THEORY OF COMPUTING, Volume 22 (4), 2026, pp. 1–29
www.theoryofcomputing.org

SPECIAL ISSUE: CCC 2021

A Lower Bound for Polynomial Calculus with Extension Rule

Yaroslav Alekseev*

Received August 12, 2021; Revised September 20, 2025; Published June 21, 2026

Abstract. A major proof complexity problem is to prove a superpolynomial lower bound on the length of Frege proofs of arbitrary depth. A more difficult question is to prove an Extended Frege lower bound. Surprisingly, proving such bounds turns out to be much easier in the algebraic setting. In this paper, we study a proof system that can efficiently simulate Extended Frege: an extension of the Polynomial Calculus proof system where we can take a square root and introduce new variables that are equivalent to algebraic circuits of arbitrary depth. We prove that an instance of the subset-sum principle, the binary value principle $1 + x_1 + 2x_2 + \ldots + 2^{n-1}x_n = 0$ (BVP_n), requires refutations of exponential bit size over $\mathbb{Q}$ in this system.

Part and Tzameret (ITCS'20) proved an exponential lower bound on the size of Res-Lin (Resolution over linear equations) refutations of BVP_n. We show that our system p-simulates Res-Lin and thus we get an alternative exponential lower bound for the size of Res-Lin refutations of BVP_n.

A preliminary version of this paper appeared in the Proceedings of the 36th Conference on Computational Complexity (CCC'21).

*Research supported by «Native towns», a social investment program of PJSC «Gazprom Neft».

ACM Classification: F.1.3

AMS Classification: 03F20

Key words and phrases: proof complexity, algebraic proofs, polynomial calculus

 DOI: 10.4086/toc.2026.v022a004

1 Introduction

In essence, the study of propositional proof complexity started with the work of Cook and Reckhow [10], which states that if there is a propositional proof system in which any unsatisfiable formula F has a short proof of unsatisfiability, then $\mathsf{NP} = \mathsf{coNP}$. In the same work Cook and Rechow introduced a notion of *p-simulation*: a proof system A p-simulates a proof system B if every tautology has a proof in A of size at most polynomially larger than in its shortest proof in B. The first superpolynomial bound on the proof size was proved in pioneering work by Tseitin [34] for regular Resolution. Since then, many proof systems have been studied, some of them are logic-style (working with disjunctions, conjunctions, and other Boolean operations) and some of them are algebraic (working with arbitrary polynomials).

In this article we consider extensions of two systems, an algebraic one and a logic-style one.

1.1 Logic-style systems

As mentioned before, the first superpolynomial lower bound on the proof size was proved in a paper by Tseitin for regular Resolution, which is a popular logic proof system. This proof system operates with the disjunctions of variables and their negations and utilizes the following inference rule:

$$\frac{A \vee x \quad B \vee \overline{x}}{A \vee B}.$$

Later, Haken [15] proved an exponential lower bound on the size of (unrestricted) Resolution refutation of the pigeonhole principle (PHP), expressing that there is no (total) injective map from a set with cardinality m to a set with cardinality n if $m > n$.

Since then, stronger logical proof systems such as Frege systems

have been considered. Unlike the Resolution proof system, a Frege proof system operates with formulas over Boolean variables and uses some sound and implicationally complete set of inference rules. Exponential lower bounds for low-depth Frege proof systems have been known for decades [1, 5, 17]. However, the situation with the proof systems of greater depth is much worse.

1.2 Resolution with counting

Another approach to strengthening Resolution is to use weak extensions in order to do some sort of counting. $\mathsf{Res}\text{-}\mathsf{Lin}$ (defined in [29]) is a system working with disjunctions of linear equations over a fixed field [1] and can be viewed as a generalization of Resolution. In the present paper we consider the $\mathsf{Res}\text{-}\mathsf{Lin}$ system over $\mathbb{Q}$.

This system utilizes the following inference rule:

$$\frac{A \vee (L_1 = 0) \quad B \vee (L_1' = 0)}{A \vee B \vee (\alpha L_1 + \beta L_1' = 0)},$$

[1] Usually $\mathsf{Res}\text{-}\mathsf{Lin}$ is defined over $\mathbb{Q}$, but arbitrary finite fields have also been considered.

where $A = (L_2 = 0) \vee (L_3 = 0) \vee \cdots \vee (L_m = 0)$, $B = (L'_2 = 0) \vee (L'_3 = 0) \vee \cdots \vee (L'_k = 0)$, α and β are any constants and each L_i and L'_i is an affine form over the initial Boolean variables.

No superpolynomial lower bounds are known for the size of refutations of CNF formulas in (DAG-like) systems that work over disjunctions of equations or disjunctions of inequalities (see [21] as the first paper defining these systems and containing partial results). Part and Tzameret [24] proved an exponential lower bound for (DAG-like) Res-Lin refutations over $\mathbb{Q}$ for the binary value principle BVP_n. Although this is the first exponential lower bound for this system, the instance does not correspond to a translation of any CNF formula.

Itsykson and Sokolov [20] considered another extension of the Resolution proof system, named $\mathsf{Res}(\oplus)$, that operates with disjunctions of linear equalities over $\mathbb{F}_2$, and proved an exponential lower bound on the size of tree-like $\mathsf{Res}(\oplus)$-proofs.

1.3 Algebraic proof systems

Algebraic proof systems such as Nullstellensatz have been developed to use algebraic techniques of Razborov and Smolensky [30, 32] in proof complexity. Lower bounds for algebraic systems started with an exponential lower bound for the Nullstellensatz [4] system. The main system considered in this paper is based on the Polynomial Calculus system [9], which is a dynamic version of Nullstellensatz. Many exponential lower bounds are known for the size of Polynomial Calculus proofs for tautologies like the Pigeonhole Principle [31, 19] and Tseitin tautologies [6]. While most results concern the representation of Boolean values by 0 and 1, there are also exponential lower bounds over the $\{-1, +1\}$ basis [33].

However, simple algebraic proof systems such as Nullstellensatz and Polynomial Calculus cannot efficiently simulate strong logic systems like Frege systems (since there is a polynomial-size Frege refutation of the Pigeonhole Principle, see [10] for example) and thus cannot provide lower bounds for these systems. In order to fix this issue, strong extensions have been considered: Grigoriev and Hirsch [13] considered algebraic systems over formulas. Following Pitassi's ideas [25, 26], Grochow and Pitassi [14] formally defined the Ideal Proof System, IPS, which can be considered as the version of Nullstellensatz where all polynomials are written as algebraic circuits.

Many other extensions of Polynomial Calculus and Nullstellensatz have also been considered. Buss, Impagliazzo, Krajíček, Pudlák, Razborov and Sgall [7] showed that there is a tight connection between the lengths of constant-depth Frege proofs with MOD_p gates and the length of Nullstellensatz refutations using extension axioms. Impagliazzo, Mouli and Pitassi [18] showed that a depth-3 extension of Polynomial Calculus called $\Sigma\Pi\Sigma$-PC p-simulates semantic CP^* (an inequalities-based system, Cutting Planes [11, 8] with coefficients written in unary) over $\mathbb{Q}$. Also, they showed that a stronger extension of Polynomial Calculus, called Depth-k-PC, *effectively*[2] p-simulates Cutting Planes and another inequalities-based system, Sum-of-Squares (for a survey about this proof system see [12]); the simulations can be conducted over $\mathbb{F}_{p^m}$ for an arbitrary prime number p if m is sufficiently large. However, the question about proving a

[2] Effective p-simulation was introduced by Pitassi and Santhanam [27] and can be viewed as a weaker version of a usual p-simulation.

superpolynomial lower bound even on the size of $\Sigma\Pi\Sigma$-PC refutations over any field remains open since it is not clear how to extend lower-bound techniques such as size–degree tradeoff to this system.

1.4 Our results

We extend Polynomial Calculus with two additional rules. One rule allows us to take a square root (this was introduced by Grigoriev and Hirsch [13] in the context of transforming refutation proofs of non-Boolean formulas into derivation proofs; our motivation to take square roots is to consider an algebraic system that is at least as strong as Res-Lin even for non-Boolean formulas, see below). Note that while fields such as the rational numbers are not closed under square roots, we define the square root derivation rule such that it applies only to polynomials that are the square of another polynomial.

Another rule is an algebraic version of Tseitin's extension rule, which allows us to introduce new variables that are equivalent to arbitrary depth algebraic circuits. We will denote our generalization of Polynomial Calculus as Ext-PC$^{\surd}$. Note that Ext-PC$^{\surd}$ p-simulates Extended Frege system (since Ext-PC$^{\surd}$ p-simulates Extended Resolution and Extended Resolution p-simulates Extended Frege [22]), but it is not obvious how to p-simulate IPS refutations in Ext-PC$^{\surd}$ (since IPS refutation polynomials are written as algebraic circuits and Ext-PC$^{\surd}$ refutations are written explicitly as a sum of monomials).

In this article we give a partial positive answer to the question raised in [18] asking for a technique for proving size lower bounds on Polynomial Calculus without proving any degree lower bounds. However, since our lower bound heavily utilizes the divisibility of integers, it works only over $\mathbb{Q}$ (by reduction to $\mathbb{Z}$) and the question about proving lower bounds over finite fields remains open. Also, we give a partial answer to another question raised in [18] by proving an exponential lower bound for the system with an extension rule even stronger than that in $\Sigma\Pi\Sigma$-PC, which is another extension of Polynomial Calculus presented in [18].

Finally, most lower bounds for algebraic and semialgebraic proof systems (see [31, 19], for example) measure the size of the polynomial as the number of monomials in it. In this article the size measure of the refutation is different and possibly weaker, but more natural in terms of Cook and Reckhow proofs. We prove an exponential lower bound on the *number of bits* we need to encode an Ext-PC$^{\surd}$-refutation. Obviously, an exponential lower bound on the number of monomials in a refutation implies an exponential lower bound on the bit-size of the refutation. However, it is not known, whether the opposite direction is true (for example, for some of the weaker systems such as Sum of Squares, the opposite direction is not true [23, 28, 16]).

We consider the following subset-sum instance, called Binary Value Principle (BVP_n) [3, 24]:

$$1 + x_1 + 2x_2 + \ldots + 2^{n-1}x_n = 0,$$
$$x_1^2 - x_1 = 0, \quad x_2^2 - x_2 = 0, \quad \ldots \quad , \quad x_n^2 - x_n = 0.$$

and prove an exponential lower bound for the size of Ext-PC$^{\surd}_{\mathbb{Q}}$ refutations of BVP_n. Note that the Binary Value Principle does not correspond to the translation of any polynomial-size CNF formula and thus the question about proving size lower bounds on the refutation of CNF formulas without proving degree lower bounds *remains open*. This also means that an exponential lower bound for $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ refutations of BVP_n does not imply superpolynomial lower bounds for any logical proof system, such as Frege or Extended Frege.

Also note that, despite that Impagliazzo, Mouli and Pitassi [18] showed that $\mathsf{Depth\text{-}}k\mathsf{\text{-}PC}$ *effectively* p-simulates Sum-of-Squares, it also does not give an alternative lower bound for Sum-of-Squares since the *effective* p-simulation can lead to an exponential blow-up for formulas such as BVP_n . Moreover, it is easy to see that there is a polynomial-size refutation of BVP_n in the Sum-of-Squares proof system.

Theorem 1.1. *Any* $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ *refutation of* BVP_n *requires size* $2^{\Omega(n)}$.

The technique we use for proving this lower bound is similar to the technique for proving the *conditional* IPS lower bound in [3]. However, since the $\mathsf{Ext\text{-}PC}$ proof system is possibly weaker than the $\mathsf{Ideal\ Proof\ System}$, we get an unconditional lower bound. The main idea of the conditional lower bound in [3] is to prove the complexity lower bound on the free term at the end of the IPS-refutation of BVP_n over $\mathbb{Z}$ and then show that $\mathsf{IPS}_{\mathbb{Z}}$ simulates $\mathsf{IPS}_{\mathbb{Q}}$. One difference is that instead of concentrating on the *complexity* of computing the free term of the proof, we concentrate on the *prime numbers* mentioned in the proof (and thus appearing as factors of the free term).

