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

On Proof complexity of Resolution over Polynomial Calculus

Erfan Khaniki*

Institute of Mathematics of CAS
Prague, Czech Republic

March 12, 2020

In memory of Arash Pourzarabi and Pouneh Gorji

Abstract

The refutation system $\mathsf{Res}_R(\mathsf{PC}_d)$ is a natural extension of resolution refutation system such that it operates with disjunctions of degree d polynomials over ring R with boolean variables. For $d = 1$, this system is called $\mathsf{Res}_R(\mathsf{lin})$. Based on properties of R, $\mathsf{Res}_R(\mathsf{lin})$ systems can be too strong to prove lower bounds for CNFs with current methods. The reachable goal might be proving lower bounds for $\mathsf{Res}_R(\mathsf{lin})$ when R is a finite field such as $\mathbb{F}_2$. Interestingly, $\mathsf{Res}_{\mathbb{F}_2}(\mathsf{lin})$ is also fairly strong, and there is no known nontrivial lower bound for it, but for $\mathsf{Res}^*_R(\mathsf{lin})$ (tree-like $\mathsf{Res}_R(\mathsf{lin})$) we know exponential lower bounds for every finite field.

For the stronger systems $\mathsf{Res}_R(\mathsf{PC}_d)$ and $\mathsf{Res}^*_R(\mathsf{PC}_d)$ for $d > 1$ on finite ring R, there is no known lower bounds till now. In this paper we will investigate these refutation systems and make some progress toward understanding these systems, including the case $d = 1$. We prove a size-width relation for $\mathsf{Res}_R(\mathsf{PC}_d)$ and $\mathsf{Res}^*_R(\mathsf{PC}_d)$ for every finite ring R. This relation is proved by a new idea to reduce the problem to the original Ben-Sasson and Wigderson size-width relation for Res and Res^* using extension variables. As a by product, we get the following new lower bounds for every finite field $\mathbb{F}$:

1. We prove the first nontrivial lower bounds for $\mathsf{Res}_{\mathbb{F}}(\mathsf{PC}_d)$ for fixed d: a nearly quadratic lower bounds for mod q Tseitin formulas ($char(\mathbb{F}) \neq q$) for suitable graphs.
2. We also prove superpolynomial and exponential lower bounds for $\mathsf{Res}^*_{\mathbb{F}}(\mathsf{PC}_d)$ where d is not too large with respect to n for the following principles:
   (a) mod q Tseitin formulas ($char(\mathbb{F}) \neq q$),
   (b) Random k-CNFs.

*e.khaniki@gmail.com

ISSN 1433-8092

1 Introduction

Resolution is the most studied refutation system in Propositional Proof Complexity. This system works with the clauses of literals. Given an unsatisfiable CNF F, a resolution refutation of F starts with this CNF and proves the empty clause. This refutation system was studied heavily in the literature, as the weakest propositional refutation system. Moreover, many SAT solvers use Resolution in some way, so studying Resolution, leads to a better understanding of the limits of Resolution based SAT solvers. Apart from understanding the limits of Resolution based SAT solvers, Resolution is a starting point for defining stronger proof systems and refutation systems. The importance of understanding stronger proof systems and refutation systems in terms of length of proofs or refutations is twofold. In point of view of mathematical logic, proving superpolynomial lower bounds for strong enough proof systems or refutation systems implies independence results in first-order theories. On the other hand, in point of view of complexity theory, proving lower bounds for proof systems and refutation systems is related to $\mathsf{NP} \neq \mathsf{CoNP}$. Proving $\mathsf{NP} \neq \mathsf{CoNP}$ is equivalent to the existence of superpolynomial lower bounds for every propositional proof system and propositional refutation system.

