A Lower Bound for Polynomial Calculus with Extension Rule

Yaroslav Alekseev
Chebyshev Laboratory, St. Petersburg State University, Russia

Abstract

A major proof complexity problem is to prove a superpolynomial lower bound on the length of Frege proofs of arbitrary depth. A more general 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 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 arbitrary depth algebraic circuits. 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 [18] proved an exponential lower bound on the size of Res-Lin (Resolution over linear equations [22]) 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.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases proof complexity, algebraic proofs, polynomial calculus

Digital Object Identifier 10.4230/LIPIcs.CCC.2021.21

Related Version *Full Version*: `https://arxiv.org/abs/2010.05660`

Funding *Yaroslav Alekseev*: research is supported by «Native towns», a social investment program of PJSC «Gazprom Neft».

Acknowledgements I would like to thank Edward A. Hirsch for guidance and useful discussions at various stages of this work. Also, I wish to thank Dmitry Itsykson and Dmitry Sokolov for very helpful comments concerning this work.

1 Introduction

In essence, the study of propositional proof complexity started with the work of Cook and Reckhow [7], which states that if there is a propositional proof system in which any unsatisfiable formula F has a short proof of unsatisfiability, then NP = CoNP. The first superpolynomial bound on the proof size was proved in a pioneering work of Tseitin [27] 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 work, we consider extensions of two systems, an algebraic one and a logic-style one.

Logic-style systems

As it was mentioned before, the first superpolynomial bound on the proof size was proved in a work of Tseitin for regular resolution, which is a popular logic proof system. Lately, Haken [11] 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, a stronger logic proof systems such as Frege systems were considered. But while exponential lower bounds for low-depth proof systems (both algebraic and logical ones) are known for decades, the situation with the higher depth proof systems is much worse. The present knowledge is limited to superpolynomial lower bounds for Frege systems over de Morgan basis (that is, without xor's or equivalences) of depth up to $\Theta(\log(n)/\log\log(n))$ [12] (see also [21] where a superpolynomial lower bound for systems of depth up to $\Theta(\sqrt{\log(n)})$ is proved).

Resolution with counting

Another approach to strengthen resolution is to use weak extensions in order to do some sort of counting. Res-Lin (defined in [22]) is a system working with disjunctions of linear equations, and can be viewed as a generalization of Resolution (we consider this system in the present paper). However, no truly exponential lower bounds are known for the size of refutations of formulas in CNF in (dag-like) systems that work over disjunctions of equations or inequalities (see [16] as the first paper defining these systems and containing partial results). Part and Tzameret [18] 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 formula in CNF.

Itsykson and Sokolov [15] considered another extension of the resolution proof system that operates with disjunctions of linear equalities over $\mathbb{F}_2$ named Res($\oplus$) and proved an exponential lower bound on the size of tree-like Res($\oplus$)-proofs.

Algebraic proof systems

Algebraic proof systems such as Nullstellensatz were developed to use some algebraic techniques of Razborov and Smolensky [23, 25] in the proof complexity case. Lower bounds for algebraic systems started with an exponential lower bound for the Nullstellensatz [2] system. The main system considered in this paper is based on the Polynomial Calculus system [6], 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 [24, 14] and Tseitin tautologies [3]. While most results concern the representation of Boolean values by 0 and 1, there are also exponential lower bounds over the $\{-1, +1\}$ basis [26].

However, simple algebraic proof systems such as Nullstellensatz and Polynomial Calculus cannot simulate strong logic systems like Frege systems and thus cannot provide lower bounds for these systems. In order to fix this issue, strong extensions were considered: Grigoriev and Hirsch [9] considered algebraic systems over formulas. Grochow and Pitassi [10] introduced the Ideal Proof System, IPS, which can be considered as the version of Nullstellensatz where all polynomials are written as algebraic circuits (see also [19, 20] for earlier versions of this system).

Many other extensions of Polynomial Calculus and Nullstellensatz have been considered also. Buss, Impagliazzo, Krajíček, Pudlák, Razborov and Sgall [4] 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 [13] showed that a depth-3 extension of Polynomial Calculus called $\Sigma\Pi\Sigma$-PC p-simulates semantic CP* (an inequalities-based system, Cutting Planes [8, 5] with coefficients written in unary) over $\mathbb{Q}$. Also, they showed that a stronger extension of Polynomial Calculus, called Depth-k-PC, p-simulates Cutting Planes and another inequalities-based system Sum-of-Squares; 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 superpolynomial lower bound even on the size of ΣΠΣ-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.

1.1 Our results

We extend Polynomial Calculus with two additional rules. One rule allows us to take a square root (it was introduced by Grigoriev and Hirsch [9] 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). 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 [17]), but it's not obvious how to p-simulate IPS refutations in Ext-PC$^{\surd}$ (since IPS refutations polynomials are written as algebraic circuits and Ext-PC$^{\surd}$ refutations are written explicitly as a sum of monomials).

In this work we give a partial positive answer to the question raised in [13] asking for a technique for proving size lower bounds on Polynomial Calculus without proving any degree lower bounds. However, our lower bound works only for field $\mathbb{Q}$ and the question about proving lower bounds over finite fields remains open. Also, we give a partial answer to another question raised in [13] by proving an exponential lower bound for the system with an extension rule even stronger than that in ΣΠΣ-PC, which is another extension of Polynomial Calculus presented in the aforementioned work.

We consider the following subset-sum instance, called Binary Value Principle (BVP$_n$) [1, 18]:

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

and prove an exponential lower bound for the size of Ext-PC$_{\mathbb{Q}}^{\surd}$ refutations of BVP$_n$. Note that Binary Value Principle does not correspond to the translation of any CNF formula and thus the question about proving the size lower bound on the refutation of formulas in CNF without proving degree lower bounds **remains open**.

▶ **Theorem 1.** *Any* Ext-PC$_{\mathbb{Q}}^{\surd}$ *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 [1]. However, since Ext-PC proof system is weaker than Ideal Proof System, we get an unconditional lower bound. The main idea of the conditional lower bound in [1] is to prove the complexity lower bound on the free term in the end of the IPS-refutation of BVP$_n$ over $\mathbb{Z}$ and then show that IPS$_{\mathbb{Z}}$ simulates 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* being mentioned in the proof (and thus appearing as factors of the free term).