In the last part of our paper we consider $\mathsf{Res\text{-}Lin}$ and show that $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ simulates $\mathsf{Res\text{-}Lin}$ and thus get an alternative lower bound for $\mathsf{Res\text{-}Lin}$.

Corollary 1.2. *Any* $\mathsf{Res\text{-}Lin}_{\mathbb{Q}}$ *refutation of* BVP_n *requires size* $2^{\Omega(n)}$.

Note that while Part and Tzameret [24] prove an exponential lower bound on the number of lines in the proof, we only prove a lower bound on the proof size (essentially, on the bit size of scalars appearing in the proof). So our result is not comparable to Part and Tzameret's.

1.5 Organization of the paper

In Section 2 we recall the definition of Polynomial Calculus (PC) and give the definitions of Polynomial Calculus with square root ($\mathsf{PC}^{\surd}$) and Extended Polynomial Calculus with square root ($\mathsf{Ext\text{-}PC}^{\surd}$).

In Section 3 we prove an exponential lower bound on the size of $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ refutations of BVP_n . We start with considering derivations with integer coefficients ($\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Z}}$) and show that the free term at the end of such refutation of BVP_n is not just large but also is divisible by all primes less than 2^n (see Theorem 3.2). Then, in Theorem 3.5, we convert proofs over $\mathbb{Q}$ into proofs over $\mathbb{Z}$ without changing the set of primes mentioned in the proof and thus get an $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ lower bound.

In Section 4 we show that $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ simulates $\mathsf{Res\text{-}Lin}$ and thus we get an alternative lower bound for the size of $\mathsf{Res\text{-}Lin}$ refutations of BVP_n .

1.6 Differences from the conference version

The main difference of this version from the conference version ([2]) is that Section 3 is rewritten to make it easier to understand. Also, some explanations have been added in various sections.

2 Preliminaries

In this paper we are going to work with polynomials over the integers or the rationals. We define the size of a polynomial roughly as the total length of the bit representation of its coefficients (including the sign bit).

Definition 2.1 (Size of an integer and a rational number)**.**

- (Integers) If $z \in \mathbb{Z}$ is written in binary then $\mathrm{Size}(z) = 1 + \lceil \log(|z| + 1) \rceil$. If z is written in unary then $\mathrm{Size}(z) = 1 + |z|$. (In both cases, the initial "1+" accounts for the sign bit, or, for $z = 0$, for the symbol "0".)
- (Fractions) If $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ then $\mathrm{Size}(p/q) = \mathrm{Size}(p) + \mathrm{Size}(q) - 1$. (The "-1" is there because we do not need a sign bit for the denominator and the denominator cannot be zero.)
- (Rationals) If $r \in \mathbb{Q}$ then write r as p/q where $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p, q) = 1$, and we set $\mathrm{Size}(r) = \mathrm{Size}(p/q)$.

Definition 2.2 (Size of a polynomial)**.** Let f be an arbitrary polynomial with integer or rational coefficients, in variables $x_1, \ldots, x_n$. We set

$$\mathrm{Size}(f) = \sum_i \mathrm{Size}(a_i)\,,$$

where the a_i are the coefficients of f (including the zero coefficients).

Following [9], we define the Polynomial Calculus proof system.

Definition 2.3 (Polynomial Calculus, [9])**.** Let $\Gamma = \{P_1, \ldots, P_m\} \subset R[x_1, \ldots, x_n]$ be a set of polynomials in the variables $x_1, \ldots, x_n$ over an integral domain R such that the system of equations $P_1 = 0, \ldots, P_m = 0$ has no solution. A Polynomial Calculus refutation of Γ is a sequence of polynomials $R_1, \ldots, R_s$ where $R_s = M$ for some constant $M \in R\backslash\{0\}$ and for every l in $\{1, \ldots, s\}$, $R_l \in \Gamma$ or is obtained through one of the following derivation rules for $j, k < l$

- $R_l = \alpha R_j + \beta R_k$ for $\alpha, \beta \in R$
- $R_l = x_i R_k$

The size of the refutation is $\sum_{l=1}^{s} \mathrm{Size}(R_l)$. The degree of the refutation is $\max_l \deg(R_l)$.

We now define $\mathsf{Ext}\text{-}\mathsf{PC}_R$, a variant of PC_R , where the proof system is additionally allowed to introduce new variables y_i corresponding to arbitrary polynomials in the original variables x_i .

Definition 2.4 (Extended Polynomial Calculus)**.** Let $\Gamma = \{P_1, \ldots, P_m\} \subset R[x_1, \ldots, x_n]$ be a set of polynomials in the variables $x_1, \ldots, x_n$ over a domain R such that the system of equations $P_1 = 0, \ldots, P_m = 0$ has no solution. An $\mathsf{Ext\text{-}PC}_R$ refutation of Γ is a PC_R refutation of a set

$$\begin{aligned}\Gamma' = \{&P_1, \ldots, P_m, y_1 - Q_1(x_1, \ldots, x_n),\\ &y_2 - Q_2(x_1, \ldots, x_n, y_1), \ldots, y_m - Q_m(x_1, \ldots, x_n, y_1, \ldots, y_{m-1})\}\end{aligned}$$

where the $Q_i \in R[\vec{x}, y_1, \ldots, y_{i-1}]$ are arbitrary polynomials and the y_i are new variables.

The size of the $\mathsf{Ext\text{-}PC}_R$ refutation is defined as the size of the corresponding PC_R refutation of Γ'.

Following [18], we define the $\Sigma\Pi\Sigma\text{-}\mathsf{PC}_R$ proof system.

Definition 2.5 ($\Sigma\Pi\Sigma\text{-}\mathsf{PC}_R$, [18])**.** Let $\Gamma = \{P_1, \ldots, P_m\} \subset R[x_1, \ldots, x_n]$ be a set of polynomials in the variables $x_1, \ldots, x_n$ over a ring R such that the system of equations $P_1 = 0, \ldots, P_m = 0$ has no solution. A $\Sigma\Pi\Sigma\text{-}\mathsf{PC}_R$ refutation of Γ is a PC_R refutation of a set $\Gamma' = \{P_1, \ldots, P_m, Q_1, \ldots, Q_m\}$, where Q_i are polynomials of the form $Q_i = y_i - (a_{i0} + \sum_j a_{ij}x_j)$ for some constants $a_{ij} \in R$.

The size of the $\Sigma\Pi\Sigma\text{-}\mathsf{PC}_R$ refutation is defined as the size of the corresponding PC_R refutation of Γ'.

Now we consider a variant of the Polynomial Calculus proof system with additional *square root derivation rule* (see [13]).

Definition 2.6 (Polynomial Calculus with square root)**.** Let $\Gamma = \{P_1, \ldots, P_m\} \subset R[x_1, \ldots, x_n]$ be a set of polynomials in the variables $x_1, \ldots, x_n$ over an integral domain R such that the system of equations $P_1 = 0, \ldots, P_m = 0$ has no solution. A $\mathsf{PC}_R^{\sqrt{}}$ refutation of Γ is a sequence of polynomials $R_1, \ldots, R_s$ where $R_s = M$ for some constant $M \in R, M \neq 0$ and for every l in $\{1, \ldots, s\}$, $R_l \in \Gamma$ or is obtained through one of the following derivation rules for $j, k < l$

- $R_l = \alpha R_j + \beta R_k$ for $\alpha, \beta \in R$
- $R_l = x_i R_k$ for some $i \in \{1, \ldots, n\}$
- $R_l^2 = R_k$ (which means that we can take square root of a polynomial if and only if it is a square of some other polynomial)

The size of the refutation is $\sum_{l=1}^{s} \mathrm{Size}(R_l)$, where $\mathrm{Size}(R_l)$ is the size of the polynomial R_l. The degree of the refutation is $\max_l \deg(R_l)$.

Remark 2.7. Usually, the Polynomial Calculus proof system is defined over algebraically closed fields, since the completeness of Polynomial Calculus is based on the Nullstellensatz theorem. In our work, we consider Polynomial Calculus and its extensions over the rings $\mathbb{Q}$ or $\mathbb{Z}$. For both of these rings, if we consider the *Boolean* case, where we add the axioms $x_i^2 - x_i = 0$, our system is complete (see [9, 3] for $\mathbb{Q}$ and $\mathbb{Z}$), which means that for every system of equations $\{f_i(\vec{x}) = 0\}$ unsatisfiable over $\{0, 1\}$ assignments there is a $\mathsf{PC}_R^{\sqrt{}}$ refutation. Also, note that if R is an integral domain and $P^2 = 0$ for some $P \in R[\vec{x}]$, then $P = 0$. This gives us the soundness for the $\mathsf{PC}_R^{\sqrt{}}$ proof system over the integral domain R.

Definition 2.8 ($\Sigma\Pi\Sigma$-$\mathsf{PC}_R^{\surd}$, Ext-$\mathsf{PC}_R^{\surd}$)**.** The proofs in $\Sigma\Pi\Sigma$-$\mathsf{PC}_R^{\surd}$ and Ext-$\mathsf{PC}_R^{\surd}$ are defined in the same way, as in Definitions 2.5 and 2.4, but instead of PC_R derivations we consider the $\mathsf{PC}_R^{\surd}$ derivations. The size of the refutation is defined the same way as in Definitions 2.5 and 2.4.

It is easy to see that $\Sigma\Pi\Sigma$-PC_R can be polynomially simulated in Ext-PC_R and $\Sigma\Pi\Sigma$-$\mathsf{PC}_R^{\surd}$ can be polynomially simulated in Ext-$\mathsf{PC}_R^{\surd}$.

3 Lower bound

In order to prove the lower bound for the Ext-$\mathsf{PC}_{\mathbb{Q}}^{\surd}$ proof system (Theorem 3.5), we consider the following subset-sum instance [3, 24]:

Definition 3.1 (Binary Value Principle BVP_n)**.** The *binary value principle* over the variables $x_1, \dots, x_n$, BVP_n for short, is the following unsatisfiable system of equations:

$$1 + x_1 + 2x_2 + \dots + 2^{n-1}x_n = 0,$$
$$x_1^2 - x_1 = 0, \quad x_2^2 - x_2 = 0, \quad \dots, \quad x_n^2 - x_n = 0.$$

As mentioned in the Introduction Part and Tzameret [24] proved an exponential lower bound for DAG-like Res-Lin refutations over $\mathbb{Q}$ for BVP_n. Also, it is known that if the Ideal Proof System admits a polynomial-size refutation of BVP_n, then with some assumptions, the Ideal Proof System over $\mathbb{Z}$ is polynomially equivalent to the Cone Proof System over $\mathbb{Z}$, where the Cone Proof System is a semi-algebraic proof system operating with circuits (see [3]). However, under the Shub–Smale conjecture, BVP_n requires superpolynomial-size refutation in the Ideal Proof System (also see [3]).

It was also mentioned in the Introduction that the technique we use for proving the lower bound is similar to the technique for proving the *conditional* IPS lower bound in [3]. The lower bound on the size of the Ext-$\mathsf{PC}_{\mathbb{Q}}^{\surd}$ refutation of BVP_n consists of two parts:

- In the first part we prove an exponential lower bound on the number of different prime factors of the constant at the end of an Ext-$\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n. The technique used to prove this lower bound is similar to the technique used to prove the conditional $\mathsf{IPS}_{\mathbb{Z}}$ lower bound.
- In the second part we transform an Ext-$\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n into an Ext-$\mathsf{PC}_{\mathbb{Q}}^{\surd}$ refutation of BVP_n in order to get the lower bound over the rationals. This part is slightly different from the corresponding transformation of $\mathsf{IPS}_{\mathbb{Z}}$ into $\mathsf{IPS}_{\mathbb{Q}}$ from [3].

