The following corollary is the first application of Theorem 20.14.

Corollary 20.16. *There exists a rooted Kripke model of* $\mathsf{HA} + \neg\theta + \mathsf{MP}$ *which is not locally* $\mathbf{I}\Delta_1$.

Proof. By Theorem 20.9 there exists a model $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathbb{N})$ such that $\mathcal{M} \not\models \mathbf{I}\Delta_1$. Note that by Lemma 20.15 $\mathsf{HA} + \neg\theta + \mathsf{MP}$ is consistent and has the existence property. This implies that $EP_{\mathsf{HA}+\neg\theta+\mathsf{MP}}$ and $Con_{\mathsf{HA}+\neg\theta+\mathsf{MP}}$ are true in $\mathbb{N}$. Note that these sentences are Π_2, so they are also true in $\mathcal{M}$. This implies that $\mathcal{M}$ satisfies the conditions which are needed in Theorem 20.14, hence

$$\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}+\neg\theta+\mathsf{MP}}) \Vdash \mathsf{HA} + \neg\theta + \mathsf{MP}$$

and also it is not locally $\mathbf{I}\Delta_1$. □

It is worth mentioning that $\mathsf{HA} + \neg\theta + \mathsf{MP}$ does not prove anything contradictory with PA and in some sense, it is close to PA, but still, we were able to construct a Kripke model of it which is not locally $\mathbf{I}\Delta_1$. The following corollary is the second application of Theorem 20.14.

Corollary 20.17. *There exists a rooted Kripke model* $\mathbf{K} \Vdash \mathsf{HA}$ *which is not locally* $\mathbf{I}\Delta_1$*, but for every* $\mathcal{L}$ *sentence* ϕ*,*

$$\mathbf{K} \Vdash \phi \Leftrightarrow \mathsf{HA} \vdash_i \phi.$$

Proof. Define

$$\mathcal{U} = \{\neg Pr_{\mathsf{HA}}(\ulcorner \phi \urcorner) \mid \mathsf{HA} \nvdash_i \phi, \phi \text{ is a sentence}\}.$$

Let $T := \mathsf{PRA} + EP_{\mathsf{HA}} + \mathcal{U}$. It is easy to see that T is a Π_2 axiomatized theory and moreover $\mathbb{N} \models T$. By Theorem 20.9 there exists a model $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathbb{N})$ such that $\mathcal{M} \not\models \mathbf{I}\Delta_1$. By the facts that $\mathbb{N} \models T$ and also T is a Π_2 axiomatized theory, we get $\mathcal{M} \models T$. So by these explanations, $\mathcal{M}$ has the required properties that are needed in Theorem 20.14, hence $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}}) \Vdash \mathsf{HA}$. This means that for every $\mathcal{L}$ sentence ϕ, if $\mathsf{HA} \vdash_i \phi$, then $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}}) \Vdash \phi$.

For the opposite direction, let ϕ be an $\mathcal{L}$ sentence such that $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}}) \Vdash \phi$. Then by Theorem 20.14 $\mathbf{C}_{\mathcal{M},\mathsf{HA}} \vdash_i \phi$. So by Lemma 20.12 $\mathcal{M} \models Pr_{\mathsf{HA}}(\ulcorner \phi \urcorner)$. If $\mathsf{HA} \nvdash_i \phi$, then $\neg Pr_{\mathsf{HA}}(\ulcorner \phi \urcorner) \in \mathcal{U}$, hence $T \vdash_c \neg Pr_{\mathsf{HA}}(\ulcorner \phi \urcorner)$ which implies $\mathcal{M} \models \neg Pr_{\mathsf{HA}}(\ulcorner \phi \urcorner)$, but this leads to a contradiction, hence $\mathsf{HA} \vdash_i \phi$. □

As we already mentioned in the Introduction, we can get more Kripke models for $\mathsf{HA} + \mathsf{ECT}_0$ from the first construction than by the second construction. We will show this fact in the rest of this subsection. For this matter, we need the following theorem.

Theorem 20.18. *([Rab62]) For any constant* k*, there is no consistent* Π_k*-axiomatized theory* T *such that* $T \vdash_c \mathsf{PA}$.