Then we consider Res-Lin and show that Ext-PC$_{\mathbb{Q}}^{\surd}$ simulates Res-Lin and thus get an alternative lower bound for Res-Lin.

▶ **Corollary 2.** *Any* Res-Lin$_{\mathbb{Q}}$ *refutation of* BVP$_n$ *requires size* $2^{\Omega(n)}$.

Note that while Part and Tzameret [18] prove an exponential lower bound on the number of lines in the proof, we prove a bound on the proof size (essentially, on the bit size of scalars appearing in the proof).

1.2 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 in 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 9). Then, in Theorem 11, 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 Res-Lin and thus we get an alternative lower bound for the size of Res-Lin refutations of BVP_n.

2 Preliminaries

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

▶ **Definition 3** (Size of a polynomial). *Let f be an arbitrary integer or rational polynomial in variables $\{x_1, \dots, x_n\}$.*

- *If $f \in \mathbb{Z}[x_1, \dots, x_n]$ then $Size(f) = \sum(\lceil \log |a_i| \rceil + 1)$ where a_i are the coefficients of f.*
- *If $f \in \mathbb{Q}[x_1, \dots, x_n]$ then $Size(f) = \sum(\lceil \log |p_i| \rceil + \lceil \log |q_i| \rceil + 1)$ where $p_i \in \mathbb{Z}$, $q_i \in \mathbb{N}$ and $\frac{p_i}{q_i}$ are the coefficients of f.*

▶ **Definition 4** (Polynomial Calculus). *Let $\Gamma = \{P_1, \dots, P_m\} \subset \mathbb{F}[x_1, \dots, x_n]$ be a set of polynomials in variables $\{x_1, \dots, x_n\}$ over a field $\mathbb{F}$ such that the system of equations $P_1 = 0, \dots, P_m = 0$ has no solution. A Polynomial Calculus refutation of Γ is a sequence of polynomials $R_1, \dots, R_s$ where $R_s = 1$ and for every l in $\{1, \dots, s\}$, $R_l \in \Gamma$ or is obtained through one of the following derivation rules for $j, k < l$*

- *$R_l = \alpha R_j + \beta R_k$ for $\alpha, \beta \in \mathbb{F}$*
- *$R_l = x_i R_k$*

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

Now we consider a variant of Polynomial Calculus proof system with additional **square root derivation rule** (see [9]). Moreover, we extend our definition from fields to **rings**.

▶ **Definition 5** (Polynomial Calculus with square root). *Let $\Gamma = \{P_1, \dots, P_m\} \subset R[x_1, \dots, x_n]$ be a set of polynomials in variables $\{x_1, \dots, x_n\}$ over a domain R such that the system of equations $P_1 = 0, \dots, P_m = 0$ has no solution. A $\mathsf{PC}^{\surd}_{R}$ refutation of Γ is a sequence of polynomials $R_1, \dots, R_s$ where $R_s = M$ for some constant $M \in R, M \neq 0$ and for every l in $\{1, \dots, s\}$, $R_l \in \Gamma$ 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 $i \in \{1, \dots, n\}$*
- *$R_l^2 = R_k$ (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 $\sum_{l=1}^{s} Size(R_l)$, where $Size(R_l)$ is the size of the polynomial R_l. The degree of the refutation is $\max_l deg(R_l)$.

▶ Note 6. We will consider $\mathbb{Q}$ or $\mathbb{Z}$ as the ring R. For both of those rings, if we consider **Boolean** case, where axioms $x_i^2 - x_i = 0$ added, our system will be complete, which means that for every unsatisfiable over $\{0, 1\}$ assignment system $\{f_i(\vec{x}) = 0\}$ there is a $\mathsf{PC}^{\surd}_{R}$ refutation. Also, note that if R is a domain and $P^2 = 0$ for some $P \in R[\vec{x}]$, then $P = 0$.

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

▶ **Definition 7** (Extended 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 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. A $\mathsf{Ext}\text{-}\mathsf{PC}_R^{\surd}$ refutation of Γ is a $\mathsf{PC}_R^{\surd}$ refutation of a set*

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

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

The size of the $\mathsf{Ext}\text{-}\mathsf{PC}_R^{\surd}$ refutation is equal to the size of the $\mathsf{PC}_R^{\surd}$ refutation of Γ'.

3 Lower bound

In order to prove the lower bound for the $\mathsf{Ext}\text{-}\mathsf{PC}_{\mathbb{Q}}^{\surd}$ proof system, we consider the following subset-sum instance [1, 18]:

▶ **Definition 8** (Binary Value Principle BVP_n)**.** *The **binary value principle** over the variables $x_1, \ldots, x_n$, BVP_n for short, is the following unsatisfiable system of equations:*

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

$$x_1^2 - x_1 = 0,\ x_2^2 - x_2 = 0,\ \ldots,\ x_n^2 - x_n = 0.$$

▶ **Theorem 9.** *Any $\mathsf{Ext}\text{-}\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n requires size $\Omega(2^n)$. Moreover, the absolute value of the constant in the end of our $\mathsf{Ext}\text{-}\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation consists of at least $C \cdot 2^n$ bits for some constant $C > 0$. Also, the constant in the end of our $\mathsf{Ext}\text{-}\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation is divisible by every prime number less than 2^n.*

Proof. Assume that $\{R_1, \ldots, R_t\}$ is an $\mathsf{Ext}\text{-}\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of BVP_n. Then we know that $\{R_1, \ldots, R_t\}$ is a $\mathsf{PC}_{\mathbb{Z}}^{\surd}$ refutation of 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 $G(\vec{x}) = 1 + \sum_{i=1}^{i=n} 2^{(i-1)}x_i$, $F_i(\vec{x}) = x_i^2 - x_i$ and $Q_i \in \mathbb{Z}[\vec{x}, y_1, \ldots, y_{i-1}]$.

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

▷ Claim 10. M is divisible by every prime number less than 2^n.

