Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 34 (2020)

On Proof complexity of Resolution over Polynomial Calculus

Erfan Khaniki*[1,2]

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

November 28, 2020

In memory of Arash Pourzarabi and Pouneh Gorji

Abstract

The proof system $\mathsf{Res}(\mathsf{PC}_d/R)$ is a natural extension of the Resolution proof system that instead of clauses of literals operates with disjunctions of degree d polynomials over a ring R with boolean variables. Proving super-polynomial lower bounds for the size of $\mathsf{Res}(\mathsf{PC}_1/R)$-refutations of CNFs is one of the important problems in propositional proof complexity. The existence of such lower bounds is even open for $\mathsf{Res}(\mathsf{PC}_1/\mathbb{F})$ when $\mathbb{F}$ is a finite field such as $\mathbb{F}_2$. In this paper, we investigate $\mathsf{Res}(\mathsf{PC}_d/R)$ and tree-like $\mathsf{Res}(\mathsf{PC}_d/R)$ and prove size-width relations for them when R is a finite ring. As an application, we get for every finite field $\mathbb{F}$ the following lower bounds on the number of clauses:

1. We prove almost quadratic lower bounds for $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$-refutations for every fixed d. The new lower bounds are for the following CNFs:
   (a) mod q Tseitin formulas ($char(\mathbb{F}) \neq q$),
   (b) Random k-CNFs with linearly many clauses.
2. We also prove super-polynomial and exponential lower bounds for tree-like $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$-refutations where d is not too large with respect to n for the following CNFs:
   (a) mod q Tseitin formulas ($char(\mathbb{F}) \neq q$),
   (b) Random k-CNFs.

The above results imply the first nontrivial lower bounds for $\mathsf{Res}(\oplus)$ [10, 11], $\mathsf{Res}(\mathsf{lin}_{\mathbb{F}})$ where $\mathbb{F}$ is a finite field [18], and $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$ [16]. Moreover, they imply the first super-polynomial and exponential lower bounds for tree-like $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$-refutations of mod q Tseitin formulas and random k-CNFs.

*e.khaniki@gmail.com

ISSN 1433-8092

1 Introduction

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

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

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

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

	Proof system	**Proof lines**
1	Cutting Planes	Linear inequalities
2	Polynomial Calculus	Polynomials
3	AC^0-Frege	Constant depth formulas
4	Frege	Formulas

We know lower bounds for the first three systems in the above list, but there are no known super-polynomial lower bounds for the Frege proof system. Since the known lower bounds for the AC^0-Frege proof system were proved by adapting the techniques which had been used to prove super-polynomial and exponential lower bounds for AC^0 circuits (see [1, 14, 19]), the natural next step seemed to be to prove lower bounds for the $\mathsf{AC}^0[p]$-Frege proof system by adapting Razborov–Smolensky approximation method that was used to prove $\mathsf{AC}^0[p]$ circuit lower bounds. However, this problem remains open to this day, and it is one of the frontier problems in propositional proof complexity. Because proving super-polynomial lower bounds for the $\mathsf{AC}^0[p]$-Frege proof system seems to be hard, reasonable subsystems of $\mathsf{AC}^0[p]$-Frege and similar proof systems that can work with some kind of limited counting was investigated in the literature. We briefly review the known results about these systems.

One of the first such systems is the AC^0-Frege proof system with the Count_p Principle, when p is a prime number. Super-polynomial lower bounds were proved on the length of proofs of the Count_q Principle when $q \neq p$ is a prime number for this system in [2, 4, 23].

Two other important proof systems are Nullstellensatz and Polynomial Calculus. There are several works about them in the literature. Here we only mention some of the first ones. The Nullstellensatz proof system was defined by Beame et al. in [4] and they proved the first degree lower bound for it which was for the Count_p Principle. Later the Polynomial Calculus proof system was defined by Clegg et al. in [7] and proved a degree separation between the Nullstellensatz proof system and Polynomial Calculus proof system. Razborov in [22] proved the first nontrivial degree lower bound for Polynomial Calculus and showed that every Polynomial Calculus refutation of the Pigeonhole Principle has degree at least $n/2+1$.

Krajíček in [15] defined the subsystem $\mathsf{F}^c_d(\mathsf{MOD}_p)$ of $\mathsf{AC}^0[p]$-Frege proof system and proved that $\mathsf{F}^c_d(\mathsf{MOD}_p)$ needs super-polynomial size for the Count_q Principle (where $q \neq p$ is a prime number) and tree-like $\mathsf{F}^c_d(\mathsf{MOD}_p)$ needs exponential size for proving the Pigeonhole Principle.

Raz and Tzameret in [21] defined the proof system $\mathsf{R}(\mathsf{lin})$ ($\mathsf{Res}(\mathsf{PC}_1/\mathbb{Z})$ in our notation) and showed that $\mathsf{R}(\mathsf{lin})$ is very strong by proving that this system has polynomial size refutations of the Pigeonhole Principle, mod q Tseitin formulas, and the Clique-Coloring Principle. They also proved an exponential lower bound for a fairly strong fragment of $\mathsf{R}(\mathsf{lin})$ using monotone feasible interpolation. Later Tzameret in [24] investigated the proof system $\mathsf{R}(\mathsf{quad})$ ($\mathsf{Res}(\mathsf{PC}_2/\mathbb{Z})$ in our notation) and proved that if it has the feasible interpolation property, then there is an efficient deterministic refutation algorithm for random 3SAT with n variables and $\Omega(n^{1.4})$ clauses.

Itsykson and Sokolov in [10, 11] introduced the proof system $\mathsf{Res}(\oplus)$ ($\mathsf{Res}(\mathsf{PC}_1/\mathbb{F}_2)$ in our notation). They investigated the power of this system from different aspects and proved that tree-like $\mathsf{Res}(\oplus)$ needs exponential size for refuting the Pigeonhole Principle and lifted versions of Tseitin formulas and Pebbling formulas. They proved these lower bounds by generalizing the well-known prover-delayer games of [20] and also by using the known communication complexity lower bounds.

In [16] Krajíček defined randomized dag-like communication games for Karchmer–Wigderson relations. He proved that $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$ (another formulation of $\mathsf{Res}(\oplus)$) has the randomized feasible interpolation property which means that from a $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$-refutation of the non-disjointness of two NP sets U and V, we can construct such a game for computing the Karchmer–Wigderson relation associated with U and V. Furthermore, he proved that such protocols correspond to monotone circuits with local oracles (CLO) in the case when U is upward closed or V is downward closed. Therefore, if we prove lower bounds for any CLO separating a monotone disjoint NP-pair, this leads to a lower bound for $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$. Using the randomized feasible interpolation, he proved that every tree-like $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$-refutation of the Hall Principle has exponential size (see Theorem 18.6.4 in [12]). He also introduced the proof system $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$ which is a natural generalization of $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$ and discussed the possibility of proving the randomized feasible interpolation property for it. Krajíček and Oliveira in [13] proved lower bounds for a subclass of CLOs (containing the class of the usual monotone circuits) separating k-cliques and the set of complete $(k-1)$-partite graphs, but it is not known whether a lower bound for this subclass is enough for getting a super-polynomial lower bound on the size of $\mathsf{R}(\mathsf{lin}/\mathbb{F}_2)$-refutations of the Clique-Coloring Principle.

