Abstract of an Award-winning PhD Thesis

Luca Aceto
ICE-TCS, School of Computer Science
Reykjavik University

Every year, the Italian Chapter of the EATCS gives an award for the Best Italian PhD Thesis in Theoretical Computer Science. The award is presented at the annual Italian Conference on Theoretical Computer Science (ICTCS), where the award recipient delivers a presentation on her/his work.

This year's award went to Ilario Bonacina for his thesis *Space in weak propositional proof systems*, which was supervised by Nicola Galesi at the University of Rome "La Sapienza". Ilario's thesis contributes to a classic and deep topic in theoretical computer science, and settles natural questions on the space complexity of proofs using Resolution and the Polynomial Calculus that had been open for about 15 years.

Ilario kindly agreed to contribute a summary of the work presented in his thesis to this issue of the Bulletin of the EATCS. I trust that his survey will be of interest to readers of the Bulletin, regardless of their main research interests. Enjoy it!

Abstract of PhD Thesis

Author: Ilario Bonacina
Title: Space in weak propositional proof systems
Language: English
Supervisor: Nicola Galesi
Institute: Sapienza University of Rome, Italy
Date: 14 December 2015

Abstract

This thesis was defended on December 14, 2015 at the Sapienza University of Rome for a Ph.D. title in Computer Science under the supervision of Prof. Nicola Galesi. It was awarded "*Best Italian PhD Thesis in Theoretical Computer Science, 2016*". The results presented in this thesis build on top of the following publications [9, 12–16].

1 Preliminaries

Propositional proof complexity, that is the complexity of propositional proofs, plays a role in the context of feasible proofs as important as the role of Boolean circuits in the context of efficient computations. Although the original motivations to study the complexity of propositional proofs came from proof-theoretical questions about first-order theories, it turns out that, essentially, the complexity of propositional proofs deals with the following question: *what can be proved by a prover with bounded computational abilities?* For instance if its computational abilities are limited to small circuits from some circuit class. Hence, propositional proof complexity mirrors to non-uniform computational complexity and indeed there is a very productive cross-fertilization of techniques between the two fields. Our understanding of propositional proof systems is similar to the general situation in complexity theory, in the sense that in both fields we can prove lower bounds in very special cases and indeed there are many very basic and important open problems, such as the very famous P *vs* NP. In propositional proof complexity the situation is similar in the sense that we can prove super-polynomial lower bounds on the length of proofs only for restricted proof systems. Indeed proving super-polynomial lower bounds on the length of proofs in *every* propositional proof system is equivalent to showing that $\mathsf{NP} \neq \mathsf{coNP}$ [21], which in turn is one of the open and very important problems in computational complexity.

In this thesis we investigate space complexity in propositional proof systems, so what is the *space*[1] of a proof? Intuitively, the space required by a refutation is the amount of information we need to keep simultaneously in memory as we work through the proof and convince ourselves that the original propositional formula is unsatisfiable. This model is inspired by the definition of space complexity for Turing machines, where a machine is given a read-only input tape from which it can download parts of the input to the working memory as needed. This model is sometimes called in the literature *blackboard model* and the name comes from the image of a teacher in front of a class of students. The goal of the teacher is to show that a propositional formula is contradictory[2] writing down clauses and performing inferences on a blackboard. In this analogy students understand inferences based on the rules of some particular proof system, for example (among others) Frege; or *Resolution*, a well studied proof system that is at the core of state-of-the-art algorithms to solve SAT instances (Res); or *Polynomial Calculus* (PC), a proof system that uses polynomials to refute contradictions. As for length of proofs, the study of space complexity for proof systems represents a great theoretical challenge and may also have practical consequences on techniques for SAT solving and their implementation.

We completely answer questions on the space complexity for Resolution and Polynomial Calculus raised for the first time in [2, 6] and since then reported many times in the literature. The results we show can be summarized as follows.

Monomial space in Polynomial Calculus We introduce a combinatorial framework to prove monomial space lower bounds. This framework belong to the class of game theoretic methods and combinatorial characterizations that are widely used in proof complexity to study complexity measures[3]. As an application we then have asymptotically optimal lower bounds on the monomial space needed to refute random k-CNF formulas (and the graph pigeonhole principle) or *Tseitin formulas* in Polynomial Calculus. Those results were conjectured to be true and posed as open problems in many works, [2, 6, 24] among others. The framework is described on a very high level in Section 2.1 of this abstract, the results about random k-CNFs in Section 3 and the ones about Tseitin formulas in Section 4.

Total space in Resolution We give another combinatorial framework to prove total space lower bounds which results in a tight connection between the total space measure and the width. Then, as corollaries, we have asymptotically optimal total

[1] The problem of the *space* taken by propositional proofs was posed for the first time by Armin Haken during the workshop "*Complexity Lower Bounds*" held at Fields Institute in Toronto 1998.