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

Base case: if $i = 1$, then

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

or

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

or

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

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

Induction step: suppose we know that R_j is divisible by $k + 1$ for any $j \leq i$. Now we will 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 $R_{i+1}(b_1, \ldots, b_n, c_1, \ldots, c_m)$ 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 $R_{i+1}(b_1, \ldots, b_n, c_1, \ldots, c_m)$ is divisible by $k + 1$ because $R_j(b_1, \ldots, b_n, c_1, \ldots, c_m)$ and $R_s(b_1, \ldots, b_n, c_1, \ldots, c_m)$ 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 $R_{i+1}(b_1, \ldots, b_n, c_1, \ldots, c_m)$ is divisible by $k + 1$ because $R_s(b_1, \ldots, b_n, c_1, \ldots, c_m)$ is divisible by $k + 1$ and b_i and c_i are integers.
4. If $R_{i+1}^2 = R_s$, then we know that $R_s(b_1, \ldots, b_n, c_1, \ldots, c_m)$ is divisible by $k + 1$. Suppose $R_{i+1}(b_1, \ldots, b_n, c_1, \ldots, c_m)$ is not divisible by $k + 1$. Then $R_{i+1}(b_1, \ldots, b_n, c_1, \ldots, c_m)^2$ is not divisible by $k + 1$ since $k + 1$ is **prime**. But $R_{i+1}(b_1, \ldots, b_n, c_1, \ldots, c_m)^2 = R_s(b_1, \ldots, b_n, c_1, \ldots, c_m)$ 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 know 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 we know that M is divisible by the product of all prime numbers less than 2^n. Then we know that $|M| > (\pi(2^n))!$ where $\pi(2^n)$ is the number of all prime numbers less than 2^n. By the prime number theorem $\pi(2^n) > C\frac{2^n}{n}$. By Stirling's approximation we get

$$|M| > \left(C\frac{2^n}{n}\right)! > C' \cdot \left(C\frac{2^n}{e \cdot n}\right)^{C\frac{2^n}{n}} > C'' \left(2^{\frac{n}{2}}\right)^{C\frac{2^n}{n}} > C'' 2^{(2^n C_0)}$$

which means that M consists of at least $C_1 \cdot 2^n$ bits and therefore any Ext-PC$_{\mathbb{Z}}^{\surd}$ refutation of BVP$_n$ requires size $\Omega(2^n)$. ◁

◀

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

▶ **Theorem 11.** *Any* Ext-PC$_{\mathbb{Q}}^{\surd}$ *refutation of* BVP$_n$ *requires size* $\Omega(2^n)$.

Proof. Assume that $\{R_1, \dots, R_t\}$ is an $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Q}}$ refutation of Γ of the size S. Then we know that $\{R_1, \dots, R_t\}$ is a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation of 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 $Q_i \in \mathbb{Q}[\vec{x}, \vec{y}]$. Also, we know that $R_t = M$ for some $M \in \mathbb{Q}$.

Consider integers $M_1, \dots, M_m$ where M_i is equal to the product of denominators of all coefficients of polynomial Q_i. Also consider all polynomials $R_j(\vec{x}, \vec{y})$ which was derived by using linear combination rule which means that $R_j = \alpha R_i + \beta R_k$. Then we consider **all** constants α and β occurring in linear combination derivations in our proof. Let's denote the set of those constants as $\{\gamma_1, \gamma_2, \dots, \gamma_l\} \subset \mathbb{Q}$. Now consider the set of all **denominators** of the constants in $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ and denote this set as $\{\delta_1, \delta_2, \dots, \delta_l\} \subset \mathbb{N}$.

Also consider the products of all denominators of coefficients of polynomials $\{R_1, \dots, R_t\}$. We will denote the set of those integers as $\{L_1, \dots, L_t\} \subset \mathbb{N}$.

Now we will construct the $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Z}}$ refutation of Γ such that the constant in the end of this proof is equal to $M_1^{c_1} \cdot M_2^{c_2} \cdots M_m^{c_m} \cdot \delta_1^{c_{m+1}} \cdots \delta_l^{c_{m+l}} \cdot L_1^{c_{m+l+1}} \cdots L_t^{c_{m+l+t}} \cdot M$ where $\{c_1, c_2, \dots, c_{m+l+t}\} \subset \mathbb{N} \cup \{0\}$.

Firstly, we will translate polynomials Q_i into some 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 $T_1^{\alpha_{11}} \cdot M_2$ where α_{11} is an **arbitrary** non-negative integer such 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 $T_i = T_1^{\alpha_{i1}} \cdot T_2^{\alpha_{i2}} \cdots T_{i-1}^{\alpha_{ii-1}} \cdot M_i$ where $\alpha_{i1}, \dots, \alpha_{ii-1}$ are **arbitrary** integers such 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 could be arbitrary large.

Now we will construct a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation $\{R'_1, \dots, R'_s\}$ of 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 refutation duplicates the original refutation $\{R_1, \dots, R_t\}$ 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 will multiply corresponding polynomial by y'_j and then multiply it by $\frac{1}{T_j}$.

Formally, we will prove the following claim:

▷ Claim 12. There is a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation $\{R'_1, \dots, R'_s\}$ of 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 properties holds:

- For every polynomial $R'_i(\vec{x}, y'_1, \dots, y'_m)$ one of the following equations holds: $R'_i(\vec{x}, y_1 \cdot T_1, \dots, y_m \cdot T_m) = R_j(\vec{x}, y_1, \dots, y_m)$ for some j or $R'_i(\vec{x}, y_1 \cdot T_1, \dots, y_m \cdot T_m) = T_k \cdot R_j(\vec{x}, y_1, \dots, y_m)$ for some k 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 linear combination with rational constants α and β (which means that $R'_i = \alpha R'_j + \beta R'_k$), then $\alpha = \frac{1}{T_f}$ and $\beta = 0$ for some f or there is some polynomial $R_h(\vec{x}, y'_1, \dots, y'_m)$ which was derived from some polynomials R_k and R_l by using linear combination with constants α and β.