3.1 Lower bound over the integers

In this section, we prove that the constant at the end of an Ext-$\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n is divisible by all prime numbers less than 2^n. This fact instantly gives us a lower bound for integer refutations and in the next section, we will use this fact to prove the lower bound over rationals. Formally, we prove the following theorem:

Theorem 3.2. *The constant at the end of any* $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ *refutation of* BVP_n *is divisible by every prime number less than* 2^n *, therefore any* $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ *refutation of* BVP_n *requires size* $\Omega(2^n)$ *.*

Proof. Assume that $R_1, \dots, R_t$ is an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n . Then $R_1, \dots, R_t$ is a $\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of some set of polynomials

$$\Gamma' = \{G(\vec{x}), F_1(\vec{x}), \dots, F_n(\vec{x}), y_1 - Q_1(\vec{x}), \dots y_m - Q_m(\vec{x}, y_1, \dots, y_{m-1})\},$$

where $G(\vec{x}) = 1 + \sum_{i=1}^{n} 2^{(i-1)} x_i$, $F_i(\vec{x}) = x_i^2 - x_i$ and $Q_i \in \mathbb{Z}[\vec{x}, y_1, \dots, y_{i-1}]$.

By the definition of an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ refutation there exists an integer constant $M \neq 0$ such that $R_t = M$.

Claim 3.3. *M is divisible by every prime number less than 2^n .*

Proof of claim: Consider an arbitrary integer $0 \leq k < 2^n$ and its binary representation $b_1, \dots, b_n$. Let $k+1$ be *prime*. Then $G(b_1, \dots, b_n) = k+1$, $F_i(b_1, \dots, b_n) = b_i^2 - b_i = 0$. Also consider integers $c_1, \dots, c_m$ such that $c_i = Q_i(b_1, \dots, b_n, c_1, c_2, \dots, c_{i-1})$. Now we prove by induction that every integer $R_i(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $k+1$ and thus M is divisible by every prime number less than 2^n .

Base case: if $i = 1$, then

$$R_i = G(b_1, \dots, b_n, c_1, \dots, c_m) = k + 1$$

or

$$R_i = F_i(b_1, \dots, b_n, c_1, \dots, c_m) = 0$$

or

$$R_i(b_1, \dots, b_n, c_1, \dots, c_m) = c_i - Q_i(b_1, \dots, b_n, c_1, \dots, c_{i-1}) = 0,$$

which means that R_i is divisible by $k+1$.

Induction step: suppose that R_j is divisible by $k+1$ for any $j \leq i$. Now we show it for R_{i+1} . There are four cases:

1. If $R_{i+1} \in \Gamma'$, then this case is equivalent to the base case and $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $k+1$.

2. If $R_{i+1} = \alpha R_j + \beta R_s$ for $\alpha, \beta \in \mathbb{Z}$ and $j, s \leq i$, then $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $k+1$ because $R_j(b_1, \dots, b_n, c_1, \dots, c_m)$ and $R_s(b_1, \dots, b_n, c_1, \dots, c_m)$ are divisible by $k+1$ and α and β are integers.

3. If $R_{i+1} = x_j R_s$ or $R_{i+1} = y_j R_s$, then $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $k+1$ because $R_s(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $k+1$ and b_j and c_j are integers.

4. If $R_{i+1}^2 = R_s$, then $R_s(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $k+1$. Suppose $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is not divisible by $k+1$. Then $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)^2$ is not divisible by $k+1$ since $k+1$ is *prime*. But

$$R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)^2 = R_s(b_1, \dots, b_n, c_1, \dots, c_m),$$

which leads us to a contradiction.

Since every $R_i(b_1,\ldots,b_n,c_1,\ldots,c_m)$ is divisible by $k+1$, we conclude that

$$M = R_t(b_1,\ldots,b_n,c_1,\ldots,c_m)$$

is divisible by every $k+1$ less than 2^n , and in particular M is divisible by every prime number less than 2^n .

So M is divisible by the product of all prime numbers less than 2^n . Then $|M| > (\pi(2^n))!$ where $\pi(2^n)$ is the number of all prime numbers less than 2^n . By the prime number theorem $\pi(2^n) > C_1\frac{2^n}{n}$ for some constant $C_1 > 0$. By Stirling's approximation we get for some constants $C_2, C_3, C_4 > 0$ that

$$|M| > \left(C_1\frac{2^n}{n}\right)! > C_2 \cdot \left(C_1\frac{2^n}{e \cdot n}\right)^{C_1\frac{2^n}{n}} > C_3\left(2^{\frac{n}{2}}\right)^{C_1\frac{2^n}{n}} > C_3 2^{(2^n C_4)},$$

which means that M consists of at least $C_5 \cdot 2^n$ bits and therefore any $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n requires size $\Omega(2^n)$. □

3.2 Lower bound over the rationals

In order to prove a lower bound over $\mathbb{Q}$, we need to convert an $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\surd}$ proof into an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ proof. The key idea of this translation is that we can create an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ proof in which the constant at the end is a product of some constants occurring in the original $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\surd}$ refutation. Since the constant at the end of the $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ refutation is divisible by all prime numbers less than 2^n , we get a lower bound on the size of constants occurring in the $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\surd}$ refutation and hence on the size of the refutation itself.

In this translation we try to multiply every line of an $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\surd}$ refutation by some constant to get a correct $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\surd}$ refutation. However, there is an obstacle to this approach: we need to somehow convert the $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\surd}$ extension variables encoding polynomials over $\mathbb{Q}$ into extension variables encoding polynomials over $\mathbb{Z}$. With this transformation, the bit size of the constants in our derivation can increase exponentially. For example, assume that we have extension variables of the form

$$y_1 = \frac{x}{2}, y_2 = y_1^2, \ldots, y_n = y_{n-1}^2.$$

These extension variables can be transformed naturally into a sequence of extension variables such that $y_i' = C \cdot y_i$ for some constant C:

$$y_1' = x, y_2' = y_1'^2, \ldots, y_n' = y_{n-1}'^2.$$

Then, if we have a line in an $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\surd}$ derivation of the form, for example

$$y_n^2 - y_{n-1} + x = 0,$$

it would be transformed into

$$\left(\frac{1}{2^{2^n}}y'_n\right)^2 - \frac{1}{2^{2^{n-1}}}y'_{n-1} + x = 0,$$

which has an exponential bit size. The main purpose of the next theorem is to deal with this obstacle.

Theorem 3.4. *Suppose we have an* $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Q}}$ *derivation* $R_1, \dots, R_t$ *from some set of polynomials,* $\Gamma = \{f_1, \dots, f_n\} \subset \mathbb{Z}[\vec{x}]$ *. Also, suppose* $R_t \in \mathbb{Q}[\vec{x}]$ *, which means that* R_t *does not depend on newly introduced variables.*

Then there is an $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Z}}$ *derivation* $R''_1, \dots, R''_{t'}$ *from* Γ *, where*

$$R''_{t'} = \delta_1^{c_1} \cdots \delta_l^{c_l} \cdot L_1^{c_{l+1}} \cdots L_t^{c_{l+t}} \cdot R_t \,,$$

and

- $c_1, c_2, \dots, c_{l+t}$ *are some non-negative integers.*
- *Each* $L_i \in \mathbb{N}$ *is the product of all denominators in the coefficients of* R_i *.*
- *The set of constants* $\{\delta_1, \delta_2, \dots, \delta_l\} \subset \mathbb{N}$ *is the set of all denominators of the constants in* $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ *where* $\{\gamma_1, \gamma_2, \dots, \gamma_l\} \subset \mathbb{Q}$ *is the set of all constants* α *and* β *occurring in linear combination derivations in our proof. This means that some* $R_j(\vec{x}, \vec{y})$ *was derived by using the linear combination rule with the constants* α *and* β *, or in other words,* $R_j = \alpha R_i + \beta R_k$ *for some previously derived polynomials* R_i *and* R_k *.*

Assuming the theorem above, we can easily prove the lower bound on the size of BVP_n refutations in $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Q}}$.

Theorem 3.5. *Any* $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Q}}$ *refutation of* BVP_n *requires size* $\Omega(2^n)$.

Proof. Consider any $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Q}}$ refutation of BVP_n of size S . By Theorem 3.4, there is an $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Z}}$ refutation of BVP_n such that the constant at the end of this refutation is equal to $\delta_1^{c_1} \cdots \delta_l^{c_l} \cdot L_1^{c_{l+1}} \cdots L_t^{c_{l+t}} \cdot M$ where M is the constant at the end of the original $\mathsf{Ext\text{-}PC}^{\sqrt{}}_{\mathbb{Q}}$ refutation. Suppose that $M = \frac{p}{q}$, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then, by Theorem 3.2, $\delta_1^{c_1} \cdots \delta_l^{c_l} \cdot L_1^{c_{l+1}} \cdots L_t^{c_{l+t}} \cdot p$ is divisible by every prime number less than 2^n . Since $\delta_1, \dots, \delta_l$, $L_1, \dots, L_t$ are positive integers, $\delta_1 \cdots \delta_l \cdot L_1 \cdots L_t \cdot p$ is divisible by every prime number less than 2^n . Also,

$$\log\lceil\delta_1\rceil + \cdots + \log\lceil\delta_l\rceil + \log\lceil L_1\rceil + \cdots + \log\lceil L_t\rceil + \log\lceil p\rceil \leq O(\mathrm{Size}(S)) \,,$$

because all the constants $L_1, \dots, L_t$ are products of denominators in the lines of our refutation $R_1, \dots, R_t$ and the constants $\delta_1, \dots, \delta_l$ are denominators of rationals in linear combinations used in our derivation.

On the other hand,

$$\delta_1 \cdots \delta_l \cdot L_1 \cdots L_t \cdot p \geq 2^{2^{\Omega(n)}} \,,$$

since our product is divisible by every prime number less than 2^n . Then $S \geq 2^{\Omega(n)}$. ◻

Now we prove Theorem 3.4.

Proof of Theorem 3.4. Since $R_1, \dots, R_t$ is an $\mathsf{Ext}\text{-}\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation from Γ, $R_1, \dots, R_t$ is a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation from some set $\Gamma' = \Gamma \cup \{y_1 - Q_1(\vec{x}), \dots, y_m - Q_m(\vec{x}, y_1, \dots, y_{m-1})\}$ where $Q_i \in \mathbb{Q}[\vec{x}, \vec{y}]$.

Our plan is:

- In Claim 3.6 we construct an $\mathsf{Ext}\text{-}\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation $R'_1, \dots, R'_s$ from $R_1, \dots, R_t$ that uses extension variables y'_i encoding polynomials over $\mathbb{Z}$.
- Given the derivation $R'_1, \dots, R'_s$, we construct by induction an $\mathsf{Ext}\text{-}\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation $R''_1, \dots, R''_f$, using the same extension variables.

Consider integers $M_1, \dots, M_m$ where each M_i is equal to the product of denominators of all coefficients of polynomial Q_i. We can assume that $\{M_1, \dots, M_m\}$ is a subset of $\{L_1, \dots, L_t\}$ since all the polynomials $y_i - Q_i$ should occur in our derivation.

Now we construct the $\mathsf{Ext}\text{-}\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation from Γ such that the polynomial at the end of this derivation is equal to

$$M_1^{c_1} \cdot M_2^{c_2} \cdots M_m^{c_m} \cdot \delta_1^{c_{m+1}} \cdots \delta_l^{c_{m+l}} \cdot L_1^{c_{m+l+1}} \cdots L_t^{c_{m+l+t}} \cdot R_t\,,$$

where $\{c_1, c_2, \dots, c_{m+l+t}\} \subset \mathbb{N} \cup \{0\}$.

First, we translate polynomials Q_i into integer polynomials Q'_i. Consider $Q'_1(\vec{x}) = M_1 \cdot Q_1(\vec{x})$ where M_1 is equal to the product of denominators of all coefficients of the polynomial Q_1. Then $Q'_1 \in \mathbb{Z}[\vec{x}]$ and $T_1 = M_1$. Then consider $Q'_2(\vec{x}, y'_1) = T_2 \cdot Q_2(\vec{x}, \frac{y'_1}{T_1})$ where T_2 is equal to $T_1^{\alpha_{11}} \cdot M_2$ and α_{11} is a non-negative integer chosen so that $Q'_2 \in \mathbb{Z}[\vec{x}, y'_1]$. Then for every i we consider $Q'_i(\vec{x}, y'_1, \dots, y'_{i-1}) = T_i \cdot Q_i(\vec{x}, \frac{y'_1}{T_1}, \dots, \frac{y'_{i-1}}{T_{i-1}})$ where $T_i = T_1^{\alpha_{i1}} \cdot T_2^{\alpha_{i2}} \cdots T_{i-1}^{\alpha_{ii-1}} \cdot M_i$ and $\alpha_{i1}, \dots, \alpha_{ii-1}$ are non-negative integers chosen so that $Q'_i \in \mathbb{Z}[\vec{x}, y'_1, \dots, y'_{i-1}]$. Note that we are not interested in the size of the integers α_{ij}, so they can be arbitrarily large.