One way of defining a stronger proof system or refutation system than Resolution is to define proof systems or refutation system based on a class of stronger function (in terms of definability) in every line of proof. For example, we have the following proof systems and refutation systems which every line is a more complicated and expressible function instead of clauses of literals:

1. linear inequalities define Cutting planes,
2. polynomials over a field define Polynomial calculus,
3. AC_0 functions define AC_0-Frege proof system,
4. NC_1 functions define Frege proof system,

We know lower bounds for the first three systems in the above list, but there are no known superpolynomial lower bounds for the Frege proof system. Because the known lower bounds for AC_0-Frege proof system was proved by Hastad switching lemma method that was used to prove lower bound for AC_0 functions computing parity function, the natural step seemed to be proving lower bounds for $\mathsf{AC}_0[p]$-Frege proof system by adopting Razborov-Smolensky approximation method. However, until today this problem is still unsolved, and it is one of the frontier problems in proof complexity. Because $\mathsf{AC}_0[p]$-Frege proof system lower bound problem seemed to be hard, people started to investigate the subsystem of this proof system. We briefly review the known results about subsystems of $\mathsf{AC}_0[p]$-Frege proof system and some other systems similar to it. Krajíček in [1], defined the subsystem $\mathsf{PK}^c_d(\oplus)$ of $\mathsf{AC}_0[2]$-Frege proof system. In this system, every line of 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. He proved $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$

needs superpolynomial size for Mod_3 principle and also, ${\mathsf{PK}^*}^{O(1)}_{O(1)}(\oplus)$ need exponential size for proving Pigeonhole principle. Later Itsykson and Sokolov in [2, 3], introduced refutation system $\mathsf{Res}_{\mathbb{F}_2}(\mathsf{lin})$. They investigated the power of this system and proved $\mathsf{Res}^*_{\mathbb{F}_2}(\mathsf{lin})$ needs exponential size for refuting the Pigeonhole principle and Tseitin formula. Krajíček in [4], proved a feasible interpolation theorem for $\mathsf{Res}_{\mathbb{F}_2}(\mathsf{lin})$. He proved that from every (tree-like) $\mathsf{Res}_{\mathbb{F}_2}(\mathsf{lin})$ refutation of disjointness of a NP-pair (U, V); we can construct a randomized (tree-like) protocols computing the Karchmer-Wigderson game associated with (U, V). Also, he proved that such protocols correspond to monotone circuits with local oracles (CLO) in case of U is upward closed or V is downward closed, so if we prove lower bounds for any CLO separating a monotone disjoint NP-pair, this will lead to a lower bound for $\mathsf{Res}_{\mathbb{F}_2}(\mathsf{lin})$. Using this feasible interpolation, he proved every $\mathsf{Res}^*_{\mathbb{F}_2}(\mathsf{lin})$ refutation of Bipartite perfect matching principle has size at least $2^{\Omega\left(\sqrt{\left(\frac{n}{\log n}\right)}\right)}$ (see theorem 18.6.4 in [5]). Krajíček and Oliveira in [6] proved lower bounds for a subclass of CLOs separating k-cliques and the set of complete $(k-1)$-partite graphs, but we do not know whether lower bound for this subclass is enough for getting a lower bound for $\mathsf{Res}_{\mathbb{F}_2}(\mathsf{lin})$. Following [1], Garlík and Kołodziejczyk in [7], considered $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$, ${\mathsf{PK}^*}^{O(1)}_{O(1)}(\oplus)$ and AC_0-Frege proof system with Mod_2 principle. They investigated relations between these proof systems and proved new lower bounds. Also they proved an extension of $\mathsf{Res}^*_{\mathbb{F}_2}(\mathsf{lin})$ is polynomially simulated by a system related to $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$, and hence they got an exponential lower bound for Mod_3 principle for $\mathsf{Res}^*_{\mathbb{F}_2}(\mathsf{lin})$. Part and Tzameret in [8], defined $\mathsf{Res}_R(\mathsf{lin})$ for every ring R, and proved several lower bounds for $\mathsf{Res}^*_R(\mathsf{lin})$ for different rings. In particular, for the finite fields $\mathbb{F}_{p^k}$, they proved exponential lower bounds for the Pigeonhole principle, mod q Tseitin formulas ($q \neq p$) and random k-CNFs. They introduced two main tools for proving these lower bounds. First, they generalized the prover-delayer game of [2] to arbitrary ring R. Second they proved a size-width relation for $\mathsf{Res}^*_R(\mathsf{lin})$ for any ring R. Following the prover-delayer method that was used in [2, 3, 8], Gryaznov in [9], proved exponential lower bounds for Ordering and Dense Linear Ordering principles in $\mathsf{Res}^*_{\mathbb{F}_2}(\mathsf{lin})$, and hence separated $\mathsf{Res}^*_{\mathbb{F}_2}(\mathsf{lin})$ and Res.

