A Framework for Space Complexity in Algebraic Proof Systems

ILARIO BONACINA and NICOLA GALESI, Sapienza University of Rome

Algebraic proof systems, such as Polynomial Calculus (PC) and Polynomial Calculus with Resolution (PCR), refute contradictions using polynomials. Space complexity for such systems measures the number of distinct monomials to be kept in memory while verifying a proof. We introduce a new combinatorial framework for proving space lower bounds in algebraic proof systems. As an immediate application, we obtain the space lower bounds previously provided for PC/PCR [Alekhnovich et al. 2002; Filmus et al. 2012]. More importantly, using our approach in its full potential, we prove $\Omega(n)$ space lower bounds in PC/PCR for random k-CNFs ($k \geqslant 4$) in n variables, thus solving an open problem posed in Alekhnovich et al. [2002] and Filmus et al. [2012]. Our method also applies to the Graph Pigeonhole Principle, which is a variant of the Pigeonhole Principle defined over a constant (left) degree expander graph.

Categories and Subject Descriptors: F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems—*Complexity of proof procedures*; F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic—*Mechanical theorem proving, proof theory*

General Terms: Theory

Additional Key Words and Phrases: Proof complexity, space complexity, algebraic proof systems, polynomial calculus, resolution, random formulae

ACM Reference Format:
Ilario Bonacina and Nicola Galesi. 2015. A framework for space complexity in algebraic proof systems. J. ACM 62, 3, Article 23 (June 2015), 20 pages.
DOI: http://dx.doi.org/10.1145/2699438

1. INTRODUCTION

The proof complexity research field was initiated by Cook and Reckhow [1979]. It studies the complexity of proving propositional tautologies in propositional proof systems or equivalently refuting contradictions. The historical motivation for investigating the complexity of proofs is the **P** vs. **NP** question. As observed in Cook and Reckhow [1979], one way of establishing **NP** $\neq$ **coNP** and hence **P** $\neq$ **NP** would be to prove that there are no *polynomially bounded* proof systems. A proof system S is *polynomially bounded* if it admits polynomial-size proofs for any tautology. In other words there exists a polynomial p such that for every tautology x there is a proof Γ_x in S of size at most $p(|x|)$, that is, p-bounded in the length of x. Studying bounds on the size of proofs in systems of increasing strength could be useful to understand better the **NP** $\neq$ **coNP** problem. Quoting J. Krajíček in Krajíček [2009]:

> "Proving that **NP** $\neq$ **coNP** showing incrementally that examples of proof systems are not polynomially bounded seems unlikely. Rarely a universal statement is proved by proving all its instances. Nevertheless proving these

A preliminary conference version of this work was published in Bonacina and Galesi [2013].
This work was supported by the John Templeton Foundation under the Project The Limits of Theorem Proving.
Authors' addresses: I. Bonacina and N. Galesi, Sapienza University of Rome, Computer Science Department, via Salaria 113, 00198 Roma, Italy; emails: bonacina@di.uniroma1.it; nicola.galesi@uniroma1.it.

DOI: http://dx.doi.org/10.1145/2699438

> lower bounds we may hope to uncover hidden computational hardness assumptions and then try to reduce the conjecture to some more approachable problem."

This is known as *Cook's program* in proof complexity. The most investigated proof systems include Resolution, a logical proof system introduced in Robinson [1965] and Blake [1937], and algebraic proof systems such as Polynomial Calculus (PC) and Polynomial Calculus with Resolution (PCR) introduced in Clegg et al. [1996] and Alekhnovich et al. [2002].

As remarked by A. Razborov in Razborov [2003] and Alekhnovich et al. [2002], proof complexity plays the same role in the field of feasible proofs as the one played by boolean circuits in the field of efficient computations. Hence, *proof size* in proof complexity should be viewed as *circuit-size* in circuit complexity. Following this analogy, a notion of *proof space* was introduced also for proof systems [Esteban and Torán 2001; Alekhnovich et al. 2002]. Thereafter, proof space has been investigated in depth, especially for Resolution, where space is measured in terms of number of clauses to be stored in memory [Esteban and Torán 2001; Alekhnovich et al. 2002; Ben-Sasson and Galesi 2003; Esteban et al. 2004; Nordström 2009; Ben-Sasson and Nordström 2011; Nordström and Håstad 2013; Filmus et al. 2012].

We consider the *space complexity measure*, introduced in Alekhnovich et al. [2002], that counts the number of distinct monomials to be kept simultaneously in a memory while verifying a proof in PC/PCR.

Previous work. PC and PCR are well-studied proof systems with respect to the size and the degree of proofs [Clegg et al. 1996; Buss et al. 2001, 1997; Razborov 1998; Pudlák and Sgall 1998; Ben-Sasson and Impagliazzo 2010; Impagliazzo et al. 1999; Alekhnovich and Razborov 2003; Galesi and Lauria 2010a, 2010b]. However, unlike in the case of Resolution, much less is known when we consider the space measure.

There are only two works in the literature so far which investigate space in PC/PCR. In Alekhnovich et al. [2002], the authors introduce the notion of space for PC/PCR and prove lower bounds only for families of unsatisfiable polynomials having high degree such as the *Pigeonhole Principle* (PHP^m_n) and the *Complete Tautologies* (CT_n). Improving the results in Alekhnovich et al. [2002] was an open problem in a twofold aspect: finding a lower bound technique working also for polynomials having small degree; finding lower bounds for other combinatorial principles, other than the Pigeonhole Principle. Recently Filmus et al. [2012] proved space lower bounds for families of polynomials of small initial degree. However, their result is specifically tailored to two variants of the Pigeonhole Principle ($\mathsf{Bit\text{-}PHP}^m_n$ and $\mathsf{XOR\text{-}PHP}^m_n$), and makes use of the same approach used by Alekhnovich et al. [2002].

Contributions. In this work, we introduce a new combinatorial framework to prove space lower bounds in algebraic proof systems. Under this framework, we obtain all the space lower bounds previously provided for PC/PCR. More importantly, we solve the open problem of proving space lower bounds in PC/PCR for random k-CNFs [Alekhnovich et al. 2002; Filmus et al. 2012]. Our technique works regardless of the degree of the initial polynomials. The Main Theorem (Theorem 3.5) of our contributions builds on the definition of *k-winning strategy* (Definition 3.4). 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. Our definition resembles the definition of k-dynamical satisfiability in Esteban et al. [2004] which was used to prove space lower bounds for Resolution. Likewise, the definition of k-winning strategy is analogous to the definition of winning strategies for the Duplicator

Table I. Summary of Results.

Formula	Initial Degree	Space	Reference
CT_n	$O(n)$	$n/4$	[Alekhnovich et al. 2002, this work]
PHP^m_n	$O(n)$	$n/4$	[Alekhnovich et al. 2002, this work]
$\mathsf{Bit\text{-}PHP}^m_n$	$O(\log n)$	$n/8$	[Filmus et al. 2012, this work]
$\mathsf{XOR\text{-}PHP}^m_n$	4	$n/4$	[Filmus et al. 2012, this work]
random k-CNFs in n vars, $k \geqslant 4$	k	$\Omega(n)$	this work
$\mathscr{G}$-PHP, $\mathscr{G}$ of left degree $d \geqslant 4$	d	$\Omega(n)$	this work
Tseitin formulas over a 4-regular graph of n vertices	4	$\Omega(\sqrt{n})$	[Filmus et al. 2013] (use our Main Theorem)

in the k-existential Spoiler-Duplicator game which led to prove that in Resolution *space is lower bounded by width* [Atserias and Dalmau 2008].

Our Main Theorem (Theorem 3.5) states the existence of a precise relation between k-winning strategies and refutation space in PC/PCR: if there exists a k-winning strategy for an unsatisfiable CNF φ, then the space needed to refute φ in PC/PCR is at least $k/4$. PC/PCR are defined over a field $\mathbb{F}$ but our result is independent from the characteristic of $\mathbb{F}$ and is valid over any field.

The first application of our Main Theorem is to re-obtain under a unique combinatorial framework all the space lower bounds provided in PC/PCR. All those proofs are obtained defining winning strategies with the right dimension and then applying the Main Theorem.

We exploit the potential of our combinatorial framework to solve the open problem proposed in Alekhnovich et al. [2002] and Filmus et al. [2012] of proving space lower bounds for a random k-CNF φ in n variables. The result (Theorem 5.5) follows from the Main Theorem and the construction of an $\Omega(n)$-winning strategy for φ. To this end we use a variant of the *Matching Game* used in Ben-Sasson and Galesi [2003] and Atserias [2004] to prove space lower bounds for random k-CNFs in Resolution. Our result holds for $k \geqslant 4$ and we discuss the case $k = 3$ as an open problem in Section 6.

Finally, we prove an analogous result (Theorem 5.7) for the Graph Pigeonhole Principle $\mathscr{G}$-PHP, which is a Pigeonhole Principle defined over an expander bipartite graph $\mathscr{G}$ with constant left degree. This result is obtained by means of the same technique used for random k-CNFs.

Table I summarizes our results in term of space lower bounds in PC/PCR and further recent developments.

Further Recent Developments. Our framework, as developed in a preliminary version of this work [Bonacina and Galesi 2013], was used in Filmus et al. [2013] to get new results for space in PC/PCR for the family of Tseitin contradictions. As a consequence of our Main Theorem, they prove that Tseitin contradictions over random 4-regular graphs of n vertices require space at least $\Omega(\sqrt{n})$. Similar techniques were used to solve the open problem proposed in Alekhnovich et al. [2002] of giving quadratic lower bounds for the total space of random k-CNFs in Resolution [Bonacina et al. 2014].

Organization of the Article. The rest of the paper is organized as follows. Section 2 contains preliminary definitions on algebraic proof systems, partial assignments, and graph properties. Section 3 introduces the notion of k-winning strategies (Definition 3.4). It includes the proof of our Main Theorem (Theorem 3.5) and the proof of the Locality Lemma (Lemma 3.3), which is the main technical tool needed for the Main Theorem. Section 4 as a first application of our method, contains the previously known space lower bounds for PC/PCR. Section 5 contains the proof of the lower bounds for random k-CNFs and for the Graph Pigeonhole Principle. It starts with a subsection proving the necessary results on matchings in bipartite graphs. Section 6 is dedicated to open problems and further research directions.

2. PRELIMINARY DEFINITIONS

$[n]$ denotes the set of integers $\{1, \dots, n\}$. Let X be a set of variables. A *literal* is a boolean constant, 0 or 1, or a variable $x \in X$ or the negation $\neg x$ of a variable x. A *clause* is a disjunction of literals: $C = (\ell_1 \vee \cdots \vee \ell_k)$. A formula φ is in Conjunctive Normal Form (CNF) if $\varphi = C_1 \wedge \cdots \wedge C_m$ where C_i are clauses. It is a k-CNF if each C_i contains at most k literals.

Given a field $\mathbb{F}$, $\mathbb{F}[X]$ is the ring of polynomials in the variables X with coefficients in $\mathbb{F}$. We use the following standard encoding, tr, of CNF formulas over X into a set of polynomials in $\mathbb{F}[X]$,

$$tr(x) = (1 - x), \qquad tr(\neg x) = x, \qquad tr\left(\bigvee_{i=1}^{n} \ell_i\right) = \prod_{i=1}^{n} tr(\ell_i).$$

Hence, for a CNF φ, $tr(\varphi) = \{tr(C) \ : \ C \in \varphi\} \cup \{x^2 - x \ : \ x \in X\}$. Observe that $tr(\varphi)$ may lead to an exponential number of monomials with respect to the number of clauses in φ. To avoid such effect, following Alekhnovich et al. [2002], we consider the ring $\mathbb{F}[X, \overline{X}]$, where $\overline{X} = \{\bar{x} \ : \ x \in X\}$ is a set of new formal variables and the intended meaning of $\bar{x}$ is $\neg x$. Over $\mathbb{F}[X, \overline{X}]$, we can define a more efficient encoding in terms of number of monomials: $\overline{tr}(\varphi) = \{\overline{tr}(C) \ : \ C \in \varphi\} \cup \{x^2 - x, x + \bar{x} - 1 \ : \ x \in X\}$, where

$$\overline{tr}(x) = \bar{x}, \qquad \overline{tr}(\neg x) = x, \qquad \overline{tr}\left(\bigvee_{i=1}^{n} \ell_i\right) = \prod_{i=1}^{n} \overline{tr}(\ell_i).$$

A set of polynomials P in $\mathbb{F}[X]$ (respectively, in $\mathbb{F}[X, \overline{X}]$) is *contradictory* if and only if $1 \in \mathbf{ideal}(P)$, that is the ideal generated by P is not a *proper* ideal in $\mathbb{F}[X]$ (respectively, in $\mathbb{F}[X, \overline{X}]$). Notice that a CNF φ is unsatisfiable if and only if $tr(\varphi)$ and $\overline{tr}(\varphi)$ are contradictory sets of polynomials.