Proof of claim. The proof is an easy (but lengthy) inductive argument and is given in the Appendix A. ◁

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

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

In order to do this we will fix a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation $\{R'_1, \dots, R'_s\}$ of Γ'' with the properties from the Claim 12 and construct a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ refutation of Γ'' by induction. Moreover, we will construct a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ refutation $\{R''_1, \dots, R''_f\}$ 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 are going to multiply each line in our $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation by some constant in order to get a correct $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ refutation. But since we cannot divide polynomials in our $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ refutation by any constant, we will duplicate original $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation 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 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 12. Then there exists a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation $\{R''_1, \dots, R''_f\}$ from Γ'' such that

- $f \le 2i^2$.
- There is some 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

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

Both *base case of induction* and *induction step* are straightforward derivations and are given in the Appendix B.

So now we have a $\mathsf{Ext\text{-}PC}^{\surd}_{\mathbb{Z}}$ refutation of Γ such that the constant in the end of this refutation is equal to $M_1^{c_1} \cdot M_2^{c_2} \cdots M_m^{c_m} \cdot \delta_1^{c_{m+1}} \cdots \delta_l^{c_{m+l}} \cdot L_1^{c_{m+l+1}} \cdots L_t^{c_{m+l+t}} \cdot M$. Suppose that $M = \frac{p'}{q'}$ where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then, from Theorem 9 we know that $M_1^{c_1} \cdot M_2^{c_2} \cdots M_m^{c_m} \cdot \delta_1^{c_{m+1}} \cdots \delta_f^{c_{m+l}} \cdot L_1^{c_{m+l+1}} \cdots L_t^{c_{m+l+t}} \cdot p'$ is divisible by every prime number less than 2^n. Since $M_1, \dots, M_m$, $\delta_1, \dots, \delta_l$, $L_1, \dots, L_t$ are positive integers we know that $M_1 \cdot M_2 \cdots M_m \cdot \delta_1 \cdots \delta_l \cdot L_1 \cdots L_t \cdot p'$ is divisible by every prime number less than 2^n. Also we know that

$$\log\lceil M_1\rceil + \dots + \log\lceil M_m\rceil + \log\lceil \delta_1\rceil + \dots + \log\lceil \delta_l\rceil + \log\lceil L_1\rceil + \dots + \log\lceil L_t\rceil + \log\lceil p\rceil \le O(Size(S))$$

because all constants $M_1, \dots, M_m, L_1, \dots, L_t$ are products of denominators in the lines of our refutation $\{R_1, \dots, R_t\}$ and constants $\delta_1, \dots, \delta_l$ are denominators of rationals in linear combinations used in our derivation.

On the other hand, we know that

$$M_1 \cdot M_2 \cdots M_m \cdot \delta_1 \cdots \delta_l \cdot L_1 \cdots L_t \cdot p' \ge 2^{2^{\Omega(n)}}$$

since our product is divisible by every prime number less than 2^n. Then we know that $S \ge 2^{\Omega(n)}$. ◀

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

Following [22], we define Res-Lin proof system.

▶ **Definition 13.** *A* ***disjunction of linear equations*** *is of the following general form:*

$$(a_1^{(1)}x_1 + \ldots + a_n^{(1)}x_n = a_0^{(1)}) \vee \cdots \vee (a_1^{(t)}x_1 + \ldots + a_n^{(t)}x_n = a_0^{(t)}) \qquad (1)$$

where $t \ge 0$ and the coefficients a_i^j are ***integers*** *(for all $0 \le i \le n$, $1 \le j \le t$). The semantics of such a disjunction is the natural one: We say that an assignment of integral values 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 **size** of the disjunction of linear equations is $\sum_{i=1}^{n}\sum_{j=1}^{t}|a_i^{(j)}|$ if all coefficients are written in **unary** notation. If all coefficients are written in **binary** notation then the **size** is equal to $\sum_{i=1}^{n}\sum_{j=1}^{t}(\lceil\log|a_i^{(j)}|\rceil+1)$.*

▶ **Definition 14.** *Let $K := \{K_1,\dots,K_m\}$ be a collection of disjunctions of linear equations. An* Res-Lin *proof from K of a disjunction of linear equations D is a finite sequence $\pi = (D_1,\dots,D_l)$ of disjunctions of linear equations, such that $D_l = D$ and for every $i \in \{1,\dots,l\}$, either $D_i = K_j$ for some $j \in \{1,\dots,m\}$, or D_i is a Boolean axiom $(x_h = 0) \vee (x_h = 1)$ for some $h \in \{1,\dots,n\}$, 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 $\alpha,\beta \in \mathbb{Z}$.*
- ***Weakening**: From a (possibly empty) disjunction of linear equations A derive $A \vee L$, where L is an arbitrary linear equation over $\{x_1,\dots,x_n\}$.*
- ***Simplification**: From $A \vee (k = 0)$ derive A, where A is a, possibly empty, disjunction of linear equations and $k \neq 0$ is a constant.*
- ***Contraction**: From $A \vee L \vee L$ derive $A \vee L$, where A is a, possibly empty, disjunction of linear equations and L is some linear equation.*

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

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

If all coefficients in our Res-Lin *proof π are written in the **unary** notation then we denote this proof an* Res-Lin$_U$ *derivation. Otherwise, if all coefficients are written in the **binary** notation then we denote this proof an* Res-Lin$_B$ *derivation.*

▶ Note 15. In the original Res-Lin proof system duplicate linear equations can be discarded from the disjunction. Instead, we will use **contraction** rule explicitly. It is easy to see that both these variants of Res-Lin system are equivalent.

▶ **Definition 16.** *Let D be a disjunction of linear equations:*

$$(a_1^{(1)}x_1 + \ldots + a_n^{(1)}x_n = a_0^{(1)}) \vee \cdots \vee (a_1^{(t)}x_1 + \ldots + a_n^{(t)}x_n = a_0^{(t)})$$

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

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

$$y_1 = a_1^{(1)}x_1 + \ldots + a_n^{(1)}x_n - a_0^{(1)},\ y_2 = a_1^{(2)}x_1 + \ldots + a_n^{(2)}x_n - a_0^{(2)},\ \ldots,$$
$$y_t = a_1^{(t)}x_1 + \ldots + a_n^{(t)}x_n - a_0^{(t)}$$

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

Now we will prove that Ext-PC$_{\mathbb{Q}}^{\surd}$ p-simulates Res-Lin$_B$ and $\Sigma\Pi\Sigma$-$PC_{\mathbb{Q}}$ p-simulates Res-Lin$_U$.