[2] In this abstract and the thesis *proofs* will be always *refutations* of contradictions. So we use the two terms interchangeably.

[3] Some examples are the Pudlák games characterizing the *size* of Resolution proofs [35] or the families of assignments characterizing Resolution *width* [3], where the width of a proof is the number of literals in the largest clause appearing in it.

lower bounds in Resolution for *Tseitin formulas* over d-regular expander graphs, completely answering open problem from [2, Open question 2] for Resolution and we prove asymptotically optimal total space lower bound in Resolution for random k-CNF formulas, completely answering an open problems from [2, 6, 25] among others. Moreover it follows an optimal separation of Resolution and *semantic* Resolution from the point of view of the total space measure, completely answering [2, Open question 4] for Resolution. The framework is described more in details in Section 2.2 of this abstract, the results for random k-CNFs in Section 3 and the ones for Tseitin formulas in Section 4.

Size and width in Resolution Together with the main results about space this thesis contains also a detour on size, cf. Section 5 of this abstract. Indeed, using the game theoretic characterization of width and size in Resolution, we are able to prove that the Strong Exponential Time Hypothesis (SETH) is consistent with a sub-system of Resolution, that is no algorithm with track formalizable in such system is able to refute SETH.

In this abstract, the numbering of theorems, corollaries, lemmas and propositions refer to their numbering in the thesis.

1.1 Resolution

Resolution (Res) [11, 38] is a sound and complete propositional proof system manipulating unsatisfiable CNF formulas. A formula is *Conjunctive Normal Form* (CNF) is a conjunction ($\wedge$) of clauses, where each clause is a disjunction ($\vee$) of *literals* and each literal is either a variable x_j or a negation of a variable $\neg x_i$. If each clause has at most k literals then it is a k-CNF formula. A Res refutation of a CNF formula φ is a sequence of clauses ending with the empty clause $\perp$ and such that each clause is either a clause from φ or can be inferred from previous clauses by the following inference rule:

$$\frac{C \vee x \qquad D \vee \neg x}{C \vee D} \ (\mathsf{Res}\ \text{rule}),$$

where C, D denote clauses and x is a variable that we say is *resolved*. A CNF formula φ is unsatisfiable if and only if the empty clause, $\perp$, can be inferred from φ using the Res rule.

To understand the complexity of Resolution proofs various hardness measures were defined and investigated. Historically, the first and most studied is the *size*: the number of clauses in a Resolution refutation π is its *size*, $\mathsf{size}(\pi)$. The *width* of a Resolution proof π, $\mathsf{width}(\pi)$, is the number of literals in the biggest clause appearing in π.

Given any unsatisfiable k-CNF formula φ in n variables, if there exists a Resolution refutation π of φ such that $\mathsf{size}(\pi) \leqslant S$ then there exists a Resolution proof

π' of φ such that

$$\mathsf{width}(\pi') \leqslant \sqrt{n \cdot O(\log S)} + k, \tag{1}$$

so if for every Resolution proof π of φ, $\mathsf{width}(\pi) \geqslant \omega(\sqrt{n \log n})$ and φ has $n^{O(1)}$ clauses then immediately we have that φ must require Resolution refutations of super-polynomial size. This is known as the "*size-width tradeoff*" [8] and it is optimal up to logarithmic factors [17]. Equation (1) is the standard tool to prove exponential size lower bounds, but in some cases it is not enough. In this thesis we prove some results on Resolution size stronger than the size lower bound we could get by the technique presented above.

Nowadays Resolution is mostly studied due to its importance in applied contexts due to a connection to the *CDCL solvers*, which are at the core of modern SAT-solvers [33]. In particular, lower bounds on Resolution size and Resolution *space* (cf. Section 2) imply lower bounds on the running time and the memory consumption of CDCL solvers.

1.2 Polynomial Calculus

In *Polynomial Calculus*, PC, [2, 20] an unsatisfiable CNF formula φ in the variables $x_1, \ldots, x_n$ is shown to be unsatisfiable first translating it into a set of multilinear monomials $tr(\varphi)$ such that φ is unsatisfiable if and only if 1 is in the ideal generated by $tr(\varphi)$ ($1 \in \text{ideal}(tr(\varphi))$) in the ring of polynomials $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots \bar{x}_n]$ where the $\bar{x}_i$ variables are new variables and $\mathbb{F}$ is a field[4]. Then, to show that $1 \in \text{ideal}(tr(\varphi))$ we use the following inference rules starting from the monomials in $tr(\varphi)$

$$\frac{p \quad q}{\alpha p + \beta q}\ \alpha, \beta \in \mathbb{F}, \qquad \frac{p}{qp}\ q \in \mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots \bar{x}_n], \qquad \frac{}{x_i^2 - x_i}, \qquad \frac{}{x_i + \bar{x}_i - 1}.$$