Following [15], Garlík and Kołodziejczyk in [8] defined the subsystem $\mathsf{PK}^c_d(\oplus)$ of $\mathsf{AC}^0[2]$-Frege proof system. In this system, every line of a proof is a disjunction such that disjuncts have depth at most d, and parities can only appear as the outermost connectives of disjuncts, and all but c disjuncts contain no parity connective at all. Then they investigated the relation between $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$, tree-like $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$ and the AC^0-Frege proof systems with the Count_2 Principle and proved several lower bounds for them. They also proved that an extension of tree-like $\mathsf{Res}(\oplus)$ is polynomially simulated by a system related to $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$, and hence they obtained an exponential lower bound for the Count_3 Principle for tree-like $\mathsf{Res}(\oplus)$. Although they did not mention it in their paper, their lower bound also works for tree-like $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F}_2)$ when $d = n^\varepsilon$ and $\varepsilon > 0$ is a small enough constant[1]. So they implicitly proved the first super-polynomial lower bound for tree-like $\mathsf{R}(\mathsf{PC}_{n^\varepsilon}/\mathbb{F}_2)$.

Part and Tzameret in [18] defined the proof system $\mathsf{Res}(\mathsf{lin}_R)$ for every ring R ($\mathsf{Res}(\mathsf{PC}_1/R)$ in our notation), and proved several lower bounds for dag-like and tree-like $\mathsf{Res}(\mathsf{lin}_R)$ for different rings. In particular, for finite fields they proved exponential lower bounds for the Pigeonhole Principle, mod q Tseitin formulas (q is a prime different from the characteristic of the field) and random k-CNFs. They used two main tools for proving these lower bounds. First, they generalized the prover-delayer game of [10] to an arbitrary ring R. Second they proved a size-width relation for tree-like $\mathsf{Res}(\mathsf{lin}_R)$ for any ring R. They also proved the first super-polynomial lower bound for dag-like $\mathsf{Res}(\mathsf{lin}_\mathbb{Q})$-refutations. This lower bound was proved for the Subset-sum Principle which is not a CNF, so the lower bound problem for CNFs remained open. It is worth noting that a size-width relation for tree-like $\mathsf{Res}(\oplus)$ was proved by Garlík and Kołodziejczyk in an unpublished manuscript before [18].

Following the prover-delayer method that was used in [10, 18], Gryaznov proved in [9] exponential lower bounds for the Ordering and Dense Linear Ordering Principles in tree-like $\mathsf{Res}(\oplus)$, and hence separated tree-like $\mathsf{Res}(\oplus)$ and Res. Regarding the separation between tree-like $\mathsf{Res}(\oplus)$ and Res, [11] strengthened Gryaznov's result by proving that a lifted version of Pebbling formulas is hard for tree-like $\mathsf{Res}(\oplus)$, but it is easy for regular Resolution.

In this paper we continue investigating the power of $\mathsf{Res}(\mathsf{PC}_1/R)$, tree-like $\mathsf{Res}(\mathsf{PC}_1/R)$ and also their generalization $\mathsf{Res}(\mathsf{PC}_d/R)$ and tree-like $\mathsf{Res}(\mathsf{PC}_d/R)$ when $d > 1$. Our main theorem (Theorem 3.1) is a new size-width relation. This theorem has two advantages to the size-width relation of [18]. First, it works for the dag-like systems such as $\mathsf{Res}(\mathsf{lin}_R)$ and more generally $\mathsf{Res}(\mathsf{PC}_d/R)$, and hence we can prove nontrivial lower bounds in the dag-like setting. Second, it is not limited to linear forms, and we can prove lower bounds for Resolution over polynomials. Moreover, the proof of this theorem uses the same strategy for the tree-like and dag-like proofs.

Contents of this paper. In section 2, we explain definitions and notations. In section 3, we state the main results. In section 4, we prove a size-width relation for $\mathsf{Res}(\mathsf{PC}_d/R)$ and tree-like $\mathsf{Res}(\mathsf{PC}_d/R)$ over every finite ring R. The novel idea that is used to prove these size-width relations is a combination of the usage of extension variables and the size-width relation of Ben-Sasson and Wigderson for Resolution [5]. In more detail, the main

[1] Private communication with Leszek Kołodziejczyk.

idea is to use the extension variables to translate refutations in $\mathsf{Res}(\mathsf{PC}_d/R)$ and tree-like $\mathsf{Res}(\mathsf{PC}_d/R)$ to Resolution refutations of some new clauses formed by these new extension variables, then use the size-width relation of Ben-Sasson and Wigderson for Resolution [5], and finally translate back to $\mathsf{Res}(\mathsf{PC}_d/R)$-refutations. In section 5, we prove lower bounds as an application of this theorem. To prove these lower bounds, we show that if a CNF formula F has a low width $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$-refutation, then it also has a low degree refutation in Polynomial Calculus over $\mathbb{F}$. This strategy was first used in [18] to relate the width of $\mathsf{Res}(\mathsf{lin}_\mathbb{F})$-refutations of F to the degree of Polynomial Calculus refutations of it. This enables us to use the known degree lower bounds for Polynomial Calculus and the new size-width relation to prove our lower bounds. We prove the first nontrivial (almost quadratic) lower bounds for $\mathsf{Res}(\mathsf{PC}_1/\mathbb{F})$ and in general for $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$ (for every fixed d) over finite fields. For the tree-like case over finite fields, we prove the first super-polynomial and exponential lower bounds for tree-like $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$ where d is limited by some sub-linear function of n. These lower bounds imply the first nontrivial (almost quadratic) lower bound for $\mathsf{Res}(\oplus)$, $\mathsf{Res}(\mathsf{lin}_\mathbb{F})$ when $\mathbb{F}$ is a finite field, and $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$. Moreover, it implies the first super-polynomial and exponential lower bounds for tree-like $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$-refutations of mod q Tseitin formulas and random k-CNFs.