Now we construct a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation $R'_1, \dots, R'_s$ from the set $\Gamma'' = \Gamma \cup \{y'_1 - Q'_1(\vec{x}), \dots y'_m - Q'_m(\vec{x}, y'_1, \dots, y'_{m-1})\}$ of the following form: this derivation duplicates the original derivation $R_1, \dots, R_t$ in all cases except when the polynomial R_i was derived by multiplying by some variable y_j from some polynomial R_k. In this case we multiply the corresponding polynomial by y'_j and then multiply it by $\frac{1}{T_j}$.

Formally, we prove the following claim:

Claim 3.6. *There is a* $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ *derivation* $R'_1, \dots, R'_s$ *from the set*
$\Gamma'' = \Gamma \cup \{y'_1 - Q'_1(\vec{x}), \dots y'_m - Q'_m(\vec{x}, y'_1, \dots, y'_{m-1})\}$ *for which the following conditions hold.*

- *For every polynomial* $R'_i(\vec{x}, y'_1, \dots, y'_m)$ *one of the following equations holds: either*

$$R'_i(\vec{x}, y_1 \cdot T_1, \dots, y_m \cdot T_m) = R_j(\vec{x}, y_1, \dots, y_m) \text{ for some } j$$

or

$$R'_i(\vec{x}, y_1 \cdot T_1, \dots, y_m \cdot T_m) = T_k \cdot R_j(\vec{x}, y_1, \dots, y_m) \text{ for some } k \text{ and } j.$$

- *If $R'_i(\vec{x}, y'_1, \dots, y'_m)$ was derived from $R'_j(\vec{x}, y'_1, \dots, y'_m)$ and $R'_k(\vec{x}, y_1, \dots, y_m)$ by taking a linear combination with rational constants α and β (which means that $R'_i = \alpha R'_j + \beta R'_k$), then one of the two conditions holds:*
  - $\alpha = \frac{1}{T_f}$ *and* $\beta = 0$ *for some* f .
  - *There is some polynomial $R_h(\vec{x}, y'_1, \dots, y'_m)$ which was derived from some polynomials R_v and R_l by using linear combination with constants α and β ($R_h = \alpha R_v + \beta R_l$).*
- *The last polynomial R_t satisfies the following polynomial equation:*

$$R'_s(x_1, \dots, x_n, T_1 \cdot y_1, \dots, T_m \cdot y_m) = R_t(x_1, \dots, x_n, y_1, \dots, y_m).$$

Proof of Claim 3.6. We construct the $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ derivation $R'_1, R'_2, \dots, R'_s$ of the set Γ'' by induction.

Induction statement: Let $R_1, \dots, R_i$ be a $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ derivation from Γ'. Then there exists a $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ derivation $R'_1, \dots, R'_p$ from Γ'' such that

- $p \le 2i$.
- For every $R_j(x_1, \dots, x_n, y_1, \dots, y_m)$ there exists an $R'_k(x_1, \dots, x_n, y'_1, \dots, y'_m)$ such that

$$R'_k(x_1, \dots, x_n, T_1 \cdot y_1, \dots, T_m \cdot y_m) = R_j(x_1, \dots, x_n, y_1, \dots, y_m).$$

- All the properties, except the last one, mentioned in the claim are true for our derivation $R'_1, \dots, R'_p$.
- The last polynomial R_i satisfies the following polynomial equation:

$$R'_p(x_1, \dots, x_n, T_1 \cdot y_1, \dots, T_m \cdot y_m) = R_i(x_1, \dots, x_n, y_1, \dots, y_m).$$

Base case: If $i = 1$ then $R_i \in \Gamma'$. If $R_i \in \Gamma$ then we can take $R'_1 = R_1$. Otherwise, if $R_i = y_j - Q_j(\vec{x})$ then we can take $R'_1 = y'_j - Q'_j(\vec{x}, y'_1, \dots, y'_{j-1})$ and $R'_2 = \frac{y'_j - Q'_j(\vec{x}, y'_1, \dots, y'_{j-1})}{T_j}$. Then it is obvious that

$$R'_2(\vec{x}, T_1 \cdot y_1, \dots, T_m \cdot y_m) = R_1(\vec{x}, y_1, \dots, y_m).$$

Induction step: Suppose we have already constructed the $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ derivation $R'_1, R'_2, \dots, R'_p$ for which the induction statement is true. Now we have five cases depending on the way the R_{i+1} is derived.

Case 1: If $R_{i+1} \in \Gamma'$ then this case is equivalent to the base case of induction.

Case 2: If $R_{i+1} = \alpha R_j + \beta R_l$ then $R'_{p+1} = \alpha R'_{j'} + \beta R'_{l'}$ where

$$R'_{j'}(x_1, \dots, x_n, T_1 \cdot y_1, \dots, T_m \cdot y_m) = R_j(x_1, \dots, x_n, y_1, \dots, y_m)$$

and

$$R'_{l'}(x_1,\dots,x_n,T_1\cdot y_1,\dots,T_m\cdot y_m) = R_l(x_1,\dots,x_n,y_1,\dots,y_m).$$

Case 3: If $R_{i+1} = x_l\cdot R_j$ then $R'_{p+1} = x_l\cdot R'_{j'}$ where

$$R'_{j'}(x_1,\dots,x_n,T_1\cdot y_1,\dots,T_m\cdot y_m) = R_j(x_1,\dots,x_n,y_1,\dots,y_m).$$

Case 4: If $R^2_{i+1} = R_j$ then we take

$$R'_{p+1}(x_1,\dots,x_n,y'_1,\dots,y'_m) = R_{i+1}(x_1,\dots,x_n,\frac{y'_1}{T_1},\dots,\frac{y'_m}{T_m})\,.$$

By the induction statement

$$R_j(x_1,\dots,x_n,y_1,\dots,y_m) = R'_{j'}(x_1,\dots,x_n,T_1\cdot y'_1,\dots,T_m\cdot y'_m)\,,$$

for some $R'_{j'}$. Thus

$$R_j(x_1,\dots,x_n,\frac{y'_1}{T_1},\dots,\frac{y'_m}{T_m}) = R'_{j'}(x_1,\dots,x_n,y'_1,\dots,y'_m).$$

So

$$R'_{p+1}(x_1,\dots,x_n,y'_1,\dots,y'_m)^2 = R_{i+1}(x_1,\dots,x_n,\frac{y'_1}{T_1},\dots,\frac{y'_m}{T_m})^2$$
$$= R_j(x_1,\dots,x_n,\frac{y'_1}{T_1},\dots,\frac{y'_m}{T_m}) = R'_{j'}(x_1,\dots,x_n,y'_1,\dots,y'_m)$$

and R'_{p+1} is derived from $R'_{j'}$.

Case 5: If $R_{i+1} = y_l\cdot R_j$ then let $R'_{p+1} = y'_l\cdot R'_{j'}$ and $R'_{p+2} = \frac{R'_{p+1}}{T_l}$ where $R'_{j'}(x_1,\dots,x_n,T_1\cdot y_1,\dots,T_m\cdot y_m) = R_j(x_1,\dots,x_n,y_1,\dots,y_m)$.

It is easy to see that in all these cases the induction statement stays true. □

Now we will show that Γ'' has a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation in which the polynomial at the end is equal to

$$M_1^{c_1}\cdot M_2^{c_2}\cdots M_m^{c_m}\cdot \delta_1^{c_{m+1}}\cdots\delta_l^{c_{m+l}}\cdot L_1^{c_{m+l+1}}\cdots L_t^{c_{m+l+t}}\cdot R_t.$$

To do this we fix a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation $R'_1,\dots,R'_s$ from Γ'' with the properties from the Claim 3.6 and construct a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation from Γ'' by induction. Moreover, we construct a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation $R''_1,\dots,R''_f$ in which every polynomial R''_i is equal to $M_1^{d_1}\cdot M_2^{d_2}\cdots M_m^{d_m}\cdot\delta_1^{d_{m+1}}\cdots\delta_l^{d_{m+l}}\cdot L_1^{d_{m+l+1}}\cdots L_t^{d_{m+l+t}}\cdot R'_i$ for some non-negative integers $d_1,\dots,d_{m+l+t}$ and some polynomial R'_i.

Informally, we multiply each line in our $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation by some constant to get a correct $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation. However, we cannot just multiply all the lines in a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation $R'_1,\dots,R'_s$

by the same constant and get a correct $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation. This happens because we can use the linear combination rule in the $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation with rational coefficients, while in $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivations we can only take a linear combination with integer coefficients. To overcome this issue, we duplicate the original $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation $R'_1, \dots, R'_s$ multiplied by some constant of the form $M_1^{d_1} \cdot M_2^{d_2} \cdots M_m^{d_m} \cdot \delta_1^{d_{m+1}} \cdots \delta_l^{d_{m+l}} \cdot L_1^{d_{m+l+1}} \cdots L_t^{d_{m+l+t}}$ every time we would like to simulate a derivation in the original proof.

Induction statement: Let $R'_1, \dots, R'_i$ be a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation from Γ'' with the properties from the Claim 3.6. Then there exists a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation $R''_1, \dots, R''_f$ from Γ'' such that

- $f \leq 2i^2$.
- There is a constant $F_i = M_1^{b_1} \cdot M_2^{b_2} \cdots M_m^{b_m} \cdot \delta_1^{b_{m+1}} \cdots \delta_l^{b_{m+l}} \cdot L_1^{b_{m+l+1}} \cdots L_t^{b_{m+l+t}} \in \mathbb{N}$ such that

$$F_i \cdot R'_1 = R''_{f-i+1},\ F_i \cdot R'_2 = R''_{f-i+2},\ \dots,\ F_i \cdot R'_i = R''_f.$$

Base case: If $i = 1$ then $R'_i \in \Gamma''$. Then we can take $R''_1 = R'_i$.

Induction step: Suppose we have already constructed the $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation $R''_1, R''_2, \dots, R''_f$ for which the induction statement is true. Then there are four cases depending on the way the R'_{i+1} is derived.

Case 1: If $R'_{i+1} \in \Gamma''$ then $F_{i+1} = F_i$ and

$$\begin{aligned} R''_{f+1} &= R'_{i+1}, \\ R''_{f+2} &= F_{i+1} \cdot R'_1, \\ R''_{f+3} &= F_{i+1} \cdot R'_2, \\ &\dots, \\ R''_{f+i+1} &= F_{i+1} \cdot R'_i, \\ R''_{f+i+2} &= F_{i+1} \cdot R'_{i+1} \end{aligned}$$

Case 2: If $R'_{i+1} = x_j R'_l$ or $R'_{i+1} = y'_j R'_l$ then $F_{i+1} = F_i$,

$$\begin{aligned} R''_{f+1} &= F_{i+1} \cdot R'_1, \\ R''_{f+2} &= F_{i+1} \cdot R'_2, \\ &\dots, \\ R''_{f+i} &= F_{i+1} \cdot R'_i \end{aligned}$$

and $R''_{f+i+1} = x_j R''_{f-i+l} = F_{i+1} \cdot R'_{i+1}$ or $R''_{f+i+1} = y'_j R''_{f-i+l} = F_{i+1} \cdot R'_{i+1}$.