These rules model the fact that ideals are closed under linear combinations and multiplications of generic polynomials. Moreover, they force the semantic meaning of the variables to be just Boolean variables and such that $\bar{x}_i = 1 - x_i$. In PC the polynomials are expressed in their expanded form as a sum of monomials, and the size of a PC proof π, $\mathsf{size}(\pi)$, is measured as the total number of monomials appearing in it[5]. As in Resolution, there are unsatisfiable formulas requiring exponentially long PC proofs and there exists a "*size-degree tradeoff*" [20], where the *degree* of a PC proof π, $\mathsf{degree}(\pi)$, is the maximum degree of a polynomial appearing in π. Given a k-CNF formula φ, if there exists a PC proof of φ such that

[4] For sake of clarity we avoid here the details of the translation $tr(\varphi)$.

[5] There are also algebraic proof systems that allow manipulations on polynomials in implicit forms and this results in stronger, not so well understood, proof systems [18, 19, 28–30, 34, 37].

$\mathsf{size}(\pi) \leqslant S$ then there exists a PC proof π' of φ such that

$$\mathsf{degree}(\pi') \leqslant \sqrt{n \cdot O(\log S)} + k. \tag{2}$$

Hence, if for every PC proof π of φ we have that $\mathsf{degree}(\pi) \geqslant \omega(\sqrt{n \log n})$ and φ has $n^{O(1)}$ clauses then φ cannot have polynomial size PC proofs. Moreover, if $\operatorname{char} \mathbb{F} \neq 2$ then some Fourier-like transformation can be used to reduce degree lower bounds to Resolution [7]. More general techniques to prove degree lower bounds, working also if $\operatorname{char} \mathbb{F} = 2$, were introduced in [1] and generalized in [26, 32]. It is interesting to notice the similarity between equation (2) and equation (1). Indeed, lot of results on the complexity of Resolution proofs are qualitatively similar to results on the complexity of PC proofs. As for Resolution, the size-degree relationship is essentially optimal [27] and most of the super-polynomial or exponential size lower bounds for PC proofs are obtained through degree lower bounds.

Our motivation to study algebraic proof systems is that they are not at all as well understood as Resolution and this lack of knowledge from the theoretical point of view might be one of the reasons for not having efficient SAT solvers properly exploiting the potential of algebraic manipulations. Moreover, the study of algebraic proof systems could shed light on major open problems in propositional proof complexity such as proving super-polynomial size lower bounds for $AC_0[p]$-Frege a Frege system where only bounded-depth formulas over the Boolean connectives and a MOD_p connective are allowed [19, 20].

2 Space

The formal definition goes as follows [2, 23]: A Resolution refutation π of a CNF formula φ is a sequence of memory configurations $\pi = (\mathfrak{M}_0, \ldots, \mathfrak{M}_\ell)$ where each $\mathfrak{M}_i$ is a set of clauses, $\mathfrak{M}_0 = \emptyset$, $\perp \in \mathfrak{M}_\ell$ and for each $i \geqslant 1$, $\mathfrak{M}_i$ is obtained from $\mathfrak{M}_{i-1}$ applying one of the following rules

(Axiom Download) $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{C\}$, where C is a clause in φ;

(Erasure) $\mathfrak{M}_i \subseteq \mathfrak{M}_{i-1}$;

(Inference) $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{C\}$ where C is the result of the Resolution inference rule applied with premises in $\mathfrak{M}_{i-1}$.

Clearly this definition can be adapted to other proof systems, for instance for PC we will just have as memory configurations sets of polynomials and as inference rules the ones from PC.

As Alekhnovich et al. [2] pointed out, the very first question, when starting the investigation of space, is how to measure the memory content/blackboard size at any given moment in time for a specified propositional proof system. Recalling Krajíček [31], the most customary measures for the size complexity of propositional proofs are the bit size and the number of lines. Among the two the bit size is the most important and can be defined analogously also for space complexity. In the case of space we measure the total number of literals in memory, the *total space*, a measure logarithmically related to the bit-size of the memory. Given a Resolution proof π we denote with $\mathsf{TSpace}(\pi)$ the maximum number of literals appearing in a memory configuration in π.