Theorem 20.19. *The following statements are true:*

1. *For every* $\mathcal{L}$ *structure* $\mathcal{M}$*, if* $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}+\mathsf{ECT}_0}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$*, then* $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$.
2. *There exists an* $\mathcal{L}$ *structure* $\mathcal{M}$ *such that* $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$*, but* $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}+\mathsf{ECT}_0}) \nVdash \mathsf{HA}$.

Proof.

1. $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}+\mathsf{ECT}_0}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$, so by Lemma 19.5 $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$, therefore by Theorem 20.6 $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$.

2. By Gödel's second incompleteness theorem, $\mathsf{HA} + \neg Con_{\mathsf{HA}} \nvdash_i \bot$. So by Π_2 conservativity of PA over HA (see [Fri78]) we have $\mathbf{Th}_{\Pi_2}(\mathsf{PA}) + \neg Con_{\mathsf{HA}} \nvdash_c \bot$. $\mathbf{Th}_{\Pi_2}(\mathsf{PA}) + \neg Con_{\mathsf{HA}}$ is a Π_2-axiomatized theory, hence by Theorem 20.18 there exists a model $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA}) + \neg Con_{\mathsf{HA}}$ such that $\mathcal{M} \not\models \mathsf{PA}$. Note that by Theorem 20.6 $\mathbf{K}(\mathcal{M}, \mathbf{T}_{\mathcal{M}}) \Vdash \mathsf{HA} + \mathsf{ECT}_0$. On the other hand $\mathcal{M} \models \neg Con_{\mathsf{HA}+\mathsf{ECT}_0}$, so $\bot \in \mathsf{EXT}(\mathcal{M}, \mathsf{HA}+\mathsf{ECT}_0)$. This implies $\mathbf{C}_{\mathcal{M},\mathsf{HA}+\mathsf{ECT}_0} \vdash_i \bot$. Hence $\mathcal{S}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}+\mathsf{ECT}_0}) = \varnothing$. This means that $\mathbf{K}(\mathcal{M}, \mathbf{C}_{\mathcal{M},\mathsf{HA}+\mathsf{ECT}_0})$ has only one node r such that $\mathcal{M}_r = \mathcal{M}$. Note that $\mathcal{M} \not\models \mathsf{PA}$, so $r \nVdash \mathsf{HA}$ and this completes the proof.

□

21 On binary Kripke models for intuitionistic first-order logic

In this section, we will prove that every countable rooted Kripke model $\mathbf{K}$ (there exists a node k in $\mathbf{K}$ such that for every k in $\mathbf{K}$, $k \leq k'$) can be transformed to a Kripke model $\mathbf{K}'$ with the infinite full binary tree as Kripke frame such that $\mathbf{K}$ and $\mathbf{K}'$ force the same sentences. This was known for the case of finite Kripke models of intuitionistic propositional logic (see Theorem 2.21 and Corollary 2.22 of [CZ97]), but to best of our knowledge it was not mentioned for the case of Kripke models of intuitionistic first-order logic in the literature. The transformation for Kripke models of intuitionistic first-order logic can be done in the same way that was done for the case of finite Kripke models of intuitionistic propositional logic, but for the sake of completeness we will state the theorem and prove it in this section.

Let $\Gamma = \{0, 1\}$ and Γ^* be the set of all finite binary strings (including empty string λ). For every $x, y \in \Gamma^*$, $x \preceq y$ iff x is a prefix of y.

Lemma 21.1. *Let* $\mathbf{K} = (K, \leq, \mathcal{M})$ *be a countable rooted Kripke model in a language* σ*. Then there is an onto function* $f : \Gamma^* \to K$*, such that:*

1. $\mathbf{K}' = (\Gamma^*, \preceq, \mathcal{M}')$ *is a Kripke model where* $\mathcal{M}'$ *is defined as* $\mathcal{M}'_x = \mathcal{M}_{f(x)}$ *for every* $x \in \Gamma^*$*,*

2. *for every* $k \in K$*, for every* $\sigma(\mathcal{M}_k)$ *sentence* ϕ*, and for every* $x \in \Gamma^*$ *such that* $f(x) = k$*,* $x \Vdash \phi$ *iff* $k \Vdash \phi$*.*