Case 3: If $R'_{i+1} = \alpha R'_j + \beta R'_k$ where $\alpha = \frac{p_1}{q_1}$ and $\beta = \frac{p_2}{q_2}$ with $\{p_1, q_1, p_2, q_2\} \subset \mathbb{Z}$, then we take $F_{i+1} = q_1 q_2 F_i$,

$$\begin{aligned} R''_{f+1} &= q_1 q_2 \cdot R''_{f-i+1} = F_{i+1} \cdot R'_1, \\ R''_{f+2} &= q_1 q_2 \cdot R''_{f-i+2} = F_{i+1} \cdot R'_2, \\ &\dots, \\ R''_{f+i} &= q_1 q_2 \cdot R''_f = F_{i+1} R'_i \end{aligned}$$

and $R''_{f+i+1} = p_1 q_2 \cdot R''_{f-i+j} + p_2 q_1 \cdot R''_{f-i+k} = F_{i+1} R'_{i+1}$. From Claim 3.6 we know that $\alpha = \frac{1}{T_k}$ for some k and $\beta = 0$, or q_2 and q_1 are equal to some δ_k and δ_r . From the induction statement

$$F_i = M_1^{b_1} \cdot M_2^{b_2} \cdots M_m^{b_m} \cdot \delta_1^{b_{m+1}} \cdots \delta_l^{b_{m+l}} \cdot L_1^{b_{m+l+1}} \cdots L_t^{b_{m+l+t}}.$$

Then, since $T_k = M_1^{r_{1k}} \cdots M_m^{r_{mk}}$,

$$F_{i+1} = M_1^{b'_1} \cdot M_2^{b'_2} \cdots M_m^{b'_m} \cdot \delta_1^{b'_{m+1}} \cdots \delta_l^{b'_{m+l}} \cdot L_1^{b'_{m+l+1}} \cdots L_t^{b'_{m+l+t}},$$

and the induction statement stays true.
Case 4: Suppose $R'^2_{i+1} = R'_j$. We have that

$$R'_{i+1}(x_1, \dots, x_n, y'_1, \dots, y'_m) = R_k(x_1, \dots, x_n, \frac{y'_1}{T_1}, \dots, \frac{y'_m}{T_m})$$

or

$$R'_{i+1}(x_1, \dots, x_n, y'_1, \dots, y'_m) = T_h \cdot R_k(x_1, \dots, x_n, \frac{y'_1}{T_1}, \dots, \frac{y'_m}{T_m}),$$

for some h . Then let $M' = L_k \cdot T_1^{\alpha_1} \cdot T_2^{\alpha_2} \cdots T_m^{\alpha_m} = L_k \cdot M_1^{\alpha'_1} \cdot M_2^{\alpha'_2} \cdots M_m^{\alpha'_m}$ for some non-negative integers $\alpha_1, \dots, \alpha_m$, such that $M' \cdot R'_{i+1}$ is an integer polynomial. Such integers $\alpha_1, \dots, \alpha_m$ exist since L_k is the product of all denominators of coefficients of polynomial R_k .

Then let $F_{i+1} = M' \cdot F_i$. It is obvious that $F_{i+1} \cdot R'_{i+1}$ is an integer polynomial. Then we can construct the following $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation:

$$\begin{aligned} R''_{f+1} &= F_i (M')^2 \cdot R''_{f-i+j} = (F_i M')^2 \cdot R'_j, \\ R''_{f+2} &= M' \cdot R''_{f-i+1} = F_{i+1} \cdot R'_1, \\ R''_{f+3} &= M' \cdot R''_{f-i+2} = F_{i+1} \cdot R'_2, \\ &\dots, \\ R''_{f+i+1} &= M' \cdot R''_f = F_{i+1} R'_i. \end{aligned}$$

Then we take $R''_{f+i+2} = F_i M' \cdot R'_{i+1}$ and since $R''_{f+1} = (F_i M')^2 \cdot R'_j$, we have that $(R''_{f+i+2})^2 = R''_{f+1}$ and we get a valid $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation.

Since $M' = L_k \cdot M_1^{\alpha'_1} \cdot M_2^{\alpha'_2} \cdots M_m^{\alpha'_m}$

$$F_{i+1} = M_1^{b'_1} \cdot M_2^{b'_2} \cdots M_m^{b'_m} \cdot \delta_1^{b'_{m+1}} \cdots \delta_l^{b'_{m+l}} \cdot L_1^{b'_{m+l+1}} \cdots L_t^{b'_{m+l+t}},$$

and the induction statement stays true.

So now we have a $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\sqrt{}}$ derivation from Γ such that the polynomial at the end of this derivation is equal to $M_1^{c_1} \cdot M_2^{c_2} \cdots M_m^{c_m} \cdot \delta_1^{c_{m+1}} \cdots \delta_l^{c_{m+l}} \cdot L_1^{c_{m+l+1}} \cdots L_t^{c_{m+l+t}} \cdot R'_s$. Also, from Claim 3.6,

$$R'_s(x_1, \dots, x_n, T_1 \cdot y_1, \dots, T_m \cdot y_m) = R_t(x_1, \dots, x_n, y_1, \dots, y_m).$$

However, since $R_t \in \mathbb{Q}[\vec{x}]$, we have that $R'_s(\vec{x}) = R_t(\vec{x})$. Then we have constructed the $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}^{\sqrt{}}$ derivation from Γ in which the polynomial at the end equals $M_1^{c_1} \cdot M_2^{c_2} \cdots M_m^{c_m} \cdot \delta_1^{c_{m+1}} \cdots \delta_l^{c_{m+l}} \cdot L_1^{c_{m+l+1}} \cdots L_t^{c_{m+l+t}} \cdot R_t$. □

4 Connection between Res-Lin , $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\sqrt{}}$ and $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$

Following [29], we define the Res-Lin proof system. To simplify our calculations, we use the following notation:

Definition 4.1 (Inner product notation)**.** For a vector $(a_1, \dots, a_n) \in R^n$ we define $\langle \vec{a}, \vec{x} \rangle$ to be the following polynomial in the variables $x_1, \dots, x_n$:

$$\langle \vec{a}, \vec{x} \rangle = a_1 x_1 + \ldots + a_n x_n .$$

Definition 4.2. A **disjunction of linear equations** is of the following general form:

$$\left(\left\langle \vec{a}^{(1)}, \vec{x} \right\rangle = a_0^{(1)}\right) \vee \cdots \vee \left(\left\langle \vec{a}^{(t)}, \vec{x} \right\rangle = a_0^{(t)}\right) \tag{1}$$

where $t \geq 0$, R is an integral domain, and the coefficients are $a_i^{(j)} \in R$ for all $0 \leq i \leq n$ and $1 \leq j \leq t$. The semantics of such a disjunction is the natural one: an assignment of values from R to the variables $x_1, \dots, x_n$ satisfies (1) if and only if there exists $j \in \{1, \dots, t\}$ so that the equation $a_1^{(j)} x_1 + \ldots + a_n^{(j)} x_n = a_0^{(j)}$ holds under the given assignment.

The next definition applies to disjunctions of linear equations either with integer or with rational coefficients, and with the integers written either in unary or in binary. We refer to Def. 2.1 for the size of integers and rationals, both in unary and in binary notation.

Definition 4.3 (Size of disjunction of linear equations)**.** For a linear equation $f : a_1 x_1 + \cdots + a_n x_n = a_0$ with integer or rational coefficients, written in unary or in binary, we write $\mathrm{Size}(f) = \sum_{i=0}^{n} \mathrm{Size}(a_i)$. For a disjunction $g = f_1 \vee \cdots \vee f_t$ of t linear equations, we write $\mathrm{Size}(g) = \sum_{j=1}^{t} \mathrm{Size}(f_j)$.

Definition 4.4. Let $K := \{K_1, \ldots, K_m\}$ be a set of disjunctions of linear equations over an integral domain R. A $\mathsf{Res\text{-}Lin}_R$ proof from K of a disjunction of linear equations D is a finite sequence $\pi = (D_1, \ldots, D_l)$ of disjunctions of linear equations over R, such that $D_l = D$ and for every $i \in \{1, \ldots, l\}$, either $D_i = K_j$ for some $j \in \{1, \ldots, m\}$, or D_i is a Boolean axiom $(x_h = 0) \vee (x_h = 1)$ for some $h \in \{1, \ldots, n\}$, or D_i was deduced by one of the following Res-Lin inference rules, using D_j, D_k for some $j, k < i$:

- **Resolution**: Let A, B be two, possibly empty, disjunctions of linear equations and let L_1, L_2 be two linear equations. From $A \vee L_1$ and $B \vee L_2$ derive $A \vee B \vee (\alpha L_1 + \beta L_2)$ where $\alpha, \beta \in R$.

- **Weakening**: From a (possibly empty) disjunction of linear equations A derive $A \vee L$, where L is an arbitrary linear equation over the variables $x_1, \ldots, x_n$.

- **Simplification**: From $A \vee (k = 0)$ derive A, where A is a, possibly empty, disjunction of linear equations and $k \in R \setminus \{0\}$ is a constant.

- **Idempotency rule**: From $A \vee L \vee L$ derive $A \vee L$, where A is a, possibly empty, disjunction of linear equations and L is a linear equation.

Note that we assume that the order of equations in the disjunction is not significant, and we explicitly contract identical equations.

A Res-Lin *refutation* of a collection of disjunctions of linear equations K is a proof of the empty disjunction from K. The *size* of a Res-Lin proof π is the total size of all the disjunctions of linear equations in π.

If all coefficients in our $\mathsf{Res\text{-}Lin}_{\mathbb{Z}}$ proof π are written in *unary* then we call this proof system Unary $\mathsf{Res\text{-}Lin}_{\mathbb{Z}}$. Otherwise, in $\mathsf{Res\text{-}Lin}_{\mathbb{Z}}$ without further specification all coefficients are written in *binary*.

Remark 4.5. In the original Res-Lin proof system (see [29]), duplicate linear equations can be discarded from the disjunction. Instead, our definition uses the *idempotency* rule explicitly. It is easy to see that these variants of the Res-Lin system polynomially simulate each other. Also, the original Res-Lin proof system was defined only for disjunctions of *integer* linear equations.

Definition 4.6. Let D be a disjunction of linear equations:

$$\left(\left\langle \vec{a}^{(1)}, \vec{x} \right\rangle = a_0^{(1)}\right) \vee \cdots \vee \left(\left\langle \vec{a}^{(t)}, \vec{x} \right\rangle = a_0^{(t)}\right).$$

We denote by $\widehat{D}$ its translation into the following system of polynomial equations:

$$y_1 \cdot y_2 \cdots y_t = 0$$

$$\begin{aligned} y_1 &= \left\langle \vec{a}^{(1)}, \vec{x} \right\rangle - a_0^{(1)}, \\ y_2 &= \left\langle \vec{a}^{(2)}, \vec{x} \right\rangle - a_0^{(2)}, \\ &\dots, \\ y_t &= \left\langle \vec{a}^{(t)}, \vec{x} \right\rangle - a_0^{(t)} \end{aligned}$$

If D is the empty disjunction, we define $\widehat{D}$ to be the single polynomial equation $1 = 0$.

Now we prove that $\Sigma\Pi\Sigma$-$\mathsf{PC}_{\mathbb{Q}}^{\surd}$ p-simulates Res-Lin and $\Sigma\Pi\Sigma$-$\mathsf{PC}_{\mathbb{Q}}$ p-simulates Unary Res-$\mathsf{Lin}_{\mathbb{Z}}$.

4.1 $\Sigma\Pi\Sigma$-$\mathsf{PC}_{\mathbb{Q}}^{\surd}$ simulation of Res-$\mathsf{Lin}_{\mathbb{Z}}$

Theorem 4.7. *Let $\pi = (D_1, \dots, D_l)$ be a Res-$\mathsf{Lin}_{\mathbb{Z}}$ proof of D_l from a collection of initial disjunctions of linear equations $Q_1, \dots, Q_m$ over the variables $x_1, \dots, x_n$. Also consider $L_1, \dots, L_t$ — all affine forms that occur in the disjunctions in our Res-$\mathsf{Lin}_{\mathbb{Z}}$ proof sequence.*

Then, there exists a $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ proof of $\widehat{D}_l$ from

$$\widehat{Q}_1 \cup \dots \cup \widehat{Q}_m \cup \{y_1 = L_1, y_2 = L_2, \dots, y_t = L_t\} \cup \{x_1^2 = x_1, \dots, x_n^2 = x_n\}$$

of size at most $O(p(\mathrm{Size}(\pi)))$ for some polynomial p.

Proof. We proceed by induction on the number of lines in π.
Base case: A Res-$\mathsf{Lin}_{\mathbb{Z}}$ axiom Q_i is translated into $\widehat{Q_i}$ and the Boolean axiom $(x_i = 0) \vee (x_i = 1)$ is translated to $x_i^2 - x_i = 0$.
Induction step: Now we simulate all the Res-$\mathsf{Lin}_{\mathbb{Z}}$ derivation rules in $\mathsf{PC}_{\mathbb{Q}}^{\surd}$.