The line complexity is not an adequate space measure as long as the language of the proof system is strong enough to handle unbounded fan-in $\wedge$ gates: in this case just $O(1)$ memory cells are sufficient as one of them can contain a big-$\wedge$ of all the formulas derived in previous steps. For Resolution, that is not closed under $\wedge$, the lines are just clauses and the clause space makes prefect sense. Indeed Esteban and Torán [23] proposed the study of such measure: given a Resolution proof π, the *clause space*[6], $\mathsf{CSpace}(\pi)$, is the maximum number of clauses appearing in a memory configuration in π. For every contradictory CNF formula in n variables φ there exists a Resolution refutation π of φ such that $\mathsf{CSpace}(\pi) \leqslant n+1$ and hence, clearly, also $\mathsf{TSpace}(\pi) \leqslant n(n+1)$ [23].

An analogue of clause space makes sense also for stronger proof systems, such as Polynomial Calculus, where we consider the number of distinct *monomials* appearing in memory configuration, and analogously as before we define the *monomial space* of a PC refutation π, $\mathsf{MSpace}(\pi)$. Since the Resolution inference rule can be simulated efficiently in PC, from the point of view of space, for every unsatisfiable CNF formula φ in n variables, there exists a PC refutation π of φ such that $\mathsf{MSpace}(\pi) \leqslant O(n)$ and $\mathsf{TSpace}(\pi) \leqslant O(n^2)$. Total space in PC is not yet well understood and the only total space lower bound for PC are the ones by Alekhnovich et al. [2] where this measure was originally introduced.

The second interesting property of space is that this measure is actually nontrivial for not too strong proof systems, indeed Alekhnovich et al. [2, Theorem 6.3] showed that any tautology in n variables has a proof in Frege with "*formula space*" $O(1)$ and total space linear in the number of variables. This fact justifies the study of space for "*weak*" proof systems where actually super-linear lower bounds on space could be achieved, although total space in Frege is still a meaningful complexity measure.

[6] As already noticed by [23], the clause space in Resolution is connected also to the pebbling game on the DAGs associated to Resolution derivations but we do not exploit this analogy.

2.1 Monomial space

We consider families of assignments, r-BG *families*, consisting of *many* partial truth assignments with a combinatorial structure we called *flippable products*. For such families we can define a notion of *rank* that turns out to be roughly the logarithm of the number of assignments in the family. The formal definition of r-BG families, too technical to be presented here, is one of the main innovations of this thesis, since it reduces space lower bounds in algebraic proof systems to a combinatorial property on families of Boolean assignments. The r-BG families resembly other combinatorial definitions used to prove lower bounds in Resolution: the definition of *k-dynamical satisfiability*[22]; the winning strategies characterizing width in Resolution[3]. An r-BG family of assignments for $tr(\varphi)$ is a family of collections of partial assignments such that each collection has rank at most r, none of the collections falsify the polynomials in $tr(\varphi)$ and they satisfy some additional combinatorial properties.

Theorem 3.6 (informal[7]). *Given an unsatisfiable CNF formula φ. If there exists a non-empty r-*BG family of partial assignments for *$tr(\varphi)$ then for every* PC *refutation π of φ,* $\mathsf{MSpace}(\pi) \geqslant \frac{r}{4}$.

All the monomial space lower bounds obtained using this theorem are not dependent on the characteristic of the ground field $\mathbb{F}$ used in PC. This result generalizes the techniques used in [2, 24] and indeed the main technical difficulty to prove Theorem 3.6 is to prove a generalization of [2, Lemma 4.14], the *Locality Lemma*. As corollaries of Theorem 3.6, we are able to re-obtain all the lower bounds on monomial space known from [2, 24] and to prove the first monomial space lower bound for random k-CNF formulas, for $k \geqslant 3$, cf. Section 3. Moreover, Filmus et al. [25] applied (a preliminary version of) Theorem 3.6 to *Tseitin formulas* over random 4-regular graphs, cf. Section 4.

2.2 Total space in Resolution

The main result here is a general technique to prove *total space* lower bounds in Resolution, cf. Theorem 2.5, and, as an application, the fact that in Resolution '*total space is lower bounded by the square of width*', cf. Corollary 2.11. Then, as corollaries, we immediately have total space lower bounds for various families of CNF formulas of interest. We postpone the discussion of the results on random k-CNF formulas to Section 3 and the results on Tseitin formulas to Section 4.

Our main theorem for total space in Resolution, Theorem 2.5, and Theorem 3.6 on monomial space have similar statements. Here, to get total space lower

[7] The result proven is actually stronger since it holds for *semantic* PC, but for simplicity we state it here just for PC.

bounds we use r-BK families of partial truth assignments introduced in [10] to characterize the *asymmetric width* in Resolution, a complexity measure similar to the width[8]. An r-BK family for φ is a collection of partial assignments not falsifying φ and such that some combinatorial extension property holds for assignments of domain bounded by r.