In this paper we will continue investigating the power of $\mathsf{Res}_R(\mathsf{lin})$, $\mathsf{Res}^*_R(\mathsf{lin})$ and also their generalization $\mathsf{Res}_R(\mathsf{PC}_d)$ and $\mathsf{Res}^*_R(\mathsf{PC}_d)$. Our main theorem (Theorem 3.5) is a size-width relation. This theorem has two advantages to the size-width relation of [8]. First, to some extent, it works for dag-like systems such as $\mathsf{Res}_R(\mathsf{lin})$ and more generally $\mathsf{Res}_R(\mathsf{PC}_d)$, and hence we can prove a nontrivial lower bound in the dag-like setting. Second, it is not limited to the linear forms, and we can prove lower bounds for Resolution over polynomial calculus.

The organization of this paper is as follows. In section 2, we explain definitions and notations. In section 3, we will prove a size-width relation for $\mathsf{Res}_R(\mathsf{PC}_d)$ and $\mathsf{Res}^*_R(\mathsf{PC}_d)$ over finite rings R. The main idea is to use extension variables to translate refutations in $\mathsf{Res}_R(\mathsf{PC}_d)$ and $\mathsf{Res}^*_R(\mathsf{PC}_d)$ to resolution refutations with additional clauses formed by these new extension variables and the original ones and then using the size-width relation of Ben-Sasson and Wigderson for resolution. In section 4, we prove lower bounds as an application of this theorem. We prove the first nontrivial lower bound for $\mathsf{Res}_R(\mathsf{lin})$ and in general for $\mathsf{Res}_R(\mathsf{PC}_d)$ (for fixed d) over finite fields (Corollary 4.3). For the tree-like case over finite fields, we prove the first superpolynomial and exponential lower bounds for $\mathsf{Res}^*_R(\mathsf{PC}_d)$ where

d is limited by some sublinear function of n (Corollary 4.5).

2 Preminarlies

Resolution (Res) is a refutation system that works with clauses of literals. Every clause in a Resolution proof is a disjunction of variables or negation of variables. Resolution refutation system has the resolution rule and the weakening rule.

The set of variables appearing in a clause D or CNF F will be denoted by $V(D)$ and $V(F)$. A resolution proof of a clause D from clauses $F = \{C_1, ..., C_k\}$ (F is a CNF) ($F \vdash D$ in notation) is a sequence such as $\pi = D_1, ..., D_l$ such that:

1. $D_l = D$,
2. for every $i < l$, D_i is in F or D_i was derived by resolution rule or weakening from previous $D_j, j < i$.

A CNF F is refutable if $F \vdash \emptyset$ where $\emptyset$ is the empty clause. Size of a refutation or proof π will be denoted by $|\pi|$, and it is the number of clauses in π. For a ring R, we define Resolution over polynomial calculus ($\mathsf{Res}_R(\mathsf{PC})$) as a refutation system like Res which works with clauses of polynomials of boolean variables, instead of literlas. So a clause in $\mathsf{Res}_R(\mathsf{PC})$ is $C = \bigvee_{i<l} f_i(\bar{x})$ such that each $f_i(\bar{x})$ is a polynomail with coeficient in R. $C = \bigvee_{i<l} f_i(\bar{x})$ is true in a boolean asignment $a \in \{0,1\}^n$ iff there exists i such that $f(a) = 0$. Following [8], we use a similar set of rules for defining $\mathsf{Res}_R(\mathsf{PC})$ as follows:

1. resolution:
$$C \vee f(\bar{x}), D \vee g(\bar{x}) \vdash C \vee D \vee af(\bar{x}) + bg(\bar{x})$$
for every $a, b \in R$,
2. weakening:
$$C \vdash C \vee f(\bar{x}),$$
3. simplification:
$$C \vee a \vdash C$$
for every $a \in R \setminus \{0\}$,
4. multiplication:
$$C \vee f(\bar{x}) \vdash C \vee x \cdot f(\bar{x}),$$

where $g(\bar{x}), f(\bar{x})$ are polynomials with coeffeicent in R and $x \in \{x_1, ..., x_n\}$ is a variable from the initial clauses. Also $\mathsf{Res}_R(\mathsf{PC})$ has 0 and $x \vee x - 1$ ($x \in \{x_1, ..., x_n\}$) as axioms. $\mathsf{Res}_R(\mathsf{PC}_d)$ is a refutation system using $\mathsf{Res}_R(\mathsf{PC})$ rules and axioms, with the restriction that every polynomial appearing in a refutation or proof should have total degree at most d. The concept of refutation and proof in $\mathsf{Res}_R(\mathsf{PC})$ and $\mathsf{Res}_R(\mathsf{PC}_d)$ is defined as Res with this minor difference that we have also some axioms (except the initial clauses) that can be used in

one step. $\mathsf{Res}_R(\mathsf{PC}_1)$ is called $\mathsf{Res}_R(\mathsf{lin})$. For the refutation systems that are defined till now, there is a tree-like version of them. For a refutation system P, P^* denotes tree-like version of it where every refutation or proof in P^* looks like a tree.

Let C be a disjunction of literals, then $w(C)$ (width of C) is the number of disjuncts in C. For a CNF $F = \{C_1, ..., C_k\}$, $w(F) = \max_{C \in F} w(C)$. For a refutation or proof π in one of the defined refutation systems, $w(\pi) = \max_{D \in \pi} w(D)$. For a refutation system P, a set of clauses F (not nessecarily nonempty) and a clause D, notation

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

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

1. $w_{R,d}(F)$ is the minimum $w(\pi)$ among all $\mathsf{Res}_R(\mathsf{PC}_d)$-refutations π of F,
2. $S_{R,d}(F)$ is the minimum $|\pi|$ among all $\mathsf{Res}_R(\mathsf{PC}_d)$-refutations π of F.

$S^*_{R,d}(F)$ is the same concept for $\mathsf{Res}^*_R(\mathsf{PC}_d)$. Res-refutation width and size corresponded to F will be denoted by $w_{\mathsf{Res}}(F)$ and $S_{\mathsf{Res}}(F)$. For Res^*, minimal refutation size of F will be denoted by $S_{\mathsf{Res}^*}(F)$.

3 Size-Width relation for $\mathsf{Res}_R(\mathsf{PC}_d)$ and $\mathsf{Res}^*_R(\mathsf{PC}_d)$

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

Proposition 3.1 *For every ring R, and every monomial $p(\bar{x}) = \prod_{i=1}^n x_i^{d_i}$ of total degree d ($\sum_{i=1}^n d_i = d$),*

$$\varnothing \left|\frac{\mathsf{Res}_R(\mathsf{PC}_d)}{2}\right. p(\bar{x}) \vee p(\bar{x}) - 1.$$

Proof. We prove 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 hyphothesis

$$\varnothing \left|\frac{\mathsf{Res}_R(\mathsf{PC}_k)}{2}\right. p'(\bar{x}) \vee p'(\bar{x}) - 1.$$

So by two times using of multiplication rule we get

$$\varnothing \left|\frac{\mathsf{Res}_R(\mathsf{PC}_{k+1})}{2}\right. x'p'(\bar{x}) \vee x'p'(\bar{x}) - x'.$$

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

$$\varnothing \left|\frac{\mathsf{Res}_R(\mathsf{PC}_{k+1})}{2}\right. x'p'(\bar{x}) \vee x' - 1.$$