- **Resolution**: Assume that $D_i = A \vee B \vee (\alpha L_1 + \beta L_2)$ where $D_j = A \vee L_1$ and $D_k = B \vee L_2$. Then, we have already derived polynomial equations

$$\begin{aligned} y_{j1} &= \left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle - a_{j0}^{(1)}, \quad \dots, \quad y_{jt_j} = \left\langle \vec{a}_j^{(t_j)}, \vec{x} \right\rangle - a_{j0}^{(t_j)}, \\ y_{k1} &= \left\langle \vec{a}_k^{(1)}, \vec{x} \right\rangle - a_{k0}^{(1)}, \quad \dots, \quad y_{kt_k} = \left\langle \vec{a}_k^{(t_k)}, \vec{x} \right\rangle - a_{k0}^{(t_k)}, \\ & y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0, \quad y_{k1} \cdot y_{k2} \cdots y_{kt_k} = 0 \end{aligned}$$

  where

$$\begin{aligned} A &= \left(\left\langle \vec{a}_j^{(2)}, \vec{x} \right\rangle = a_{j0}^{(2)} \right) \vee \dots \vee \left(\left\langle \vec{a}_j^{(t_j)}, \vec{x} \right\rangle = a_{j0}^{(t_j)} \right), \\ B &= \left(\left\langle \vec{a}_k^{(2)}, \vec{x} \right\rangle = a_{k0}^{(2)} \right) \vee \dots \vee \left(\left\langle \vec{a}_k^{(t_k)}, \vec{x} \right\rangle = a_{k0}^{(t_k)} \right), \\ L_1 &= \left(\left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle = a_{j0}^{(1)} \right), \ L_2 = \left(\left\langle \vec{a}_k^{(1)}, \vec{x} \right\rangle = a_{k0}^{(1)} \right). \end{aligned}$$

Then we derive $y_{j1} \cdot y_{j2} \cdots y_{jt_j} \cdot y_{k2} \cdots y_{kt_k} = 0$, $y_{k1} \cdot y_{j2} \cdots y_{jt_j} \cdot y_{k2} \cdots y_{kt_k} = 0$ and thus $(\alpha y_{j1} + \beta y_{k1}) \cdot y_{j2} \cdots y_{jt_j} \cdot y_{k2} \cdots y_{kt_k} = 0$. Then there is an equation $y_i = L_i$ from the set $\{y_1 = L_1, y_2 = L_2, \ldots, y_t = L_t\}$ for which

$$L_i = \alpha \left(\left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle - a_{j0}^{(1)} \right) + \beta \left(\left\langle \vec{a}_k^{(1)}, \vec{x} \right\rangle - a_{k0}^{(1)} \right).$$

Then we derive $y_i = \alpha y_{j1} + \beta y_{k1}$ and $y_i \cdot y_{j2} \cdots y_{jt_j} \cdot y_{k2} \cdots y_{kt_k} = 0$, which together with the corresponding linear equations for $y_i, y_{j2}, \ldots, y_{jt_j}, y_{k2}, \ldots, y_{kt_k}$ give $\widehat{D}_i$.

- **Weakening**: Assume that $D_i = D_j \vee L$ where L is a linear equation. Then, we have already derived polynomial equations

$$y_{j1} = \left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle - a_{j0}^{(1)}, \ \ldots, \ y_{jt_j} = \left\langle \vec{a}_j^{(t_j)}, \vec{x} \right\rangle - a_{j0}^{(t_j)},$$
$$y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0.$$

There is a variable y_0 for which $y_0 = b_1 x_1 + \ldots + b_n x_n - b_0$ where L is a linear equation $b_1 x_1 + \ldots + b_n x_n = b_0$. From $y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0$ we derive $y_0 \cdot y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0$, which together with the corresponding linear equations for $y_0, y_{j1}, y_{j2}, \ldots, y_{jt_j}$ gives us $\widehat{D}_i$.

- **Simplification**: Suppose that $D_i = A$ and $D_j = A \vee (k = 0)$ where $k \in \mathbb{Z}$, $k \neq 0$. Then, we have already derived polynomial equations

$$y_{j1} = \left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle - a_{j0}^{(1)}, \ \ldots, y_{jt_j-1} = \left\langle \vec{a}_j^{(t_j-1)}, \vec{x} \right\rangle - a_{j0}^{(t_j-1)}, \ y_{jt_j} = k,$$
$$y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0.$$

From equation $y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0$ we can derive equation $y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} \cdot k = 0$ from which we derive $y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} = 0$. Together with the corresponding linear equations for $y_{j1}, y_{j2}, \ldots, y_{jt_j-1}$ this equation gives us $\widehat{D}_i$.

- **Idempotency rule**: Assume that $D_i = A \vee L$ and $D_j = A \vee L \vee L$ where L is a linear equation. Then, we have already derived polynomial equations

$$y_{j1} = \left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle - a_{j0}^{(1)}, \ \ldots, \ y_{jt_j-1} = y_{jt_j} = \left\langle \vec{a}_j^{(t_j-1)}, \vec{x} \right\rangle - a_{j0}^{(t_j-1)},$$
$$y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} \cdot y_{jt_j} = 0.$$

Then we can derive $y_{jt_j-1} = y_{jt_j}$ and $y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot (y_{jt_j-1}^2) = 0$. Using multiplication we derive $y_{j1}^2 \cdot y_{j2}^2 \cdots y_{jt_j-2}^2 \cdot (y_{jt_j-1}^2) = 0$ from which we derive the equation $y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} = 0$ by using the square root rule. This equation together with the corresponding linear equations for $y_{j1}, y_{j2}, \ldots, y_{jt_j-1}$ gives us $\widehat{D}_i$.

Having the polynomial simulation of every $\mathsf{Res}\text{-}\mathsf{Lin}_{\mathbb{Z}}$ derivation rule, we can conclude our proof. ◻

Corollary 4.8. *Suppose we have a* Res-Lin$_{\mathbb{Z}}$ *refutation* π *of a collection of linear equations* $Q_1, \ldots, Q_m$ *over variables* $x_1, \ldots, x_n$ *. Then, there exists a* $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}^{\surd}$ *refutation of*

$$\widehat{Q}_1 \cup \ldots \cup \widehat{Q}_m \cup \{x_1^2 = x_1, \ldots, x_n^2 = x_n\}$$

of size at most $O(p(\mathrm{Size}(\pi)))$ *for some polynomial* p *.*

Proof. For each affine form L in a Res-Lin$_{\mathbb{Z}}$ refutation π we introduce a new variable $y = L$ via the extension rule. Then, we can apply Theorem 4.7 to construct an $O(p(\mathrm{Size}(\pi)))$ refutation. □

Now we will show that our lower bound provides an interesting counterpart to a result from [24].

Theorem 4.9 ([24])**.** *Any* Res-Lin$_{\mathbb{Z}}$ *refutation of* $1 + x_1 + \ldots + 2^{n-1}x_n = 0$ *has size* $2^{\Omega(n)}$ *.*

Proof. By Theorem 3.5, any Ext-PC$_{\mathbb{Q}}^{\surd}$ refutation of BVP$_n$ requires size $2^{\Omega(n)}$. Since Ext-PC$_{\mathbb{Q}}^{\surd}$ polynomially simulates the $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}^{\surd}$ proof system, from Corollary 4.8 we get that there is a polynomial p such that for any Res-Lin$_{\mathbb{Z}}$ refutation of BVP$_n$ of size S the equation $p(S) \geq C_0 \cdot 2^{C_1 \cdot n}$ holds. Then for some constant C the equation $S \geq 2^{C \cdot n}$ holds. □

4.2 $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}$ simulation of Unary Res-Lin$_{\mathbb{Z}}$

In this section we show that we do not need the square root derivation rule to simulate Res-Lin with unary coefficients.

Theorem 4.10. *Let* $\pi = (D_1, \ldots, D_l)$ *be an* Unary Res-Lin$_{\mathbb{Z}}$ *proof sequence of* D_l *from a collection of initial disjunctions of linear equations* $Q_1, \ldots, Q_m$ *. Then, there exists a* $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}$ *proof of* $\widehat{D}_l$ *from* $\widehat{Q}_1 \cup \ldots \cup \widehat{Q}_m$ *of size at most* $O(p(\mathrm{Size}(\pi)))$ *for some polynomial* p *.*

Proof. To prove this theorem we will use the following lemma from [18]:

Lemma 4.11 ([18], revision 2 of the ECCC report, lemma 7, p.32)**.** *Let* Γ *be the following set of polynomial equations:*

$$\begin{gathered} x_0 = f(\vec{x}), \quad x_1 = f(\vec{x}) - 1, \quad \ldots, \quad x_a = f(\vec{x}) - a, \\ y_0 = g(\vec{x}), \quad y_1 = g(\vec{x}) - 1, \quad \ldots, \quad y_b = g(\vec{x}) - b, \\ x_0 \cdot x_1 \cdot x_2 \cdots x_a = 0, \quad y_0 \cdot y_1 \cdot y_2 \cdots y_b = 0, \end{gathered}$$

where f *and* g *are affine forms over variables* $\vec{x}$ *. Then we can introduce new variables* $z, z_1, \ldots, z_{a+b}$ *using the following* $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}$ *extension rule:*

$$z_0 = f(\vec{x}) + g(\vec{x}), \quad z_1 = f(\vec{x}) + g(\vec{x}) + 1, \quad z_2 = f(\vec{x}) + g(\vec{x}) + 2, \quad \ldots, \quad z_{a+b} = f(\vec{x}) + g(\vec{x}) + a + b,$$

and derive equation

$$z_0 \cdot z_1 \cdot z_2 \cdots z_{a+b} = 0.$$

from Γ *in* $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}$ *with a derivation of size* $poly(ab)$ *and using only extensions of the original variables* $\vec{x}$ *.*

We prove Theorem 4.10 by induction on the lines of π .

Base case: An Unary Res-Lin$_{\mathbb{Z}}$ axiom Q_i is translated to $\widehat{Q_i}$ and the Boolean axiom $(x_i = 0) \vee (x_i = 1)$ is translated to $x_i^2 - x_i = 0$.

Induction step: Now we simulate all the Unary Res-Lin$_{\mathbb{Z}}$ derivation rules in $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}$.

- **Resolution**, **Weakening**, **Simplification** rules: the simulation is the same as in Theorem 4.7.
- **Idempotency rule**: Assume that $D_i = A \vee L$ and $D_j = A \vee L \vee L$ where L is a linear equation. Then, we have already derived polynomial equations

$$y_{j1} = \left\langle \vec{a}_j^{(1)}, \vec{x} \right\rangle - a_{j0}^{(1)}, \ \ldots, \ y_{jt_j-1} = y_{jt_j} = \left\langle \vec{a}_j^{(t_j-1)}, \vec{x} \right\rangle - a_{j0}^{(t_j-1)},$$

$$y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} \cdot y_{jt_j} = 0.$$

Then we can derive $y_{jt_j-1} = y_{jt_j}$ and $y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot (y_{jt_j-1}^2) = 0$.