▶ **Theorem 17.** *Let $\pi = (D_1,\dots,D_l)$ be an* Res-Lin$_B$ *proof sequence of D_l from some collection of initial disjunctions of linear equations $Q_1,\dots,Q_m$. Also consider $L_1,\dots,L_t$ – all affine forms that we have in all disjunctions in our* Res-Lin$_B$ *proof sequence.*

Then, there exists a PC$_{\mathbb{Q}}^{\surd}$ *proof of $\widehat{D}_l$ from $\widehat{Q}_1 \cup \ldots \cup \widehat{Q}_m \cup \{y_1 = L_1, y_2 = L_2, \dots, y_t = L_t\}$ of size at most $O(p(Size(\pi)))$ for some polynomial p.*

Proof. The proof is a straightforward induction and is given in the Appendix C. ◀

Following [13], we define the $\Sigma\Pi\Sigma$-PC_R proof system.

▶ **Definition 18** ([13]). *Let $\Gamma = \{P_1, \ldots, P_m\} \subset R[x_1, \ldots, x_n]$ be a set of polynomials in 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 $\Sigma\Pi\Sigma$-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 $\Sigma\Pi\Sigma$-PC_R refutation is equal to the size of the PC_R refutation of Γ'.

▶ **Theorem 19.** *Let $\pi = (D_1, \ldots, D_l)$ be an $\mathsf{Res\text{-}Lin}_U$ proof sequence of D_l, from some 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 $O(p(Size(\pi)))$ for some polynomial p.*

Proof. To prove this theorem we will use the following lemma from [13]:

▶ **Lemma 20** ([13], revision 2 of the ECCC report, lemma 7, p.32). *Let $\Gamma = \{P_1, \ldots, P_a, Q_1, \ldots, Q_b, X, Y\}$ be a set of polynomials such that*

$$P_1 = x_1 - (x-1),\ P_2 = x_2 - (x-2),\ \ldots, P_a = x_a - (x-a),$$

$$Q_1 = y_1 - (y-1),\ Q_2 = y_2 - (y-2),\ \ldots, Q_b = y_b - (y-b),$$

$$X = x \cdot x_1 \cdot x_2 \cdots x_a,\ Y = y \cdot y_1 \cdot y_2 \cdots y_b.$$

Then we can introduce new variables $z, z_1, \ldots, z_{a+b}$ using the $\Sigma\Pi\Sigma$-$PC_{\mathbb{Q}}$ extension rule and derive Γ' from Γ in $\Sigma\Pi\Sigma$-$PC_{\mathbb{Q}}$ with a derivation of size $poly(ab)$, where $\Gamma' = \{Z_0, Z_1, \ldots, Z_{a+b}, Z\}$ and

$$Z_0 = z-(x+y),\ Z_1 = z_1-(x+y+1),\ Z_2 = z_2-(x+y+2),\ \ldots, Z_{a+b} = z_{a+b}-(x+y+a+b),$$

$$Z = z \cdot z_1 \cdot z_2 \cdots z_{a+b}.$$

Now we will prove the theorem by induction on lines in π.
Base case: An $\mathsf{Res\text{-}Lin}_U$ axiom Q_i is translated into $\widehat{Q_i}$ and $\mathsf{Res\text{-}Lin}_U$ Boolean axiom $(x_i = 0) \vee (x_i = 1)$ is translated into PC axiom $x_i^2 - x_i = 0$.
Induction step: Now we will simulate all $\mathsf{Res\text{-}Lin}_U$ derivation rules in the $\Sigma\Pi\Sigma$-$PC_{\mathbb{Q}}$ proof.

- **Resolution**, **Weakening**, **Simplification** rules simulation is the same as in Theorem 17.
- **Contraction**: 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

  $$y_{j1} = (a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n - a_{j0}^{(1)}),\ \ldots,\ y_{jt_j-1} = y_{jt_j} = (a_{j1}^{(t_j)}x_1 + \ldots + a_{jn}^{(t_j)}x_n - a_{j0}^{(t_j)}),$$

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

  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 lemma we can introduce new variables $\{z_{-M}, \ldots, z_M\}$ and derive

  $$z_{-M} = y_{jt_{j-1}} + M,\ , z_{-M+1} = y_{jt_{j-1}} + M - 1, \ldots, z_0 = y_{jt_{j-1}},\ z_M = y_{jt_{j-1}} - M,$$

  $$z_{-M} \cdot z_{-M+1} \cdots z_{M-1} \cdot z_M = 0,$$

  where $M = |a_{j1}^{(t_{j-1})}| + |a_{j2}^{(t_{j-1})}| + \ldots + |a_{jn}^{(t_{j-1})}|$. Then we can substitute $y_{jt_j} - k$ for each z_k one by one and get equation

  $$f(y_{jt_{j-1}}) = 0$$

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

$$y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot f(y_{jt_{j-1}}) = b_1 \cdot y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot y_{jt_j-1} + \\ + y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot (y^2_{jt_j-1}) \cdot (b_2 + b_3 \cdot y_{jt_{j-1}} + \ldots + b_{2M+1} \cdot y^{2M-1}_{jt_{j-1}}) = 0.$$

Now, using the equation $y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot (y^2_{jt_j-1}) = 0$ we can 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 can derive $y_{j1} \cdot y_{j2} \cdots y_{jt_j-2} \cdot y_{jt_j-1} = 0$. This equation is the last part of $\widehat{D}_i$ because other parts were derived earlier.

◀

Now we will show that our lower bound provides an interesting counterpart to a result from [18].

▶ **Theorem 21** ([18]). *Any* Res-Lin$_B$ *refutation of* $1 + 2x_1 + \ldots + 2^n x_n = 0$ *is of the size* $2^{\Omega(n)}$.

Proof. From Theorem 11 we know that any Ext-PC$^{\surd}_{\mathbb{Q}}$ refutation of BVP$_n$ requires size $2^{\Omega(n)}$ and thus from Theorem 17 we know that there is some polynomial p such that for any Res-Lin$_B$ refutation of BVP$_n$ of size S the equation $p(S) \geq C_0 \cdot 2^{C_1 \cdot n}$ holds. Then we know that for some constant C the equation $S \geq 2^{C \cdot n}$ holds. ◀

Also we will show that there is no straightforward translation of Res-Lin$_B$ derivations into Ext-PC$_{\mathbb{Q}}$ refutations.

