Space in weak propositional proof systems*
a 20 pages abstract

Ilario Bonacina

April 7, 2016

1 In the thesis

We consider logical proof systems from the point of view of their *space complexity*, in particular we focus on the following two: *Resolution*, a well studied proof system that is at the core of state-of-the-art algorithms to solve SAT instances; *Polynomial Calculus*, a proof system that uses polynomials to refute contradictions. The *space* of a proof[1], informally speaking, measures the size of an auxiliary memory that a verifier needs to check the correctness of the proof. As for the size measure, 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. Since its introduction space proof complexity was source of important problems concerning complexity of proofs in several proof systems.

We completely answer questions on the space complexity for Resolution and Polynomial Calculus raised for the first time in [3, 11] and since then reported many times in the literature. Such questions concern the *total space* in Resolution, that is the total number of literals to be kept in an auxiliary memory and the *monomial space* in Polynomial Calculus, the number of distinct monomials to be kept in an auxiliary memory. We address the problems defining new combinatorial families of assignments nicely related to the complexity measures of interest. The frameworks we introduce to prove space lower bounds belong to the class of game theoretic methods and combinatorial characterizations that are widely used in proof complexity to study complexity measures. Some examples are the Pudlák games characterizing the *size* of Resolution proofs [65] or the families of assignments characterizing Resolution *width* [5], where the width of a proof is the number of literals in the largest clause appearing in it. 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. 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, [3, 11, 41] among others. The framework

*This thesis was defended on December 14, 2015 at the Sapienza University of Rome for a Ph.D. title in Computer Science. The results presented in this thesis build on top of the following publications [19, 24–28].

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

is described in Section 3 of this abstract, the results about random k-CNFs in Section 5 and the ones about Tseitin formulas in Section 6.

Total space in Resolution We give a 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 lower bounds in Resolution for *Tseitin formulas* over d-regular expander graphs, completely answering open problem from [3, Open question 2] and we prove asymptotically optimal total space lower bound in Resolution for random k-CNF formulas, completely answering an open problems from [3, 11, 42] 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 [3, Open question 4] for Resolution.

The framework and the separation between Resolution and semantic Resolution are described more in details in Section 4 of this abstract, the results for random k-CNFs in Section 5 and the ones for Tseitin formulas in Section 6.

Size and width in Resolution Together with the main results about space this thesis contains also a detour on size, cf. Section 7 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. This strengthens and simplifies a result in [10]. More precisely we show a *strong* width lower bound for Resolution and a *strong* size lower bound for a generalisation of *regular* Resolution.

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

2 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, cf. [8, 69]. 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 $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$. 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 $\mathsf{NP} \neq \mathsf{coNP}$ [35], 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* of a proof? We saw that proof systems have some analogies with computational complexity and in that context space notions have been investigated: for example the size of a working-tape

needed by a Turing machine to compute a given function. Pictorially, we could state the space question in proof complexity as *what is the smallest blackboard a teacher needs to present the proof of a theorem to a class of students?*

There are many proof systems that are studied in the literature, for example the common 'textbook' proof systems for propositional logic based on axioms and inference rules, usually modus ponens, cf. [35], those are called Frege systems. In this thesis we focus on two particular propositional proof systems called Resolution and Polynomial Calculus. Such proof systems operate with formulas in *Conjunctive Normal Form* (CNF): 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.

2.1 Resolution

Resolution (Res) [23, 73] is a sound and complete propositional proof system manipulating unsatisfiable CNF formulas. 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:

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

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, cf. the surveys [8, 60, 64, 66, 71, 75]. 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.

A technique that turned out to be very useful in proving superpolynomial lower bounds and exponential lower bounds on the size of Resolution proofs is the "*size-width tradeoff*" by Ben-Sasson and Wigderson [18]: given an 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, $\mathsf{width}(\pi) \geqslant \omega(\sqrt{n \log n})$ then immediately φ must require Resolution refutations of super-polynomial size. Bonet and Galesi [30] proved that such result is optimal up to a logarithmic factor. Nowadays 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 *DPLL algorithm* [37, 38] and the *CDCL solvers* [6, 58, 76], which are at the core of the state-of-the-art SAT solvers used nowaday. By construction Resolution polynomially-simulates the CDCL solvers on unsatisfiable instances, hence, in particular, lower bounds on Resolution size and Resolution *space* (cf. Section 2.3) imply lower bounds on the running time and the memory consumption of CDCL solvers. For more details on the connection between Resolution, proof complexity and SAT solvers we refer to [60].

2.2 Polynomial Calculus

In *Polynomial Calculus*, PC, [3, 34] 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[2]. 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. There are algebraic proof systems that allow manipulations on polynomials in an implicit form and this results in stronger, not so well understood, proof systems, cf. [31, 32, 46–48, 63, 68]. In this thesis we focus on the proof system PC and actually on some stronger *semantic* super-system of it, cf. Section 2.4.

As in Resolution, there are unsatisfiable formulas requiring exponentially long PC proofs [34, 44, 57, 70] and there exists a "*size-degree tradeoff*", where the *degree* of a PC proof π, $\mathsf{degree}(\pi)$, is the maximum degree of a polynomial appearing in π. Impagliazzo, Pudlák, and Sgall [52] showed that degree lower bounds imply PC size lower bounds: given a k-CNF formula φ, if there exists a PC proof of φ such that $\mathsf{size}(\pi) \leqslant S$ 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 $\mathsf{degree}(\pi) \geqslant \omega(\sqrt{n \log n})$ then φ cannot have polynomial size PC proofs. It is interesting to notice the similarity between this lower bound and the one for Resolution, cf. 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 [44] and most of the super-polynomial or exponential size lower bounds for PC proofs are obtained through degree lower bounds.

In particular, if $\operatorname{char} \mathbb{F} \neq 2$ then some Fourier-like transformation can be used to reduce degree lower bounds to Resolution [14]. Another interesting result that depends on the characteristic of the ground field $\operatorname{char} \mathbb{F} \neq 2$ is the one by Razborov [72] about the hardness of *pseudorandom generators* for the Polynomial Calculus over the ground field $\mathbb{F}$. A more general technique to prove degree lower bounds, working also if $\operatorname{char} \mathbb{F} = 2$, was introduced in [1] and generalized in [43, 57].

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 is 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 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 [32, 34].

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

2.3 Space

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.