2 Preliminaries

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

1. Resolution:

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

2. Weakening:

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

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

A CNF formula is a set of clauses. The set of variables appearing in a clause D and a CNF formula F are denoted by $V(D)$ and $V(F)$. A Resolution derivation of a clause D from the CNF formula $F = \{C_1, ..., C_k\}$, shown as $F \vdash D$, is a sequence $\pi = D_1, ..., D_l$ such that:

1. $D_l = D$,

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

For a ring R, we define Resolution over Polynomial Calculus, $\mathsf{Res}(\mathsf{PC}/R)$, as a proof system like Res which works with clauses of polynomials of boolean variables (no negative variables), instead of literals. So a clause in $\mathsf{Res}(\mathsf{PC}/R)$ is $C = \bigvee_{i<l} f_i(\bar{x})$ such that each $f_i(\bar{x})$ is a polynomial with coefficients in R. Moreover, there is no repetition of polynomials in a clause. $C = \bigvee_{i<l} f_i(\bar{x})$ is true under a boolean assignment $a \in \{0,1\}^n$ iff there exists an i such that $f_i(a) = 0$. Following [18], we use a similar set of rules for defining $\mathsf{Res}(\mathsf{PC}/R)$:

1. Resolution:

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

   for every $a, b \in R$,

2. Weakening:

$$\frac{C}{C \vee f(\bar{x})}$$

3. Simplification:

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

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

4. Multiplication:

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

where $g(\bar{x}), f(\bar{x})$ are polynomials with coefficients in R and $x \in \{x_1, ..., x_n\}$ is a variable from the initial clauses. Furthermore, $\mathsf{Res}(\mathsf{PC}/R)$ has 0 and $x \vee x - 1$ ($x \in \{x_1, ..., x_n\}$) as axioms. A $\mathsf{Res}(\mathsf{PC}/R)$ derivation of a clause D from the CNF formula $F = \{C_1, ..., C_k\}$, $F \vdash D$ is a sequence $\pi = D_1, ..., D_l$ such that:

1. $D_l = D$,

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

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

In this paper, we study the length of refutations in the $\mathsf{Res}(\mathsf{PC}_d/R)$ and tree-like $\mathsf{Res}(\mathsf{PC}_d/R)$. A CNF formula F is refutable if $F \vdash \emptyset$ where $\emptyset$ is the empty clause. The size of a derivation π is denoted by $|\pi|$, and it is the number of clauses in π. This measure lower bounds the usual bit-size of proofs, therefore our lower bounds also hold for the bit-size measure too.

Let $\pi = D_1, .., D_l$ be a derivation in one of the defined proof systems. The graph G_π associated with π is a DAG with D_is as nodes, and for every derivation step directed edges are added from the assumptions clauses to the consequence clause. π is called tree-like iff G_π is a tree. In general, it is possible to make any derivation tree-like by making copies of the initial clauses. If P is one of the defined proof systems, then P^* denotes tree-like P.

Let C be a disjunction of literals or polynomials, then $\mathsf{m}[C]$ is the set of disjuncts of C and $\mathsf{w}(C)$ (width of C) is the number of disjuncts in C, so $\mathsf{w}(C) = |\mathsf{m}[C]|$. For a CNF formula $F = \{C_1, ..., C_k\}$, $\mathsf{w}(F) = \max_{C \in F} \mathsf{w}(C)$. For a derivation π in one of the defined proof systems, $\mathsf{w}(\pi) = \max_{D \in \pi} \mathsf{w}(D)$. For a proof system P, a set of clauses F (not necessarily nonempty) and a clause D, the notation

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

means that there exists a P-derivation π for D from F such that $\mathsf{w}(\pi) \leq w$. If F is an unsatisfiable CNF and R is a ring, then the refutation size and the width corresponding to F in $\mathsf{Res}(\mathsf{PC}_d/R)$ are respectively:

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

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

$\mathsf{S}^*_{R,d}(F)$ is the refutation size corresponding to F in $\mathsf{Res}^*(\mathsf{PC}_d/R)$. Res-refutation width and size corresponding to F is denoted by $\mathsf{w}_{\mathsf{Res}}(F)$ and $\mathsf{S}_{\mathsf{Res}}(F)$. For Res^*, minimal refutation size of F is denoted by $\mathsf{S}_{\mathsf{Res}^*}(F)$.

It is easy to see that (tree-like) $\mathsf{Res}(\mathsf{PC}_1/\mathbb{F}_2)$ simulates (tree-like) $\mathsf{Res}(\oplus)$ of [10, 11] and (tree-like) $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F}_2)$ simulates (tree-like) $\mathsf{R}(\mathsf{PC}_d/\mathbb{F}_2)$ of [16].

3 Main results

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

Theorem 3.1 *(Size-Width relation) Let R be a finite ring and F be an unsatisfiable CNF in n variables, then for every d, the following inequalities hold:*

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

2. $\frac{\mathsf{w}_{R,d}(F)}{|R|} - 1 \leq \max\{3, \mathsf{w}(F)\} + O\left(\sqrt{\left(2n + 3\mathsf{S}_{R,d}(F)\right)\log(3\mathsf{S}_{R,d}(F))}\right)$.

where log *is the binary logarithm.*

Proof. See section 4. ∎

Using the above theorem we prove new lower bounds for the mod q Tseitin formulas and random k-CNFs.

Definition 3.1 *(mod q Tseitin formulas) Let $G = (V, E)$ be a directed d-regular graph. For every $(v, u) \in E$, we have a fixed variable $x_{u,v}$. Let $\sigma : V \to \mathbb{F}_q$ (q is a prime number). Then mod q Tseitin formula $T_q(G, \sigma)$ is a CNF encoding of the following equations for every $v \in V$:*

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

Note that $T_q(G, \sigma)$ is unsatsifiable iff $\sum_{v\in V} \sigma(v) \not\equiv 0 \pmod q$. This formula has $O(2^d|V|)$ clauses and each clause has width $O(d)$. So in particular, the number of clauses of this formula is linear in the number of variables when d is a fixed constant. This is important for our almost quadratic lower bound for $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$, because for every unsatisfiable CNF formula F, $|F| \leq \mathsf{S}_{R,d}(F)$.

Definition 3.2 *(Random k-CNF) A random k-CNF is a formula $F \sim \mathcal{F}_k^{n,\Delta}$ with n variables that is generated by picking randomly and independently $\Delta \cdot n$ clauses from the set of all $2^k\binom{n}{k}$ clauses of width k.*

The following corollaries explain the new lower bounds.

Corollary 3.2 *Let $\mathbb{F}$ be a finite field. Then the following lower bounds hold:*

1. *If q is a fixed prime such that char$(\mathbb{F}) \neq q$, then there exists a constant d_q such that for every fixed d the following holds. If $c \geq d_q$, then for every large enough n and every c-regular Ramanujan graph G on n nodes (augmented with arbitrary orientation of its edges) and for every function σ such that $T_q(G, \sigma)$ is unsatisfiable, $n^{2-\frac{(\log\log n)^2}{\log n}} \leq \mathsf{S}_{\mathbb{F},d}(T_q(G, \sigma))$.*
2. *Let $F \sim \mathcal{F}_k^{n,\Delta}$, $k \geq 3$ and $\Delta = \Delta(n)$ is such that $\Delta = c$ for some constant c with the property that $c2^{-k} \geq 0.7$. Then with probability $1 - o(1)$, $n^{2-\frac{(\log\log n)^2}{\log n}} \leq \mathsf{S}_{\mathbb{F},d}(F)$.*

Proof. See section 5. ■

Corollary 3.3 *Let $\mathbb{F}$ be a finite field. Then The following lower bounds hold:*