Proof. Without loss of generality, we can assume $(K, \leq)$ is a tree (see Theorem 6.8 in the second chapter of [Tv88]) with the root r. Also, we can assume that for every $k \in K$, there is a $k' \in K$ different from k such that $k \leq k'$. This is true because for every $k \in K$ that does not have relation with any other nodes, we can put an infinite countable path above k such that the classical structure of every node in this path is $\mathcal{M}_k$. This transformation does not change the sentences that were forced in the original model. For every $k \in K$, define neighbor of k as

$$\mathcal{N}_k = \{k' \in K | k \leq k' \wedge k \neq k' \wedge \forall k'' \in K(k \leq k'' \wedge k'' \leq k' \to k = k'' \vee k' = k'')\}.$$

For every $k \in K$, fix an onto function $g_k : \mathbb{N} \to \mathcal{N}_k$ such that for every $k' \in \mathcal{N}_k$, $\{n \in \mathbb{N} | g_k(n) = k'\}$ is infinite. Now we define f inductively with a sequence of partial function $f_0 \subset f_1 \subset \dots$ and then we put $f = \bigcup_{n \in \mathbb{N}} f_n$. Put $f_0(\lambda) = r$. For a function h, let $\mathsf{Dom}(h)$ be domain of h. Let

$$\mathcal{A}_n = \{x \in \Gamma^* | x \in \mathsf{Dom}(f_n), x0 \notin \mathsf{Dom}(f_n), x1 \notin \mathsf{Dom}(f_n)\}.$$

Now f_{n+1} is defined inductively from f_n as follows:

$$f_{n+1}(x) = \begin{cases} f_n(x) & x \in \mathsf{Dom}(f_n) \\ f_n(y) & x = y0^m, \text{ for some } y \in \mathcal{A}_n, m \in \mathbb{N} \\ g_{f_n(y)}(m) & x = y0^m1, \text{ for some } y \in \mathcal{A}_n, m \in \mathbb{N}. \end{cases}$$

It is easy to see that $\mathsf{Dom}(f) = \Gamma^*$.

Claim 21.1. *For every $k \in K$, for every $x \in \Gamma^*$ if $f(x) = k$, then*

$$\{k' \in K | k \leq k'\} = \{f(y) \in K | y \in \Gamma^*, x \preceq y\}.$$

This claim is easy to prove considering the definition of f and the fact that g_k functions enumerate neighbors infinitely many times.

Using this claim, we can finish the proof. The proof goes by induction on the complexity of ϕ. We will only mention a nontrivial case in the induction steps. All other cases can be treated similarly. Let $\phi := \psi \to \eta$ and $k \Vdash \psi \to \eta$. Let $x \in \Gamma^*$ be such that $f(x) = k$. Suppose for some $y \succeq x$, we know $y \Vdash \psi$. So by the induction hypothesis, $f(y) \Vdash \psi$ and by Claim 21.1, we know $f(y) \geq k$, hence $f(y) \Vdash \eta$, therefore by the induction hypothesis we get $y \Vdash \eta$, so $x \Vdash \phi$. □

Corollary 21.2. *There exists a Kripke model of* HA *with $(\Gamma^*, \preceq)$ as the Kripke frame that is not locally* $\mathbf{I}\Delta_1$.

Proof. Here we apply the idea of [Jeř11] with some modifications. Let $\mathbf{K}$ be a rooted Kripke model with the root r in a language σ. Let $\mathcal{U}$ be a countable set of sentences of σ. It is easy to see that $\mathbf{K}$ can be represented by a suitable two-sorted classical structure $\mathbf{M_K}$ such that:

1. For every $\phi \in \mathcal{U}$, "$r \Vdash \phi$" is first-order definable in $\mathbf{M_K}$ by the sentence ϕ_F.
2. For every $\phi \in \mathcal{U}$, "$\mathcal{M}_r \models \phi$" is first-order definable in $\mathbf{M_K}$ by the sentence ϕ_M.

By applying the downward Löwenheim–Skolem theorem on $\mathbf{M_K}$ we get a countable substructure of $\mathbf{M_K}$ like $\mathbf{M'_K}$ such that:

1. $\mathbf{M'_K}$ is a representation of a countable rooted Kripke model in the language σ.
2. For every $\phi \in \mathcal{U}$, $\mathbf{M_K} \models \psi$ iff $\mathbf{M'_K} \models \psi$, for $\psi \in \{\phi_F, \phi_M\}$.