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 have

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

■

Proposition 3.2 *Let R be a finite ring. Then for every polynomial $p(\bar{x}) \in R[\bar{x}]$ of total degree d,*

$$\varnothing \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|+1} \bigvee_{a \in R} p(\bar{x}) - a.$$

Proof. We prove the proposition by induction on the number of degree non-zero 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 weakening rule on 0 to prove 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 nonzero degree monomial than $f(\bar{x})$, hence by induction hyphothesis,

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

By Proposition 3.1,

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

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

$$\varnothing \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|+1} f(\bar{x}) - 1 \vee \bigvee_{a \in R} bf(\bar{x}) + g(\bar{x}) - a.$$

By the same argument, we get

$$\varnothing \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|+1} f(\bar{x}) \vee \bigvee_{a \in R} bf(\bar{x}) + g(\bar{x}) - a - b.$$

Therefore by resolution 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

$$\varnothing \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|+1} \bigvee_{a \in R} p(\bar{x}) - a.$$

■

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

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

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

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 translation of polynomials. For every CNF F and every (tree-like) $\mathsf{Res}_R(\mathsf{PC}_d)$-refutation π of F, we use the following mapping to translate polynomials in clauses of π to atomic variables:

$$Q(f) = \begin{cases} x_i & f = x_i - 1 \\ \neg x_i & f = x \\ t & f = 0 \\ \neg t & f = a, a \in R \setminus \{0\} \\ q_f & \text{o.w.} \end{cases}$$

where t is a new atomic variable and its intended meaning is true. The CNF $\mathsf{Ex}(\pi)$ contains the following clauses:

1. $t \in \mathsf{Ex}(\pi)$, if there is a resolution rule of multiplication rule such that one of the polynomials appearing in these rule is a constant polynomial.

2. if resolution rule is used in π to derive $af + bg$ from f and g, then

$$\neg Q(f) \vee \neg Q(g) \vee Q(af + bg) \in \mathsf{Ex}(\pi),$$

3. if multiplication rule is used to derive $x \cdot f$ from f, then $\neg Q(f) \vee Q(x \cdot f) \in \mathsf{Ex}(\pi)$.

The previous translation will be used to prove property (I). To prove property (II), we need another translation from clauses definable in $V(\mathsf{Ex}(\pi)\cup F)$ to clauses of polynomials of degree at most d. For this purpose, we will 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:

$$Q'(r) = \begin{cases} x_i - 1 & r = x_i \\ x_i & r = \neg x_i \\ 0 & r = t \\ 1 & r = \neg t \\ f & r = q_f \\ \bigvee_{a \in R\setminus\{0\}} f - a & r = \neg q_f \end{cases}$$

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

1. *There exists a Res-refutation π' of $\mathsf{Ex}(\pi) \cup F$ 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 $\mathsf{Ex}(\pi) \cup F$, if*

$$\mathsf{Ex}(\pi) \cup F \vdash^{\mathsf{Res}}_{w} C,$$

then

$$F \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|(w+1)} Q'(C).$$

Proof. 1. Let π_u be a subsequence of π such that

   (a) $\emptyset$ is the last clause in π_u,

   (b) every nonempty clause C of π appears in π_u iff for every disjunct of nonzero degree of C such as f, there is an application of resolution rule or multiplication rule on f or f is derived by an application of resolution rule or multiplication rule in π.

   Note that π is a $\mathsf{Res}_R(\mathsf{PC}_d)$-refutation of F, hence π' becomes a $\mathsf{Res}_R(\mathsf{PC}_d)$-refutation of F too. Because there is no superfluous application of the weakening rule in π_u, we can simulate π_u in Res with help of clauses in $\mathsf{Ex}(\pi)$. Note that the number of clauses in $\mathsf{Ex}(\pi)$ is equal to the number of resolution rules and multiplication rules and hence it is bounded by $|\pi| - |F|$. Simulating π_u in Res can be done by using the additional clauses in $\mathsf{Ex}(\pi)$ in size at most $2|\pi|$ (the reason is that for simulating the resolution rule in $\mathsf{Res}_R(\mathsf{PC}_d)$, we should use the corresponding clause in $\mathsf{Ex}(\pi)$ and using two resolution rule in Res), and hence the total size of π' is at most $2|\pi| + |\pi| - |F| + |F| = 3|\pi|$. Moreover if π is tree-like, then π_u is also tree-like. This implies this simulation in Res is also tree-like.