2.1. Partial Assignments

A *partial assignment over* X is a map $\alpha : X \longrightarrow \{0, 1, \star\}$, where X is a set of variables. The *domain* of α is $\mathrm{dom}(\alpha) = \alpha^{-1}(\{0, 1\})$ and we say that α is *assigning* a value to x if and only if $x \in \mathrm{dom}(\alpha)$. Λ denotes the partial assignment with the empty domain.

Given a partial assignment α and a CNF φ, we can apply α to φ obtaining a new formula $\alpha(\varphi)$ in this way: substitute each variable x in φ with the value $\alpha(x)$ if $x \in \mathrm{dom}(\alpha)$, or otherwise leave x untouched. Then simplify the result with the usual rules: $0 \vee A \equiv A$, $1 \vee A \equiv 1$, $0 \wedge A \equiv 0$, $1 \wedge A \equiv A$. We say that α *satisfies* φ and we write $\alpha \vDash \varphi$, if $\alpha(\varphi) = 1$. Similarly, for a family F of partial assignments, we write $F \vDash \varphi$ if for each $\alpha \in F$, $\alpha \vDash \varphi$.

For each partial assignment α over $X \cup \overline{X}$, we assume that it is respecting the intended meaning of the variables, that is $\alpha(\bar{x}) = 1 - \alpha(x)$ for each $x, \bar{x} \in \mathrm{dom}(\alpha)$. In particular, it is always possible to extend to $X \cup \overline{X}$ an assignment β over X respecting the previous property. Given a polynomial p in $\mathbb{F}[X, \overline{X}]$ and an assignment α we define $\alpha(p)$ the application of α to p as follows: substitute each variable x in p with the value $\alpha(x)$ if $x \in \mathrm{dom}(\alpha)$ and each variable $\bar{x}$ with $\alpha(\bar{x})$, or otherwise leave the variable untouched. Then simplify the result with the rules: $0 \cdot m \equiv 0$, $1 \cdot m \equiv m$ and $m - m \equiv 0$ where m is a monomial in p.

Definition 2.1 ($\vDash_I$). Let p be a polynomial in $\mathbb{F}[X, \overline{X}]$, I an ideal in $\mathbb{F}[X, \overline{X}]$ and α a partial assignment over $X \cup \overline{X}$. The notation $\alpha \vDash_I p$ means that $\alpha(p) \in I$.

If F is a family of partial assignments and P a set of polynomials, we write $F \vDash_I P$ if $\alpha \vDash_I p$ for each $\alpha \in F$ and $p \in P$. We say that F is *I-consistent* if $F \vDash_I I$, that is for every $p \in I$ and $\alpha \in F$, $\alpha(p) \in I$.

Notice that if φ is a CNF and α is a partial assignment satisfying φ, then $\alpha(\overline{tr}(\varphi)) = 0$ and in particular $\alpha \vDash_I \overline{tr}(\varphi)$ for any ideal I. Moreover, given a set of partial assignments F, a set of polynomials P and an ideal I, if $F \vDash_I P$ then $F \vDash_I \mathbf{ideal}(P)$.

Two partial assignments are *disjoint* if they have disjoint domains. Given two disjoint partial assignments α and β, their *union* $\alpha \cup \beta$ is the partial assignment

$$\alpha \cup \beta(x) = \begin{cases} \alpha(x) & \text{if } x \in \text{dom}(\alpha), \\ \beta(x) & \text{if } x \in \text{dom}(\beta), \\ \star & \text{otherwise.} \end{cases}$$

Given a partial assignment α over X and $Y \subseteq X$, the *restriction* $\alpha\restriction_Y$ is the partial assignment

$$\alpha \restriction_Y (x) = \begin{cases} \alpha(x) & \text{if } x \in Y, \\ \star & \text{otherwise.} \end{cases}$$

β *extends* α ($\alpha \subseteq \beta$) if $\beta \restriction_{\text{dom}(\alpha)} = \alpha$. Given a family F of partial assignments over X and given $Y \subseteq X$, we define $F \restriction_Y = \{\alpha \restriction_Y \, : \, \alpha \in F\}$. Given two sets F and F' of partial assignments, $F' \subseteq F$ if each assignment in F' is also in F.

2.2. Algebraic Proof Systems and Monomial Space

Polynomial Calculus (PC) is an algebraic proof system defined in Clegg et al. [1996] and working on polynomials in $\mathbb{F}[X]$. Starting from a set of initial contradictory polynomials P in $\mathbb{F}[X]$, PC allows to derive the polynomial 1 using the following inference rules: for any $p, q \in \mathbb{F}[X]$

$$\frac{p \qquad q}{\alpha p + \beta q} \; \forall \alpha, \beta \in \mathbb{F}, \qquad\qquad \frac{p}{xp} \forall x \in X.$$

To force 0/1 solutions, we always include the *Boolean axioms* $\{x^2 - x\}_{x \in X}$ among the initial polynomials, as in the case of the polynomial encoding of CNFs.

Polynomial Calculus with Resolution (PCR) is an algebraic proof system defined in Alekhnovich et al. [2002] for polynomials in $\mathbb{F}[X, \overline{X}]$, allowing a compact representation of CNFs. Starting from a set of initial contradictory polynomials P in $\mathbb{F}[X, \overline{X}]$, PCR allows to derive the polynomial 1 using the same inference rules and axioms of PC over $\mathbb{F}[X, \overline{X}]$ and the further *Boolean axioms* $\{x + \overline{x} - 1\}_{x \in X}$ to respect the intended meaning of the variables.

With $P \vdash q$ we denote a *derivation* of q from P, which is a sequence of polynomials $(p_0, \ldots, p_\ell)$ such that $p_\ell = q$ and each p_i is either an initial polynomial (either in P or a Boolean axiom) or it is inferred by previous polynomials in the sequence by one of the inference rules. We call *refutation* a derivation of the polynomial 1.

PC and PCR are *correct* and *complete* proof systems: correctness come from the fact that if $P \vdash g$ then $g \in \mathbf{ideal}(P)$ and obviously g vanish on the variety $V(P)$, that is the set of zeroes of P. Completeness comes as a corollary of Hilbert's Nullstellensatz [Cox et al. 1997] or by Gröebner bases algorithm [Clegg et al. 1996]. We do not require $\mathbb{F}$ to be algebraically closed due to the fact that we always consider set of polynomials that include the boolean axioms.

In order to study space of proofs we rephrase the definition of derivation in PC/PCR following the model proposed in Alekhnovich et al. [2002]. 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.

Definition 2.2 (PC/PCR *Derivation*). Given a set of initial polynomials P, a PC/PCR *derivation of a polynomial q from P* ($P \vdash_{\mathsf{PC}} q$, respectively, $P \vdash_{\mathsf{PCR}} q$) is a sequence $(\mathfrak{M}_0, \ldots, \mathfrak{M}_\ell)$ of sets of polynomials, called *memory configurations*, such that: $\mathfrak{M}_0 = \emptyset$, $q \in \mathfrak{M}_\ell$ and for all $i \leqslant \ell$, $\mathfrak{M}_i$ is obtained by $\mathfrak{M}_{i-1}$ by applying one of the following rules.

Axiom Download. $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{p\}$, where $p \in P$.
Inference Adding. $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{p\}$, where p is some polynomial inferred from polynomials occurring in $\mathfrak{M}_{i-1}$ using the inference rules of PC/PCR.
Erasure. $\mathfrak{M}_i \subseteq \mathfrak{M}_{i-1}$.

Let I be an ideal, a *semantical* PCR *derivation of q from P with respect to I* ($P \vdash_I q$) is a sequence of memory configurations $(\mathfrak{M}_0, \ldots, \mathfrak{M}_\ell)$ such that: $\mathfrak{M}_0 = \emptyset$, $q \in \mathfrak{M}_\ell$ and for all $i \leqslant \ell$, $\mathfrak{M}_i$ is obtained by $\mathfrak{M}_{i-1}$ by the following rule.

Semantical Inference with respect to I. $\mathfrak{M}_i \subseteq \mathbf{ideal}(\mathfrak{M}_{i-1} \cup \{p\}) + I$, for some $p \in P$, where $\mathbf{ideal}(\mathfrak{M}_{i-1} \cup \{p\}) + I$ is just the (standard) sum among ideals.

Semantical PCR *derivations with respect to I* are a generalization of *semantical* PCR *derivations* as defined in [Alekhnovich et al. 2002]. A *semantical* PCR *derivation* correspond to setting $I = \{0\}$ in our previous definition.

Definition 2.3 (*Monomial Space*). The *(monomial) space* $\mathrm{MSpace}(S)$ of a set of polynomials S is the number of distinct monomials occurring in S. The (monomial) space $\mathrm{MSpace}(\Gamma)$ of a semantical PCR refutation Γ is the maximal (monomial) space of a memory configuration in Γ. We denote by

$$\mathrm{MSpace}(P \vdash_I 1)$$

the minimal $\mathrm{MSpace}(\Gamma)$ over all semantical PCR refutations Γ of P. Analogously we can define $\mathrm{MSpace}(P \vdash_{\mathsf{PC}} 1)$ and $\mathrm{MSpace}(P \vdash_{\mathsf{PCR}} 1)$. For a CNF formula φ the notation $\mathrm{MSpace}(\varphi \vdash_I \bot)$ refers implicitly to $\mathrm{MSpace}(\overline{tr}(\varphi) \vdash_I 1)$.

Notice that $\mathrm{MSpace}(P \vdash_{\mathsf{PC}} 1) \geqslant \mathrm{MSpace}(P \vdash_{\mathsf{PCR}} 1) \geqslant \mathrm{MSpace}(P \vdash_I 1)$ for any ideal I, hence the lower bounds we give for $\mathrm{MSpace}(P \vdash_I 1)$ hold also for $\mathrm{MSpace}(P \vdash_{\mathsf{PC}} 1)$ and $\mathrm{MSpace}(P \vdash_{\mathsf{PCR}} 1)$. Moreover, given two ideals I, J, if $I \subseteq J$, then $\mathrm{MSpace}(P \vdash_I 1) \geqslant \mathrm{MSpace}(P \vdash_J 1)$.

2.3. Matchings and Expansion

Let $\mathscr{G} = (U \cup V, E)$ be a bipartite graph and let $k \geqslant 1$ be an integer. Let $A \subseteq U$, we say that $\pi \subseteq E$ is a *k-matching of A in V* if the vertices in A are mapped by π into pairwise disjoint subsets of V of size k. More precisely, for each $u \in U$ let $\pi(u) = \{v \in V \ : \ (u, v) \in \pi\}$. Then

(1) for each $u \in A$, $\pi(u)$ is nonempty;
(2) for each u and u', if $u \neq u'$ then $\pi(u)$ and $\pi(u')$ are disjoint sets;
(3) for each $u \in A$, $|\pi(u)| = k$.

Given $A \subseteq U$, let $\pi(A) = \bigcup_{u \in A} \pi(u)$.

Let $N_{\mathscr{G}}(A)$ be the set of neighborhoods of A in the graph $\mathscr{G}$. We use the following application of Hall's Theorem.