Let $\mathbf{K}(\mathcal{M}, \mathbf{T}_\mathcal{M})$ be the rooted Kripke model from Corollary 20.10. Let $\mathcal{U} =$ HA$\cup\{\varphi\}$ where φ is an instance of Δ_1 induction that fails in the classical structure of the root of $\mathbf{K}(\mathcal{M}, \mathbf{T}_\mathcal{M})$. Following the same argument on $\mathbf{K}(\mathcal{M}, \mathbf{T}_\mathcal{M})$ and $\mathcal{U}$, we get a countable rooted Kripke model $\mathbf{K}'$ of HA that is not locally $\mathbf{I}\Delta_1$. Hence applying Lemma 21.1 on $\mathbf{K}'$ finishes the proof. □

22 Concluding remarks and open problems

Problem 11 can be asked about other theories than HA. One can ask the same question about arithmetic over sub-intuitionistic logic too. One of these logics is Visser's Basic logic, and its extension Extended Basic logic. The model theory of arithmetic over these logics were investigated in [Rui98, AH08, AKS20]. From the point of view of Problem 11, it is proved in [AH08] that every irreflexive node in a Kripke model of BA (Basic Arithmetic) is locally $\mathbf{I}\exists_1^+$. So In general, every irreflexive node in a Kripke model of the natural extension of BA such as EBA (Extended Basic Arithmetic) is locally $\mathbf{I}\Sigma_1$ (see Corollary 3.33 in [AKS20]). Also it is proved in [AKS20] that every Kripke model of EBA is locally $\mathbf{Th}_{\Pi_2}(\mathbf{I}\Sigma_1) + \mathbf{Th}_{\Pi_1}(\mathsf{PA})$. Note that every Kripke model of HA is also a Kripke model of BA and EBA. So Corollary 20.10 applies to these theories too, and this solves Problem 11 for these theories. Furthermore, this shows that the known positive results are the best we can get for BA and EBA.

Focusing on the proof of Theorem 19.3, we essentially use ECT_0 for proving the existence and the disjunction properties of $\mathbf{T}_{\mathcal{M}}$. We do not know whether ECT_0 is essential for such a model construction, so we have the following question:

Problem 13. *Does* HA + Diag($\mathcal{M}$) *have the existence property for every* $\mathcal{M} \models \mathbf{Th}_{\Pi_2}(\mathsf{PA})$*?*

An interesting problem which we could not answer is the following:

Problem 14. *Is there any Kripke model* $\mathbf{K} \Vdash \mathsf{HA}$ *such that for every node* k *in* $\mathbf{K}$*,* $\mathcal{M}_k \not\models \mathsf{PA}$*?*

Another unsolved question in the direction of completeness with respect to locally PA Kripke models is the following:

Problem 15. *Does* HA *have completeness with respect to its class of locally* PA *Kripke models?*

By the result of [Bus93], for every sentence ϕ such that $\mathsf{HA} \nvdash_i \phi$, there exists a locally PA Kripke model $\mathbf{K}$ such that $\mathbf{K} \nVdash \phi$, but this result does not say anything about whether $\mathbf{K}$ is a Kripke model of HA or not.

We call a rooted tree Kripke frame $(K, \leq)$, a PA-frame iff for every Kripke model $\mathbf{K} \Vdash \mathsf{HA}$ with frame $(K, \leq)$, $\mathbf{K}$ is locally PA. Let $\mathcal{F}_{\mathsf{PA}}$ be the set of all PA-frames. We know that semi narrow rooted tree Kripke frames are in $\mathcal{F}_{\mathsf{PA}}$. On the other hand, by Corollary 21.1 infinite full binary tree is not in $\mathcal{F}_{\mathsf{PA}}$. So we have the following question:

Problem 16. *Is there a nice characterization of* $\mathcal{F}_{\mathsf{PA}}$*?*

Bibliography

[AH02] M. Ardeshir and B. Hesaam. Every Rooted Narrow Tree Kripke Model of HA is Locally PA. *Mathematical Logic Quarterly*, 48(3):391–395, 2002.

[AH08] M. Ardeshir and B. Hesaam. An Introduction to Basic Arithmetic. *Logic Journal of the IGPL*, 16(1):1–13, 2008.