Theorem 2.5 (informal)**.** *Given an unsatisfiable CNF formula φ, if there exists a non-empty r-*BK family of assignments for φ *then any* Res *refutation of φ must pass through a memory configuration of at least $r/2$ clauses each at least of $r/2$ many literals. Hence, in particular any* Res *refutation of φ require total space $r^2/4$.*

Corollary 2.11 (informal)**.** *Let φ be an unsatisfiable k-CNF formula, if there exists a* Res *refutation π of φ such that* $\mathsf{TSpace}(\pi) \leqslant T$ *then there exists a* Res *refutation π' of φ such that* $\mathsf{width}(\pi') \leqslant O(\sqrt{T}) + k$.

There are many of such CNF formulas φ with the properties above, for example random k-CNFs (see next Section). Moreover it follows an optimal separation between Resolution and a *semantic* version of it from the point of view of the total space measure. In the thesis there are also some lower bounds on total space for semantic Resolution and for a bounded version of it.

3 Random *k*-CNFs

Let k a positive integer and Δ a positive real number, an (n, k, Δ)-*random CNF formula* φ is a k-CNF formula with n variables and Δn clauses picked uniformly at random from the set of all CNF formulas in the variables $\{x_1, \dots, x_n\}$ which consist of exactly Δn clauses, each clause containing exactly k literals and no variable appears twice in a clause. For large enough Δ (depending on k), with high probability, an (n, k, Δ)-random CNF formula is unsatisfiable and there exists a constant $\gamma > 0$ such that for each Res refutation π of φ, $\mathsf{width}(\pi) \geqslant \gamma n$ [8].

Theorem 4.36 (informal)**.** *Let $k \geqslant 3$ and $\Delta > 1$. If φ is a (n, k, Δ)-random CNF, then for large n, with high probability, (1) for every* Res *refutation π of φ,* $\mathsf{TSpace}(\pi) \geqslant \Omega(n^2)$*; and (2) for every* PC *refutation π of φ,* $\mathsf{MSpace}(\pi) \geqslant \Omega(n)$.

The total space lower bound completely answers an open problem on the total space complexity in Resolution of random k-CNF formulas from [2, 6, 25] among others. It follows immediately by Corollary 2.11 and it also shows an optimal separation between semantic Resolution and Resolution from the point of view of total space and thus completely answers [2, Open question 4] for Resolution.

[8] This characterization is similar to the characterization of width in [3].

The lower bound on monomial space was conjectured to be true and posed as an open problem in many works, for instance [2, 6, 24]. The proof of this result use Theorem 3.6 and essentially consists in constructing an $\Omega(n)$-BG family of partial assignments for φ[9]. This technical construction relies on some combinatorial games over bipartite graphs, the *Cover Games*, and to some variations of Hall's theorem to objects similar to matchings, V-matchings and VW-matchings.

4 Tseitin formulas

Tseitin formulas, $\mathsf{Tseitin}(G, \sigma)$, are essentially Boolean encodings of the fact that the total degree of any graph is an even number[10]. Tseitin formulas are one of the standard tools used in proof complexity to prove lower bounds and trade-offs, for example they have used to prove the very first super-polynomial lower bound for Resolution Tseitin [39], result improved then to an exponential lower bound in [40]; they have been investigated regarding the width [8], clause space [23] and regarding size-space trade-offs in both Res and PC [4]. Notice that Tseitin formulas have polynomial size refutations in PC over $\mathbb{F}_2$, essentially mimicking Gaussian elimination. In [8] it is proved that for every Resolution refutation π of $\mathsf{Tseitin}(G, \sigma)$,

$$\mathsf{width}(\pi \vdash \bot) \geqslant e(G), \tag{3}$$

where $e(G)$ is the *connectivity expansion* of $G = (V, E)$: for any set E' of at most $e(G)$ edges it holds that $G' = (V, E \setminus E')$ has a (unique) connected component of size strictly larger than $|V|/2$. If $e(G) = \Omega(|V|)$, which happens for example for random d-regular graphs (w.h.p.), then from equation (3) and (1) it follows an exponential lower bound on the size of Resolution refutations of Tseitin formulas. Then as an application of Corollary 2.11 we answer the open problem from [2, Open question 2] concerning total space lower bounds for Tseitin formulas in Resolution.

Theorem 4.7 (informal). *Let $G = (V, E)$ be a connected d-regular graph and σ an odd-weight function over V, then for every Resolution proof π of* $\mathsf{Tseitin}(G, \sigma)$

$$\mathsf{TSpace}(\pi) \geqslant \Omega((e(G) - d)^2).$$

[9] An analogue result holds also for the *matching principle over a graph G*, G-PHP, where G is an expander bipartite graph with left degree at least 3, cf. Theorem 4.38.