▶ **Theorem 22.** *Any* Ext-PC$_{\mathbb{Q}}$*-derivation of* $1 + x_1 + \ldots + 2^{n-1}x_n = 0$ *from equation* $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ *requires size* $2^{\Omega(n)}$.

Proof. The proof of this theorem essentially copies the proof of Theorem 11 and consists of two parts. In the first part we prove that if we have an Ext-PC$_{\mathbb{Z}}$-derivation of $M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ from equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ where $M \in \mathbb{Z}, M \neq 0$, then M is divisible by every prime number less than 2^n.

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

For the full proof see Appendix D. ◀

Open Problems

1. Theorem 17 says that Ext-PC$^{\surd}_{\mathbb{Q}}$ p-simulates any Res-Lin$_B$ derivation. However, from Theorem 22 we know that simulation from Theorem 17 doesn't work for Ext-PC$_{\mathbb{Q}}$. Is the square root rule necessary, that is, can we p-simulate the Res-Lin$_B$ refutation in the Ext-PC$_{\mathbb{Q}}$ proof system?
2. A major question is to prove an exponential lower bound on the size of the $\Sigma\Pi\Sigma$-PC$_{\mathbb{Q}}$ refutation of a translation of formula in CNF.

3. Theorem 21 says that any $\mathsf{Res\text{-}Lin}_B$ refutation of BVP_n requires size $2^{\Omega(n)}$. Does the exponential lower bound on the size of the $\mathsf{Res\text{-}Lin}_B$ refutation imply the exponential lower bound on the number of lines in the $\mathsf{Res\text{-}Lin}_B$ refutation? Do we necessarily need large coefficients in some $\mathsf{Res\text{-}Lin}_B$ refutations with a small number of lines? Or if there is a $\mathsf{Res\text{-}Lin}_B$ refutation with a small number of lines then there is a $\mathsf{Res\text{-}Lin}_B$ refutation with a small number of lines and small coefficients?

References

1 Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, and Iddo Tzameret. Semi-algebraic proofs, IPS lower bounds and the τ-conjecture: Can a natural number be negative? In *Proceedings of the 52th Annual ACM Symposium on Theory of Computing (STOC 2020)*, pages 54–67, 2020.

2 Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc. (3)*, 73(1):1–26, 1996. doi:10.1112/plms/s3-73.1.1.

3 Sam Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *Journal of Computer and System Sciences*, 62(2):267–289, 2001. doi:10.1006/jcss.2000.1726.

4 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. *Computational Complexity*, 6(3):256–298, 1996. doi:10.1007/BF01294258.

5 V. Chvátal, W. Cook, and M. Hartmann. On cutting-plane proofs in combinatorial optimization. *Linear Algebra and its Applications*, 114-115:455–499, 1989. Special Issue Dedicated to Alan J. Hoffman. doi:10.1016/0024-3795(89)90476-X.

6 Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 174–183, New York, 1996. ACM.

7 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *J. Symb. Log.*, 44(1):36–50, 1979. doi:10.2307/2273702.

8 W. Cook, C. R. Coullard, and G. Turan. On the complexity of cutting plane proofs. *Discrete Applied Mathematics*, 18:25–38, 1987.

9 Dima Grigoriev and Edward A. Hirsch. Algebraic proof systems over formulas. *Theoret. Comput. Sci.*, 303(1):83–102, 2003. Logic and complexity in computer science (Créteil, 2001).

10 Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6):37:1–37:59, 2018. doi:10.1145/3230742.

11 Armin Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985.

12 Johan Håstad. On small-depth Frege proofs for tseitin for grids. *J. ACM*, 68(1), 2020. doi:10.1145/3425606.

13 Russell Impagliazzo, Sasank Mouli, and Toniann Pitassi. The surprising power of constant depth algebraic proofs. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '20, page 591–603, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3373718.3394754.

14 Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. doi:10.1007/s000370050024.

15 Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Annals of Pure and Applied Logic*, 171(1):102722, 2020. doi:10.1016/j.apal.2019.102722.

16 Jan Krajíček. Discretely ordered modules as a first-order extension of the cutting planes proof system. *The Journal of Symbolic Logic*, 63(4):1582–1596, 1998.

17 Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *Journal of Symbolic Logic*, 54(3):1063–1079, 1989. doi:10.2307/2274765.

18 Fedor Part and Iddo Tzameret. Resolution with counting: Different moduli and dag-like lower bounds. In *12th Innovations in Theoretical Computer Science Conference, ITCS 2020, January, 2020, Seattle, WA, USA*, 2020.

19 Toniann Pitassi. Algebraic propositional proof systems. In *Descriptive complexity and finite models (Princeton, NJ, 1996)*, volume 31 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 215–244. Amer. Math. Soc., Providence, RI, 1997.

20 Toniann Pitassi. Unsolvable systems of equations and proof complexity. In *Proceedings of the International Congress of Mathematicians, Vol. III (Berlin, 1998)*, pages 451–460, 1998.

21 Toniann Pitassi, Benjamin Rossman, Rocco A. Servedio, and Li-Yang Tan. Poly-logarithmic Frege depth lower bounds via an expander switching lemma. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page 644–657, New York, NY, USA, 2016. Association for Computing Machinery. doi:10.1145/2897518.2897637.

22 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.

23 Alexander A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987. doi:10.1007/BF01137685.

24 Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complexity*, 7(4):291–324, 1998.

25 Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC 1987)*, pages 77–82, 1987. doi:10.1145/28395.28404.

26 Dmitry Sokolov. (semi)algebraic proofs over {± 1} variables. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, page 78–90, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3357713.3384288.

27 Grigori Tseitin. *On the complexity of derivations in propositional calculus*, pages 466–483. Studies in constructive mathematics and mathematical logic Part II. Consultants Bureau, New-York-London, 1968.