LEMMA 2.4 [ALEKHNOVICH ET AL. 2002]. *Let $\mathscr{G} = (U \cup V, E)$ be a bipartite graph. If for every set $A \subseteq U$, $|N_{\mathscr{G}}(A)| \geqslant 2|A|$, then there exists a 2-matching of U in V.*

This lemma immediately implies that if $A \subseteq U$ is the smallest set not having a 2-matching in $\mathscr{G}$, then $|N_{\mathscr{G}}(A)| < 2|A|$.

Definition 2.5 (*(s, δ)-expansion*). Let $\mathscr{G} = (U \cup V, E)$ a bipartite graph, $\mathscr{G}$ is an *(s, δ)-expander* if

$$\forall A \subseteq U,\ |A| \leqslant s \to |N_{\mathscr{G}}(A)| \geqslant \delta|A|.$$

Notice that, from the previous lemma, for any $\epsilon > 0$ if $\mathscr{G} = (U \cup V, E)$ is a $(s, 2+\epsilon)$-expander then every subset of U of size at most s has a 2-matching.

3. MAIN THEOREM

Throughout this section, we let X be a set of variables, $\mathbb{F}$ a field and I an ideal in $\mathbb{F}[X, \overline{X}]$. We consider partial assignments over $X \cup \overline{X}$ respecting the intended meaning of the variables $\overline{X}$.

Let F be a family of partial assignments, $\mathrm{dom}(F)$ is the union of the domains of the assignments in F. We say that a set of partial assignments F is *flippable* if and only if, for all $x \in \mathrm{dom}(F)$, there exist $\alpha, \beta \in F$ such that $\alpha(x) = 1 - \beta(x)$. Two families of partial assignments F and F' are *domain-disjoint* if $\mathrm{dom}(F) \cap \mathrm{dom}(F') = \emptyset$.

Given $H_1, \ldots, H_t$ nonempty pairwise domain-disjoint sets of assignments,[1] 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 $t = 0$, $\mathcal{H} = \{\Lambda\}$. $\mathrm{dom}(\mathcal{H}) = \bigcup_i \mathrm{dom}(H_i)$ and we call the H_is the *factors* of $\mathcal{H}$. Notice that $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$ defines implicitly the partition of $\mathrm{dom}(\mathcal{H})$ given by $\{\mathrm{dom}(H_1), \ldots, \mathrm{dom}(H_t)\}$.[2] Given a product family $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$, there could be many ways of factorizing it, when we write $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$ it means that we fixed its representation as a product. Hence, two product-families with the same set of assignments but with different factorization are different objects.

For a product-family $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$, the *rank* of $\mathcal{H}$, $\|\mathcal{H}\|$ is the number of factors of $\mathcal{H}$ different from $\{\Lambda\}$. We do not count $\{\Lambda\}$ in the rank since $\mathcal{H} \otimes \{\Lambda\} = \mathcal{H}$. 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 $\mathcal{H}$.

Definition 3.1 (*2-Merge*). 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, $Z_J \subseteq \bigotimes_{j \in J} H_j$ and $\mathcal{Z} \restriction_{\mathrm{dom}(H_j)} = H_j$ for all $j \in [t]$. Notice that, if $\mathcal{H}$ is flippable, then $\mathcal{Z}$ is also flippable.

Consider the following example that will be central in the proof of the *Locality Lemma* (Lemma 3.3).

Example 3.2. Let m be a monomial and $\mathcal{H} = H_1 \otimes H_2$ be a flippable product-family such that $\mathrm{var}(m) \cap \mathrm{dom}(H_i) \neq \emptyset$ for $i = 1, 2$. Let $O_{m,i} = \{\alpha \in H_i \ :\ \alpha(m) = 0\}$. We have that

$$\mathcal{Z} = Z_{\{1,2\}} = (O_{m,1} \otimes H_2) \cup (H_1 \otimes O_{m,2})$$

is a 2-merge on $\mathcal{H}$. $\mathcal{Z}$ is a product-family since it has only one factor.

[1] As said in Section 2.1, we always suppose that the partial assignments are respecting the intended meaning of the variables in $\overline{X}$, that is if $x \in \mathrm{dom}(\alpha)$ then $\alpha(\bar{x}) = 1 - \alpha(x)$, hence, a variable x is in $\mathrm{dom}(H_i)$ if and only if $\bar{x}$ is in $\mathrm{dom}(H_i)$.

[2] These partitions were called *pseudopartitions* in the preliminary version of this article [Bonacina and Galesi 2013].

As in Alekhnovich et al. [2002], a key property in our space lower bound proof is a Locality Lemma. Informally it asserts that if a set S of polynomials is satisfiable by a 2-merge on a product family $\mathcal{H}$, then it is possible to build a new 2-merge $\mathcal{Z}'$ on a new product-family $\mathcal{H}'$ such that $\mathcal{Z}'$ still satisfies S and $\mathcal{H}' \sqsubseteq \mathcal{H}$ has rank bounded by the monomial space of S.

Lemma 3.3 (Locality Lemma). *Let I be a proper ideal in $\mathbb{F}[X, \overline{X}]$, S a set of polynomials in $\mathbb{F}[X, \overline{X}]$, $\mathcal{H}$ a flippable product-family and $\mathcal{Z}$ a 2-merge on $\mathcal{H}$ such that $\mathcal{Z} \vDash_I S$. Then there exist a flippable product-family $\mathcal{H}' \sqsubseteq \mathcal{H}$ and $\mathcal{Z}'$ a 2-merge on $\mathcal{H}'$ such that: $\mathcal{Z}' \vDash_I S$ and $\|\mathcal{H}'\| \leqslant 4 \cdot \mathrm{MSpace}(S)$.*

Proof. Let $\mathcal{H} = H_1 \otimes \cdots \otimes H_t$ and $\mathcal{Z} = Z_{J_1} \otimes \cdots \otimes Z_{J_r}$. Let $\mathscr{G} = (U \cup V, E)$ be the following bipartite graph: U is the set of all distinct monomials in S, $V = \{J_1, \ldots, J_r\}$ and $(m, J_i) \in E$ if and only if a variable of m appears in $\mathrm{dom}(Z_{J_i})$. For a set $M \subseteq U$, let $N_{\mathscr{G}}(M)$ be the set of the neighbors of M in $\mathscr{G}$ and let $\mathcal{H}_M$ and $\mathcal{Z}_M$ be the following two product-families:

$$\mathcal{Z}_M = \bigotimes_{J_i \in N_{\mathscr{G}}(M)} Z_{J_i}, \qquad \mathcal{H}_M = \bigotimes_{J_i \in N_{\mathscr{G}}(M)} \bigotimes_{j \in J_i} H_j.$$

Let M be a set of maximal size in U such that $|N_{\mathscr{G}}(M)| \leqslant 2|M|$. Let $M^c = U \setminus M$. By maximality of M, for each $A \subseteq M^c$, $|N_{\mathscr{G}}(A) \setminus N_{\mathscr{G}}(M)| \geqslant 2|A|$. Hence, by Lemma 2.4, M^c admits a 2-matching π into $V \setminus N_{\mathscr{G}}(M)$.

For each monomial m in M^c let $\pi(m) = \{L_m, K_m\}$, where $L_m, K_m \in \{J_1, \ldots, J_r\}$. By definition of $\mathscr{G}$, there is a variable x of m in $\mathrm{dom}(Z_{L_m})$. Let $\ell_m \in L_m$ such that x in $\mathrm{dom}(H_{\ell_m})$ (if there are more than one possible ℓ_m, we choose one). Let $k_m \in K_m$, obtained analogously.

Define the product-family $\mathcal{H}'$ as

$$\mathcal{H}' = \mathcal{H}_M \otimes \bigotimes_{m \in M^c} H_{\ell_m} \otimes H_{k_m}.$$

We have that clearly $\mathcal{H}' \sqsubseteq \mathcal{H}$ and hence it is a flippable product-family. The rank of $\mathcal{H}'$ is $\|\mathcal{H}'\| = \|\mathcal{H}_M\| + 2|M^c|$. Since $|N_{\mathscr{G}}(M)| \leqslant 2|M|$, and since the J_i's are of size at most 2, we have that $\|\mathcal{H}_M\| \leqslant 4|M|$. Hence, putting it all together, $\|\mathcal{H}'\| \leqslant 4|U| = 4 \cdot \mathrm{MSpace}(S)$.

The construction of $\mathcal{Z}'$ goes as follows. Let $O_{m,i} = \{\alpha \in H_i \ : \ \alpha(m) = 0\}$. Observe that if a variable x of m is in $\mathrm{dom}(H_i)$ then $O_{m,i}$ is nonempty since H_i is flippable and hence there is always an assignment in H_i setting x to satisfy m. As in Example 3.2, let

$$Z_{\{\ell_m, k_m\}} = (O_{m,\ell_m} \otimes H_{k_m}) \cup (H_{\ell_m} \otimes O_{m,k_m}).$$

Let $\mathcal{Z}'$ be

$$\mathcal{Z}' = \mathcal{Z}_M \otimes \bigotimes_{m \in M^c} Z_{\{\ell_m, k_m\}}.$$

It is straightforward to see that $\mathcal{Z}'$ is a 2-merge on $\mathcal{H}'$, hence is remaining to prove only that $\mathcal{Z}' \vDash_I S$. Consider the following claim.

Claim 1. $\mathcal{Z}' \subseteq \mathcal{Z} \restriction_{\mathrm{dom}(\mathcal{H}')}$.

Proof. By construction, $\mathcal{Z}_M = \mathcal{Z} \restriction_{\mathrm{dom}(\mathcal{H}_M)}$, hence we have to prove that for each $m \in M^c$,

$$\mathcal{Z}' \restriction_{\mathrm{dom}(H_{\ell_m}) \cup \mathrm{dom}(H_{k_m})} \subseteq \mathcal{Z} \restriction_{\mathrm{dom}(H_{\ell_m}) \cup \mathrm{dom}(H_{k_m})} .$$

This follows immediately from the following chain of inequalities

$$\mathcal{Z}' \restriction_{\mathrm{dom}(H_{\ell_m}) \cup \mathrm{dom}(H_{k_m})} \overset{(\star)}{=} Z_{\{\ell_m, k_m\}} \overset{(\dagger)}{\subseteq} H_{\ell_m} \otimes H_{k_m} \overset{(\star\star)}{=} \mathcal{Z} \restriction_{\mathrm{dom}(H_{\ell_m}) \cup \mathrm{dom}(H_{k_m})} .$$

The equality ($\star$) is by definition and the containment ($\dagger$) follows by construction. The equality ($\star\star$) follow since, by definition of $\mathcal{Z}$, $\mathcal{Z}\restriction_{\mathrm{dom}(H_j)} = H_j$ and L_m and K_m are disjoint sets. □

To prove that $\mathcal{Z}' \vDash_I S$, let $\alpha \in \mathcal{Z}'$. As $\mathcal{Z}' \subseteq \mathcal{Z} \restriction \mathrm{dom}(\mathcal{H}')$, there exists $\beta \in \mathcal{Z}$ extending α by setting variables not appearing in any $m \in M$. Hence, by construction, if $m \in M^c$, then $0 = \alpha(m) = \beta(m)$ and if $m \in M$ then $\alpha(m) = \beta(m)$. Then, α and β give the same value to the monomials in S and, by hypothesis, $\beta \vDash_I S$, hence $\alpha \vDash_I S$. □

The next definition is at the core of the proof of the Main Theorem (Theorem 3.5). A family of flippable product-families is called a *strategy* and denoted by $\mathscr{L}$.

Definition 3.4 (*k-Winning Strategy*). Let P be a set of polynomials in $\mathbb{F}[X, \overline{X}]$ and I a proper ideal in $\mathbb{F}[X, \overline{X}]$. A nonempty strategy $\mathscr{L}$ is *k-winning for P with respect to I* if and only if for every $\mathcal{H} \in \mathscr{L}$ the following conditions hold:

(1) $\mathcal{H}$ is I-consistent (*consistency property*);
(2) for each $\mathcal{H}' \sqsubseteq \mathcal{H}$, $\mathcal{H}' \in \mathscr{L}$ (*restriction property*);
(3) if $\|\mathcal{H}\| < k$, then, for each $p \in P$, there exists a I-consistent flippable product-family $\mathcal{H}_p$, domain-disjoint from $\mathcal{H}$, such that $\mathcal{H} \otimes \mathcal{H}_p \in \mathscr{L}$ and $\mathcal{H} \otimes \mathcal{H}_p \vDash_I p$ (*extension property*).