[10] Formally the Tseitin formulas are defined as follows. Let $G = (V, E)$ be a finite connected graph of degree at most d over n vertices and $\sigma : V \to \{0, 1\}$ be such that $\sum_{v \in V} \sigma(v) \equiv 1 \pmod 2$. Consider now the set of Boolean variables $X = \{x_e : e \in E\}$ and for each $v \in V$ let $\mathsf{PARITY}_{v,\sigma}$ be the CNF formula expressing the following parity: $\sum_{e \ni v} x_e \equiv \sigma(v) \pmod 2$. The *Tseitin formula*, $\mathsf{Tseitin}(G, \sigma)$, is then $\bigwedge_{v \in V} \mathsf{PARITY}_{v,\sigma}$.

In particular if G is a 3-regular expander graph over n vertices then every Resolution refutation π is such that $\mathsf{TSpace}(\pi) = \Theta(n^2)$.

Regarding the monomial space in Polynomial Calculus the picture is more complex. We do not know non-trivial monomial space lower bound for Tseitin formulas over 3-regular expander graphs. Yet we have some monomial space lower bounds for some Tseitin formulas. In particular the following results showed by Filmus et al. [25] relying on a preliminary version of Theorem 3.6:

• If $G = (V, E)$ is a d-regular graph with edges with multiplicity 2, then for every PC refutation π of $\mathsf{Tseitin}(G, \sigma)$, $\mathsf{MSpace}(\pi) \geqslant \Omega(e(G) - d)$.

• If $G = (V, E)$ is a random d-regular graph on n vertices, where $d \geqslant 4$, then w.h.p. for each PC refutation of $\mathsf{Tseitin}(G, \sigma)$, $\mathsf{MSpace}(\pi) \geqslant \Omega(\sqrt{n})$.

5 Strong size lower bounds

Given a k-CNF formula in n variables φ, we call a Resolution size lower bound *strong*[11] if for every Resolution refutation π of φ,

$$\mathsf{size}(\pi) \geqslant 2^{(1-\epsilon_k)n},$$

where $\lim_{k\to\infty} \epsilon_k = 0$. Similarly a width lower bound is *strong*[12] if for every Resolution refutation π of φ $\mathsf{width}(\pi) \geqslant (1 - \epsilon_k)n$, where $\lim_{k\to\infty} \epsilon_k = 0$.

We show a strong size lower bound for a sub-system of Resolution where at most a fraction of δ variables can be resolved multiple times along any path in a refutation DAG of an unsatisfiable CNF formula. We called *δ-regular* Resolution such system in between unconstrained Resolution and *regular* Resolution, a variation of Resolution where are allowed as valid only the Resolution refutations that have a DAG structure where along any path no variable is resolved twice. Similarly we can define *tree-like* Resolution, a variation of Resolution where are allowed as valid only the Resolution refutation that have a tree-like structure. Before our result strong size lower bounds were known for tree-like Resolution [36] and for regular Resolution [5]. Our results both improve and simplify the strong size lower bound from Beck and Impagliazzo [5] and improve the asymptotic of the ϵ_k for tree-like and regular Resolution. More precisely we prove the following.

[11] Proving a strong exponential size lower bound for Resolution will mean that no SAT-solver purely based on Conflict Driven Clause Learning will be able to refute the *Strong Exponential Time Hypothesis*, due to the fact that such solvers are polynomially simulated by Resolution.

[12] It is always the case that strong width lower bounds in Resolution imply strong size lower bound in *tree-like* Resolution, due to the size-width tradeoff for tree-like Resolution [8]. This is not the case for general Resolution, since the best known general tradeoff between width and size, equation (1), has some constant loss.

Corollary 5.8 (informal)**.** *For any large enough n and $k \in \mathbb{N}$ there exists an unsatisfiable k-CNF formula ψ in n variables such that for every δ-regular Resolution refutation π of ψ* $\mathsf{size}(\pi) \geqslant 2^{(1-\epsilon_k)n}$, *where both ϵ_k and δ are $\widetilde{O}(k^{-1/4})$.*

The first ingredient to prove this result is a strong width lower bound.

Theorem 5.6 (informal)**.** *For any large n and k, there exist an unsatisfiable k-CNF formula φ on n variables such that for every Resolution refutation π of φ* $\mathsf{width}(\pi) \geqslant (1 - \zeta_k)n$, *where $\zeta_k = \widetilde{O}(k^{-1/3})$.*

Notice that the best possible would be $\zeta_k = O(k^{-1})$ since for every unsatisfiable k-CNF formula on n variables there exists a tree-like Resolution of size at most $2^{\left(1-\Omega(k^{-1})\right)n}$, cf. Theorem 5.2.