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*. 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 particular CNF formula is contradictory 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 Frege or Res or PC among others.

The formal definition goes as follows [3, 40, 53]: 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, $\mathfrak{M}_0 = \emptyset$, $\bot \in \mathfrak{M}_\ell$ 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 memory configurations as sets of polynomials and as inference rules the ones from PC.

As Alekhnovich et al. [3] 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 [56], 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*[3], 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.

We already saw a proof system, Resolution, that is not closed under $\wedge$. For this system the lines are just clauses and the clause space makes prefect sense. Indeed Esteban and Torán [40] proposed the study of such measure: given a Resolution proof π, the *clause space*[4], $\mathsf{CSpace}(\pi)$, is the maximum number of clauses appearing in a memory configuration in π.

[3] Alekhnovich et al. [3] called this measure *variable space* but we prefer to call it *total space* following [15–17, 59, 61, 82]. The reason to do this is to distinguish this measure from another one, the *variable space*, where different occurrences of the same variable are not counted, cf. [82].

[4] As already noticed by [40], 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.

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, $\mathsf{MSpace}(\pi)$.

Some works on space related issues in Resolution and in some stronger proof systems are the followings: [3, 5, 12, 40] studied space in Resolution and in particular concerning trade-offs [7, 9, 16, 17, 61, 62]; [15, 39] studied space-related questions for *Resolution over k-DNFs*, a variation of Resolution handling k-DNF formulas instead of clauses; [3, 19, 24, 41, 42] studied space in Polynomial Calculus and for tradeoffs for example [9, 61]; [45] recently showed some results on space in *Cutting Planes*.

2.3.1 Upper bounds

Esteban and Torán [40] showed that all contradictions can be refuted within polynomial space for any 'reasonable' space measure. More precisely they showed that 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 $\mathsf{TSpace}(\pi) \leqslant n(n+1)$.

Since the Resolution inference rule can be simulated efficiently in PC, from the point of view of space, the upper bounds in Resolution carry on for PC. Hence, 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. [3] where this measure was originally introduced.

The second interesting property of space is that this measure is actually non-trivial for not too strong proof systems, indeed Alekhnovich et al. [3, 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.

2.4 Semantic Resolution and semantic Polynomial Calculus

Going back to space measures in general, interestingly a phenomenon happens: for some space measures the actual inference rules of the proof systems do not matter, that is the space lower bound holds for some *semantic* version of the proof systems. What matters in such cases are the objects manipulated by the system, for example clauses or polynomials. This phenomenon was first observed in [3] for the clause space, for monomial space for some restricted class of formulas and for Frege in general. The definition of semantic Resolution and PC follows closely the definition using memory configurations we saw before, the only thing that changes[5] is the inference rule.

A *semantic* Res refutation of a CNF formula φ is sequence of memory configurations $(\mathfrak{M}_0, \ldots, \mathfrak{M}_\ell)$ where $\mathfrak{M}_0 = \emptyset$, $\bot \in \mathfrak{M}_\ell$, and $\mathfrak{M}_i$ is a set of clauses obtained from $\mathfrak{M}_{i-1}$, which is the result of an axiom download, an erasure or a

(Semantic inference) $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{C\}$, where $\mathfrak{M}_{i-1} \vDash C$, that is for each truth assignment α, if $\alpha \vDash \mathfrak{M}_{i-1}$ then $\alpha \vDash C$.

Regarding PC we have the notion of *I-semantic* PC refutation, where I is an ideal. Taking $I = \{0\}$ this notion is equivalent to the notion of *semantic* PC refutation from [3]. Let I be

[5] For sake of clarity here we simplified a bit the actual definition of such systems in the thesis.

an ideal in $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$, an *$I$-semantic* PC refutation of a CNF φ, is a sequence of memory configurations $(\mathfrak{M}_0, \ldots, \mathfrak{M}_\ell)$ such that: $\mathfrak{M}_0 = \emptyset$, $1 \in \mathfrak{M}_\ell$ and for all $i \leqslant \ell$, $\mathfrak{M}_i$ is a set of polynomials obtained by $\mathfrak{M}_{i-1}$ by an axiom download, an erasure or an

(I-Semantic Inference) $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{p\}$, for some $p \in \text{ideal}(\mathfrak{M}_{i-1}) + I$. Where $\text{ideal}(\mathfrak{M}_{i-1}) + I$ is just the sum among ideals[6].

In this thesis we show that asymptotically optimal monomial space lower bounds for semantical PC refutations hold for more general class of formulas than the ones in [3, 41] and that for total space in Resolution the actual inference rule *does* matter, that is we show a separation between Resolution and semantical Resolution.

2.5 Game theoretic methods

In proof complexity game theoretic methods and combinatorial characterizations of hardness measures have a long history. Games characterizing size of proofs have been introduced for example for Resolution [49, 65] and bounded-depth Frege [13], but game theoretic measures have proven to be useful also when studying other hardness measures [5, 22]. The most notable example is the game and combinatorial characterization of Resolution width by Atserias and Dalmau [5]. In [5] the authors connected the width hardness measure to a combinatorial family of assignments and then to a game derived by the existential Ehrenfeucht-Fraïssé k-pebble game as used by Kolaitis and Vardi [54, 55] in the context of finite model theory and DATALOG. Games have proven to be useful also in the context of tree-like Resolution as shown by the optimal bounds obtained by Beyersdorff, Galesi, and Lauria [20, 21]. The frameworks we introduce to prove space lower bounds belong to the class of game theoretic methods and combinatorial characterizations that are widely used in proof complexity to study complexity measures.

3 Monomial space

The space lower bound in Polynomial Calculus (Theorem 3.6) is one of the main contributions of this thesis and builds on the definition of r-BG *family*. This definition is one of the main innovations of this work, since it reduces space lower bounds in algebraic proof systems to a combinatorial property on families of Boolean assignments.

We consider families of assignments, 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 is roughly lower bounding the number of monomials. This notion of rank turns out to be roughly the logarithm of the number of assignments in the family. Then the monomial space lower bound we show, Theorem 3.6, has a high level structure similar to known space lower bounds, such as for example the one in [5]. Our definition of r-BG families resembles the definition of *k-dynamical satisfiability* in [39] which was used to prove space lower bounds for Resolution. Likewise, the definition of r-BG family is analogous to the definition of winning strategies for the Duplicator in the k-existential Spoiler-Duplicator game which led to the proof that in Resolution '*clause space is lower bounded by width*', cf. [5]. We now can state an informal version of Theorem 3.6, leaving to Section 3.1 more details on the construction of r-BG families.