1. *If q is a fixed prime such that char$(\mathbb{F}) \neq q$, then there exists a constant d_q such that for every fixed d the following holds. If $c \geq d_q$, then for every large enough n and every c-regular Ramanujan graph G on n nodes (augmented with arbitrary orientation of its edges) and for every function σ such that $T_q(G, \sigma)$ is unsatisfiable, $\mathsf{S}^*_{\mathbb{F},d(n)}(T_q(G, \sigma))$ is*
   (a) *super-polynomial if for every natural number k, $\frac{n}{k\log n}$ eventually dominates $d(n)$.*
   (b) *exponential if there exists $\varepsilon \in (0, 1)$ such that n^ε eventually dominates $d(n)$.*

2. *Let $F \sim \mathcal{F}_k^{n,\Delta}$, $k \geq 3$ and $\Delta = \Delta(n)$ is such that $\Delta = o(n^{\frac{k-2}{2}})$. Then with probability $1 - o(1)$, $\mathsf{S}^*_{\mathbb{F},d(n)}(F)$ is*
   - (a) *super-polynomial if for every natural number k', $\frac{n}{k'\Delta^{2/(k-2)} \cdot \log \Delta \cdot \log n}$ eventually dominates $d(n)$.*
   - (b) *exponential if there exists $\varepsilon \in (0,1)$ such that $\frac{n^{\varepsilon}}{\Delta^{2/(k-2)} \cdot \log \Delta}$ eventually dominates $d(n)$.*

Proof. See section 5. ■

As we mentioned in Preliminaries the proved lower bounds in Corollaries 3.2 and 3.3 also hold for the bit-size of proofs.

4 Size-Width relation for $\mathsf{Res}(\mathsf{PC}_d/R)$ and $\mathsf{Res}^*(\mathsf{PC}_d/R)$

In this section, we prove the size-width relation in a sequence of propositions and lemmas. In the next section we prove the lower bounds using the size-width relation.

Proposition 4.1 *For every ring R, and every monomial $p(\bar{x}) = \prod_{i=1}^{n} x_i^{d_i}$ of total degree d ($\sum_{i=1}^{n} d_i = d$),*

$$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{2} p(\bar{x}) \vee p(\bar{x}) - 1.$$

Proof. We prove this proposition by induction on d. The statement is true for $d \leq 1$. Because we have boolean axioms for every variable and also 0 is an axiom. Let $p(\bar{x}) = x'p'(\bar{x})$ with total degree $d = k+1$. By induction hypothesis

$$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_k/R)}_{2} p'(\bar{x}) \vee p'(\bar{x}) - 1.$$

So by two times using of the multiplication rule we get

$$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_{k+1}/R)}_{2} x'p'(\bar{x}) \vee x'p'(\bar{x}) - x'.$$

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

$$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_{k+1}/R)}_{2} x'p'(\bar{x}) \vee x' - 1.$$

By applying the resolution rule on $x'p'(\bar{x}) \vee x'p'(\bar{x}) - x'$ and $x'p'(\bar{x}) \vee x' - 1$, we get

$$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_{k+1}/R)}_{2} x'p'(\bar{x}) \vee x'p'(\bar{x}) - 1.$$

■

Proposition 4.2 *Let R be a finite ring. Then for every polynomial $p(\bar{x}) \in R[\bar{x}]$ of total degree d,*

$$\varnothing \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1}} \bigvee_{a\in R} p(\bar{x}) - a.$$

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

$$\varnothing \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1}} \bigvee_{a\in R} g(\bar{x}) - a.$$

By Proposition 4.1,

$$\varnothing \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{2}} f(\bar{x}) \vee f(\bar{x}) - 1.$$

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

$$\varnothing \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1}} f(\bar{x}) - 1 \vee \bigvee_{a\in R} bf(\bar{x}) + g(\bar{x}) - a.$$

By the same argument, we get

$$\varnothing \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1}} f(\bar{x}) \vee \bigvee_{a\in R} bf(\bar{x}) + g(\bar{x}) - a - b.$$

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

$$\varnothing \mathrel{\Big|\!\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1}} \bigvee_{a\in R} p(\bar{x}) - a.$$

■

Let R be a finite ring. Suppose π is a P-refutation of a CNF formula F in variables $V(F) = \{x_1, ..., x_n\}$, $P \in \{\mathsf{Res}^*(\mathsf{PC}_d/R), \mathsf{Res}(\mathsf{PC}_d/R)\}$. For every polynomial $f(\bar{x}) \in R[\bar{x}]$ of total degree at most d, we define a new atomic variable q_f. To prove the size-width relation, we translate polynomials that appeared in π to new atomic variables by a mapping Q. Furthermore, we define a new CNF formula $\mathsf{Ex}(\pi)$ using these new variables and original ones such that:

(I) $\mathsf{S}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)) \leq 3|\pi|$. Moreover, if π is tree-like, then we have $\mathsf{S}_{\mathsf{Res}^*}(\mathsf{Ex}(\pi) \cup Q(F)) \leq 3|\pi|$.

(II) An upper bound for $\mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F))$ implies an upper bound for $\mathsf{w}_{R,d}(F)$.

Using the above relations and the Ben-Sasson and Wigderson size-width relation for (tree-like) Res, we prove our size-width relation.

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

$$Q(f) = q_f.$$

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

The CNF formula $\mathsf{Ex}(\pi)$ contains the following clauses:

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

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

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

4. If the resolution rule is used in π to derive $af + bg$ from f and g, then
$$\neg q_f \vee \neg q_g \vee q_{af+bg} \in \mathsf{Ex}(\pi).$$

5. If the multiplication rule is used to derive $g \cdot f$ from f, then
$$\neg q_f \vee q_{g \cdot f} \in \mathsf{Ex}(\pi).$$

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

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

For a clause C, $Q'(C)$ is $\bigvee_{r \in C} Q'(r)$ $(Q'(\emptyset) = \emptyset)$. Now we are ready to state the lemma for proving properties (I) and (II).

Lemma 4.3 *For a finite ring R and every CNF formula F, let π be a $\mathsf{Res}(\mathsf{PC}_d/R)$-refutation of F, then the following statements are true:*

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

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

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

then

$$F \mathrel{\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|(w+1)}} Q'(C^*).$$

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

Claim 1 *Let $f(\bar{x}) \in R[\bar{x}]$ be a polynomial, then if the step*

$$\frac{C}{C \vee f(\bar{x})}$$

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

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

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

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

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

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

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

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

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

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

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

So the appended derivation is the following:

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

ii. $f(\bar{x}) = g(\bar{x})$:

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

A. $\neg q_f \lor q_{af+bf}$,

B. $Q(C) \lor q_{af+bf}$,

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

So the appended derivation is the following:

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

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

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

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

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

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

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

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

Note that for every i the inequality $|\pi'_i| \leq |\pi'_{i-1}| + 3$ holds, hence $|\pi'| \leq 3|\pi|$.