Now consider the equation $y_{jt_j-1} = a_{j1}^{(t_j-1)} x_1 + a_{j2}^{(t_j-1)} x_2 + \ldots + a_{jn}^{(t_j-1)} x_n - a_{j0}^{(t_j-1)}$. Using the extension rule we can introduce new variables

$$\begin{aligned} &z_{-M_1}^{(1)}, z_{-M_1+1}^{(1)}, \ldots, z_{M_1-1}^{(1)}, z_{M_1}^{(1)}, \\ &z_{-M_2}^{(2)}, z_{-M_2+1}^{(2)}, \ldots, z_{M_2-1}^{(2)}, z_{M_2}^{(2)}, \\ &\ldots, \\ &z_{-M_n}^{(n)}, z_{-M_n+1}^{(n)}, \ldots, z_{M_n-1}^{(n)}, z_{M_n}^{(n)}, \end{aligned}$$

with the following equations for each $1 \le i \le n$:

$$\begin{aligned} z_{-M_i}^{(i)} &= a_{j1}^{(t_j-1)} x_1 + \ldots + a_{ji}^{(t_j-1)} x_i - a_{j0}^{(t_j-1)} - M_i , \\ z_{-M_i+1}^{(i)} &= a_{j1}^{(t_j-1)} x_1 + \ldots + a_{ji}^{(t_j-1)} x_i - a_{j0}^{(t_j-1)} - M_i + 1, \\ &\ldots, \\ z_{M_i-1}^{(i)} &= a_{j1}^{(t_j-1)} x_1 + \ldots + a_{ji}^{(t_j-1)} x_i - a_{j0}^{(t_j-1)} + M_i - 1, \\ z_{M_i}^{(i)} &= a_{j1}^{(t_j-1)} x_1 + \ldots + a_{ji}^{(t_j-1)} x_i - a_{j0}^{(t_j-1)} + M_i , \end{aligned}$$

where $M_i = |a_{j0}^{(t_j-1)}| + |a_{j1}^{(t_j-1)}| + \ldots + |a_{ji}^{(t_j-1)}|$ for $1 \le i \le n$.

Now, having the equation $(a_{j1}^{(t_j-1)} x_1) \cdot (a_{j1}^{(t_j-1)} x_1 - a_{j1}^{(t_j-1)}) = 0$ from the Boolean axiom for the variable x_1 , we can derive using Lemma 4.11 that

$$z_{-M_1}^{(1)} \cdot z_{-M_1+1}^{(1)} \cdots z_{M_1-1}^{(1)} \cdot z_{M_1}^{(1)} = 0.$$

In this case, we take $f(\vec{x}) = a_{j1}^{(t_j-1)} x_1 + |a_{j1}^{(t_j-1)}|$, $g(\vec{x}) = |a_{j0}^{(t_j-1)}|$, $a = 2|a_{j1}^{(t_j-1)}|$, $b = 2|a_{j0}^{(t_j-1)}|$.

After that again using Lemma 4.11, we can derive the following equations one by one:

$$z^{(i)}_{-M_i} \cdot z^{(i)}_{-M_i+1} \cdots z^{(i)}_{M_i-1} \cdot z^{(i)}_{M_i} = 0.$$

In order to do so for each $2 \le i \le n$ we take $f(\vec{x}) = a^{(t_j-1)}_{j1} x_1 + \ldots + a^{(t_j-1)}_{ji-1} x_{i-1} - a^{(t_j-1)}_{j0} + M_{i-1}$, $g(\vec{x}) = a^{(t_j-1)}_{ji} x_i + |a^{(t_j-1)}_{ji}|$, $a = 2M_{i-1}$, $b = 2|a^{(t_j-1)}_{ji}|$. Here we use the Boolean axioms for the variables $x_2, \ldots, x_n$ to derive $(a^{(t_j-1)}_{ji} x_i) \cdot (a^{(t_j-1)}_{ji} x_i - a^{(t_j-1)}_{ji}) = 0$.

Informally, each equation of the form $z^{(i)}_{-M_i} \cdot z^{(i)}_{-M_i+1} \cdots z^{(i)}_{M_i-1} \cdot z^{(i)}_{M_i} = 0$ encodes the fact that the value of $a^{(t_j-1)}_{j1} x_1 + \ldots + a^{(t_j-1)}_{ji} x_i - a^{(t_j-1)}_{j0}$ lies inside $[-M_i, M_i]$ for any Boolean assignment of variables.

Finally, we derive the following system of equations:

$$\begin{aligned}
z^{(n)}_{-M_n} &= \left\langle \vec{a}^{(t_j-1)}_j, \vec{x} \right\rangle - a^{(t_j-1)}_{j0} - M_n\,,\\
z^{(n)}_{-M_n+1} &= \left\langle \vec{a}^{(t_j-1)}_j, \vec{x} \right\rangle - a^{(t_j-1)}_{j0} - M_n + 1,\\
&\ldots,\\
z^{(n)}_{M_n-1} &= \left\langle \vec{a}^{(t_j-1)}_j, \vec{x} \right\rangle - a^{(t_j-1)}_{j0} + M_n - 1,\\
z^{(n)}_{M_n} &= \left\langle \vec{a}^{(t_j-1)}_j, \vec{x} \right\rangle - a^{(t_j-1)}_{j0} + M_n\,,\\
z^{(n)}_{-M_n} \cdot z^{(n)}_{-M_n+1} &\cdots z^{(n)}_{M_n-1} \cdot z^{(n)}_{M_n} = 0,
\end{aligned}$$

from which we derive that

$$\begin{aligned}
z^{(n)}_{-M_n} &= y_{jt_j-1} - M_n,\\
z^{(n)}_{-M_n+1} &= y_{jt_j-1} - M_n + 1,\\
&\ldots,\\
z^{(n)}_{M_n-1} &= y_{jt_j-1} + M_n - 1,\\
z^{(n)}_{M_n} &= y_{jt_j-1} + M_n,
\end{aligned}$$

where $M_n = |a^{(t_j-1)}_{j0}| + |a^{(t_j-1)}_{j1}| + |a^{(t_j-1)}_{j2}| + \ldots + |a^{(t_j-1)}_{jn}|$. Then, having the equations $z^{(n)}_k = y_{jt_j-1} + k$, we can substitute $y_{jt_j-1} + k$ for each $z^{(n)}_k$ into the equation $z^{(n)}_{-M_n} \cdot z^{(n)}_{-M_n+1} \cdots z^{(n)}_{M_n-1} \cdot z^{(n)}_{M_n} = 0$ one by one and get

$$h(y_{jt_j-1}) = 0,$$

where $h(y_{jt_j-1}) = b_1 \cdot y_{jt_j-1} + b_2 \cdot y^2_{jt_j-1} + \ldots + b_{2M_n+1} \cdot y^{2M_n+1}_{jt_j-1}$ is a polynomial from $\mathbb{Z}[y_{jt_j-1}]$ and $b_1 = ((M_n)!)^2 \cdot (-1)^{M_n}$. Then we derive the following equation by using the multiplication rule:

$$y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot h(y_{jt_j-1}) = b_1 \cdot y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot y_{jt_j-1} + \\ + y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot (y_{jt_j-1}^2) \cdot (b_2 + b_3 \cdot y_{jt_j-1} + \ldots + b_{2M_n+1} \cdot y_{jt_j-1}^{2M_n-1}) = 0.$$

Now, using the equation $y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot (y_{jt_j-1}^2) = 0$ we derive $b_1 \cdot y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot y_{jt_j-1} = 0$ and since $b_1 \neq 0$ we derive $y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot y_{jt_j-1} = 0$. This equation together with the corresponding linear equations for $y_{j1}, y_{j2}, \ldots, y_{jt_j-1}$ gives $\widehat{D}_i$. ◻

4.3 $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$ cannot simulate the square root derivation rule

The following statement shows that the square root rule cannot be eliminated in $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\sqrt{}}$ derivations. As a corollary of this theorem we get that the simulation from Theorem 4.7 does not apply to $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$.

Theorem 4.12. *Any* $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$*-derivation of*

$$1 + x_1 + \ldots + 2^{n-1}x_n = 0$$

from the equation

$$(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$$

requires size $2^{\Omega(n)}$.

Proof. The proof of this theorem essentially mimics the proof of Theorem 3.5 and consists of two parts. First, we prove the following claim.

Claim 4.13. *For any* $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}$*-derivation of* $M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ *from the equation* $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ *where* $M \in \mathbb{Z} \setminus \{0\}$, *the constant* M *is divisible by every prime number less than* 2^n.

Second, we apply Theorem 3.4 to prove that for every $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$-derivation of $(1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ from the equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ there is an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}$-derivation of $M_1^{\alpha_1} \cdots M_k^{\alpha_k} \cdot (1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ from the equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ where $M_i \in \mathbb{Z}$, $M_i \neq 0$, and the M_i are denominators from the original $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$-derivation. Then $M_1 \cdots M_k$ is divisible by all prime numbers less than 2^n and thus the size of the original $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$-derivation is $2^{\Omega(n)}$.

Proof of Claim 4.13. Assume that $R_1, \ldots, R_t$ is an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}$-derivation of $M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ from the equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$. Then $R_1, \ldots, R_t$ is a $\mathsf{PC}_{\mathbb{Z}}$-derivation from some set

$$\Gamma' = \{G(\vec{x}), F_1(\vec{x}), \ldots, F_n(\vec{x}), y_1 - Q_1(\vec{x}), \ldots y_m - Q_m(\vec{x}, y_1, \ldots, y_{m-1})\},$$

where $G(\vec{x}) = (1 + \sum_{i=1}^n 2^{(i-1)}x_i)^2$, $F_i(\vec{x}) = x_i^2 - x_i$, $Q_i \in \mathbb{Z}[\vec{x}, y_1, \ldots, y_{i-1}]$ and $R_t = M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n)$.

Now consider an arbitrary integer $0 \leq k < 2^n$ and its binary representation $b_1, \dots, b_n$. Then

$$G(b_1, \dots, b_n) = (k+1)^2, \quad F_i(b_1, \dots, b_n) = b_i^2 - b_i = 0.$$

Also consider integers $c_1, \dots, c_m$ such that $c_i = Q_i(b_1, \dots, b_n, c_1, c_2, \dots, c_{i-1})$. Now we prove by induction that every integer $R_i(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $(k+1)^2$ and thus M is divisible by every prime number less than 2^n since $1 + b_1 + \ldots + 2^{n-1} b_n = k + 1$.

Base case: if $i = 1$, then

$$R_i = G(b_1, \dots, b_n, c_1, \dots, c_m) = (k+1)^2$$

or

$$R_i = F_i(b_1, \dots, b_n, c_1, \dots, c_m) = 0$$

or

$$R_i(b_1, \dots, b_n, c_1, \dots, c_m) = c_i - Q_i(b_1, \dots, b_n, c_1, \dots, c_{i-1}) = 0,$$

which means that R_i is divisible by $(k+1)^2$.

Induction step: suppose we know that R_j is divisible by $(k+1)^2$ for any $j \leq i$. Now we show it for R_{i+1}. There are three cases:

1. If $R_{i+1} \in \Gamma'$, then this case is equivalent to the base case and $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $(k+1)^2$.

2. If $R_{i+1} = \alpha R_j + \beta R_s$ for $\alpha, \beta \in \mathbb{Z}$ and $j, s \leq i$, then $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $(k+1)^2$ because $R_j(b_1, \dots, b_n, c_1, \dots, c_m)$ and $R_s(b_1, \dots, b_n, c_1, \dots, c_m)$ are divisible by $(k+1)^2$ and α and β are integers.

3. If $R_{i+1} = x_j R_s$ or $R_{i+1} = y_j R_s$, then $R_{i+1}(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $(k+1)^2$ because $R_s(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $(k+1)^2$ and b_i and c_i are integers.

Since every $R_i(b_1, \dots, b_n, c_1, \dots, c_m)$ is divisible by $(k+1)^2$, we know that

$$R_t(b_1, \dots, b_n, c_1, \dots, c_m) = M \cdot (k+1)$$

is divisible by $(k+1)^2$. Then M is divisible by $k+1$ and thus M is divisible by every prime number less than 2^n. ◻

Now assume that $R_1, \dots, R_t$ is an $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$-derivation of size S from an arbitrary set of equations $\Gamma \subset \mathbb{Z}[\vec{x}]$ where $R_t = 1 + x_1 + \ldots + 2^{n-1} x_n$. Then we know that $R_1, \dots, R_t$ is a $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ refutation of a set $\Gamma' = \Gamma \cup \{y_1 - Q_1(\vec{x}), \dots, y_m - Q_m(\vec{x}, y_1, \dots, y_{m-1})\}$ where $Q_i \in \mathbb{Q}[\vec{x}, \vec{y}]$. As in Theorem 3.4, we consider all products of denominators of polynomials Q_i, R_i and all denominators in linear combination derivations (derivations of the form $\alpha R_j + \beta R_s$). Let us denote those constants by T_i. We know that $\prod T_i \leq 2^{O(S)}$. From Theorem 3.4 we know that there is an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}$-derivation $R'_1, \dots, R'_f$ from the set Γ for which $R'_f = T_1^{\alpha_1} \cdots T_r^{\alpha_r} R_t$, where $\alpha_i \in \mathbb{N} \cup \{0\}$.