[6] Given two ideals I, J in $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$, $I + J = \{a + b : a \in I \wedge b \in J\}$.

Theorem 3.6 (informal)**.** *Given a field $\mathbb{F}$, an ideal I in $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$ and an unsatisfiable CNF formula φ in the variables $x_1, \ldots, x_n$. If there exists a non-empty r-BG family of partial assignments for $tr(\varphi)$ w.r.t. I then for every I-semantic PC refutation π of φ, $\mathsf{MSpace}(\pi) \geqslant \frac{r}{4}$.*

This result generalizes the techniques used in [3, 41] and indeed the main technical difficulty to prove Theorem 3.6 is to prove a generalization of [3, Lemma 4.14], the *Locality Lemma*, cf. Section 3.1. In particular, for the class of flippable products, we are able to re-prove all the lower bounds on monomial space from [3, 41]. More importantly, Theorem 3.6 allows to prove the first monomial space lower bound for random k-CNF formulas, for $k \geqslant 3$, and for the graph pigeonhole principle over a graph of (left) degree at least 3, cf. Section 5. Moreover, Filmus et al. [42] applied (a preliminary version of) Theorem 3.6 to *Tseitin formulas* over random 4-regular graphs, cf. Section 6.

All the monomial space lower bounds we obtain are not dependent on the characteristic of the field $\mathbb{F}$, where $\mathbb{F}$ is used as ground field in PC. So the result about Tseitin formulas [42] is particularly interesting over $\mathbb{F}_2$ since over that field they have polynomial size PC refutations but those refutations, for the space lower bound shown, must require large monomial space.

3.1 r-BG families and the locality lemma

Given a set of partial truth assignments F, $\mathrm{dom}(F)$ is the union of the domain of all the partial assignments in F. Given non-empty sets of partial truth assignments $H_1, \ldots, H_t$ pairwise domain-disjoint, the *product-family* $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$ is the following set of assignments

$$\mathcal{H} = H_1 \otimes \cdots \otimes H_t = \{\alpha_1 \cup \cdots \cup \alpha_t : \alpha_i \in H_i\},$$

or, if $t = 0$, $\mathcal{H} = \{\lambda\}$, a set containing just the empty partial assignment λ. We call the H_is the *factors* of $\mathcal{H}$ and the *rank* of $\mathcal{H}$, $\|\mathcal{H}\|$, is the number of factors of $\mathcal{H}$ different from $\{\lambda\}$. The domain of $\mathcal{H}$ is $\bigcup_i \mathrm{dom}(H_i)$.

The same set of assignments could correspond to many product-families: in particular each family of assignments can be seen as a product of just one single factor. When we write $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$ it means that we fixed a particular representation of the set of assignment as a product: the representation has $H_1, \ldots, H_t$ as factors. We do not count the $\{\lambda\}$ factors in the rank since they do not carry any additional information: the set of assignments corresponding to $\mathcal{H} \otimes \{\lambda\}$ always coincide with $\mathcal{H}$. Given two product-families $\mathcal{H}$ and $\mathcal{H}'$ we write $\mathcal{H}' \sqsubseteq \mathcal{H}$ if and only if each factor of $\mathcal{H}'$ different from $\{\lambda\}$ is also a factor of $\mathcal{H}$. In particular $\{\lambda\} \sqsubseteq \mathcal{H}$ for any $\mathcal{H}$.

We are interested in particular product-families such that each factor is *flippable*. A set of partial truth assignments F is *flippable* if and only if for all $v \in \mathrm{dom}(F)$ there exists α and β in F such that $\alpha(v) = 1$ and $\beta(v) = 0$. We call a product-family whose factors are flippable a *flippable product-family* or simply a *flippable product*. Finally, given an ideal I in $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$ we say that a family of partial truth assignments F is *I-consistent* if for every $p \in I$ and $\alpha \in F$, $p|_\alpha \in I$, where $p|_\alpha$ denote the polynomial p restricted assigning variables according to α. We then have all the ingredients to define what an r-BG family is.

Definition 3.4 (r-BG family (informal))**.** *Let P be a set of polynomials in $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$ and I a proper ideal in such ring. A family of flippable products $\mathscr{F}$ is a r-BG family for P with respect to I if and only if for every $\mathcal{H} \in \mathscr{F}$ the following three conditions hold:*

(CONSISTENCY) *$\mathcal{H}$ is I-consistent;*

(RESTRICTION) *for each* $\mathcal{H}' \sqsubseteq \mathcal{H}$, $\mathcal{H}' \in \mathscr{F}$;

(EXTENSION) *if* $\|\mathcal{H}\| < k$, *then for each* $p \in P$ *there exists a* I*-consistent flippable product* $\mathcal{H}_p$, *domain-disjoint from* $\mathcal{H}$, *such that*

1. $\mathcal{H} \otimes \mathcal{H}_p \in \mathscr{F}$ *and*
2. *for every partial truth assignment* $\alpha \in \mathcal{H} \otimes \mathcal{H}_p$, $p|_\alpha \in I$.

As in [3] a key property in our monomial space lower bound proofs is a *Locality Lemma*. This Lemma is a generalization of analogue results in [3, 25, 41]. Informally, such lemma asserts that if a set S of polynomials is satisfiable by a product family $\mathcal{Z}$, then it is possible to build a new product-family $\mathcal{Z}'$ that still satisfies S but it has rank bounded by the number of distinct monomials in S. The product families we need consider in the lemma have some particular structure and we called them *2-merges*. Let $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$ be a product-family. A 2-*merge* on $\mathcal{H}$ is a product-family $\mathcal{Z} = Z_{J_1} \otimes \cdots \otimes Z_{J_r}$, where $J_1, \ldots, J_r$ are pairwise disjoint subsets of $[t]$ of size at most 2, $Z_{J_i} \subseteq \bigotimes_{j \in J_i} H_j$ and $\mathcal{Z} \restriction_{\mathrm{dom}(H_j)} = H_j$ for all $j \in [t]$.