The second ingredient to prove Corollary 5.8 is an hardness amplification result, Theorem 5.5, proved using characterizations of Resolution size [35] and width [3] as games. Given a CNF formula φ in n variables, the *ℓ-xorification* of φ, $\varphi[\oplus^\ell]$, is a formula over ℓn new Boolean variables obtained by replacing each occurrence of x_i in φ with $y_i^1 \oplus \cdots \oplus y_i^\ell$ where y_i^j are fresh new variables.

Theorem 5.5 (informal)**.** *Let φ an unsatisfiable CNF formula in n variables and let W, δ and ℓ be parameters. If for every Resolution refutation π of φ,* $\mathsf{width}(\pi) \geqslant W$, *then for every δ-regular Resolution refutation π' of $\varphi[\oplus^\ell]$,*

$$\mathsf{size}(\pi') \geqslant 2^{(1-\epsilon)W\ell},$$

where $\epsilon = \frac{1}{\ell}\log\left(\frac{e^3\ell n}{W}\right) + \frac{\delta n}{W}\log\left(\frac{e^3\ell}{\delta}\right)$.

References

[1] Michael Alekhnovich and Alexander A. Razborov. "Lower Bounds for Polynomial Calculus: Non-Binomial Case". In: *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*. IEEE Computer Society, 2001, pp. 190–199.

[2] Michael Alekhnovich et al. "Space Complexity in Propositional Calculus". In: *SIAM J. Comput.* 31.4 (2002), pp. 1184–1211.

[3] Albert Atserias and Víctor Dalmau. "A combinatorial characterization of resolution width". In: *J. Comput. Syst. Sci.* 74.3 (2008), pp. 323–334.

[4] Chris Beck, Jakob Nordström, and Bangsheng Tang. "Some trade-off results for polynomial calculus: extended abstract". In: *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*. Ed. by Dan Boneh, Tim Roughgarden, and Joan Feigenbaum. ACM, 2013, pp. 813–822.

[5] Christopher Beck and Russell Impagliazzo. "Strong ETH holds for regular resolution". In: *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*. Ed. by Dan Boneh, Tim Roughgarden, and Joan Feigenbaum. ACM, 2013, pp. 487–494.

[6] Eli Ben-Sasson. "Expansion in Proof Complexity". Hebrew University. PhD thesis. Hebrew University, 2001.

[7] Eli Ben-Sasson and Russell Impagliazzo. "Random CNF's are Hard for the Polynomial Calculus". In: *Computational Complexity* 19.4 (2010), pp. 501–519.

[8] Eli Ben-Sasson and Avi Wigderson. “Short proofs are narrow - resolution made simple”. In: *J. ACM* 48.2 (2001), pp. 149–169.

[9] Patrick Bennett et al. “Space proof complexity for random 3-CNFs”. In: *CoRR* abs/1503.01613 (2015).

[10] Olaf Beyersdorff and Oliver Kullmann. “Unified Characterisations of Resolution Hardness Measures”. In: *Theory and Applications of Satisfiability Testing - SAT 2014 - 17th International Conference, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*. Ed. by Carsten Sinz and Uwe Egly. Vol. 8561. Lecture Notes in Computer Science. Springer, 2014, pp. 170–187.

[11] Archie Blake. “Canonical Expressions in Boolean Algebra”. University of Chicago. PhD thesis. University of Chicago, 1937.

[12] Ilario Bonacina and Nicola Galesi. “A Framework for Space Complexity in Algebraic Proof Systems”. In: *J. ACM* 62.3 (June 2015), 23:1–23:20.

[13] Ilario Bonacina and Nicola Galesi. “Pseudo-partitions, transversality and locality: a combinatorial characterization for the space measure in algebraic proof systems”. In: *Innovations in Theoretical Computer Science, ITCS ’13, Berkeley, CA, USA, January 9-12, 2013*. Ed. by Robert D. Kleinberg. ACM, 2013, pp. 455–472.

[14] Ilario Bonacina, Nicola Galesi, and Neil Thapen. “Total Space in Resolution”. In: *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*. IEEE Computer Society, 2014, pp. 641–650.

[15] Ilario Bonacina and Navid Talebanfard. “Improving resolution width lower bounds for k-CNFs with applications to the Strong Exponential Time Hypothesis”. In: *Information Processing Letters* 116.2 (2015), pp. 120 –124.

[16] Ilario Bonacina and Navid Talebanfard. “Strong ETH and Resolution via Games and the Multiplicity of Strategies”. In: *10th International Symposium on Parameterized and Exact Computation (IPEC 2015)*. Ed. by Thore Husfeldt and Iyad Kanj. Vol. 43. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015, pp. 248–257.

[17] Maria Luisa Bonet and Nicola Galesi. “Optimality of size-width tradeoffs for resolution”. In: *Computational Complexity* 10.4 (2001), pp. 261–276.