2. We prove this part by induction on the number of steps of proving C. If the number of steps in proving C is zero, then C is one of the initial clauses $\mathsf{Ex}(\pi) \cup F$. If C is in F, then there is nothing to prove, otherwise C is a clause in $\mathsf{Ex}(\pi)$. We prove The nontrivial case here. The other cases have similar proofs. Suppose C is $\neg q_f \vee \neg q_g \vee q_{af+bg}$. Hence

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

   By Proposition 3.2,

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

   and

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

hence by resolution rule we get

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

A similar argument works when the clause corresponds to a multiplication rule. Now suppose the statment is true for clauses that can be proved by at most k number of steps. Suppose C and D are clauses in variables of $\mathsf{Ex}(\pi) \cup F$ such that:

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

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

where $r \in V(\mathsf{Ex}(\pi) \cup F)$. So by induction hyphothesis

(a) $F \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|(w_1+1)} Q'(C) \vee Q'(r)$,

(b) $F \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{|R|(w_2+1)} Q'(D) \vee Q'(\neg r)$.

We prove the nontrivial case here. The other cases can be treated in a similar way. Suppose r is q_f for some polynomial f. So what we have are $Q'(C) \vee f$ and $Q'(D) \vee \bigvee_{a\in R\setminus\{0\}} f - a$. By applying resolution and simplification rules $|R|$ times, we can derive $Q'(C) \vee Q'(D)$. Note that

$$\mathsf{Ex}(\pi) \cup F \vdash^{\mathsf{Res}}_{\max\{w_1,w_2,w(C\vee D)\}} C \vee D.$$

Also, width of proving $Q'(C) \vee Q'(D)$ is at most

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

which is less than

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

so

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

is less than

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

and this completes the proof.

■

For proving the size-width relation for (tree-like) $\mathsf{Res}_R(\mathsf{PC}_d)$, we need the size-width relation of Ben-Sasson and Wigderson which was proved in the seminal paper [10].

Theorem 3.4 *([10]) For every unsatisfiable CNF F in n variables, the following inequalities hold:*

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

where log *is the binary logarithm.*

Theorem 3.5 *(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. $\frac{w_{R,d}(F)}{|R|} - 1 \leq \max\{3, w(F)\} + O\left(\sqrt{\big(n + 3S_{R,d}(F)\big)\log(3S_{R,d}(F))}\right)$.
2. $\frac{w_{R,d}(F)}{|R|} - 1 \leq \max\{3, w(F)\} + \log(3S^*_{R,d}(F))$.

Proof. We prove the first inequality. The proof of the second inequality is similar. Let π be the minimal size $\mathsf{Res}_R(\mathsf{PC}_d)$-refutation of F ($|\pi| = S_{R,d}(F)$). By first part of Lemma 3.3, $S_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup F) \leq 3|\pi|$. On the other hand, by second part of Lemma 3.3, $\frac{w_{R,d}(F)}{|R|} - 1 \leq w_{\mathsf{Res}}(\mathsf{Ex}(\pi) \cup F)$, so by the first inequality of Theorem 3.4,

$$\frac{w_{R,d}(F)}{|R|} - 1 \leq \max\{3, w(F)\} + O\left(\sqrt{|V(\mathsf{Ex}(\pi) \cup F)| \log(3S_{R,d}(F))}\right)$$