Lemma 3.9 (Locality Lemma (informal))**.** *Let* I *be an ideal in* $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$, S *a set of polynomials in* $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$, $\mathcal{H}$ *a non-empty flippable product and* $\mathcal{Z}$ *a* 2*-merge on* $\mathcal{H}$ *such that for every truth assignment* $\alpha \in \mathcal{Z}$ *and for every* $p \in S$, $p|_\alpha \in I$. *Then there exist a flippable product* $\mathcal{H}' \sqsubseteq \mathcal{H}$ *and a non-empty* 2*-merge* $\mathcal{Z}'$ *on* $\mathcal{H}'$ *such that:*

- *for every truth assignment* $\alpha \in \mathcal{Z}'$ *and for every* $p \in S$, $p|_\alpha \in I$;
- $\|\mathcal{H}'\|$ *is at most 4 times the number of distinct monomials of* S.

4 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 5 and the results on Tseitin formulas to Section 6. Here we informally describe the more theoretical results: Theorem 2.5, the connection between total space and the width and the separation between Resolution and semantic Resolution from the point of view of total space.

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 bounds we use r-BK families of partial truth assignments.

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* $r^2/4$.

The definition of r-BK families goes as follows.

Definition 2.4 (r-BK, Beyersdorff and Kullmann [22])**.** *A family* $\mathscr{F}$ *of assignments is* r-BK for a CNF formula φ *if it has the following properties:*

(CONSISTENCY) *for every $\alpha \in \mathscr{F}$ and every clause C in φ, α does not falsifies C;*

(EXTENSION) *If $\alpha \in \mathscr{F}$ and $\beta \subseteq \alpha$ is such that $|\operatorname{dom}(\beta)| < r$, then for every variable $x \notin \operatorname{dom}(\alpha)$ there exist $\beta_0, \beta_1 \in \mathscr{F}$ with $\beta \subseteq \beta_0, \beta_1$ such that $\beta_0(x) = 0$ and $\beta_1(x) = 1$.*

This definition is crucial and as Beyersdorff and Kullmann [22, Theorem 22] show this property is characterizing the *asymmetric width* in Resolution, a complexity measure similar to the width. Indeed this characterization is done in a similar way as the characterization of width given in [5]. Using Theorem 2.5 and the properties of asymmetric width we then easily show the following.

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*

$$\mathsf{width}(\pi') \leqslant O(\sqrt{T}) + k.$$

If φ is an unsatisfiable CNF formula in n variables and $O(n)$ clauses than clearly it can be refuted in *semantic* Resolution in total space $O(n)$. On the other hand, if we know by other means that each Res refutation of φ require width $\Omega(n)$ then we have that all Res refutations will require total space $\Omega(n^2)$. Hence it follows an optimal separation between Resolution and *semantic* Resolution from the point of view of the total space measure. There are many of such CNF formulas φ with the properties above, for example random k-CNFs (see next Section). In the thesis there are also some lower bounds on total space for semantic resolution and for a bounded version of it, the interested reader could look at Section 2.5 of the thesis.

5 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 $\{x_1, \ldots, x_n\}$ 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, $\mathsf{width}(\pi) \geqslant \gamma n$, cf. [18, 33]. Then immediately by Corollary 2.11 we have the following.

Theorem 4.36 (part on total space, informal)**.** *Let $k \geqslant 3$ and $\Delta > 1$. If φ is a (n, k, Δ)-random CNF, then for large n, with high probability, any* Res *refutation of φ passes through a memory configuration containing $\Omega(n)$ clauses each at least of $\Omega(n)$ many literals, hence of total space $\Omega(n^2)$.*

This result completely answers an open problem on the total space complexity of random k-CNF formulas from [3, 11, 42] among others. It also shows an optimal separation between semantic Resolution and Resolution from the point of view of total space and thus completely answers [3, Open question 4] for Resolution.

Regarding the monomial space we show an optimal (linear) lower bound for random k-CNF formulas in PC but, contrary to the above result for total space, the proof is a bit more involved and we sketch an overview of it in Section 5.1.

Theorem 4.36 (part on monomial space, informal)**.** *Let $k \geqslant 3$ and $\Delta > 1$. If φ is a (n, k, Δ)-random CNF, then for large n, with high probability, for every I-semantic* PC *refutation π of φ,* $\mathsf{MSpace}(\pi) \geqslant \Omega(n)$*, where I is the ideal generated by the Boolean axioms $\{x_i^2 - x_i\}_{i=1,\ldots,n}$ and $\{x_i + \bar{x}_i - 1\}_{i=1,\ldots,n}$.*

A weaker version of this result was conjectured to be true and posed as an open problem in many works, for instance [3, 11, 41]. The proof of this result use Theorem 3.6 and essentially consists in constructing an $\Omega(n)$-BG family for φ[7].

5.1 An $\Omega(n)$-BG family for random k-CNFs

The space lower bound in Polynomial Calculus to refute random k-CNF formulas, Theorem 4.36, relies on an explicit construction of an r-BG family for such formulas. This is done in Section 4.8 of the thesis and such construction relies on some general games, the *Cover Games*, defined in Section 4.6 of the thesis. Such games are an extension of the *Matching Game* devised in [12] but unlike previous works that deal with classical matchings in bipartite graphs, here the game is generalized to *$\mathscr{C}$-matchings*. While a classical matching is a collection of vertex disjoint edges, intuitively, a *$\mathscr{C}$-matching* in a bipartite graph G is a collection of vertex-disjoint subgraphs of G isomorphic to some graph from the collection of graphs $\mathscr{C}$. For example a V-matching in a graph G is a collection of vertex disjoint subgraphs of G that looks like a V and similarly in VW-matchings subgraphs that look like V or W are allowed. Then informally, given a bipartite graph G, the *Matching Game* guarantees that there is a family of matchings $\mathscr{F}$ such that each matching in $\mathscr{F}$ can be enlarged to cover new vertexes in G or shrunk while remaining in $\mathscr{F}$ and the family $\mathscr{F}$ has large matchings in it. The same kind of game is addressed for $\mathscr{C}$-matchings: the *Cover Game* guarantees that there is a family of $\mathscr{C}$-matchings $\mathscr{L}$ such that each to $\mathscr{C}$-matching in $\mathscr{L}$ can be added new connected components to cover new vertexes in G or removed connected components while remaining in $\mathscr{L}$ and the family $\mathscr{L}$ contains $\mathscr{C}$-matchings with many connected components.