2. We prove this part by induction on the number of steps of deriving C^*.

   (a) Base step:
   If the number of steps in deriving C^* is one, then C^* is one of the initial clauses of $\mathsf{Ex}(\pi) \cup Q(F)$. Therefore we have the following cases:

   i. $C^* \in Q(F)$:
   In this case $Q'(C^*)$ is a clause of F, so

   $$F \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{w} Q'(C^*).$$

   ii. $C^* = q_0$:
   0 is an axiom of $\mathsf{Res}(\mathsf{PC}_d/R)$, so

   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{1} 0.$$

   iii. $C^* = \neg q_a$ for some $a \in R \setminus \{0\}$:
   Note that $Q'(\neg q_a) = \bigvee_{b \in R \setminus \{0\}} a - b$ which is $\bigvee_{b \in R \setminus \{a\}} b$. 0 is an axiom of $\mathsf{Res}(\mathsf{PC}_d/R)$, so by $|R| - 1$ times use of the weakening rule we get

   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{|R|-1} \bigvee_{b \in R \setminus \{a\}} b.$$

   iv. $C^* = q_{x_i} \vee q_{x_i - 1}$:
   $Q'(q_{x_i} \vee q_{x_i-1})$ is $x_i \vee x_i - 1$ which is an axiom of $\mathsf{Res}(\mathsf{PC}_d/R)$, so

   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{2} x_i \vee x_i - 1.$$

   v. $C^* = \neg q_f \vee \neg q_g \vee q_{af+bg}$:

   A. $f(\bar{x}) \neq g(\bar{x})$:
   Note that

   $$\mathsf{Ex}(\pi) \cup Q(F) \vdash^{\mathsf{Res}}_{3} C^*.$$

   By Proposition 4.2,

   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{|R|+1} \bigvee_{c \in R} f(\bar{x}) - c$$

   and

   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/R)}_{|R|+1} \bigvee_{c \in R} g(\bar{x}) - c,$$

   hence by the resolution rule we get

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

B. $f(\bar{x}) = g(\bar{x})$:
Note that

$$\mathsf{Ex}(\pi) \cup Q(F) \,\Big|\!\frac{\mathsf{Res}}{2}\, C^*$$

because $C^* = \neg q_f \vee q_{af+bf}$. By Proposition 4.2,

$$\varnothing \,\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1} \bigvee_{c \in R} f(\bar{x}) - c,$$

hence by the multiplication rule we get

$$\varnothing \,\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1} (a+b)f(\bar{x}) \vee \bigvee_{c \in R \setminus \{0\}} f(\bar{x}) - c.$$

vi. $C^* = \neg q_f \vee q_{g \cdot f}$:
Note that

$$\mathsf{Ex}(\pi) \cup Q(F) \,\Big|\!\frac{\mathsf{Res}}{2}\, C^*.$$

By Proposition 4.2,

$$\varnothing \,\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1} \bigvee_{c \in R} f(\bar{x}) - c,$$

hence by the multiplication rule we get

$$\varnothing \,\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|+1} g(\bar{x}) \cdot f(\bar{x}) \vee \bigvee_{c \in R \setminus \{0\}} f(\bar{x}) - c.$$

(b) Induction step:

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

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

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

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

B. $\mathsf{Ex}(\pi) \cup Q(F) \,\Big|\!\frac{\mathsf{Res}}{w_2}\, D \vee \neg q_f$ in at most k steps.

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

A. $F \,\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|(w_1+1)} Q'(C \vee q_f)$.

B. $F \,\Big|\!\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|(w_2+1)} Q'(D \vee \neg q_f)$.

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

$$H := \{f(\bar{x}) - c | c \in R\},$$

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

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

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

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

which is less than or equal to

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

which is less than or equal to

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

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

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

which is less than or equal to

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

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

$$\mathsf{Ex}(\pi) \cup Q(F) \vert\frac{\mathsf{Res}}{w} C \vee D$$

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

A. $\mathsf{Ex}(\pi) \cup Q(F) \vert\frac{\mathsf{Res}}{w_1} C$ in at most k steps.

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

A. $F \vert\frac{\mathsf{Res}(\mathsf{PC}_d/R)}{|R|(w_1+1)} Q'(C)$.

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

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

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

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

which is less than or equal to

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

which is less than or equal to

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

■

For proving the size-width relation for (tree-like) $\mathsf{Res}(\mathsf{PC}_d/R)$, we need the size-width relation of Ben-Sasson and Wigderson which was proved in the seminal paper [5].

Theorem 4.4 *([5]) For every unsatisfiable CNF formula F in n variables, the following inequalities hold:*

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

where log *is the binary logarithm.*

4.1 Proof of Theorem 3.1

1. Let π be a minimal size $\mathsf{Res}^*(\mathsf{PC}_d/R)$-refutation of F ($|\pi| = \mathsf{S}^*_{R,d}(F)$). By the first part of Lemma 4.3,
$$\mathsf{S}_{\mathsf{Res}^*}(\mathsf{Ex}(\pi) \cup Q(F)) \leq 3\mathsf{S}^*_{R,d}(F).$$
On the other hand, by the second part of Lemma 4.3,
$$\frac{\mathsf{w}_{R,d}(F)}{|R|} - 1 \leq \mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)).$$
Furthermore, $\mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) \leq \max\{3, \mathsf{w}(F)\}$, because $\mathsf{w}(\mathsf{Ex}(\pi)) \leq 3$ by the way we constructed it. Note that by the first inequality of Theorem 4.4
$$\mathsf{w}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)) \leq \mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) + \log \mathsf{S}_{\mathsf{Res}^*}(\mathsf{Ex}(\pi) \cup Q(F)).$$
So putting these inequalities together we get
$$\frac{\mathsf{w}_{R,d}(F)}{|R|} - 1 \leq \max\{3, \mathsf{w}(F)\} + \log 3\mathsf{S}^*_{R,d}(F).$$

2. The proof of this part is similar to the proof of the previous part with some extra efforts. Let π be a minimal size $\mathsf{Res}(\mathsf{PC}_d/R)$-refutation of F ($|\pi| = \mathsf{S}_{R,d}(F)$). By the first part of Lemma 4.3,
$$\mathsf{S}_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup Q(F)) \leq 3\mathsf{S}_{R,d}(F).$$

On the other hand, by the second part of Lemma 4.3,

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

Furthermore, $\mathsf{w}(\mathsf{Ex}(\pi) \cup Q(F)) \le \max\{3, \mathsf{w}(F)\}$, because $\mathsf{w}(\mathsf{Ex}(\pi)) \le 3$ by the way we constructed it. Note that by the second inequality of Theorem 4.4

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

so putting these inequalities together we get

$$\frac{\mathsf{w}_{R,d}(F)}{|R|} - 1 \le \max\{3, \mathsf{w}(F)\} + O\left(\sqrt{|V\left(\mathsf{Ex}(\pi) \cup Q(F)\right)| \log 3\mathsf{S}_{R,d}(F)}\right).$$

To complete the proof, it is sufficient to bound the value of $|V(\mathsf{Ex}(\pi) \cup Q(F))|$. Note that F is a CNF, so every disjunct in a clause of it is of the form of x or $x - 1$ where $x \in V(F)$. By the fact that F has n variables, we can deduce that $|V(Q(F))| \le 2n$. Moreover, if we look at the way $\mathsf{Ex}(\pi)$ was constructed, we can see that for every step in π, we add a clause with at most three new variables to $\mathsf{Ex}(\pi)$, so this implies $V(\mathsf{Ex}(\pi)) \le 3|\pi|$. From these facts we get

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

so we get the desired inequality which is

$$\frac{\mathsf{w}_{R,d}(F)}{|R|} - 1 \le \max\{3, \mathsf{w}(F)\} + O\left(\sqrt{(2n + 3\mathsf{S}_{R,d}(F)) \log 3\mathsf{S}_{R,d}(F)}\right).$$

■

5 Application of the Size-Width relation to Lower bounds

In this section, we prove the lower bounds for $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$ and $\mathsf{Res}^*(\mathsf{PC}_d/\mathbb{F})$ for every finite field $\mathbb{F}$. We use the same strategy as [18] by proving width lower bounds from degree lower bounds of Polynomial Calculus refutations.