Note that the number of new variables that appear in $\mathsf{Ex}(\pi)$ is at most three times of the number of rules that are used in π (we introduced new clauses in $\mathsf{Ex}(\pi)$ for resolution rule and multiplication rule and in each of them we used at most three new varibales). Because the number of rules that are used in π is less that $|\pi|$, we have $|V(\mathsf{Ex}(\pi) \cup F)| \leq n + 3S_{R,d}(F)$, hence

$$\frac{w_{R,d}(F)}{|R|} - 1 \leq \max\{3, w(F)\} + O\left(\sqrt{\big(n + 3S_{R,d}(F)\big)\log(3S_{R,d}(F))}\right).$$

■

4 Application of Size-Width relation to Lower bounds

In this section, we prove new lower bounds for $\mathsf{Res}_{\mathbb{F}}(\mathsf{PC}_d)$ and $\mathsf{Res}^*_{\mathbb{F}}(\mathsf{PC}_d)$ for every finite field $\mathbb{F}$. We use the same strategy as [8] by proving width lower bounds from degree lower bounds of PC-refutations. Next lemma explains this fact.

Lemma 4.1 *Let F be an unsatisfiable CNF. Then for every finite ring R and every d, if $F \vdash^{\mathsf{Res}_R(\mathsf{PC}_d)}_{w} \emptyset$, then F has a PC_R-refutation of degree at most wd.*

Proof. The proof of this lemma is similar to the proof of Proposition 26 in [8]. The idea is that we replace each clause $C = \bigvee_{i=1}^{k} f_i(\bar{x})$ by polynomial $h_C(\bar{x}) = \prod_{i=1}^{k} f_i(\bar{x})$ and fill the gaps to make it a PC_R-refutation. For filling the gaps, we should argue how resolution and multiplication rule in the original refutation can be applied here. The case of multiplication rule is easy, because we have the multiplication rule in PC_R too. For the case of resolution rule, suppose we derive $C \vee D \vee af(\bar{x}) + bg(\bar{x})$ from clauses $C \vee f$ and $D \vee g$. For simulating this rule in PC, we should prove $h_{C \vee D \vee af+bg}$ from $h_{C \vee f}$ and $h_{D \vee g}$. It is easy to see that we can prove $h_{C \vee D \vee f}$ from $h_{C \vee f}$ with a proof of degree at most $deg(h_{C \vee D \vee f})$. By the same argument one can get $h_{C \vee D \vee g}$ from $h_{D \vee g}$ with a proof of degree at most $deg(h_{C \vee D \vee f})$. For the last step we use addition rule in polynomial calculus to derive $h_{C \vee D \vee af+bg}$ from $h_{C \vee D \vee f}$ and $h_{C \vee D \vee g}$. Note that because every clause in original proof has width at most w and also every polynomial in the original proof has degree at most d, this transformation construct a PC_R-proof of degree at most wd. ∎

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

Definition 4.1 *(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 CNF encoding of 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. This is important for our nearly quadratic lower bound for $\mathsf{Res}_{\mathbb{F}}(\mathsf{PC}_d)$, because for every unsatisfiable CNF F, $|F| \leq S_{R,d}(F)$. We use the following degree lower bound on $T_q(G, \sigma)$.

Theorem 4.2 *([11]) 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 $\Omega(dn)$.*

As we know, for every fixed d, there exists an infinite family of d-regular Ramanujan graphs (see [12]), hence for every fixed d, there exists an infinite family of d_q-regular Ramanujan garphs $\mathcal{G}$ such that lower bound of Theorem 4.2 works on mod q Tseitin formulas defined based on members of $\mathcal{G}$.