Part of our contribution deals with extending classical results for matchings to V-matchings and VW-matchings. In particular we prove an analogue of Hall's Theorem, cf. Theorem 4.11, for VW-matchings; we prove an analogue of the Matching Game for V-matchings, cf. Theorem 4.15; we prove an analogue of the Matching Game for VW-matchings, cf. Theorem 4.22.

We will construct such $\mathscr{C}$-matchings in the case of random k-CNF formula φ in the *clauses-variables adjacency graph* associated to φ, cf. Definition 4.34. Informally, it is a bipartite graph with on one side the clauses of φ and on the other side the variables of φ and edges if a variable appears in a clause. That is we have that the *semantics* of the vertices in the two elements of the bipartition of our bipartite graphs is different and our $\mathscr{C}$-matchings have to respect such semantical difference. In order to do so we assume that the *bipartite graphs* are subgraphs of the infinite bipartite graph B with vertex set $\mathbb{N} \times \{0,1\}$ and such that $\{(n,b),(m,b')\} \in E(B)$ if and only if $b \neq b'$. Given a bipartite graph G we call $V(G) \cap \{(n,0) \ : \ n \in \mathbb{N}\}$ the *lower part* of G, $L(G)$, and similarly $V(G) \cap \{(n,1) \ : \ n \in \mathbb{N}\}$ is the *upper part* of G, $U(G)$.

We then focus on V-matchings and the VW-matchings: particular $\mathscr{C}$-matchings in which each connected component looks like a 'V', a 'W' or a singleton from $U(G)$. Alekhnovich et al. [3] observed that a version of Hall's theorem holds for V-matchings. Here we prove a version of Hall's Theorem that holds for VW-matchings, cf. Theorem 4.11.

We then define a game over bipartite graphs using $\mathscr{C}$-matchings that is associated with r-BG families. The *Cover Game*, $\mathsf{CoverGame}_{\mathscr{C}}(G,\mu)$, is a game between two players, Choose (he) and Cover (she), on a bipartite graph G. At each step i of the game the players maintain a $\mathscr{C}$-matching F_i in G. They start with the empty $\mathscr{C}$-matching and at step $i+1$ Choose can

[7] 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.

1. remove a connected component from F_i, or

2. if the number of connected components of F_i is strictly less than μ, pick a vertex (either in $L(G)$ or $U(G)$) and challenge Cover to find a $\mathscr{C}$-matching F_{i+1} in G such that

   (a) each connected component of F_i is also a connected component of F_{i+1};

   (b) F_{i+1} covers the vertex picked by Choose.

Cover loses the game $\mathsf{CoverGame}_{\mathscr{C}}(G, \mu)$ if at some point she cannot answer a challenge by Choose. Otherwise, Cover wins.

Our main interest in such games are the winning strategies for Cover and the fact that, for some graphs G, similar to the clauses-variables adjacency graphs we just saw, the winning strategies for Cover in the game $\mathsf{CoverGame}_{\mathscr{C}}(G, \mu)$ provide μ-BG families, cf. Lemma 4.13 and Lemma 4.14. This allow the application of such construction not only to the clauses-variables adjacency graph of a (n, k, Δ)-random CNF formula but also, for example, to some adjacency graphs of the graph pigeonhole principle.

It is then remained to show that, under some assumptions on the graph G, Cover has winning strategies for $\mathsf{CoverGame}_{\mathsf{V}}(G, \mu)$ and for $\mathsf{CoverGame}_{\mathsf{VW}}(G, \mu)$ for large μ, where μ is related to the expansion properties of the graph G. This, informally, is the content of Theorem 4.15 and Theorem 4.22[8]. These guarantee a winning strategy for Cover in the game $\mathsf{CoverGame}_{\mathsf{V}}(G, \mu)$ and $\mathsf{CoverGame}_{\mathsf{VW}}(G, \mu)$. They rely on two main ingredients:

1. G is a $(\gamma n, \delta)$-*bipartite expander* graph, that is

$$\forall A \subseteq L(G),\ |A| \leqslant \gamma n \to |N_G(A)| \geqslant \delta |A|,$$

   where $\delta \geqslant 1.95$.

2. some (technical) upper bound on the number of high degree vertices in $U(G)$.

We then prove that random bipartite graphs satisfy the conditions (1.) and (2.) above with $\mu = \Omega(n)$ and hence the the construction of the $\Omega(n)$-BG family for random k-CNF formulas follows from the winning strategies for Cover.

6 Tseitin formulas

Tseitin formulas are essentially Boolean encodings of the fact that the total degree of any graph is an even number. Those formulas were originally used by Tseitin [78] to present the first super-polynomial lower bound on refutation size for regular Resolution, a restricted form of the Resolution proof system. Then they were used to prove exponential lower bounds on the size of Resolution refutations, for example in [74, 80]. Since then the Tseitin formulas became one of the standard tools used in proof complexity to prove lower bounds and trade-offs, for example they have been investigated regarding the width, cf. [18], clause space, cf. [40] and Beck, Nordström, and Tang [9] regarding size-space trade-offs in Polynomial Calculus.

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. An *odd-weight* function $\sigma : V \to \{0, 1\}$ is a function σ

[8]Both of them can be seen also as extensions of constructions that can be found in the literature for matchings for example in [4, 12].

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 the conjunction $\mathsf{Tseitin}(G, \sigma) = \bigwedge_{v \in V} \mathsf{PARITY}_{v,\sigma}$. The formula $\mathsf{Tseitin}(G, \sigma)$ is a d-CNF formula over at most $dn/2$ variables and $n2^{d-1}$ clauses. The formula $\mathsf{Tseitin}(G, \sigma)$ is unsatisfiable if and only if σ is odd-weight [81].

Ben-Sasson and Wigderson [18, Theorem 4.4] proved that given a connected graph $G = (V, E)$ and an odd-weight function on V, 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:

$$e(G) = \min \left\{ |E \cap (V' \times (V \setminus V'))| : V' \subseteq V \wedge |V'| \in \left[\frac{|V|}{3}, \frac{2|V|}{3} \right] \right\}.$$

Hence, given G and σ as above, a size lower bound follows from the size-width tradeoff [18]: for every Resolution refutation π of $\mathsf{Tseitin}(G, \sigma)$

$$\mathsf{size}(\pi) \geqslant 2^{\Omega(e(G))}.$$

Moreover if G is a connectivity expander, that is $e(G) = \Omega(|V|)$, then from the previous equation it follows an exponential lower bound on the size of Resolution refutations of Tseitin formulas. This lower bound holds, for instance, for random d-regular graphs since they are connectivity expanders with high probability.