[AKS20] M. Ardeshir, E. Khaniki, and M. Shahriari. Provably total recursive functions and MRDP theorem in Basic Arithmetic and its extensions. *arXiv*, (2003.01603), 2020.

[AMZ18] M. Abiri, M. Moniri, and M. Zaare. From forcing to satisfaction in Kripke models of intuitionistic predicate logic. *Logic Journal of the IGPL*, 26(5):464–474, 2018.

[AMZ19] M. Abiri, M. Moniri, and M. Zaare. Forcing and satisfaction in Kripke models of intuitionistic arithmetic. *Logic Journal of the IGPL*, 27(5):659–670, 2019.

[ARS03] M. Ardeshir, W. Ruitenburg, and S. Salehi. Intuitionistic Axiomatizations for Bounded Extension Kripke Models. *Annals of Pure and Applied Logic*, 124(1-3):267–285, 2003.

[Bus93] S. R. Buss. Intuitionistic Validity in T-Normal Kripke Structures. *Annals of Pure and Applied Logic*, 59(3):159–173, 1993.

[CZ97] A. V. Chagrov and M. Zakharyaschev. *Modal Logic*, volume 35 of *Oxford logic guides*. Oxford University Press, 1997.

[Fri78] H. Friedman. Classically and intuitionistically provably recursive functions. In G. H. Müller and D. S. Scott, editors, *Higher Set Theory*, volume 669 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, 1978.

[Jeř11] E. Jeřábek. Intuitionistic Lowenheim-Skolem? (answer). *MathOverflow*, 2011. https://mathoverflow.net/q/54319.

[Mar93] Z. Marković. On the structure of kripke models of heyting arithmetic. *Mathematical Logic Quarterly*, 39(1):531–538, 1993.

[Moj18] M. Mojtahedi. Localizing finite-depth Kripke models. *Logic Journal of the IGPL*, 27(3):239–251, 2018.

[Mon02] M. Moniri. H-theories, fragments of HA and PA-normality. *Archive for Mathematical Logic*, 41(1):101–105, 2002.

[Par70] Ch. Parsons. On a Number Theoretic Choice Schema and its Relation to Induction. In A. Kino, J. Myhill, and R.E. Vesley, editors, *Intuitionism and Proof Theory: Proceedings of the Summer Conference at Buffalo N.Y. 1968*, volume 60 of *Studies in Logic and the Foundations of Mathematics*, pages 459–473. Elsevier, 1970.

[Poł06] T. Połacik. Partially-Elementary Extension Kripke Models: A Characterization and Applications. *Logic Journal of the IGPL*, 14(1):73–86, 2006.

[Rab62] M. O. Rabin. Non-standard models and independence of the induction axiom. Essays Found. Math., dedicat. to A. A. Fraenkel on his 70th Anniv., 287-299 (1962)., 1962.

[Rui98] W. Ruitenburg. Basic predicate calculus. *Notre Dame Journal of Formal Logic*, 39(1):18–46, 1998.

[Sla04] T. A. Slaman. Σ_n-bounding and Δ_n-induction. *Proceedings of the American Mathematical Society,*, 132(8):2449–2456, 2004.

[Smo73] C. Smoryński. Applications of Kripke models. In A.S. Troelstra, editor, *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, volume 344 of *Lecture Notes in Mathematics*. Springer Berlin Heidelberg, 1973.

[Smo77] C. Smoryński. The Incompleteness Theorems. In J. Barwise, editor, *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*, pages 821–865. Elsevier, 1977.

[Smo85] C. Smoryński. *Self-reference and modal logic.* Universitext. Springer, New York, NY, 1985.

[Tv88] A. S. Troelstra and D. van Dalen. *Constructivism in mathematics. An introduction. Volume I*, volume 121. Amsterdam etc.: North-Holland, 1988.

[vMKV86] D. van Dalen, H. Mulder, E. C. W. Krabbe, and A. Visser. Finite Kripke models of HA are locally PA. *Notre Dame Journal of Formal Logic*, 27(4):528–532, 1986.

[Weh96] K. F. Wehmeier. Classical and intuitionistic models of arithmetic. *Notre Dame Journal of Formal Logic*, 37(3):452–461, 1996.