Notice that, by the restriction property, $\{\Lambda\}$ is in any k-winning strategy.

Theorem 3.5 (Main Theorem). *Let P be a contradictory set of polynomials in $\mathbb{F}[X, \overline{X}]$, I a proper ideal in $\mathbb{F}[X, \overline{X}]$, and $k \geqslant 1$ an integer. Suppose that there exists a nonempty k-winning strategy $\mathscr{L}$ for P with respect to I. Then* $\mathrm{MSpace}(P \vdash_I 1) \geqslant k/4$.

Proof. Let $\Gamma = (\mathfrak{M}_0, \ldots, \mathfrak{M}_s)$ be a semantical PCR refutation of P with respect to I. Assume by contradiction that $\mathrm{MSpace}(\Gamma) < k/4$. By induction on $i = 0, \ldots, s$, we show the following inductive property:

$$\text{there exist a nonempty product-family } \mathcal{H}_i \in \mathscr{L} \text{ and a nonempty } \mathcal{Z}_i \text{ 2-merge on } \mathcal{H}_i \text{ such that } \mathcal{Z}_i \vDash_I \mathbf{ideal}(\mathfrak{M}_i) + I. \tag{1}$$

Before proving the statement, we show how the inductive property implies a contradiction. In the last step, then there exists some assignment $\alpha \in \mathcal{Z}_s$ such that for every polynomial $p \in \mathbf{ideal}(\mathfrak{M}_s) + I$, $\alpha(p) \in I$. However, $1 \in \mathfrak{M}_s$, hence $1 = \alpha(1) \in I$, which instead is a proper ideal.

Initially set $\mathcal{H}_0 = \{\Lambda\} \in \mathscr{L}$ and $\mathcal{Z}_0 = \mathcal{H}_0$. Then $\mathcal{H}_0$ is trivially I-consistent, hence trivially $\mathcal{Z}_0 \vDash_I \mathbf{ideal}(\mathfrak{M}_0) + I = I$.

Let $\mathfrak{M}_{i+1} = \mathbf{ideal}(\mathfrak{M}_i \cup \{p\}) + I$ with $p \in P$. If $\mathcal{Z}_i \vDash_I p$, we have nothing to do: set $\mathcal{H}_{i+1} = \mathcal{H}_i \in \mathscr{L}$ and $\mathcal{Z}_{i+1} = \mathcal{Z}_i$. Otherwise, suppose that $\mathcal{Z}_i \nvDash_I p$. By the Locality Lemma, used with parameters $\mathcal{H} = \mathcal{H}_i$, $\mathcal{Z} = \mathcal{Z}_i$ and $S = \mathfrak{M}_i$, we find $\mathcal{H}' \sqsubseteq \mathcal{H}_i$ and a nonempty $\mathcal{Z}'$ 2-merge on $\mathcal{H}'$ such that $\mathcal{Z}' \vDash_I \mathfrak{M}_i$ and $\|\mathcal{H}'\| \leqslant 4\,\mathrm{MSpace}(\mathfrak{M}_i)$. Observe that, as $\mathscr{L}$ is a k-winning strategy, then by the *restriction property*, $\mathcal{H}' \in \mathscr{L}$, since $\mathcal{H}' \sqsubseteq \mathcal{H}_i$ and $\mathcal{H}_i \in \mathscr{L}$. By the *I-consistency property* of $\mathscr{L}$, $\mathcal{H}'$ is I-consistent and then $\mathcal{Z}'$ is I-consistent, hence $\mathcal{Z}' \vDash_I \mathbf{ideal}(\mathfrak{M}_i) + I$.

Since, by hypothesis, $\mathrm{MSpace}(\mathfrak{M}_i) < k/4$, then $\|\mathcal{H}'\| < k$ and, by the *extension property* applied to $\mathcal{H}'$ and p, there is an I-consistent flippable product-family $\mathcal{H}_p$, domain-disjoint from $\mathcal{H}'$, such that $\mathcal{H}_{i+1} = \mathcal{H}' \otimes \mathcal{H}_p \vDash_I p$ and $\mathcal{H}_{i+1} \in \mathscr{L}$. Set $\mathcal{Z}_{i+1} = \mathcal{Z}' \otimes \mathcal{H}_p$. It remains to show that $\mathcal{Z}_{i+1}$ is a 2-merge on $\mathcal{H}_{i+1}$ and $\mathcal{Z}_{i+1} \vDash_I \mathbf{ideal}(\mathfrak{M}_{i+1}) + I$.

The first property follows by the definition of $\mathcal{Z}_{i+1}$ and of $\mathcal{H}_{i+1}$, since $\mathcal{Z}'$ is a 2-merge on $\mathcal{H}'$. The second property, that is $\mathcal{Z}_{i+1} \vDash_I \mathbf{ideal}(\mathfrak{M}_{i+1}) + I$, follows because:

(1) $\mathcal{Z}_{i+1} \vDash_I \mathbf{ideal}(\mathfrak{M}_i) + I$, since $\mathcal{Z}' \vDash_I \mathbf{ideal}(\mathfrak{M}_i) + I$ and $\mathcal{H}_p$ is I-consistent, and (2) $\mathcal{Z}_{i+1} \vDash_I p$, since $\mathcal{H}_{i+1} = \mathcal{H}_i \otimes \mathcal{H}_p \vDash_I p$ and $\mathcal{Z}_{i+1} \subseteq \mathcal{H}_{i+1}$ as $\mathcal{Z}_{i+1}$ is a 2-merge on $\mathcal{H}_{i+1}$. □

In the Main Theorem, we do not make any assumption on the structure of the set of initial polynomials P. If we have some assumptions on P, it is possible to have an analogous result requiring k-winning strategies just for a subset of P. This in particular can be useful when in P we have some monomials of high initial degree.

THEOREM 3.6. *Let $P = P_1 \cup P_2$ a contradictory set of polynomials in the variables $X \cup \overline{X}$ and let I be the trivial ideal $I = \{0\}$. Suppose that:*

(1) *there exists a nonempty k-winning strategy $\mathscr{L}$ for P_1 with respect to the ideal I; and*
(2) *every polynomial in P_2 is a monomial such that for each $m \in P_2$ and for each $\mathcal{H} \in \mathscr{L}$ with $\|\mathcal{H}\| < k$, then either there exists a variable in m not in* $\mathrm{dom}(\mathcal{H})$ *or $\mathcal{H} \vDash_I m$.*

Then, $\mathrm{MSpace}(P \vdash_I 1) > k/4$.

PROOF. The proof is essentially the same as in the Main Theorem (Theorem 3.5). We use the same notation. Assume by contradiction that $\mathrm{MSpace}(\Gamma) \leqslant k/4$. We have to prove the induction property (property (1) in the proof of Theorem 3.5) only when we download a monomial from P_2, since in the other cases the proof is the same as in Theorem 3.5. Let $\mathfrak{M}_{i+1} = \mathfrak{M}_i \cup \{m\}$, with $m \in P_2$. Then, $\mathrm{MSpace}(\mathfrak{M}_i) \leqslant k/4 - 1$. By the Locality Lemma, used with parameters $\mathcal{H} = \mathcal{H}_i$, $\mathcal{Z} = \mathcal{Z}_i$ and $S = \mathfrak{M}_i$, we find a $\mathcal{H}' \in \mathscr{L}$, a nonempty $\mathcal{Z}'$ 2-merge of $\mathcal{H}'$ such that $\mathcal{Z}' \vDash_I \mathfrak{M}_i$ and

$$\|\mathcal{H}'\| \leqslant 4\,\mathrm{MSpace}(\mathfrak{M}_i) \leqslant 4(k/4 - 1) \leqslant k - 4.$$

By hypothesis (2), either $\mathcal{H}' \vDash_I m$ or there exists a variable $x \in \mathrm{var}(m) \setminus \mathrm{dom}(\mathcal{H}')$. In the first case, just set $\mathcal{H}_{i+1} = \mathcal{H}'$ and $\mathcal{Z}_{i+1} = \mathcal{Z}'$. Since $\mathscr{L}$ is a k-winning strategy by the *extension property* applied on $\mathcal{H}'$ and $x^2 - x$, there exists a product-family $\mathcal{H}_{x^2-x}$ domain-disjoint from $\mathcal{H}'$ such that $\mathcal{H}' \otimes \mathcal{H}_{x^2-x} \in \mathscr{L}$ and $\mathcal{H}' \otimes \mathcal{H}_{x^2-x} \vDash_I x^2 - x$. Since $x \notin \mathrm{dom}(\mathcal{H}')$, then $x, \overline{x} \in \mathrm{dom}(\mathcal{H}_x)$ and using closure of $\mathscr{L}$ under $\sqsubseteq$, we can assume that $\mathcal{H}_{x^2-x}$ is just one factor containing x in its domain. Hence, $\|\mathcal{H}' \otimes \mathcal{H}_{x^2-x}\| < k$ and then either $\mathcal{H}' \otimes \mathcal{H}_{x^2-x} \vDash_I m$ or there is a variable $y \in \mathrm{var}(m)$ but not in $\mathrm{dom}(\mathcal{H}' \otimes \mathcal{H}_{x^2-x})$. In the first case, set $\mathcal{H}_{i+1} = \mathcal{H}' \otimes \mathcal{H}_{x^2-x}$ and $\mathcal{Z}_{i+1} = \mathcal{Z}' \otimes \mathcal{H}_{x^2-x}$. In the second case, by the *extension property* of $\mathscr{L}$ applied to $\mathcal{H}' \otimes \mathcal{H}_{x^2-x}$ and $y^2 - y$, we get a product-family $\mathcal{H}_{y^2-y}$ domain-disjoint from $\mathcal{H}' \otimes \mathcal{H}_{x^2-x}$ such that $\mathcal{H}' \otimes \mathcal{H}_{x^2-x} \otimes \mathcal{H}_{y^2-y} \in \mathscr{L}$ and $\mathcal{H}' \otimes \mathcal{H}_{x^2-x} \otimes \mathcal{H}_{y^2-y} \vDash_I y^2 - y$. Exactly as shown previously, for $x, \bar{x}$, we have that $y, \bar{y} \in \mathrm{dom}(\mathcal{H}_{y^2-y})$. Set $\mathcal{H}_{i+1} = \mathcal{H}' \otimes \mathcal{H}_{x^2-x} \otimes \mathcal{H}_{y^2-y}$ and $\mathcal{Z}_{i+1} = \mathcal{Z}' \otimes \{\alpha \in H_{x^2-x} \otimes H_{y^2-y} : \alpha \vDash_I m\}$. $\mathcal{Z}_{i+1} \vDash_I \mathfrak{M}_{i+1}$ and $\mathcal{Z}_{i+1}$ is a 2-merge on $\mathcal{H}_{i+1}$. □

4. FROM THE MAIN THEOREM TO KNOWN SPACE LOWER BOUNDS

In this section, we re-prove the known space lower bounds [Alekhnovich et al. 2002; Filmus et al. 2012] for PCR as a consequence of the Main Theorem (Theorem 3.5) and Theorem 3.6.

Complete Tree Tautologies. Let n be a natural number, the axioms of CT_n are all the possible n-clauses in the variables $X = \{x_1, \ldots, x_n\}$ plus the Boolean axioms.

THEOREM 4.1 [ALEKHNOVICH ET AL. 2002]. *Let I be the trivial ideal $I = \{0\}$, then* $\mathrm{MSpace}(\mathsf{CT}_n \vdash_I \bot) > n/4$.

PROOF. We use Theorem 3.6. Choose as P_1 the Boolean axioms, as P_2 the other axioms of CT_n.