Concerning total space lower bounds in Resolution, as an application of Corollary 2.11 we answer the open problem from [3, Open question 2] concerning total space lower bounds for Tseitin formulas.

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 $\mathsf{Tseitin}(G, \sigma)$*

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

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. [42] relying on Theorem 3.6 as appeared in [25]:

- If $G = (V, E)$ is a d-regular graph with double edges[9] and σ any odd-weight function over V, then for every PC refutation π of $\mathsf{Tseitin}(G, \sigma)$

$$\mathsf{MSpace}(\pi) \geqslant \Omega(e(G) - d). \tag{4}$$

[9]That is each edge has multiplicity 2.

More in general they showed that given an unsatisfiable k-CNF formula φ and its *xorification* $\varphi[\oplus]$, then if there exists a PC refutation π of $\varphi[\oplus]$ such that $\mathsf{MSpace}(\pi) \leqslant M$ then there exists a Resolution refutation π' of φ such that

$$\mathsf{width}(\pi') \leqslant 4M + k - 1.$$

The *xorification* of a CNF formula φ is a new CNF formula $\varphi[\oplus]$ obtained by replacing each occurrence of a variable x_i in φ with the XOR of two new variables $x_i' \oplus x_i''$ and then expanding everything as a CNF formula using the definition of the XOR and the De Morgan rules.

- If $G = (V, E)$ is a random d-regular graph on n vertices, where $d \geqslant 4$, then, with high probability, for every odd-weight function σ on V and for each PC refutation of $\mathsf{Tseitin}(G, \sigma)$

$$\mathsf{MSpace}(\pi) \geqslant \Omega(\sqrt{n}). \tag{5}$$

It is known that Tseitin formulas have polynomial size refutations in Polynomial Calculus over $\mathbb{F}_2$, essentially mimicking Gaussian elimination. On the other hand, the monomial space lower bounds showed are based on Theorem 3.6 which do not depend on the characteristic of the ground field. That is despite Tseitin formulas over $\mathbb{F}_2$ have short PC refutations, such refutations still require large monomial space.

7 Strong size lower bounds

The last results shown are about size and width in Resolution. Given a k-CNF formula in n variables φ, we call a *strong* Resolution size lower bound the following kind of lower bound: for every Resolution refutation π of φ

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

where $\epsilon_k \to 0$ as $k \to \infty$. Similarly a *strong* width lower bound is a lower bound of the form: for every Resolution refutation π of φ

$$\mathsf{width}(\pi) \geqslant (1 - \epsilon_k)n,$$

where $\epsilon_k \to 0$ as $k \to \infty$.

We show a strong size lower bound for what we called δ-*regular* Resolution, 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. This system is 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. An example of non-regular minimal-size Resolution refutation presented directly as a DAG is in Figure 1 on the following page. 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. We recall that tree-like Resolution is exponentially weaker than regular Resolution, that, in turn is exponential weaker than Resolution, cf. [2, 29, 77, 79].

The size-width relationship by [18, Corollary 3.4] for tree-like Resolution has the following form: if an unsatisfiable CNF formula φ has a tree-like Resolution refutation π of size at most S then there exists a Resolution refutation π' of φ such that

$$\mathsf{width}(\pi') \leqslant \log S + k. \tag{6}$$

Hence a strong width lower bound in Resolution implies a strong size lower bound in tree-like Resolution. This is not the case for general Resolution, since the best known general relation between width and size [18] has some constant loss, see equation (1).

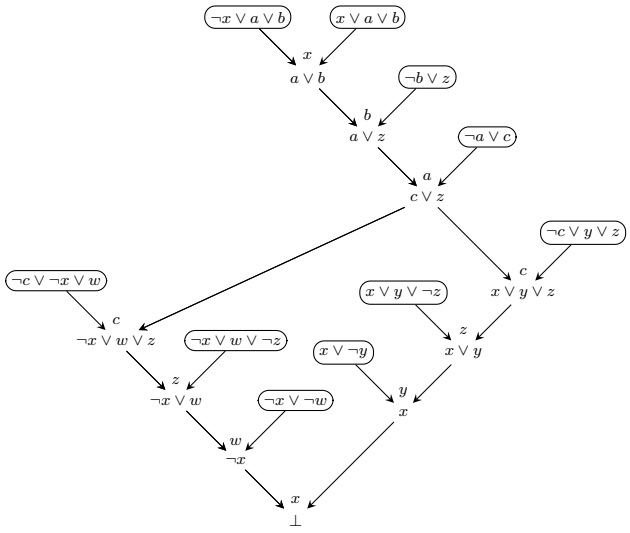

Figure 1: An example of Resolution refutation [50].

Before our result strong size lower bounds were only known for tree-like Resolution [67] and for regular Resolution [10]. Our results both improve and simplify the strong size lower bound from Beck and Impagliazzo [10] and improve the asymptotic of the ϵ_k for tree-like and regular Resolution. More precisely we prove the following.

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 $\zeta_k = \widetilde{O}(k^{-1/3})$.

The width lower bound above is a modification of the analogue of [10, Theorem 5.5]. This width lower bound holds for a family of CNF formulas encoding unsatisfiable linear systems of equations over a finite field with p elements, $\mathbb{F}_p$, for large enough p. The main technical difference, between this width lower bound and [10], is in the way such linear systems over $\mathbb{F}_p$ are encoded using Boolean variables. Encoding such systems of linear equations in a more efficient way gives a better asymptotic: $\zeta_k = \widetilde{O}(k^{-1/3})$ instead of $\zeta_k = \widetilde{O}(k^{-1/4})$ of [10]. 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. 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 ϵ is a well-behaved function[10] *of δ,W and ℓ.*

To prove this result we use Pudlák's characterization of Resolution size as games [65] and the characterization of width as games [5]. Informally, in both games we have two players Prover and Delayer that play on some formula φ. Prover has the objective of showing that the formula φ is unsatisfiable by querying variables. Delayer on the other hand wants to play as long as possible before the formula is falsified while answering to the queries Prover asks her. The size of Resolution proofs of φ is then characterized as the minimal number of *records*, i.e. partial assignments, Prover has to consider in a winning strategy. The width of Resolution proofs of φ is then characterized by the minimal number of variables that the Prover is allowed to have assigned at the same time in a record. The size in δ-regular Resolution is characterized by the number of records in a Pudlák game where Prover is allowed to re-query in each run of the game at most δn variables, where n is the number of variables of the formula φ on which they are playing, cf. Theorem 5.4.