Let $\mathbb{F}$ be a field. Then Polynomial Calculus over the field $\mathbb{F}$, $\mathsf{PC}/\mathbb{F}$ is a proof system that works with polynomials with coefficients in $\mathbb{F}$. A polynomial $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ is true under the boolean assignment $a \in \{0,1\}^n$ iff $f(a) = 0$. $\mathsf{PC}/\mathbb{F}$ has the following rules:

1. Addition:

$$\frac{f(\bar{x}) \qquad g(\bar{x})}{af(\bar{x}) + bg(\bar{x})}$$

for every $a, b \in \mathbb{F}$,

2. Multiplication:

$$\frac{f(\bar{x})}{x \cdot f(\bar{x})}$$

where $f(\bar{x}), g(\bar{x})$ are polynomials with coefficients in $\mathbb{F}$ and $x \in \{x_1, ..., x_n\}$ is a variable from the initial polynomials. Moreover, $\mathsf{PC}/\mathbb{F}$ has $x^2 - x$ for every $x \in \{x_1, ..., x_n\}$ as an axiom. A $\mathsf{PC}/\mathbb{F}$- derivation of a polynomial $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ from a set of polynomials $F \subseteq \mathbb{F}[\bar{x}]$, $F \vdash f$ is a sequence $\pi = D_1, ..., D_l$ such that:

1. $D_l = f$,

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

A $\mathsf{PC}/\mathbb{F}$-refutation of a set $F \subseteq \mathbb{F}[\bar{x}]$ is a derivation of 1 from F ($F \vdash 1$). One of the important measure for Polynomial calculus derivations is the degree measure. For a polynomial $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ let $\mathsf{d}(f)$ be the degree of $f(\bar{x})$. For a set $F \subseteq \mathbb{F}[\bar{x}]$ (not necessarily nonempty) and a polynomial $f(\bar{x}) \in \mathbb{F}[\bar{x}]$, the notation

$$F \mathrel{\Big|\!\frac{\mathsf{PC}/\mathbb{F}}{d}} f$$

means there exists a $\mathsf{PC}/\mathbb{F}$-proof π for f from F such that the degree of each polynomial in π is at most d.

Let $C = \{f_1, ..., f_l\}$ be a clause of polynomials over the field $\mathbb{F}$. Then the arithmetization of C is the polynomial $h_C(\bar{x}) = \prod_{f \in C} f(\bar{x})$ ($h_\emptyset(\bar{x}) = 1$).

To prove the relation between $\mathsf{Res}_\mathbb{F}(\mathsf{PC})$ and $\mathsf{PC}/\mathbb{F}$ we need the following lemma.

Lemma 5.1 *Let $\mathbb{F}$ be a field and $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ be a polynomial. Then the following statements are true:*

1. *For every polynomial $g(\bar{x}) \in \mathbb{F}[\bar{x}]$,*

$$\{f(\bar{x})\} \mathrel{\Big|\!\frac{\mathsf{PC}/\mathbb{F}}{\mathsf{d}(f)+\mathsf{d}(g)}} g(\bar{x}) \cdot f(\bar{x}).$$

2. *If $\mathbb{F}$ is a finite field such that $char(\mathbb{F}) = p$ for some prime p, then*

$$\{f^2(\bar{x})\} \mathrel{\Big|\!\frac{\mathsf{PC}/\mathbb{F}}{p \cdot \mathsf{d}(f)}} f(\bar{x}).$$

Proof. 1. Let $g(\bar{x}) = \sum_{p \in A} p(\bar{x})$ where A is a set of monomials with coefficients in $\mathbb{F}$. For every $p(\bar{x}) = a \prod_{i=1}^n x_i^{d_i}$ in A where $a \in \mathbb{F}$, we have

$$\{f(\bar{x})\} \mathrel{\Big|\!\frac{\mathsf{PC}/\mathbb{F}}{\mathsf{d}(f)+\mathsf{d}(p)}} u_p(\bar{x}) \cdot f(\bar{x})$$

by $\mathsf{d}(p)$ applications of the multiplication rule where $u_p(\bar{x}) = \frac{1}{a}p(\bar{x})$. So by adding $u_p(\bar{x}) \cdot f(\bar{x})$ for every $p(\bar{x}) \in A$ using the addition rule we get

$$\{f(\bar{x})\} \vdash^{\mathsf{PC}/\mathbb{F}}_{\mathsf{d}(f)+\max_{p\in A}\{\mathsf{d}(u_p)\}} \sum_{p\in A} p(\bar{x}) \cdot f(\bar{x})$$

which means

$$\{f(\bar{x})\} \vdash^{\mathsf{PC}/\mathbb{F}}_{\mathsf{d}(f)+\mathsf{d}(g)} g(\bar{x}) \cdot f(\bar{x}).$$

2. Let $f(\bar{x}) = \sum_{q\in A} q(\bar{x})$ where A is a set of monomials with coefficients in $\mathbb{F}$. It is well-known that the identity $(x+y)^p = x^p + y^p$ is true in every field of characteristic p. Therefore

   $$f^p(\bar{x}) = \sum_{q\in A} q^p(\bar{x})$$

   which implies

   $$\{f^2(\bar{x})\} \vdash^{\mathsf{PC}/\mathbb{F}}_{p\cdot\mathsf{d}(f)} \sum_{q\in A} q^p(\bar{x})$$

   by the previous part of the lemma. Moreover, it is easy to prove that for every monomial $q(\bar{x}) = \prod_{i=1}^{n} x_i^{d_i}$ and every $k \geq 1$, $\varnothing \vdash^{[\mathsf{PC}/\mathbb{F}, k\cdot\mathsf{d}(q)]} q^k(\bar{x}) - q(\bar{x})$. This can be proved by induction on $\mathsf{d}(q)$ and using the fact that $x^2 - x$ is an axiom for every $x \in \{x_1, ..., x_n\}$. This implies that by applications of the addition rule we get

   $$\{f^2(\bar{x})\} \vdash^{\mathsf{PC}/\mathbb{F}}_{p\cdot\mathsf{d}(f)} \sum_{q\in A} q^p(\bar{x}) - (q^p(\bar{x}) - q(\bar{x}))$$

   which means

   $$\{f^2(\bar{x})\} \vdash^{\mathsf{PC}/\mathbb{F}}_{p\cdot\mathsf{d}(f)} f(\bar{x}).$$

■

Now we are ready to state the relation between $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$ and $\mathsf{PC}/\mathbb{F}$. This is the generalization of Theorem 45 in [18].