Given $i \in [n]$, let H_i be the following set of partial assignments of domain $\{x_i, \bar{x}_i\}$

$$H_i = \{\{x_i \mapsto 0, \bar{x}_i \mapsto 1\},\ \ \{x_i \mapsto 1, \bar{x}_i \mapsto 0\}\}.$$

By construction H_i is flippable and I-consistent.

The strategy $\mathscr{L}$ is defined as follows: $\mathcal{H} \in \mathscr{L}$ if and only if there exists $A \subseteq [n]$ such that

$$\mathcal{H} = \bigotimes_{i \in A} H_i.$$

We prove that $\mathscr{L}$ is a n-winning strategy for P_1 with respect to the ideal I. $\mathscr{L}$ is nonempty as for $A = \emptyset$ the definition implies that $\{\Lambda\} \in \mathscr{L}$. By construction, $\mathcal{H} \in \mathscr{L}$ imply that $\mathcal{H}$ is I-consistent. The *restriction* and *extension* properties are clear.

Moreover, each $\mathcal{H} \in \mathscr{L}$ with rank $< n$ leaves a variable unassigned in every monomial in P_2. □

The Pigeonhole Principle. Let $m, n \in \mathbb{N}$ be two integers such that $m > n$ and $X = \{x_{ij} : i \in [m], j \in [n]\}$ be a set of variables. The intended meaning of x_{ij} is the truth value of "the pigeon i goes into the hole j". The standard encoding of the Pigeonhole Principle PHP^m_n is the conjunction of the following clauses:

(1) $\neg x_{ij} \vee \neg x_{i'j}$ for all $i \neq i' \in [m]$ and for all $j \in [n]$ (*injectivity axioms*);
(2) $x_{i1} \vee x_{i2} \vee \cdots \vee x_{in}$ for all $i \in [m]$.

Notice that $\overline{tr}$ encodes the previous CNF as an unsatisfiable set of monomials of maximum degree n. It can be encoded in PCR also as a set of small degree polynomials where axioms in (2) are substituted by $\sum_j x_{ij} - 1$. This makes sense when proving degree lower bounds but it trivially implies space lower bounds, as already some axioms require a large number of monomials.

The *onto* version of the Pigeonhole Principle, $\mathsf{ontoPHP}^m_n$, is the conjunction of the following clauses:

(1) $\neg x_{ij} \vee \neg x_{i'j}$ for all $i \neq i' \in [m]$ and for all $j \in [n]$ (*injectivity axioms*);
(2) $x_{i1} \vee x_{i2} \vee \cdots \vee x_{in}$ for all $i \in [m]$;
(3) for all $j \in [n]$, $x_{1j} \vee x_{2j} \vee \cdots \vee x_{mj}$ (*onto axioms*).

Clearly, for any ideal, I, MSpace($\mathsf{PHP}^m_n \vdash_I 1$) $\geqslant$ MSpace($\mathsf{ontoPHP}^m_n \vdash_I 1$). We prove a space lower bound for $\mathsf{ontoPHP}^m_n$.

Theorem 4.2 ([Alekhnovich et al. 2002]). *Let I be the trivial ideal $I = \{0\}$, then* MSpace($\mathsf{ontoPHP}^m_n \vdash_I \perp$) $> n/4$.

Proof. We apply Theorem 3.6. Let P_1 be the set of the Boolean axioms plus the polynomial encoding of the axioms in (1); P_2 is the set of polynomial encodings of the axioms in (2) and (3).

Given $j \in [n]$, let H_j be the following set of partial assignments of domain $\{x_{ij}, \bar{x}_{ij} : i \in [m]\}$:

$$H_j = \{\alpha_{1j}, \ldots, \alpha_{mj}\},$$

where α_{ij} is the Boolean assignment setting x_{ij} to 1 and the other variables $x_{i'j}$ to 0. By construction, H_j is flippable and I-consistent.

The strategy $\mathscr{L}$ is defined as follows: $\mathcal{H} \in \mathscr{L}$ if and only if there exists a set of holes $A \subseteq [n]$ such that

$$\mathcal{H} = \bigotimes_{j \in A} H_j.$$

We prove that $\mathscr{L}$ is a n-winning strategy for P_1 with respect to the ideal I. $\mathscr{L}$ is nonempty as for $A = \emptyset$ the definition implies that $\{\Lambda\} \in \mathscr{L}$. By construction, $\mathcal{H} \in \mathscr{L}$ imply that $\mathcal{H}$ is I-consistent.

The *restriction property* is immediate from the definition. For the *extension property*, let $p \in P_1$ and $\mathcal{H} \in \mathscr{L}$, with $\|\mathcal{H}\| < n$ such that $\mathcal{H} = \bigotimes_{j' \in A} H_{j'}$ for some $A \subseteq [n]$. There is exactly one $j \in [n]$ such that $\mathrm{var}(p) \subseteq \mathrm{dom}(H_j)$. If $j \in A$, then, by construction, $\mathcal{H} \vDash_I p$ hence we take $\mathcal{H}_p = \{\Lambda\}$. If $j \notin A$, then H_j is domain-disjoint from $\mathcal{H}$, $\mathcal{H} \otimes H_j \in \mathscr{L}$ and by construction is such that $\mathcal{H} \otimes H_j \vDash_I p$. Take $\mathcal{H}_p = H_j$ in this case.

P_2 satisfies the hypothesis of Theorem 3.6, since every $\mathcal{H} \in \mathscr{L}$ of rank $< n$ leaves unset at least one variable in each each axiom in (2). Moreover, each axiom in (3) is either set to 0 or unset by elements in $\mathscr{L}$. □

The Bit-Pigeonhole Principle. Let $m, n \in \mathbb{N}$ be two integers such that $m > n$ and $n = 2^k$ for $k \in \mathbb{N}$. Let $X = \{x_{ij} \ : \ i \in [m], \ j \in [k]\}$, where x_{ij} is "the jth bit of the binary representation of the hole where the pigeon i is mapped to". The axioms of the *Bit-Pigeonhole Principle* $\mathsf{Bit\text{-}PHP}^m_n$, are clauses $B^h_{i,i'}$ meaning that two distinct pigeons i and i' cannot go into the same hole h because they differ on some bit of the binary representation of h. More formally, given distinct $i, i' \in [m]$ and $h \in [n]$ let $B^h_{i,i'} = \bigvee_{j=1}^{k} \left(x_{ij} \neq h_j \vee x_{i'j} \neq h_j\right)$, where h_j is the jth bit of the binary representation of h. $\mathsf{Bit\text{-}PHP}^m_n$ is the conjunction of the $B^h_{i,i'}$ for $h \in [n]$ and $i \neq i' \in [m]$.

THEOREM 4.3 [FILMUS ET AL. 2012]. *Let I be the ideal generated by the Boolean axioms, then* $\mathrm{MSpace}(\mathsf{Bit\text{-}PHP}^m_n \vdash_I \bot) \geqslant n/8$.

PROOF. We use the Main Theorem (Theorem 3.5) and we give a $n/2$-winning strategy $\mathscr{L}$ for $\mathsf{Bit\text{-}PHP}^m_n$ with respect to the ideal I.

Given a hole h with binary representation $(h_1, \ldots, h_k)$, let $\bar{h}$ be $(1 - h_1, \ldots, 1 - h_k)$. Given a set of holes A, $\overline{A} = \{\bar{h} \ : \ h \in A\}$. The notation $\left[i \mapsto h, i' \mapsto \bar{h}\right]$ where $i, i' \in [m]$ and $h \in [n]$ is a shortcut for the partial assignment α with domain $\{x_{ij}, x_{i'j}, \bar{x}_{ij}, \bar{x}_{i'j} \ : \ j \in [k]\}$ such that $\alpha(x_{ij}) = h_j$ and $\alpha(x_{i'j}) = 1 - h_j$. The assignment α is intended to respect the meaning of the $\bar{x}_{ij}$, that is, $\alpha(\bar{x}_{ij}) = 1 - \alpha(x_{ij})$ and similarly for $\alpha(x_{i'j})$.

Given $h \in [n/2]$ and $\sigma : \{h, \bar{h}\} \to [m]$ an injective mapping,[3] let H^σ_h be the following set of partial assignments of domain $\{x_{\sigma(h)j}, x_{\sigma(\bar{h})j}, \bar{x}_{\sigma(h)j}, \bar{x}_{\sigma(\bar{h})j} \ : \ j \in [k]\}$:

$$H^\sigma_h = \{\left[\sigma(h) \mapsto h, \sigma(\bar{h}) \mapsto \bar{h}\right], \quad \left[\sigma(h) \mapsto \bar{h}, \sigma(\bar{h}) \mapsto h\right]\}.$$

By construction, H^σ_h is flippable and I-consistent.

The strategy $\mathscr{L}$ is defined as follows: $\mathcal{H} \in \mathscr{L}$ if and only if there exists a set of holes $A \subseteq [n/2]$ and there exists an injective mapping $\sigma : A \cup \overline{A} \to [m]$ such that

$$\mathcal{H} = \bigotimes_{h \in A} H^\sigma_h .$$

We prove that $\mathscr{L}$ is a $n/2$-winning strategy for $\mathsf{Bit\text{-}PHP}^m_n$ with respect to the ideal I. $\mathscr{L}$ is nonempty as for $A = \emptyset$, the definition implies that $\{\Lambda\} \in \mathscr{L}$. By construction, $\mathcal{H} \in \mathscr{L}$ imply that $\mathcal{H}$ is I-consistent.

The restriction property of $\mathscr{L}$ is obvious, hence we focus on the extension property. Let $\mathcal{H} = \bigotimes_{h \in A} H^\sigma_h \in \mathscr{L}$ such that $\|\mathcal{H}\| < n/2$ and consider $p = \overline{tr}(B^h_{i,i'})$. If both $i, i' \in \sigma(A \cup \overline{A})$, then, by construction, $\mathcal{H} \vDash_I p$, hence we can take $\mathcal{H}_p = \{\Lambda\}$. Otherwise, without loss of generality, assume $i' \notin \sigma(A \cup \overline{A})$. As $\|\mathcal{H}\| = |A| < n/2$, there is some hole $h' \in [n/2] \backslash A$ and σ' injective such that $\sigma' = \sigma \cup \{h' \mapsto i'\} \cup \{\bar{h}' \mapsto j\}$ with j outside $\sigma(A \cup \overline{A}) \cup \{i'\}$. If $i \notin \sigma(A \cup \overline{A})$, take $j = i$. Let $\mathcal{H}_p = H^{\sigma'}_{h'}$: it is clearly I-consistent and domain-disjoint from $\mathcal{H}$. Define $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}_p = \bigotimes_{h \in A'} H^{\sigma'}_h \in \mathscr{L}$, where $A' = A \cup \{h'\}$. Notice that $\mathcal{H}' \vDash_I p$,

[3] Notice that, as $h \in [n/2]$, then h and $\bar{h}$ are distinct.

as each assignment in $\mathcal{H}'$ set i and i' to go into two distinct holes. More precisely, if $i \in \sigma(A \cup \overline{A})$, then i goes somewhere inside $A \cup \overline{A}$ and i' goes either in h' or $\bar{h}'$. If $i \notin \sigma(A \cup \overline{A})$, then, by construction, i goes in $\bar{h}'$ and i' goes to h' or vice-versa. □

The XOR-Pigeonhole Principle. Let $m, n \in \mathbb{N}$ be two integers such that $m > n$ and let $X = \{x_{i,j} \,:\, i \in [m],\ j \in [n] \cup \{0\}\}$ be a set of variables. A pigeon $i \in [m]$ is considered assigned to a hole $j \in [n]$ when $x_{i,j-1} \not\equiv x_{i,j}$ is true. The *XOR-Pigeonhole Principle*, introduced in Filmus et al. [2012], expresses the following weaker form of the Pigeonhole Principle: if each pigeon is assigned to an odd number of holes, then there exists a hole with at least two pigeons. The formula $\mathsf{XOR\text{-}PHP}^m_n$ is a contradictory 4-CNF encoding the negation of the principle as follows:

(1) for each $i \in [m]$, $x_{i,0} \not\equiv x_{i,n}$, that is $(x_{i,0} \vee x_{i,n}) \wedge (\neg x_{i,0} \vee \neg x_{i,n})$;
(2) for all distinct $i, i' \in [m]$ and all $j \in [n] \cup \{0\}$, $(x_{i,j-1} \equiv x_{i,j}) \vee (x_{i',j-1} \equiv x_{i',j})$, that is

$$\begin{aligned}&(x_{i,j-1} \vee \neg x_{i,j} \vee x_{i',j-1} \vee \neg x_{i',j}) \wedge (\neg x_{i,j-1} \vee x_{i,j} \vee \neg x_{i',j-1} \vee x_{i',j})\\ &\wedge (x_{i,j-1} \vee \neg x_{i,j} \vee \neg x_{i',j-1} \vee x_{i',j}) \wedge (\neg x_{i,j-1} \vee x_{i,j} \vee x_{i',j-1} \vee \neg x_{i',j}).\end{aligned}$$

THEOREM 4.4 [FILMUS ET AL. 2012]. *Let I be the ideal generated by the Boolean axioms, then MSpace* $(\mathsf{XOR\text{-}PHP}^m_n \vdash_I \perp) \geqslant (n-1)/4$.