A Proof of the Claim 12

▶ **Claim 12.** *There is a* $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ *refutation* $\{R'_1, \dots, R'_s\}$ *of 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 properties holds:*

- *For every polynomial* $R'_i(\vec{x}, y'_1, \dots, y'_m)$ *one of the following equations holds:* $R'_i(\vec{x}, y_1 \cdot T_1, \dots, y_m \cdot T_m) = R_j(\vec{x}, y_1, \dots, y_m)$ *for some* j *or* $R'_i(\vec{x}, y_1 \cdot T_1, \dots, y_m \cdot T_m) = T_k \cdot R_j(\vec{x}, y_1, \dots, y_m)$ *for some* k *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 linear combination with rational constants* α *and* β *(which means that* $R'_i = \alpha R'_j + \beta R'_k$*), then* $\alpha = \frac{1}{T_f}$ *and* $\beta = 0$ *for some* f *or there is some polynomial* $R_h(\vec{x}, y'_1, \dots, y'_m)$ *which was derived from some polynomials* R_k *and* R_l *by using linear combination with constants* α *and* β*.*

Proof of claim. We will construct $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ refutation $\{R'_1, R'_2, \dots, R'_s\}$ 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

- $p \leq 2i$.
- For every $R_j(x_1, \dots, x_n, y_1, \dots, y_m)$ there exists some $R'_k(x_1, \dots, x_n, y'_1, \dots, y'_m)$ 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 mentioned in the claim are true for our derivation $\{R'_1, \dots, R'_p\}$.

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's 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 $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ refutation $\{R'_1, R'_2, \dots, R'_p\}$ 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 we know that

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

for some $R'_{j'}$. Thus we know that

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

So we know that

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

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

Case 5: If $R_{i+1} = y_l \cdot R_j$ then we take $R'_{p+1} = y'_l \cdot R'_{j'}$ 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's easy to see that in all these cases the induction statement stays true. ◁

B Induction form the Theorem 11

Induction statement. Let $\{R'_1, \dots, R'_i\}$ be a $\mathsf{PC}^{\surd}_{\mathbb{Q}}$ derivation from Γ'' with the properties from the Claim 12. Then there exists a $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ derivation $\{R''_1, \dots, R''_f\}$ from Γ'' such that

- $f \le 2i^2$.
- There is some 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 $\mathsf{PC}^{\surd}_{\mathbb{Z}}$ refutation $\{R''_1, R''_2, \dots, R''_f\}$ 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

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

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

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

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 $\beta = \frac{p_2}{q_2}$ where $\{p_1, q_1, p_2, q_2\} \subset \mathbb{Z}$. Then we can take $F_{i+1} = q_1 q_2 F_i$,

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

and $R''_{f+i+1} = p_1 q_2 \cdot R''_{f-i+j} + p_2 q_1 \cdot R''_{f-i+k} = M_{i+1} R'_{i+1}$. From the Claim 12 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 we know that

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

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

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

and the induction statement stays true.

Case 4: Suppose $R'^2_{i+1} = R'_j$. We know 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 we can take $M' = L_k \cdot T_1^{\alpha_1} \cdot T_2^{\alpha_2} \cdots T_m^{\alpha_m} = L_k \cdot M_1^{\alpha'_1} \cdot M_2^{\alpha'_2} \cdots M_m^{\alpha'_m}$ for some non-negative integers $\alpha_1, \dots, \alpha_m$, such that $M' \cdot R'_{i+1}$ is an integer polynomial. We know that such integers $\alpha_1, \dots, \alpha_m$ exist since L_k is the product of all denominators of coefficients of polynomial R_k.

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

$$R''_{f+1} = F_i(M')^2 \cdot R''_{f-i+j} = (F_iM')^2 \cdot R'_j,\ R'_{f+2} = M' \cdot R'_{f-i+1} = F_{i+1} \cdot R_1,$$
$$R'_{f+3} = M' \cdot R'_{f-i+2} = F_{i+1} \cdot R_2,\ \dots,\ R'_{f+i+1} = M' \cdot R'_f = F_{i+1}R_i.$$

Then we can take $R''_{f+i+2} = F_iM' \cdot R'_{i+1}$ and since $R''_{f+1} = (F_iM')^2 \cdot R'_j$ we know that $(R''_{f+i+2})^2 = R''_{f+1}$ and we get a correct $\mathsf{PC}_{\mathbb{Z}}^{\surd}$ derivation.

Since $M' = L_p \cdot M_1^{\alpha'_1} \cdot M_2^{\alpha'_2} \cdots M_m^{\alpha'_m}$ we know that

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

and the induction statement stays true.

C Proof of the Theorem 17

▶ **Theorem 17.** *Let $\pi = (D_1, \dots, D_l)$ be an* $\mathsf{Res\text{-}Lin}_B$ *proof sequence of D_l from some collection of initial disjunctions of linear equations $Q_1, \dots, Q_m$. Also consider $L_1, \dots, L_t$ – all affine forms that we have in all disjunctions in our* $\mathsf{Res\text{-}Lin}_B$ *proof sequence.*

Then, there exists a $\mathsf{PC}_{\mathbb{Q}}^{\surd}$ *proof of $\widehat{D}_l$ from $\widehat{Q}_1 \cup \ldots \cup \widehat{Q}_m \cup \{y_1 = L_1, y_2 = L_2, \dots, y_t = L_t\}$ of size at most $O(p(Size(\pi)))$ for some polynomial p.*

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

- **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

  $$y_{j1} = (a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n - a_{j0}^{(1)}),\ \dots,\ y_{jt_j} = (a_{j1}^{(t_j)}x_1 + \ldots + a_{jn}^{(t_j)}x_n - a_{j0}^{(t_j)}),$$
  $$y_{k1} = (a_{k1}^{(1)}x_1 + \ldots + a_{kn}^{(1)}x_n - a_{k0}^{(1)}),\ \dots,\ y_{kt_k} = (a_{k1}^{(t_k)}x_1 + \ldots + a_{kn}^{(t_k)}x_n - a_{k0}^{(t_k)}),$$
  $$y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0,\ y_{k1} \cdot y_{k2} \cdots y_{kt_k} = 0$$

  where

  $$A = (a_{j1}^{(2)}x_1 + \ldots + a_{jn}^{(2)}x_n = a_{j0}^{(2)}) \vee \cdots \vee (a_{j1}^{(t_j)}x_1 + \ldots + a_{jn}^{(t_j)}x_n = a_{j0}^{(t_j)}),$$
  $$B = (a_{k1}^{(2)}x_1 + \ldots + a_{kn}^{(2)}x_n = a_{k0}^{(2)}) \vee \cdots \vee (a_{k1}^{(t_k)}x_1 + \ldots + a_{kn}^{(t_k)}x_n = a_{k0}^{(t_k)})$$
  $$L_1 = (a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n = a_{j0}^{(1)}),\ L_2 = (a_{k1}^{(1)}x_1 + \ldots + a_{kn}^{(1)}x_n = a_{k0}^{(1)}).$$