For a CNF formula F, let $H_F = \{h_C | C \in F\}$.

Lemma 5.2 *Let F be a CNF. Then for every finite field $\mathbb{F}$ (char($\mathbb{F}$)=p), every clause C^*, and every d, if $F \vdash^{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}_{w} C^*$, then $H_F \vdash^{\mathsf{PC}/\mathbb{F}}_{pwd} h_{C^*}$.*

Proof. The proof of this lemma is similar to the proof of Proposition 26 in [18] using induction on the number of the steps in derivation of C^* from F.

1. Base step:

   If the number of steps in deriving C^* is one, then C^* is one of the initial clauses of F or an axiom. Therefore we have the following cases:

   (a) $C^* \in F$:
   In this case
   $$C^* \vdash^{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}_{\mathsf{w}(C^*)} C^*,$$
   so
   $$\{h_{C^*}(\bar{x})\} \vdash^{\mathsf{PC}/\mathbb{F}}_{d\mathsf{w}(C^*)} h_{C^*}(\bar{x}).$$

   (b) 0:
   0 is an axiom of $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$, so
   $$\varnothing \vdash^{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}_{1} 0.$$
   Note that $x_i^2 - x_i$ is an axiom in $\mathsf{PC}/\mathbb{F}$. So we can derive 0 by using the addition rule on $x_i^2 - x_i$, therefore
   $$\varnothing \vdash^{\mathsf{PC}/\mathbb{F}}_{2} 0.$$

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

2. Induction step:

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

      i. $F \vdash^{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}_{w_1} C \vee f(\bar{x})$ in at most k steps.
      ii. $F \vdash^{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}_{w_2} D \vee g(\bar{x})$ in at most k steps.

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

      i. $H_F \vdash^{\mathsf{PC}/\mathbb{F}}_{pw_1d} h_{C \vee f}(\bar{x})$.
      ii. $H_F \vdash^{\mathsf{PC}/\mathbb{F}}_{pw_2d} h_{D \vee g}(\bar{x})$.

   Let $E := \mathsf{m}[C \vee D]$. Then by the first part of Lemma 5.1

i. $\{h_{C\vee f}(\bar{x})\} \mid\frac{\mathsf{PC}/\mathbb{F}}{\mathsf{d}(h_E)+\mathsf{d}(f)} h_E(\bar{x}) \cdot f(\bar{x})$.

ii. $\{h_{D\vee g}(\bar{x})\} \mid\frac{\mathsf{PC}/\mathbb{F}}{\mathsf{d}(h_E)+\mathsf{d}(g)} h_E(\bar{x}) \cdot g(\bar{x})$.

Hence by application of the addition rule we get

$$h_E(\bar{x})(af(\bar{x}) + bg(\bar{x}))$$

and the degree of deriving this polynomial is at most

$$\max\{pw_1d, pw_2d, \mathsf{d}(h_E(af + bg))\}.$$

To prove an upper bound for the above quantity we should consider the following cases:

i. $af(\bar{x}) + bg(\bar{x}) \notin E$:
In this case,

$$h_E(\bar{x})(af(\bar{x}) + bg(\bar{x})) = h_{C\vee D\vee af+bg}(\bar{x}).$$

Therefore

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

so the degree of deriving $h_{C\vee D\vee af+bg}(\bar{x})$ is at most

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

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

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

By the second part of Lemma 5.1 we have

$$\{(af(\bar{x}) + bg(\bar{x}))^2\} \mid\frac{\mathsf{PC}/\mathbb{F}}{p\mathsf{d}(af+bg)} af(\bar{x}) + bg(\bar{x}).$$

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

$$\max\{pw_1d, pw_2d, \mathsf{d}(h_E(af + bg)), \mathsf{d}(h_{E'}) + p\mathsf{d}(af + bg)\}.$$

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

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

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

$$\max\{pw_1d, pw_2d, d(\mathsf{w}(C \vee D \vee af + bg) + 1), d(\mathsf{w}(C \vee D) - 1) + pd\}$$

which is less than or equal to

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

(b) Weakening rule: Suppose C is a clause in variables of F and $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ such that

$$F \Big|\frac{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}{w}\, C \vee f(\bar{x})$$

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

i. $F \Big|\frac{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}{w_1}\, C$ in at most k steps.

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

i. $H_F \Big|\frac{\mathsf{PC}/\mathbb{F}}{pw_1d}\, h_C(\bar{x})$.

Note that $h_{C\vee f}(\bar{x}) = h_C(\bar{x}) \cdot f(\bar{x})$, hence by the first part of Lemma 5.1

i. $\{h_C(\bar{x})\} \Big|\frac{\mathsf{PC}/\mathbb{F}}{\mathsf{d}(h_C)+\mathsf{d}(f)}\, h_{C\vee f}(\bar{x})$.

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

$$\max\{pw_1d, \mathsf{d}(h_{C\vee f})\}$$

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

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

(c) Simplification rule:
Suppose C is a clause in variables of F and $a \in \mathbb{F} \setminus \{0\}$ such that

$$F \Big|\frac{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}{w}\, C$$

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

i. $F \Big|\frac{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}{w_1}\, C \vee a$ in at most k steps.

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

i. $H_F \Big|\frac{\mathsf{PC}/\mathbb{F}}{pw_1d}\, h_{C\vee a}(\bar{x})$.

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

$$\max\{pw_1d, \mathsf{d}(h_C)\} \leq pw_1d.$$

(d) Multiplication rule:
Suppose C is a clause in variables of F and $f(\bar{x}), g(\bar{x}) \in \mathbb{F}[\bar{x}]$ such that

$$F \Big|\frac{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}{w}\, C \vee g(\bar{x}) \cdot f(\bar{x})$$

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

i. $F \left| \frac{\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})}{w_1} \right. C \vee f(\bar{x})$ in at most k steps.

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

i. $H_F \left| \frac{\mathsf{PC}/\mathbb{F}}{pw_1 d} \right. h_{C\vee f}(\bar{x})$.