Corollary 4.3 *Let $\mathbb{F}$ be a finite field and q be a fixed prime such that $char(\mathbb{F}) \neq q$. Then there exists a constant d_q such that for every fiexd d the following holds. If $c \geq d_q$, then for every large enough n and every c-regular Ramanujan graph G on n vertecis (augmented with arbitrary orientation of its edges) and for every function σ such that $T_q(G, \sigma)$ is unsatisfiable, $n^{2-\frac{(\log\log n)^2}{\log n}} \leq S_{\mathbb{F},d}(T_q(G, \sigma))$.*

Proof. Suppose for large enough n, $S_{\mathbb{F},d}(T_q(G,\sigma)) < n^{2-\frac{(\log\log n)^2}{\log n}}$. Note that by Lemma 4.1 and Theorem 4.2,

$$w_{\mathbb{F},d}(T_q(G,\sigma)) = \Omega(\frac{c}{d}n).$$

So there exists $\varepsilon > 0$ such that for large enough n, $\varepsilon n \leq w_{\mathbb{F},d}(T_q(G,\sigma))$, hence by Theorem 3.5 and the assumption at the begining of the proof, for large enough n, we have:

$$\varepsilon' n \leq c' + \sqrt{\left(n + 3n^{2-\frac{(\log\log n)^2}{\log n}}\right)\log(3n^{2-\frac{(\log\log n)^2}{\log n}})}$$

for some positive ε' and c' is a constant. Therefore

$$(\varepsilon' n - c')^2 \leq \left(n + 3n^{2-\frac{(\log\log n)^2}{\log n}}\right)\log(3n^{2-\frac{(\log\log n)^2}{\log n}}),$$

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. ∎

Definition 4.2 *(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.*

Theorem 4.4 *([11]) 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 $\mathbb{F}$.*

Corollary 4.5 *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 fiexd d the following holds. If $c \geq d_q$, then for every large enough n and every c-regular Ramanujan graph G on n vertecis (augmented with arbitrary orientation of its edges) and for every function σ such that $T_q(G,\sigma)$ is unsatisfiable, $S^*_{\mathbb{F},d(n)}(T_q(G,\sigma))$ is*
   (a) *superpolynomial if for every natrual 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 probablility $1 - o(1)$, $S^*_{\mathbb{F},d(n)}(F)$ is*
   (a) *superpolynomial 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. The argument for this corollary is the same as the argument in Corollary 4.3 using the degree lower bounds of Theorems 4.2 and 4.4. ∎

Acknowledgment

We are indebted to Pavel Pudlák for many invaluable discussions that we have had about this work. We are also grateful to Susanna F. de Rezende for discussions about communication complexity and lifting theorems. This research was supported by the project EPAC, funded by the Grant Agency of the Czech Republic under the grant agreement no. 19-27871X.

References

[1] J. Krajíček, *Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over polynomial calculus*, Proceedings of MFCS '97, volume 1295 of Lecture Notes in Computer Science, 85–90, Springer, 1997.

[2] D. Itsykson, D. Sokolov, *Lower bounds for splittings by linear combinations*, Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25–29, 2014, Proceedings, Part II, (2014), 372–383.

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

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

[5] J. Krajíček, *Proof complexity*, Encyclopedia of Mathematics and Its Applications, Vol.170, Cambridge University Press, Cambridge - New York - Melbourne, (March 2019), 530pp.

[6] J. Krajíček, I. C. Oliveira, *On monotone circuits with local oracles and clique lower bounds*, Chicago Journal of Theoretical Computer Science, (2018), 1-18.

[7] M. Garlík, L. A. Kołodziejczyk, *Some subsystems of constant-depth Frege with parity*, ACM Transactions on Computational Logic, Article No. 29, (2018).

[8] F. Part, I. Tzameret, *Resolution with counting: lower bounds over different moduli*, Electronic Colloquium on Computational Complexity (ECCC), 25, (2018)

[9] S. Gryaznov, *Notes on Resolution over Linear Equations*, van Bevern R., Kucherov G. (eds) Computer Science – Theory and Applications, CSR (2019), Lecture Notes in Computer Science, vol 11532, Springer, Cham.

[10] E. Ben-Sasson, A. Wigderson, *Short proofs are narrow - resolution made simple*, Journal of ACM, 48-(2), 2001.

[11] M. Alekhnovich, A. A. Razborov, *Lower bounds for polynomial calculus: non-binomial case*, Proceedings 42nd IEEE Symposium on Foundations of Computer Science, Newport Beach, CA, USA, 2001, pp. 190-199.

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

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il