A way to prove a δ-regular Resolution size lower bound is to show that, in order to win, Prover must keep a large number of records and we can do that by producing a lot of sufficiently different strategies for Delayer. To construct such strategies we use the characterization of Resolution width as a game [5], played on the original formula φ. At a very high level, the crucial idea here is to use a winning strategy for Delayer in the width game on φ as a template for many different strategies for Delayer for the size game on $\varphi[\oplus^\ell]$. Prover must win against each of them, hence in his winning strategy he must have a lot of distinct records, since the strategies of Delayer are sufficiently different. Then, the desired size lower bound follows from a counting argument.

We end this section on size lower bounds with a justification for why we called the results shown *strong*.

7.1 Connection with the Strong Exponential Time Hypothesis

There are several non-trivial algorithms known to solve k-SAT, that is the decision problem for satisfiability of k-CNF formulas. Despite this however, the exact complexity of k-SAT under suitable hardness assumptions remains unknown. Formalizing what this complexity could be, Impagliazzo and Paturi [51] formulated the following two hypotheses: let

$$\sigma_k = \inf\{\delta : k\text{-SAT can be solved in time } O(2^{\delta n})\},$$

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

the *Exponential Time Hypothesis*, ETH, states that $\sigma_k > 0$, for every $k \geqslant 3$; the *Strong Exponential Time Hypothesis*, SETH, states that $\lim_{k\to\infty} \sigma_k = 1$. Both ETH and SETH are stronger than NP $\neq$ P and hence any proof is far beyond reach at the moment but such hypotheses are important in *parameterized complexity* [36].

However one can ask whether SETH holds for specific algorithms or class of algorithms. Clearly, one may ask for such result for a *class of algorithms* rather than for a specific one. Natural proof systems, such as Resolution, model the the run of certain k-SAT algorithms on unsatisfiable instances, hence strong size lower bound for Resolution (or tree-like/regular Resolution) implies lower bounds on the running time consistent with SETH. For example, proving a strong exponential size lower bound for Resolution will mean that no CDCL solver will be able to refute SETH, due to the fact that CDCL solvers are polynomially simulated by Resolution.

Exponential size lower bounds for Resolution consistent with ETH are known from a long time, cf. for instance [80]. These are $2^{\Omega(n)}$ lower bounds for k-CNF formulas on n variables and hence not strong enough to support SETH. Although it is widely believed that there should exists strong size lower bounds for Resolution and stronger propositional proof systems, at the moment the strongest proof system for which we have strong size lower bound is δ-regular Resolution, Corollary 5.8.

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. "An Exponential Separation between Regular and General Resolution". In: *Theory of Computing* 3.1 (2007), pp. 81–102.

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

[4] Albert Atserias. "On sufficient conditions for unsatisfiability of random formulas". In: *J. ACM* 51.2 (2004), pp. 281–311.

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

[6] Roberto J. Bayardo Jr. and Robert Schrag. "Using CSP Look-Back Techniques to Solve Real-World SAT Instances". In: *Proceedings of the Fourteenth National Conference on Artificial Intelligence and Ninth Innovative Applications of Artificial Intelligence Conference, AAAI 97, IAAI 97, July 27-31, 1997, Providence, Rhode Island*. Ed. by Benjamin Kuipers and Bonnie L. Webber. AAAI Press / The MIT Press, 1997, pp. 203–208.

[7] Paul Beame, Christopher Beck, and Russell Impagliazzo. "Time-space tradeoffs in resolution: superpolynomial lower bounds for superlinear space". In: *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*. Ed. by Howard J. Karloff and Toniann Pitassi. ACM, 2012, pp. 213–232.

[8] Paul Beame and Toniann Pitassi. "Propositional Proof Complexity: Past, Present, and Future". In: *Current Trends in Theoretical Computer Science*. 2001, pp. 42–70.

[9] 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.

[10] 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.

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

[12] Eli Ben-Sasson and Nicola Galesi. "Space complexity of random formulae in resolution". In: *Random Struct. Algorithms* 23.1 (2003), pp. 92–109.

[13] Eli Ben-Sasson and Prahladh Harsha. “Lower bounds for bounded depth Frege proofs via Pudlák-Buss games”. In: *ACM Trans. Comput. Log.* 11.3 (2010).

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

[15] Eli Ben-Sasson and Jakob Nordström. “A Space Hierarchy for k-DNF Resolution”. In: *Electronic Colloquium on Computational Complexity (ECCC)* 16 (2009), p. 47.

[16] Eli Ben-Sasson and Jakob Nordström. “Understanding Space in Proof Complexity: Separations and Trade-offs via Substitutions”. In: *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*. Ed. by Bernard Chazelle. Tsinghua University Press, 2011, pp. 401–416.

[17] Eli Ben-Sasson and Jakob Nordström. “Understanding space in resolution: optimal lower bounds and exponential trade-offs”. In: *Computational Complexity of Discrete Problems, 14.09. - 19.09.2008*. Ed. by Peter Bro Miltersen et al. Vol. 08381. Dagstuhl Seminar Proceedings. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2008.

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

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

[20] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. “A characterization of tree-like Resolution size”. In: *Inf. Process. Lett.* 113.18 (2013), pp. 666–671.

[21] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. “A lower bound for the pigeonhole principle in tree-like Resolution by asymmetric Prover-Delayer games”. In: *Inf. Process. Lett.* 110.23 (2010), pp. 1074–1077.

[22] 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.

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

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] Maria Luisa Bonet and Nicola Galesi. “A Study of Proof Search Algorithms for Resolution and Polynomial Calculus”. In: *40th Annual Symposium on Foundations of Computer Science, FOCS ’99, 17-18 October, 1999, New York, NY, USA*. IEEE Computer Society, 1999, pp. 422–432.

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

[31] 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.

[32] 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.