  Then we can 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 some equation $y_i = L_i$ from the set $\{y_1 = L_1, y_2 = L_2, \dots, y_t = L_t\}$, for which holds

  $$L_i = \alpha(a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n - a_{j0}^{(1)}) + \beta(a_{k1}^{(1)}x_1 + \ldots + a_{kn}^{(1)}x_n - a_{k0}^{(1)}).$$

  Then we can 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 is part of $\widehat{D}_i$.

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

  $$y_{j1} = (a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n - a_{j0}^{(1)}),\ \ldots,\ y_{jt_j} = (a_{j1}^{(t_j)}x_1 + \ldots + a_{jn}^{(t_j)}x_n - a_{j0}^{(t_j)}),$$
  $$y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0.$$

  We know that there is some variable y_0 for which $y_0 = b_1x_1 + \ldots b_nx_n - b_0$ where L is a linear equation $b_1x_1 + \ldots b_nx_n = b_0$. From $y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0$ we can derive $y_0 \cdot y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0$ which is part of $\widehat{D}_i$.
- **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

  $$y_{j1} = (a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n - a_{j0}^{(1)}),\ \ldots,$$
  $$y_{jt_j-1} = (a_{j1}^{(t_j-1)}x_1 + \ldots + a_{jn}^{(t_j-1)}x_n - a_{j0}^{(t_j-1)}),\ y_{jt_j} = k,$$
  $$y_{j1} \cdot y_{j2} \cdots y_{jt_j} = 0.$$

  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 can derive $y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} = 0$ which is part of $\widehat{D}_i$.
- **Contraction**: Assume that $D_i = A \vee L$ and $D_j \vee L \vee L$ where L is a linear equation. Then, we have already derived polynomial equations

  $$y_{j1} = (a_{j1}^{(1)}x_1 + \ldots + a_{jn}^{(1)}x_n - a_{j0}^{(1)}),\ \ldots,\ y_{jt_j-1} = y_{jt_j} = (a_{j1}^{(t_j)}x_1 + \ldots + a_{jn}^{(t_j)}x_n - a_{j0}^{(t_j)}),$$
  $$y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} \cdot y_{jt_j} = 0.$$

  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 can derive $y_{j1}^2 \cdot y_{j2}^2 \cdots y_{jt_j-2}^2 \cdot (y_{jt_j-1}^2) = 0$ from which we can derive the equation $y_{j1} \cdot y_{j2} \cdots y_{jt_j-1} = 0$ by using the square root rule. This equation is the last part of $\widehat{D}_i$ because other parts were derived earlier. ◀

D Proof of the theorem 22

▶ **Theorem 22.** *Any* Ext-PC$_{\mathbb{Q}}$*-derivation of* $1 + x_1 + \ldots + 2^{n-1}x_n = 0$ *from equation* $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ *requires size* $2^{\Omega(n)}$.

Proof. Firstly, we need the following claim:

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

Proof of claim. Assume that $\{R_1, \ldots, R_t\}$ is an Ext-PC$_{\mathbb{Z}}$-derivation of $M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ from equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$. Then we know that $\{R_1, \ldots, R_t\}$ is a PC$_{\mathbb{Z}}$ refutation of 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 $G(\vec{x}) = (1 + \sum_{i=1}^{i=n} 2^{(i-1)}x_i)^2$, $F_i(\vec{x}) = x_i^2 - x_i$, $Q_i \in \mathbb{Z}[\vec{x}, y_1, \ldots, y_{i-1}]$ and $R_t = M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n)$.

Now consider arbitrary integer number $0 \leq k < 2^n$ and its binary representation $b_1, \ldots, b_n$. Then $G(b_1, \ldots, b_n) = (k+1)^2$, $F_i(b_1, \ldots, b_n) = b_i^2 - b_i = 0$. Also consider integers $c_1, \ldots, c_m$ such that $c_i = Q_i(b_1, \ldots, b_n, c_1, c_2, \ldots, c_{i-1})$. Now we will prove by induction that every integer number $R_i(b_1, \ldots, b_n, c_1, \ldots, c_m)$ 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 will 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 we know that 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 Ext-PC$_{\mathbb{Q}}$-derivation from arbitrary set of equations $\Gamma \subset \mathbb{Z}[\vec{x}]$ of the size S. Then we know that $\{R_1, \dots, R_t\}$ is a PC$_{\mathbb{Q}}^{\surd}$ refutation of 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 $Q_i \in \mathbb{Q}[\vec{x}, \vec{y}]$. Like in the proof of Theorem 11 we can consider all products of denominators of polynomials Q_i, R_i and all denominators in linear combination rule. Let's denote those constants as T_i. We know that $\prod T_i \leq 2^{\Omega(S)}$. From the proof of Theorem 11 we know that there is an Ext-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 $\alpha_i \in \mathbb{N}$.

Then we can consider

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

and $R_t = 1 + x_1 + \ldots + 2^{n-1}x_n$. Then we know that for every Ext-PC$_{\mathbb{Q}}$-derivation of $1 + x_1 + \ldots + 2^{n-1}x_n = 0$ from equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ of size S there is an Ext-PC$_{\mathbb{Z}}$-derivation of $M \cdot (1 + x_1 + \ldots + 2^{n-1}x_n) = 0$ from equation $(1 + x_1 + \ldots + 2^{n-1}x_n)^2 = 0$ where $M = T_1^{\alpha_1} \cdots T_r^{\alpha_r}$ and $T_1 \cdots T_r \leq 2^{\Omega(S)}$. However, from previous claim 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 $2^{2^{\Omega(n)}} \leq T_1 \cdots T_r \leq 2^{\Omega(S)}$ which means that $S \geq 2^{\Omega(n)}$. ◁

◀