PROOF. Given $i \in [m]$ and $j \in [n]$, let $H_{i\mapsto j}$ be the following set of partial assignments of domain $\{x_{ij'}, \bar{x}_{ij'} \,:\, j' \in [n] \cup \{0\}\}$:

$$H_{i\mapsto j} = \{\alpha_{ij}, \alpha^*_{ij}\},$$

where $\alpha_{ij}(x_{ij'}) = 1$ if and only if $j' < j$ and $\alpha^*_{ij}(x_{i'j}) = 1 - \alpha_{ij}(x_{ij'})$. Both α_{uv} and α^*_v are intended to respect the intended meaning of the $\bar{x}_{u'v}$, that is, $\alpha^*_v(\bar{x}_{u'v}) = 1 - \alpha^*_v(x_{u'v})$ and similarly for α_{uv}. Both α_{ij} and α^*_{ij} are intended to respect the meaning of the $\bar{x}_{ij'}$, that is $\alpha_{ij}(\bar{x}_{ij'}) = 1 - \alpha_{ij}(x_{ij'})$ and similarly for α^*_{ij}. By construction, $H_{i\mapsto j}$ is flippable and I-consistent.

The strategy $\mathscr{L}$ is defined as follows: $\mathcal{H} \in \mathscr{L}$ if and only if there exists a set $A \subseteq [m]$ of size at most $n-1$ and there exists an injective mapping $\mu : A \longrightarrow [n]$ such that

$$\mathcal{H} = \bigotimes_{i \in A} H_{i\mapsto \mu(i)}.$$

We prove that $\mathscr{L}$ is a $(n-1)$-winning strategy for $\mathsf{XOR\text{-}PHP}^m_n$ with respect to the ideal I. $\mathscr{L}$ is nonempty as for $A = \emptyset$ the definition implies that $\{\Lambda\} \in \mathscr{L}$. By construction, $\mathcal{H} \in \mathscr{L}$ implies that $\mathcal{H}$ is I-consistent.

The restriction property is immediate from the definition. To prove the *extension property*, let $\mathcal{H} = \bigotimes_{i\in A} H_{i\mapsto\mu(i)} \in \mathscr{L}$ with $\|\mathcal{H}\| < n-1$ and p the polynomial encoding of a initial clause C from $\mathsf{XOR\text{-}PHP}^m_n$. Let us suppose first that C is a clause from some $(x_{i,j-1} \equiv x_{i,j}) \vee (x_{i',j-1} \equiv x_{i',j})$. If both i and i' are in A, then, by construction, $\mathcal{H} \vDash_I p$ and we can take $\mathcal{H}_p = \{\Lambda\}$. If $i \notin A$, then, as μ is an injective assignment of at most $n-2$ pigeons, we can find a hole h *different from* j which is not in $\mu(A)$. Then let $\mu' = \mu \cup \{i \mapsto h\}$ and $\mathcal{H}' = \bigotimes_{\ell\in A\cup\{i\}} H_{\ell\mapsto\mu'(\ell)} = \mathcal{H} \otimes H_{i\mapsto h}$. By construction $H_{i\mapsto h} \vDash_I p$, hence $\mathcal{H}' \vDash_I p$. In this case, take $\mathcal{H}_p = H_{i\mapsto h}$. Similarly, if $C = (x_{i,0} \not\equiv x_{i,n})$, we proceed as before extending μ to assign the pigeon i somewhere (if needed). □

Notice that in Filmus et al. [2012] is proved that MSpace$(\mathsf{XOR\text{-}PHP}^m_n \vdash_I \perp) > n/4$, for the ideal $I = \{0\}$.

5. BIPARTITE EXPANSION, RANDOM CNF FORMULAS AND THE GRAPH-PIGEONHOLE PRINCIPLE

In this section, we build a $\Omega(n)$-winning strategy for random k-CNFs in n variables when $k \geqslant 4$ and for the Graph Pigeonhole Principle. To this end, we use a variant of the *Matching Game* devised in Ben-Sasson and Galesi [2003] to prove space lower bounds for random k-CNFs in Resolution. Unlike previous works that deal with 1-matchings in bipartite graphs [Ben-Sasson and Galesi 2003; Atserias 2004], here we consider 2-matchings. However, the proofs of the main properties remain similar and we follow the simplified version of Atserias [2004].

Definition 5.1 (*(r, s)-Double Matching Property*). Let $r, s \in \mathbb{N}$ be two integers such that $r \leqslant s$ and $\mathscr{G} = (U \cup V, E)$ be a bipartite graph. Given two sets $A \subseteq U$ and $B \subseteq V$ we say that $(\mathscr{G}, A, B)$ has the (r, s)-*double matching property* if $|A| \leqslant r$, $|B| = 2|A|$ and for every $C \subseteq U \setminus A$, if $|C| \leqslant s - |A|$ then there exists a 2-matching of C into $V \setminus B$.

$(\mathscr{G}, \emptyset, \emptyset)$ has the (s, s)-double matching property if $\mathscr{G} = (U \cup V, E)$ is a $(s, 2+\epsilon)$-expander bipartite graph for some positive constant ϵ. This follows immediately from the expansion property and Lemma 2.4.

LEMMA 5.2 (EXTENSION LEMMA). *Let ϵ be a positive constant and $\mathscr{G} = (U \cup V, E)$ be a bipartite graph of left degree at most d which is a $(s, 2+\epsilon)$-expander. Let $A \subseteq U$ and $B \subseteq V$ be two sets such that $|A| < r$ and $(\mathscr{G}, A, B)$ has the (r, s)-double matching property with $r \leqslant \frac{\epsilon s}{d(d-1)+\epsilon}$. Then, for each $u \in U \setminus A$, there exists a 2-matching π_u of u into $V \setminus B$ such that $(\mathscr{G}, A \cup \{u\}, B \cup \pi_u(u))$ has the (r, s)-double matching property.*

PROOF. Fix $u \in U \setminus A$ and let Π be the set of 2-matchings of u into $V \setminus B$, that is $\Pi = \{\{(u, v), (u, w)\} : v \neq w \wedge v, w \in V \setminus B\}$. $\Pi \neq \emptyset$ since $|A| < r \leqslant s$ and the (r, s)-double matching property of $(\mathscr{G}, A, B)$ implies that $\{u\}$ has at least one 2-matching into $V \setminus B$. Notice that $|\Pi| \leqslant \binom{d}{2} = d(d-1)/2$.

Let $A' = A \cup \{u\}$ and for each $\pi \in \Pi$ let $B_\pi = B \cup \pi(u)$. Suppose, for the sake of contradiction, that for each $\pi \in \Pi$, $(\mathscr{G}, A', B_\pi)$ does not have the (r, s)-double matching property. We have that $|A'| \leqslant r$, because $|A| < r$, and clearly for each $\pi \in \Pi$, $|B_\pi| = 2|A'|$. This means that, for each $\pi \in \Pi$, there exists a set $C_\pi \subseteq U \setminus A'$ of size at most $s - |A'|$ that does not admit a 2-matching into $V \setminus B_\pi$. Let D_π be a minimal size C_π with this property. Then, by Lemma 2.4, we have that

$$\forall \pi \in \Pi \qquad |N_{\mathscr{G}}(D_\pi) \cap (V \setminus B_\pi)| < 2|D_\pi|, \tag{2}$$

and by the expansion property of $\mathscr{G}$, since $|D_\pi| \leqslant s - |A'| < s$, we have that

$$\forall \pi \in \Pi \qquad (2+\epsilon)|D_\pi| \leqslant |N_{\mathscr{G}}(D_\pi)|. \tag{3}$$

Using the fact that $|N_{\mathscr{G}}(D_\pi)| = |N_{\mathscr{G}}(D_\pi) \cap (V \setminus B_\pi)| + |N_{\mathscr{G}}(D_\pi) \cap B_\pi|$ and then bounding the first part of the sum using Eq. (2) and the second part using the trivial upper bound $|B_\pi|$, we obtain, by Eq. (3), $(2+\epsilon)|D_\pi| < 2|D_\pi| + |B_\pi|$. Hence, it follows that

$$\forall \pi \in \Pi \qquad 2|A'| = |B_\pi| > \epsilon |D_\pi|. \tag{4}$$

The following claim will help us to find a lower bound for $|D_{\pi^*}|$ for some $\pi^* \in \Pi$.

CLAIM 2. *$\Omega = \bigcup_{\pi \in \Pi} D_\pi \cup \{u\}$ does not admit a 2-matching into $V \setminus B$.*

PROOF. Assume by contradiction that there exists a 2-matching σ of Ω into $V \setminus B$. Take $\pi_\sigma \in \Pi$ such that $\pi_\sigma(u) = \sigma(u)$. As $\sigma(D_{\pi_\sigma}) \subseteq V \setminus B$ and, by construction of D_{π_σ}, $\sigma(D_{\pi_\sigma}) \nsubseteq V \setminus B_{\pi_\sigma}$, then $\sigma(D_{\pi_\sigma}) \cap \pi_\sigma(u) \neq \emptyset$. Therefore, since $u \notin D_{\pi_\sigma}$, we have found two elements, u and some element in D_{π_σ}, both mapped by σ into the same element. This is a contradiction. □

We have that the set Ω in the claim is such that $\Omega \subseteq U \backslash A$ and $(\mathscr{G}, A, B)$, by hypothesis, has the (r, s)-double matching property, so we must have that

$$|\Omega| > s - |A|.$$

This implies that $\sum_{\pi \in \Pi} D_\pi > s - |A| - 1$, so there exists $\pi^* \in \Pi$ such that

$$|D_{\pi^*}| > \frac{s - |A'|}{|\Pi|}. \tag{5}$$

Putting together Eqs. (4) and (5) and observing that $|\Pi| \leqslant d(d-1)/2$, we obtain that

$$|A'| > \epsilon \frac{s - |A'|}{d(d-1)}.$$

From this, a contradiction arises immediately:

$$|A'| > \frac{\epsilon}{d(d-1) + \epsilon} \cdot s = r. \quad \square$$

Lemma 5.3 (Retraction Lemma). *Let ϵ be a positive constant and $\mathscr{G} = (U \cup V, E)$ be a $(s, 2+\epsilon)$- expander bipartite graph and let $A \subseteq U$ and $B \subseteq V$ two sets such that $(\mathscr{G}, A, B)$ has the (r, s)-double matching property with $r \leqslant \frac{\epsilon s}{2+\epsilon}$. Then, for each $u \in A$ and for each 2-matching π of u into B, $(\mathscr{G}, A \backslash \{u\}, B \backslash \pi(u))$ has the (r, s)-double matching property.*

Proof. Let $A' = A \backslash \{u\}$ and $B' = B \backslash \pi(u)$. Clearly, $|A'| \leqslant r$ and $B' = 2|A'|$. Let $C \subseteq U \backslash A'$ be of size at most $s - |A'|$. If $u \in C$, then $C \backslash \{u\} \subseteq U \backslash A$, and has size at most $s - |A'| - 1 = s - |A|$. Hence, there exists a 2-matching σ of $C \backslash \{u\}$ into $V \backslash B$. By hypothesis, π is a 2-matching of u into B. So $\pi \cup \sigma$ is a 2-matching of C into $V \backslash B'$.