[33] Vasek Chvátal and Endre Szemerédi. “Many Hard Examples for Resolution”. In: *J. ACM* 35.4 (1988), pp. 759–768.

[34] 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.

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

[36] Marek Cygan et al. *Parameterized Algorithms*. Springer, 2015.

[37] Martin Davis, George Logemann, and Donald W. Loveland. "A machine program for theorem-proving". In: *Commun. ACM* 5.7 (1962), pp. 394–397.

[38] Martin Davis and Hilary Putnam. "A Computing Procedure for Quantification Theory". In: *J. ACM* 7.3 (1960), pp. 201–215.

[39] 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.

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

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

[42] 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.

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

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

[45] Nicola Galesi, Pavel Pudlák, and Neil Thapen. "The Space Complexity of Cutting Planes Refutations". 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. 433–447.

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

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

[48] 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.

[49] Armin Haken. "The Intractability of Resolution". In: *Theor. Comput. Sci.* 39 (1985), pp. 297–308.

[50] Wenqi Huang and Xiangdong Yu. "A DNF without Regular Shortest Consensus Path". In: *SIAM Journal on Computing* 16.5 (1987), pp. 836–840.

[51] Russell Impagliazzo and Ramamohan Paturi. "On the Complexity of k-SAT". In: *J. Comput. Syst. Sci.* 62.2 (2001), pp. 367–375.

[52] Russell Impagliazzo, Pavel Pudlák, and Jiri Sgall. "Lower Bounds for the Polynomial Calculus and the Gröbner Basis Algorithm". In: *Computational Complexity* 8.2 (1999), pp. 127–144.

[53] Hans Kleine Büning and Theodor Lettmann. *Aussagenlogik - Deduktion und Algorithmen*. Leitfäden und Monographien der Informatik. Teubner, 1994.

[54] Phokion G. Kolaitis and Moshe Y. Vardi. "Conjunctive-Query Containment and Constraint Satisfaction". In: *J. Comput. Syst. Sci.* 61.2 (2000), pp. 302–332.

[55] Phokion G. Kolaitis and Moshe Y. Vardi. "On the Expressive Power of Datalog: Tools and a Case Study". In: *J. Comput. Syst. Sci.* 51.1 (1995), pp. 110–134.

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

[57] 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.

[58] Matthew W. Moskewicz et al. "Chaff: Engineering an Efficient SAT Solver". In: *Proceedings of the 38th Design Automation Conference, DAC 2001, Las Vegas, NV, USA, June 18-22, 2001*. ACM, 2001, pp. 530–535.

[59] Jakob Nordström. "Narrow Proofs May Be Spacious: Separating Space and Width in Resolution". In: *SIAM J. Comput.* 39.1 (2009), pp. 59–121.

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

[61] Jakob Nordström. "Pebble Games, Proof Complexity, and Time-Space Trade-offs". In: *Logical Methods in Computer Science* 9.3 (2013).

[62] Jakob Nordström and Johan Håstad. "Towards an Optimal Separation of Space and Length in Resolution". In: *Theory of Computing* 9 (2013), pp. 471–557.

[63] 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.

[64] Toniann Pitassi. "Propositional Proof Complexity: A Survey on the State of the Art, Including Some Recent Results". In: *Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science, LICS 2011, June 21-24, 2011, Toronto, Ontario, Canada*. IEEE Computer Society, 2011, p. 119.

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

[66] Pavel Pudlák. "Twelve Problems in Proof Complexity". In: *Computer Science - Theory and Applications, Third International Computer Science Symposium in Russia, CSR 2008, Moscow, Russia, June 7-12, 2008, Proceedings*. Ed. by Edward A. Hirsch et al. Vol. 5010. Lecture Notes in Computer Science. Springer, 2008, pp. 13–27.

[67] 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.

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

[69] Alexander A. Razborov. "Lower Bounds for Propositional Proofs and Independence Results in Bounded Arithmetic". In: *Automata, Languages and Programming, 23rd International Colloquium, ICALP96, Paderborn, Germany, 8-12 July 1996, Proceedings*. Ed. by Friedhelm Meyer auf der Heide and Burkhard Monien. Vol. 1099. Lecture Notes in Computer Science. Springer, 1996, pp. 48–62.

[70] Alexander A. Razborov. "Lower Bounds for the Polynomial Calculus". In: *Computational Complexity* 7.4 (1998), pp. 291–324.

[71] Alexander A. Razborov. "Proof Complexity of Pigeonhole Principles". In: *Developments in Language Theory, 5th International Conference, DLT 2001, Vienna, Austria, July 16-21, 2001, Revised Papers*. Ed. by Werner Kuich, Grzegorz Rozenberg, and Arto Salomaa. Vol. 2295. Lecture Notes in Computer Science. Springer, 2001, pp. 100–116.

[72] Alexander A. Razborov. "Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution". In: *Annals of Mathematics* 181 (2015), pp. 415–472.

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

[74] Uwe Schöning. "Resolution Proofs, Exponential Bounds, and Kolmogorov Complexity". In: *Mathematical Foundations of Computer Science 1997, 22nd International Symposium, MFCS'97, Bratislava, Slovakia, August 25-29, 1997, Proceedings*. Ed. by Igor Prívara and Peter Ruzicka. Vol. 1295. Lecture Notes in Computer Science. Springer, 1997, pp. 110–116.

[75] Nathan Segerlind. "The Complexity of Propositional Proofs". In: *Bulletin of Symbolic Logic* 13.4 (2007), pp. 417–481.

[76] João P. Marques Silva and Karem A. Sakallah. "GRASP: A Search Algorithm for Propositional Satisfiability". In: *IEEE Trans. Computers* 48.5 (1999), pp. 506–521.

[77] Gunnar Stålmarck. "Short resolution proofs for a sequence of tricky formulas". English. In: *Acta Informatica* 33.3 (1996), pp. 277–280.

[78] 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.

[79] Alasdair Urquhart. "A Near-Optimal Separation of Regular and General Resolution". In: *SIAM J. Comput.* 40.1 (2011), pp. 107–121.

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

[81] Alasdair Urquhart. "The complexity of propositional proofs". In: *Bulletin of Symbolic Logic* 1.4 (1995), pp. 425–467.

[82] Alasdair Urquhart. "The Depth of Resolution Proofs". In: *Studia Logica* 99.1-3 (2011), pp. 349–364.