Then we can consider

$$\Gamma = \{(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0, x_1^2 - x_1 = 0, \ldots, x_n^2 - x_n = 0\},$$

and we know that for every $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$-derivation of $1 + x_1 + \ldots + 2^{n-1}x_n = 0$ from the equation $(1+x_1+\ldots+2^{n-1}x_n)^2 = 0$ of size S there is an $\mathsf{Ext\text{-}PC}_{\mathbb{Z}}$-derivation of $M\cdot(1+x_1+\ldots+2^{n-1}x_n) = 0$ from the equation $(1+x_1+\ldots+2^{n-1}x_n)^2 = 0$ where $M = T_1^{\alpha_1}\cdots T_r^{\alpha_r}$ and $T_1\cdots T_r \leq 2^{O(S)}$. However, from Claim 4.13 we know that M is divisible by all prime numbers less than 2^n. Then $T_1^{\alpha_1}\cdots T_r^{\alpha_r}$ is divisible by all prime numbers less than 2^n which means that $T_1\cdots T_r$ is divisible by all prime numbers less than 2^n. Then $2^{2^{\Omega(n)}} \leq T_1\cdots T_r \leq 2^{O(S)}$ which means that $S \geq 2^{\Omega(n)}$. □

5 Open Problems

1. Theorem 4.7 says that $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}^{\sqrt{}}$ p-simulates any $\mathsf{Res\text{-}Lin}$ derivation. However, from Theorem 4.12 we know that the simulation from Theorem 4.7 does not work for $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$. Is the square root rule necessary, that is, can we p-simulate $\mathsf{Res\text{-}Lin}$ refutations in the $\mathsf{Ext\text{-}PC}_{\mathbb{Q}}$ proof system?

2. A major question is whether it is possible to apply the technique from Section 3 to prove an exponential lower bound on the size of refutations of a CNF formula even in a weak extension of Polynomial Calculus such as $\Sigma\Pi\Sigma\text{-}\mathsf{PC}_{\mathbb{Z}}$.

3. Theorem 4.9 says that any $\mathsf{Res\text{-}Lin}$ refutation of BVP_n requires size $2^{\Omega(n)}$. Does an exponential lower bound on the size of $\mathsf{Res\text{-}Lin}$ refutations imply an exponential lower bound on the number of lines in $\mathsf{Res\text{-}Lin}$ refutations? Do we necessarily need large coefficients in some $\mathsf{Res\text{-}Lin}$ refutations with a small number of lines? Or is it the case that if there is a $\mathsf{Res\text{-}Lin}$ refutation with a small number of lines, then there is a $\mathsf{Res\text{-}Lin}$ refutation with a small number of lines and small coefficients?

References

[1] MIKLÓS AJTAI: The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994. Preliminary version in FOCS'88. [doi:10.1007/BF01302964] 2

[2] YAROSLAV ALEKSEEV: A lower bound for polynomial calculus with extension rule. In *Proc. 36th Comput. Complexity Conf. (CCC'21)*, pp. 21:1–18. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2021. [doi:10.4230/LIPIcs.CCC.2021.21] 6

[3] YAROSLAV ALEKSEEV, DIMA GRIGORIEV, EDWARD A. HIRSCH, AND IDDO TZAMERET: Semialgebraic proofs, IPS lower bounds, and the τ-conjecture: Can a natural number be negative? *SIAM J. Comput.*, 53(3):648–700, 2024. Preliminary version in STOC'20. [doi:10.1137/20M1374523] 4, 5, 7, 8

[4] PAUL BEAME, RUSSELL IMPAGLIAZZO, JAN KRAJÍČEK, TONIANN PITASSI, AND PAVEL PUDLÁK: Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc.*, 73(1):1–26, 1996. [doi:10.1112/plms/s3-73.1.1] 3

[5] STEPHEN BELLANTONI, TONIANN PITASSI, AND ALASDAIR URQUHART: Approximation and small-depth Frege proofs. *SIAM J. Comput.*, 21(6):1161–1179, 1992. [doi:10.1137/0221068] 2

[6] SAM BUSS, DIMA GRIGORIEV, RUSSELL IMPAGLIAZZO, AND TONIANN PITASSI: Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. System Sci.*, 62(2):267–289, 2001. [doi:10.1006/jcss.2000.1726] 3

[7] SAMUEL R. BUSS, RUSSELL IMPAGLIAZZO, JAN KRAJÍČEK, PAVEL PUDLÁK, ALEXANDER A. RAZBOROV, AND JIŘÍ SGALL: Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Comput. Complexity*, 6(3):256–298, 1996. [doi:10.1007/BF01294258] 3

[8] VAŠEK CHVÁTAL, WILLIAM J. COOK, AND MARK E. HARTMANN: On cutting-plane proofs in combinatorial optimization. *Lin. Alg. Appl.*, 114–115:455–499, 1989. [doi:10.1016/0024-3795(89)90476-X] 3

[9] MATTHEW CLEGG, JEFFERY EDMONDS, AND RUSSELL IMPAGLIAZZO: Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proc. 28th STOC*, pp. 174–183. ACM Press, 1996. [doi:10.1145/237814.237860] 3, 6, 7

[10] STEPHEN A. COOK AND ROBERT A. RECKHOW: The relative efficiency of propositional proof systems. *J. Symbolic Logic*, 44(1):36–50, 1979. This is a journal version of Cook–Reckhow, STOC'74 and Reckhow's 1976 PhD Thesis (U. Toronto). [doi:10.2307/2273702] 2, 3

[11] WILLIAM J. COOK, COLLETTE R. COULLARD, AND GYÖRGY TURÁN: On the complexity of cutting plane proofs. *Discr. Appl. Math.*, 18(1):25–38, 1987. [doi:10.1016/0166-218X(87)90039-4] 3

[12] NOAH FLEMING, PRAVESH KOTHARI, AND TONIANN PITASSI: Semialgebraic proofs and efficient algorithm design. *Found. Trends Theor. Comp. Sci.*, 14(1–2):1–221, 2019. [doi:10.1561/0400000086, ECCC:TR19-106] 3

[13] DIMA GRIGORIEV AND EDWARD A. HIRSCH: Algebraic proof systems over formulas. *Theoret. Comput. Sci.*, 303(1):83–102, 2003. [doi:doi:10.1016/S0304-3975(02)00446-2] 3, 4, 7

[14] JOSHUA A. GROCHOW AND TONIANN PITASSI: Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6):37:1–59, 2018. [doi:10.1145/3230742] 3

[15] ARMIN HAKEN: The intractability of resolution. *Theoret. Comput. Sci.*, 39(2–3):297–308, 1985. [doi:10.1016/0304-3975(85)90144-6] 2

[16] TUOMAS HAKONIEMI: Monomial size vs. bit-complexity in Sums-of-Squares and Polynomial Calculus. In *Proc. 36th Ann. ACM/IEEE Symp. on Logic in Computer Science (LICS'21)*, pp. 55:1–7. ACM Press, 2021. [doi:10.1109/LICS52264.2021.9470545] 4

[17] JOHAN HÅSTAD: On small-depth Frege proofs for Tseitin for grids. *J. ACM*, 68(1):1:1–31, 2020. [doi:10.1145/3425606] 2

[18] RUSSELL IMPAGLIAZZO, SASANK MOULI, AND TONIANN PITASSI: The surprising power of constant depth algebraic proofs. In *Proc. 35th Ann. ACM/IEEE Symp. on Logic in Computer Science (LICS'20)*, pp. 591–603. ACM Press, 2020. [doi:10.1145/3373718.3394754] 3, 4, 5, 7, 21

[19] RUSSELL IMPAGLIAZZO, PAVEL PUDLÁK, AND JIŘÍ SGALL: Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Comput. Complexity*, 8(2):127–144, 1999. [doi:10.1007/s000370050024] 3, 4

[20] DMITRY ITSYKSON AND DMITRY SOKOLOV: Resolution over linear equations modulo two. *Ann. Pure Appl. Logic*, 171(1):102722:1–31, 2020. [doi:10.1016/j.apal.2019.102722] 3

[21] JAN KRAJÍČEK: Discretely ordered modules as a first-order extension of the cutting planes proof system. *J. Symbolic Logic*, 63(4):1582–1596, 1998. [doi:10.2307/2586668] 3

[22] JAN KRAJÍČEK AND PAVEL PUDLÁK: Propositional proof systems, the consistency of first order theories and the complexity of computations. *J. Symbolic Logic*, 54(3):1063–1079, 1989. [doi:10.2307/2274765] 4

[23] RYAN O'DONNELL: SOS is not obviously automatizable, even approximately. In *Proc. 8th Innovations in Theoret. Comp. Sci. Conf. (ITCS'17)*, pp. 59:1–10. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017. [doi:10.4230/LIPIcs.ITCS.2017.59] 4

[24] FEDOR PART AND IDDO TZAMERET: Resolution with counting: Dag-like lower bounds and different moduli. *Comput. Complexity*, 30(2):1–71, 2021. Preliminary version in ITCS'20. [doi:10.1007/s00037-020-00202-x] 3, 4, 5, 8, 21

[25] TONIANN PITASSI: Algebraic propositional proof systems. In NEIL IMMERMAN AND PHOKION KOLAITIS, editors, *Descriptive Complexity and Finite Models*, volume 31 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pp. 215–244. Amer. Math. Soc., 1997. 3

[26] TONIANN PITASSI: Unsolvable systems of equations and proof complexity. In *Proc. Internat. Congress of Mathematicians, Vol. III (Berlin, 1998)*, pp. 451–460. Documenta Mathematica, 1998. Accessible at EMS Press. 3

[27] TONIANN PITASSI AND RAHUL SANTHANAM: Effectively polynomial simulations. In *Proc. 1st Innovations in Comp. Sci. Conf. (ICS'10)*, pp. 370–382. Tsinghua U., 2010. Accessible at Tsinghua U. 3

[28] PRASAD RAGHAVENDRA AND BENJAMIN WEITZ: On the bit complexity of Sum-of-Squares proofs. In *Proc. 44th Internat. Colloq. on Automata, Languages, and Programming (ICALP'17)*, pp. 80:1–13. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017. [doi:10.4230/LIPIcs.ICALP.2017.80] 4

[29] RAN RAZ AND IDDO TZAMERET: Resolution over linear equations and multilinear proofs. *Ann. Pure Appl. Logic*, 155(3):194–224, 2008. [doi:10.1016/j.apal.2008.04.001] 2, 17, 18

[30] ALEXANDER A. RAZBOROV: Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Math. Notes. Acad. Sci. USSR (English translation)*, 41(4):333–338, 1987. [doi:10.1007/BF01137685] 3

[31] ALEXANDER A. RAZBOROV: Lower bounds for the polynomial calculus. *Comput. Complexity*, 7(4):291–324, 1998. [doi:10.1007/s000370050013] 3, 4

[32] ROMAN SMOLENSKY: Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th STOC*, pp. 77–82. ACM Press, 1987. [doi:10.1145/28395.28404] 3

[33] DMITRY SOKOLOV: (Semi)algebraic proofs over ±1 variables. In *Proc. 52nd STOC*, pp. 78–90. ACM Press, 2020. [doi:10.1145/3357713.3384288] 3

[34] GRIGORI S. TSEITIN: *On the complexity of derivations in propositional calculus*. Studies in constructive mathematics and mathematical logic Part II. Consultants Bureau, New-York-London, 1968. Reproduced in Automation of Reasoning, Springer, 1983. 2

AUTHOR

Yaroslav Alekseev
Research Engineer
Chebyshev Laboratory at
St. Petersburg State University
Saint-Petersburg, Russia
tolstreg@gmail.com
https://chebyshev.spbu.ru/en/people/iaroslav-alekseev/

ABOUT THE AUTHOR

YAROSLAV ALEKSEEV was born in Saint-Petersburg, Russia. The work was done while he was a Master's student in mathematics at the Saint-Petersburg State University under the supervision of Edward A. Hirsch. After completing his Master's degree, he became a Ph. D. student at the Technion under the supervision of Yuval Filmus. His research interests include proof complexity and computational complexity.