If $u \notin C$ and $|C| \leqslant s - |A'| - 1 = s - |A|$, then by the (r, s)-double matching property we have a 2-matching of C into $V \backslash B$.

The remaining case is when $u \notin C$ and $|C| = s - |A'|$, then for every $w \in C$, there exists a 2-matching of $C \backslash \{w\} \subseteq U \backslash A$ into $V \backslash B \subseteq V \backslash B'$. If C does not have a 2-matching into $V \backslash B'$, it follows that C is of minimal size. Using Lemma 2.4, it follows that

$$|N_{\mathscr{G}}(C) \cap (V \backslash B')| < 2|C|. \tag{6}$$

From the fact that $\mathscr{G}$ is a $(s, 2+\epsilon)$-expander, the fact that $|C| \leqslant s - |A'| \leqslant s$, and Eq. (6), it follows that

$$(2+\epsilon)|C| \leqslant |N_{\mathscr{G}}(C)| < 2|C| + |B'|.$$

So $|B'| > \epsilon|C|$. Summarizing, we have $|C| = s - |A'|$, and $2|A'| = |B'|$, so $2|A'| > \epsilon(s - |A'|)$, which implies the contradiction:

$$|A'| > \frac{\epsilon s}{2+\epsilon} = r. \quad \square$$

5.1. Random *k*-CNFs

Let $n, k, \Delta \in \mathbb{N}$ and let $X = \{x_1, \ldots, x_n\}$ be a set of n variables. $\mathcal{R}(n, \Delta, k)$ is the probability distribution obtained by the following experiment: choose independently uniformly at random Δn clauses from the set of all possible k-clauses over X. We are interested in studying the asymptotic properties of a randomly chosen k-CNF $\varphi \sim \mathcal{R}(n, \Delta, k)$ as n approaches infinity. It is well known that when Δ exceeds a certain constant θ_k (that only depends on k), φ is almost surely unsatisfiable. Hence, we always consider $\varphi \sim \mathcal{R}(n, \Delta, k)$, where Δ is a constant (depending on k) bigger than θ_k.

Let φ be a CNF and X be the set of variables appearing in φ. The *adjacency graph of* φ is a bipartite graph $\mathscr{G}_\varphi = (U \cup V, E)$ such that U is the set of clauses of φ, $V = X$ and $(C, x) \in E$ if and only if x or $\neg x$ appears in C. If φ is a k-CNF, then $\mathscr{G}_\varphi$ has left degree k.

The proof of the next theorem is standard and can be found, for instance in Chvátal and Szemerédi [1988], Beame and Pitassi [1996], Ben-Sasson and Wigderson [2001], and Ben-Sasson and Galesi [2003].

THEOREM 5.4. *For any $k \geqslant 4$ and any constant ϵ with $0 < \epsilon < k - 3$, there is a constant $\delta = \delta_{k,\epsilon}$ such that if $\varphi \sim \mathcal{R}(n, \Delta, k)$, then, with high probability, the adjacency graph of φ is a $(s, 2 + \epsilon)$-expander, with $s = \delta \Delta^{-\frac{1+\epsilon}{k-3-\epsilon}} n$.*

Lemma 5.1 in Ben-Sasson and Galesi [2003] is exactly the previous theorem for $k \geqslant 3$, for $0 < \epsilon < k - 2$ and for $(s, 1 + \epsilon)$-expanders, with $s = \delta \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}} n$. That proof can be easily adapted for the expansion factor $2 + \epsilon$ but requiring $k \geqslant 4$.

THEOREM 5.5. *Let $k \geqslant 4$ be an integer and $\Delta \geqslant \theta_k$ be two constants. If $\varphi \sim \mathcal{R}(n, \Delta, k)$, then there exists a constant $c_{k,\Delta} \geqslant 1$ such that, with high probability,*

$$\mathrm{MSpace}(\varphi \vdash_I \bot) \geqslant \frac{n}{4c_{\Delta,k}},$$

where I is the ideal generated by the Boolean axioms.

PROOF. Fix a positive $\epsilon < k - 3$ as required in Theorem 5.4. With high probability, the adjacency graph $\mathscr{G}_\varphi = (U \cup V, E)$ of φ is a $(s, 2+\epsilon)$-expander, with $s = \delta \Delta^{-\frac{1+\epsilon}{k-3-\epsilon}} n$ and δ some constant depending on k and ϵ. Let $c = c_{\Delta,k,\epsilon} = \epsilon^{-1} \delta^{-1} \Delta^{\frac{1+\epsilon}{k-3-\epsilon}} (k(k-1) + \epsilon)$, hence

$$\frac{n}{c} = \frac{\epsilon s}{k(k-1)+\epsilon} = \min\left\{ s, \frac{\epsilon s}{2+\epsilon}, \frac{\epsilon s}{k(k-1)+\epsilon} \right\}. \tag{7}$$

To prove the result, we give a n/c-winning strategy $\mathscr{L}$ for φ with respect to I.

Given a clause C in φ and a 2-matching π of C in V, let H_C^π be the set of the partial assignments α of domain $\pi(C) \cup \{\bar{x} \ : \ x \in \pi(C)\}$ such that $\alpha \vDash_I \overline{tr}(C)$. For example, if $C = x \vee \neg y \vee C'$ and $\pi(C) = \{x, y\}$, then $\overline{tr}(C) = \bar{x} y \cdot \overline{tr}(C')$ and

$$H_C^\pi = \left\{ \left\{ \begin{matrix} x \mapsto 0, & y \mapsto 0, \\ \bar{x} \mapsto 1, & \bar{y} \mapsto 1, \end{matrix} \right\}, \left\{ \begin{matrix} x \mapsto 1, & y \mapsto 1, \\ \bar{x} \mapsto 0, & \bar{y} \mapsto 0, \end{matrix} \right\}, \left\{ \begin{matrix} x \mapsto 1, & y \mapsto 0, \\ \bar{x} \mapsto 0, & \bar{y} \mapsto 1, \end{matrix} \right\} \right\}.$$

The strategy $\mathscr{L}$ is defined as follows: $\mathcal{H} \in \mathscr{L}$ if and only if there exists a set $A \subseteq U$ and there exists a 2-matching π of A into V such that

(1) $|A| \leqslant n/c$;
(2) $(\mathscr{G}_\varphi, A, \pi(A))$ has the $(n/c, s)$-double matching property[4];
(3) $\mathcal{H} = \bigotimes_{C \in A} H_C^\pi$.

We prove that $\mathscr{L}$ is a n/c-winning strategy for φ with respect to the ideal I. $\mathscr{L}$ is nonempty as $\mathscr{G}_\varphi$ is an $(s, 2 + \epsilon)$-expander so $(\mathscr{G}_\varphi, \emptyset, \emptyset)$ has the $(n/c, s)$-double matching property and so $\{\Lambda\} \in \mathscr{L}$. By construction, $\mathcal{H} \in \mathscr{L}$ imply that $\mathcal{H}$ is I-consistent.

For the restriction property, assume $\mathcal{H}' \sqsubseteq \mathcal{H}$ with $\mathcal{H} = \bigotimes_{C \in A} H_C^\pi \in \mathscr{L}$. Then $\mathcal{H}' = \bigotimes_{C \in A'} H_C^{\pi'}$, for some $A' \subseteq A$ where π' is the restriction of π to A'. Property (1) and (3) are immediate. To prove property (2) we use the Retraction Lemma (Lemma 5.3). $|A| \leqslant n/c$ and the parameter n/c in the $(n/c, s)$-double matching property of $(\mathscr{G}_\varphi, A, \pi(A))$ fulfills the hypothesis of the *Retraction Lemma*. Hence, we obtain that $(\mathscr{G}_\varphi, A', \pi'(A'))$ has the $(n/c, s)$-double matching property repeatedly applying the lemma to $(\mathscr{G}_\varphi, A, \pi(A))$ removing one by one the clauses $C \in A \backslash A'$ and the corresponding $\pi(C)$ from $\pi(A)$.

[4] Recall that, as defined in Section 2.3, $\pi(A) = \bigcup_{C \in A} \pi(C)$.

To prove the extension property, take $\mathcal{H} = \bigotimes_{D\in A} H^{\pi}_{D} \in \mathscr{L}$ with $\|\mathcal{H}\| < n/c$ and let $p = \overline{tr}(C)$ be an axiom, where $C \in \varphi$. By construction, p is a monomial and we can suppose that $\mathcal{H} \nvDash_I p$ (otherwise, just take $\mathcal{H}_p = \{\Lambda\}$). We apply the Extension Lemma (Lemma 5.2) to $(\mathscr{G}_\varphi, A, \pi(A))$ since $|A| < n/c$ and the parameter n/c fulfills the hypothesis the lemma. Then there exists a 2-matching π_C of C into $V\backslash\pi(A)$ such that $(\mathscr{G}, A\cup\{C\}, \pi(A)\cup\pi_C(C))$ has the $(n/c, s)$-double matching property. Let $\mathcal{H}_p = H^{\pi_C}_C$ be the set of the partial assignments α of domain $\pi_C(C)$ such that $\alpha \vDash_I C$. $\mathcal{H}_p$ is an I-consistent flippable family domain-disjoint from $\mathcal{H}$. Let $A' = A\cup\{C\}$ and $\pi' = \pi\cup\pi_C$, then $\mathcal{H}\otimes\mathcal{H}_p = \bigotimes_{D\in A'} H^{\pi'}_D$ is a flippable product-family in $\mathscr{L}$ and $\mathcal{H}\otimes\mathcal{H}_p \vDash_I p$, as already $\mathcal{H}_p \vDash_I p$. □

5.2. The Graph-Pigeonhole Principle

Let $\mathscr{G} = (U\cup V, E)$ be a bipartite graph with U and V two disjoint sets of size respectively $n+1$ and n and let $X = \{x_{u,v} \ : \ (u, v) \in E\}$. The intuitive meaning of the variables $x_{u,v}$ is the same as in PHP^m_n, that is "the pigeon u goes to hole v". The formula $\mathscr{G}$-PHP is the conjunction of the following clauses:

(1) $\neg x_{u,v} \vee \neg x_{u',v}$ for all $(u, v) \in E$ and $(u', v) \in E$ with $u \neq u'$ (*injectivity axioms*);
(2) $P_u = \bigvee_{v\,:\,(u,v)\in E} x_{u,v}$ for all $u \in U$.

THEOREM 5.6. *Let ϵ be a positive constant and $\mathscr{G} = (U\cup V, E)$ be a bipartite graph with left degree d. If $\mathscr{G}$ is a $(s, 2+\epsilon)$-expander, then MSpace $(\mathscr{G}$-PHP $\vdash_I \bot) \geqslant \frac{r}{4}$, where $r = \frac{\epsilon s}{d(d-1)+\epsilon}$ and I is the ideal generated by the polynomial encoding of the injectivity axioms of $\mathscr{G}$-PHP and the Boolean axioms.*

PROOF. Fix $r = \frac{\epsilon s}{d(d-1)+\epsilon}$. To prove the result, we give a r-winning strategy $\mathscr{L}$ for $\mathscr{G}$-PHP with respect to the ideal I.

Given $v \in V$, let H_v be the following set of partial assignments of domain $\{x_{u'v}, \bar{x}_{u'v} \ : \ u' \in N(v)\}$

$$H_v = \{\alpha^*_v\} \cup \{\alpha_{uv} \ : \ u \in N(v)\},$$

where α_{uv} is the Boolean assignment setting x_{uv} to 1 and all the other variables $x_{u'v}$ to 0 and α^*_v is the Boolean assignment setting all the variables $x_{u'v}$ to 0. Both α_{uv} and α^*_v are intended to respect the meaning of the $\bar{x}_{u'v}$, that is, $\alpha^*_v(\bar{x}_{u'v}) = 1 - \alpha^*_v(x_{u'v})$ and similarly for α_{uv}.