Note that by the first part of Lemma 5.1

$$\{h_{C\vee f}(\bar{x})\} \left| \frac{\mathsf{PC}/\mathbb{F}}{\mathsf{d}(h_{C\vee f})+\mathsf{d}(g)} \right. g(\bar{x}) \cdot h_{C\vee f}(\bar{x}).$$

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

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

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

i. $h_{C\vee g\cdot f}(\bar{x}) = g(\bar{x}) \cdot h_{C\vee f}(\bar{x})$:
In this case we know

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

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

ii. $h_{C\vee g\cdot f}(\bar{x}) \neq g(\bar{x}) \cdot h_{C\vee f}(\bar{x})$:
In this case

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

where $E := \mathsf{m}[C] \setminus \{g(\bar{x}) \cdot f(\bar{x})\}$. Note that by the second part of Lemma 5.1

$$\{(g(\bar{x}) \cdot f(\bar{x}))^2\} \left| \frac{\mathsf{PC}/\mathbb{F}}{p\cdot\mathsf{d}(g\cdot f)} \right. g(\bar{x}) \cdot f(\bar{x}).$$

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

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

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

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

■

For proving width lower bounds for (tree-like) $\mathsf{Res}(\mathsf{PC}_d/\mathbb{F})$ ($\mathbb{F}$ is a finite field) we use the known degree lower bounds for $\mathsf{PC}/\mathbb{F}$.

Theorem 5.3 *([3]) For any field $\mathbb{F}$ and for any fixed prime q such that $char(\mathbb{F}) \neq q$, there exists a constant d_q such that the following holds. If $d \geq d_q$ and G is a d-regular Ramanujan graph on n vertices (augmented with arbitrary orientation of its edges), then for every function σ such that $T_q(G, \sigma)$ is unsatisfiable, every $\mathsf{PC}/\mathbb{F}$-refutation of $T_q(G, \sigma)$ has degree $\Omega(dn)$.*

Actually, the above theorem holds for any good enough expander graph. It is well-known that for every fixed d, there exists an infinite family of d-regular Ramanujan graphs (see [17]), hence for every fixed d, there exists an infinite family of d_q-regular Ramanujan graphs $\mathcal{G}$ such that lower bound of Theorem 5.3 works on mod q Tseitin formulas defined based on members of $\mathcal{G}$.

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

Theorem 5.4 *([3]) Let $F \sim \mathcal{F}_k^{n,\Delta}$, $k \geq 3$ and $\Delta = \Delta(n)$ is such that $\Delta = o(n^{\frac{k-2}{2}})$. Then every $\mathsf{PC}/\mathbb{F}$-refutation of F has degree $\Omega(\frac{n}{\Delta^{2/(k-2)} \cdot \log \Delta})$ with probability $1 - o(1)$ for any field $\mathbb{F}$.*

5.1 Proof of Corollary 3.2

1. Suppose for a large enough n, $\mathsf{S}_{\mathbb{F},d}(T_q(G,\sigma)) < n^{2-\frac{(\log\log n)^2}{\log n}}$. Note that by Lemma 5.2 and Theorem 5.3,
$$\mathsf{w}_{\mathbb{F},d}(T_q(G,\sigma)) = \Omega(\frac{c}{pd}n).$$
So there exists an $\varepsilon > 0$ such that for a large enough n, $\varepsilon n \leq \mathsf{w}_{\mathbb{F},d}(T_q(G,\sigma))$, hence by Theorem 3.1 and the assumption at the beginning of the proof, for a large enough n, we have:
$$\varepsilon' n \leq c' + \sqrt{\left(2n + 3n^{2-\frac{(\log\log n)^2}{\log n}}\right) \log(3n^{2-\frac{(\log\log n)^2}{\log n}})}$$
for some positive ε' and c' is a constant. Therefore
$$(\varepsilon' n - c')^2 \leq \left(2n + 3n^{2-\frac{(\log\log n)^2}{\log n}}\right) \log(3n^{2-\frac{(\log\log n)^2}{\log n}}),$$
but this is not true because $n^{2-\frac{(\log\log n)^2}{\log n}} \log(n^{2-\frac{(\log\log n)^2}{\log n}}) = o(n^2)$, hence we get a contradiction and this completes the proof.

2. The proof of this part is similar to the proof of the previous part by using Theorem 5.4. Also, it is not hard to show that if $F \sim \mathcal{F}_k^{n,\Delta}$ and Δ satisfies the assumption of the corollary, then with probability $1 - o(1)$ F is unsatisfiable (see [6]).

■

5.2 Proof of Corollary 3.3

The argument for this corollary is the same as the argument in Corollary 3.2 using the degree lower bounds of Theorems 5.3 and 5.4. ■

Acknowledgment

We are indebted to Pavel Pudlák for many invaluable discussions that we have had about this work. We are grateful to Susanna F. de Rezende for discussions about communication complexity and lifting theorems. We also thank Leszek Kołodziejczyk and Iddo Tzameret for their comments on the draft of this paper. We thank Fedor Part for pointing to us that the second part of Lemma 5.1 is needed in the proof of Lemma 5.2. We are also grateful to Susanna F. de Rezende and Ahmadreza Rahimi for reading the draft of this paper and pointing out some English problems. This research was supported by the GACR grant 19-27871X and the Specific university research project SVV-2020-260589.

References

[1] Miklós Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994. Preliminary version in *FOCS '88*.

[2] Miklós Ajtai. The independence of the modulo p counting principles. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC '94)*, pages 402—411, 1994.

[3] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS '01)*, pages 190–199, October 2001.

[4] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science (FOCS '94)*, pages 794–806, November 1994.

[5] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99)*, pages 517–526, May 1999.

[6] Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35(4):759–768, October 1988.

[7] 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 Theory of Computing (STOC '96)*, pages 174–183, May 1996.

[8] Michal Garlík and Leszek Aleksander Kołodziejczyk. Some subsystems of constant-depth frege with parity. *ACM Trans. Comput. Logic*, 19(4), November 2018.

[9] Svyatoslav Gryaznov. Notes on resolution over linear equations. In *Computer Science – Theory and Applications (CSR '19)*, pages 168—179, 2019.

[10] Dmitry Itsykson and Dmitry Sokolov. Lower bounds for splittings by linear combinations. In *Mathematical Foundations of Computer Science (MFCS '14)*, pages 372—383, 2014.

[11] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Annals of Pure and Applied Logic*, 171(1), 2020.

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

[13] Jan Krajícek and Igor Carboni Oliveira. On monotone circuits with local oracles and clique lower bounds. *Chic. J. Theor. Comput. Sci.*, 2018.

[14] Jan Krajíček, Pavel Pudlák, and Alan R. Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7(1):15–40, 1995. Preliminary version in *STOC '92*.

[15] Jan Krajíček. Lower bounds for a proof system with an exponential speed-up over constant-depth frege systems and over polynomial calculus. In *Mathematical Foundations of Computer Science (MFCS '97)*, pages 85—90, 1997.

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

[17] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

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

[19] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993. Preliminary version in *STOC '92*.

[20] Pavel Pudlák and Russell Impagliazzo. A lower bound for DLL algorithms for k-SAT (preliminary version). In *Proceedings of the 11th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '00)*, pages 128–136, January 2000.

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

[22] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, December 1998.

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

[24] Iddo Tzameret. Sparser random 3-sat refutation algorithms and the interpolation problem - (extended abstract). In *Proceedings of the 41st International Colloquium on Automata, Languages and Programming (ICALP '14)*, pages 1015–1026, 2014.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il