[18] Samuel R. Buss et al. “Linear Gaps Between Degrees for the Polynomial Calculus Modulo Distinct Primes”. In: *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, May 1-4, 1999, Atlanta, Georgia, USA*. Ed. by Jeffrey Scott Vitter, Lawrence L. Larmore, and Frank Thomson Leighton. ACM, 1999, pp. 547–556.

[19] Samuel R. Buss et al. “Proof Complexity in Algebraic Systems and Bounded Depth Frege Systems with Modular Counting”. In: *Computational Complexity* 6.3 (1997), pp. 256–298.

[20] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. “Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability”. In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. Ed. by Gary L. Miller. ACM, 1996, pp. 174–183.

[21] Stephen A. Cook and Robert A. Reckhow. “The Relative Efficiency of Propositional Proof Systems”. In: *J. Symb. Log.* 44.1 (1979), pp. 36–50.

[22] Juan Luis Esteban, Nicola Galesi, and Jochen Messner. “On the complexity of resolution with bounded conjunctions”. In: *Theor. Comput. Sci.* 321.2-3 (2004), pp. 347–370.

[23] Juan Luis Esteban and Jacobo Torán. “Space Bounds for Resolution”. In: *Inf. Comput.* 171.1 (2001), pp. 84–97.

[24] Yuval Filmus et al. “Space Complexity in Polynomial Calculus”. In: *SIAM J. Comput.* 44.4 (2015), pp. 1119–1153.

[25] Yuval Filmus et al. “Towards an Understanding of Polynomial Calculus: New Separations and Lower Bounds - (Extended Abstract)”. In: *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*. Ed. by Fedor V. Fomin et al. Vol. 7965. Lecture Notes in Computer Science. Springer, 2013, pp. 437–448.

[26] Nicola Galesi and Massimo Lauria. “On the Automatizability of Polynomial Calculus”. In: *Theory Comput. Syst.* 47.2 (2010), pp. 491–506.

[27] Nicola Galesi and Massimo Lauria. “Optimality of size-degree tradeoffs for polynomial calculus”. In: *ACM Trans. Comput. Log.* 12.1 (2010), p. 4.

[28] Dima Grigoriev and Edward A. Hirsch. “Algebraic proof systems over formulas”. In: *Electronic Colloquium on Computational Complexity (ECCC)* 8.11 (2001).

[29] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. “Complexity of semi-algebraic proofs”. In: *Electronic Colloquium on Computational Complexity (ECCC)* 103 (2001).

[30] Joshua A. Grochow and Toniann Pitassi. “Circuit Complexity, Proof Complexity, and Polynomial Identity Testing”. In: *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*. IEEE Computer Society, 2014, pp. 110–119.

[31] Jan Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Cambridge University Press, 1995.

[32] Mladen Mikša and Jakob Nordström. “A Generalized Method for Proving Polynomial Calculus Degree Lower Bounds”. In: *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*. Ed. by David Zuckerman. Vol. 33. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015, pp. 467–487.

[33] Jakob Nordström. “On the Interplay Between Proof Complexity and SAT Solving”. In: *ACM SIGLOG News* 2.3 (Aug. 2015), pp. 19–44.

[34] Toniann Pitassi. “Algebraic Propositional Proof Systems”. In: *Descriptive Complexity and Finite Models, Proceedings of a DIMACS Workshop, January 14-17, 1996, Princeton University*. Ed. by Neil Immerman and Phokion G. Kolaitis. Vol. 31. DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, 1996, pp. 215–244.

[35] Pavel Pudlák. “Proofs as Games”. In: *The American Mathematical Monthly* 107.6 (2000), pp. 541–550.

[36] Pavel Pudlák and Russell Impagliazzo. “A lower bound for DLL algorithms for k-SAT (preliminary version)”. In: *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, January 9-11, 2000, San Francisco, CA, USA*. Ed. by David B. Shmoys. ACM/SIAM, 2000, pp. 128–136.

[37] Ran Raz and Iddo Tzameret. “The Strength of Multilinear Proofs”. In: *Computational Complexity* 17.3 (2008), pp. 407–457.

[38] John Alan Robinson. “A Machine-Oriented Logic Based on the Resolution Principle”. In: *J. ACM* 12.1 (1965), pp. 23–41.

[39] G.S. Tseitin. “On the Complexity of Derivation in Propositional Calculus”. English. In: *Automation of Reasoning*. Ed. by Jörg H. Siekmann and Graham Wrightson. Symbolic Computation. Springer Berlin Heidelberg, 1983, pp. 466–483.

[40] Alasdair Urquhart. “Hard examples for resolution”. In: *J. ACM* 34.1 (1987), pp. 209–219.