Given $u \in U$ and $v, v' \in N(u)$ let $O^u_{\{v,v'\}}$ be the following set of partial assignments of domain $\mathrm{dom}(H_v) \cup \mathrm{dom}(H_{v'})$:

$$O^u_{\{v,v'\}} = (\{\alpha_{uv}\} \otimes H_{v'}) \cup (H_v \otimes \{\alpha_{uv'}\}).$$

By construction, $O^u_{\{v,v'\}}$ is flippable, I-consistent and $O^u_{v,v'} \vDash_I \overline{tr}(P_u)$.

The strategy $\mathscr{L}$ is defined as follows: $\mathcal{H} \in \mathscr{L}$ if and only if there exists $A \subseteq U$ and a 2-matching π of A into V such that:

(1) $|A| \leqslant r$,
(2) $(\mathscr{G}, A, \pi(A))$ has the (r, s)-double matching property[5];
(3) $\mathcal{H} = \bigotimes_{u\in A} O^u_{\pi(u)}$.

We prove that $\mathscr{L}$ is a r-winning strategy for $\mathscr{G}$-PHP with respect to the ideal I. $\mathscr{L}$ is nonempty as $(\mathscr{G}, \emptyset, \emptyset)$ has the (r, s)-double matching property and so $\{\Lambda\} \in \mathscr{L}$. By construction for each $\mathcal{H} \in \mathscr{L}$, $\mathcal{H}$ is I-consistent.

[5] Recall that, as defined in Section 2.3, $\pi(A) = \bigcup_{u\in A} \pi(u)$.

For the restriction property assume $\mathcal{H}' \sqsubseteq \mathcal{H}$ with $\mathcal{H} = \bigotimes_{u \in A} O^u_{\pi(u)} \in \mathscr{L}$. Then $\mathcal{H}' = \bigotimes_{u \in A'} O^u_{\pi'(u)}$, for some $A' \subseteq A$ where π' is the restriction of π to A'. Property (1) and (3) are immediate. To prove property (2), we use the Retraction Lemma (Lemma 5.3). $|A| \leqslant r$ and the parameter r in the (r, s)-double matching property of $(\mathscr{G}, A, \pi(A))$ fulfills the hypothesis of the Retraction Lemma. Hence, we obtain that $(\mathscr{G}, A', \pi'(A'))$ has the (r, s)-double matching property repeatedly applying the lemma to $(\mathscr{G}, A, \pi(A))$ removing one by one the clauses $u \in A \backslash A'$ and the corresponding $\pi(u)$ from $\pi(A)$.

To prove the extension property, take $\mathcal{H} = \bigotimes_{u' \in A} O^{u'}_{\pi(u')} \in \mathscr{L}$ with $\|\mathcal{H}\| < r$ and let $p = \overline{tr}(P_u)$ be an axiom, where $P_u \in \mathscr{G}$-PHP. We can suppose that $\mathcal{H} \nvDash_I p$ (otherwise, just take $\mathcal{H}_p = \{\Lambda\}$). We apply the Extension Lemma (Lemma 5.2) to $(\mathscr{G}, A, \pi(A))$ since $|A| < r$ and the parameter r fulfills the hypothesis the lemma. Then there exists a 2-matching π_u of u into $V \backslash \pi(A)$ such that $(\mathscr{G}, A \cup \{u\}, \pi(A) \cup \pi_u(u))$ has the (r, s)-double matching property. Let $\mathcal{H}_p = O^u_{\pi_u(u)}$ be the set of the partial assignments α of domain $\pi_u(u)$ such that $\alpha \vDash_I p$. $\mathcal{H}_p$ is an I-consistent flippable family domain-disjoint from $\mathcal{H}$. Let $A' = A \cup \{u\}$ and $\pi' = \pi \cup \pi_u$, then $\mathcal{H} \otimes \mathcal{H}_p = \bigotimes_{v \in A'} O^v_{\pi(v)}$ is a flippable product-family in $\mathscr{L}$ and $\mathcal{H} \otimes \mathcal{H}_p \vDash_I p$, as already $\mathcal{H}_p \vDash_I p$. □

THEOREM 5.7. *There exists a constant degree $d \geqslant 4$ bipartite graph $\mathscr{G} = (U \cup V, E)$ with $|U| = n + 1$ and $|V| = n$, such that*

$$\text{MSpace}(\mathscr{G}\text{-PHP} \vdash_I \bot) \geqslant \Omega(n/d^3),$$

where I is the ideal generated by the polynomial encoding of the injectivity axioms of $\mathscr{G}$-PHP and the Boolean axioms.

PROOF. Theorem 2.46 and Lemma 2.29 in Ben-Sasson [2001] prove that there exists a degree d bipartite graph $\mathscr{G} = (U \cup V, E)$ with $|U| = n + 1$ and $|V| = n$ which is a $(\Omega(n/d), 7d/8 - 1)$-expander. If $d \geqslant 4$, then $\mathscr{G}$ is a $(2+\epsilon)$-bipartite expander for a suitable positive ϵ. The theorem then follows from the previous theorem applied to $\mathscr{G}$-PHP. □

6. OPEN PROBLEMS

Space lower bounds for 3-CNFs. For every unsatisfiable CNF formula φ in n variables there is a trivial $O(n)$ upper bound for the monomial space needed to refute it in PCR. In particular, for formulas such as random 3-CNFs or the Tseitin contradiction over a 3-regular expander graphs (see Table I). Is there a monomial space lower bound for refuting those formulas in PCR asymptotically matching the trivial upper bound?

A partial result in this direction is obtained in Bennet et al. [2015] where it is proved that, given a random 3-CNF φ in n variables, any PCR refutation of φ require, with high probability, monomial space $\Omega(n)$.

Degree vs Space/Width vs Space. Is there a relation between space and degree in PCR (or width in Resolution and Space in PCR), similar to the one between width and space for Resolution [Atserias and Dalmau 2008]?

ACKNOWLEDGMENTS

We would like to thank Massimo Lauria, Neil Thapen, and Novella Bartolini for carefully reading a preliminary manuscript of this work and for suggesting several ways to improve the clarity of the final writing. We would like to thank Jacob Nordström, Eli Ben-Sasson, Mladen Mikša, and Mark Vinyals for interesting discussions on space in algebraic proof systems. We thank anonymous referees whose questions contributed significantly to improve the quality of this work.

REFERENCES

Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. 2002. Space complexity in propositional calculus. *SIAM J. Comput.* 31, 4, 1184–1211.

Michael Alekhnovich and Alexander A. Razborov. 2003. Lower bounds for polynomial calculus: Non-binomial case. In *Proceedings of the Steklov Institute of Mathematics*, Vol. 242. 18–35.

Albert Atserias. 2004. On sufficient conditions for unsatisfiability of random formulas. *J. ACM* 51, 2, 281–311.

Albert Atserias and Víctor Dalmau. 2008. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.* 74, 3, 323–334.

Paul Beame and Toniann Pitassi. 1996. Simplified and improved resolution lower bounds. In *Proceedings of FOCS*. IEEE Computer Society, 274–282.

Eli Ben-Sasson. 2001. Expansion in proof complexity. Ph.D. dissertation, Hebrew University.

Eli Ben-Sasson and Nicola Galesi. 2003. Space complexity of random formulae in resolution. *Random Struct. Algorithms* 23, 1, 92–109.

Eli Ben-Sasson and Russell Impagliazzo. 2010. Random CNF's are hard for the polynomial calculus. *Computat. Complex.* 19, 4, 501–519.

Eli Ben-Sasson and Jakob Nordström. 2011. Understanding space in proof complexity: Separations and trade-offs via substitutions. In *Proceedings of ICS*, Bernard Chazelle (Ed.), Tsinghua University Press, 401–416.

Eli Ben-Sasson and Avi Wigderson. 2001. Short proofs are narrow - Resolution made simple. *J. ACM* 48, 2, 149–169.

Patrick Bennet, Ilario Bonacina, Nicola Galesi, Tony Huynh, Mike Molloy, and Paul Wollan. 2015. Space proof complexity for random 3-CNFs. *arXiv*. (2015) http://arxiv.org/abs/1503.01613.

Archie Blake. 1937. Canonical expressions in Boolean algebra. Ph.D. dissertation, University of Chicago.

Ilario Bonacina and Nicola Galesi. 2013. Pseudo-partitions, transversality and locality: A combinatorial characterization for the space measure in algebraic proof systems. In *Proceedings of ITCS*. Robert D. Kleinberg (Ed.), ACM, 455–472.

Ilario Bonacina, Nicola Galesi, and Neil Thapen. 2014. Total space in resolution. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 641–650.

Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. 2001. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.* 62, 2, 267–289.

Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiri Sgall. 1997. Proof complexity in algebraic systems and bounded depth frege systems with modular counting. *Computat. Complex.* 6, 3, 256–298.

Vasek Chvátal and Endre Szemerédi. 1988. Many hard examples for resolution. *J. ACM* 35, 4, 759–768.

Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. 1996. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of STOC*. Gary L. Miller (Ed.), ACM, 174–183.

Stephen A. Cook and Robert A. Reckhow. 1979. The relative efficiency of propositional proof systems. *J. Symb. Log.* 44, 1, 36–50.

David A. Cox, John Little, and Donal O'Shea. 1997. *Ideals, Varieties, and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra* 2nd Ed., Springer. I–XIII, 1–536.

Juan Luis Esteban, Nicola Galesi, and Jochen Messner. 2004. On the complexity of resolution with bounded conjunctions. *Theoret. Comput. Sci.* 321, 2–3, 347–370.

Juan Luis Esteban and Jacobo Torán. 2001. Space bounds for resolution. *Inf. Comput.* 171, 1, 84–97.

Yuval Filmus, Massimo Lauria, Mladen Mikša, Jakob Nordström, and Marc Vinyals. 2013. Towards an understanding of polynomial calculus: New separations and lower bounds - (Extended Abstract). In *Proceedings of ICALP (1)*, Fedor V. Fomin, Rusins Freivalds, Marta Z. Kwiatkowska, and David Peleg (Eds.), (Lecture Notes in Computer Science) vol. 7965, Springer, 437–448.

Yuval Filmus, Massimo Lauria, Jakob Nordström, Neil Thapen, and Noga Ron-Zewi. 2012. Space complexity in polynomial calculus. In *Proceedings of IEEE Conference on Computational Complexity*. IEEE, 334–344.

Nicola Galesi and Massimo Lauria. 2010a. On the automatizability of polynomial calculus. *Theory Comput. Syst.* 47, 2, 491–506.

Nicola Galesi and Massimo Lauria. 2010b. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Trans. Comput. Log.* 12, 1, 4.

Russell Impagliazzo, Pavel Pudlák, and Jiri Sgall. 1999. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Comput. Complex.* 8, 2, 127–144.

Jan Krajíček. 2009. Propositional proof complexity I. Manuscript available at author's webpage.

Jakob Nordström. 2009. Narrow proofs may be spacious: Separating space and width in resolution. *SIAM J. Comput.* 39, 1, 59–121.

Jakob Nordström and Johan Håstad. 2013. Towards an optimal separation of space and length in resolution. *Theory Comput.* 9, 471–557.

Pavel Pudlák and Jiří Sgall. 1998. Algebraic models of computation and interpolation for algebraic proof systems. *DIMACS Series in Discrete Math. Theoret. Comput. Sci.* 39, 279–295.

Alexander A. Razborov. 1998. Lower bounds for the polynomial calculus. *Computat. Complex.* 7, 4, 291–324.

Alexander A. Razborov. 2003. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Manuscript available at author's webpage.*

John Alan Robinson. 1965. A machine-oriented logic based on the resolution principle. *J. ACM* 12, 1, 23–41.

Received June 2013; revised March 2014, August 2014, and November 2014; accepted November 2014