Space proof complexity for random 3-CNFs via a $(2 - \epsilon)$-Hall's Theorem

Ilario Bonacina[*]   Nicola Galesi[*]   Tony Huynh[*†]   Paul Wollan[*†]

November 6, 2014

Abstract

We investigate the space complexity of refuting 3-CNFs in Resolution and algebraic systems. No lower bound for refuting any family of 3-CNFs was previously known for the *total space* in resolution or for the *monomial space* in algebraic systems. Using the framework of [10], we prove that every *Polynomial Calculus with Resolution* refutation of a random 3-CNF φ in n variables requires, with high probability, $\Omega(n/\log n)$ *distinct monomials* to be kept simultaneously in memory. The same construction also proves that every *Resolution* refutation φ requires, with high probability, $\Omega(n/\log n)$ clauses each of width $\Omega(n/\log n)$ to be kept at the same time in memory. This gives a $\Omega(n^2/\log^2 n)$ lower bound for the *total space* needed in Resolution to refute φ. The results answer questions about space complexity of 3-CNFs posed in [16, 15, 11, 10].

The main technical innovation is a variant of *Hall's theorem*. We show that in bipartite graphs G with bipartition (L, R) and left-degree at most 3, L can be covered by certain families of disjoint paths, called $(2, 4)$-*matchings*, provided that L expands in R by a factor of $(2 - \epsilon)$, for $\epsilon < \frac{1}{23}$.

1 Introduction

During the last decade, an active line of research in proof complexity has been the space complexity of proofs and how space is related to other complexity measures (like size, length, width, degree) [14, 1, 6, 5, 3, 7, 18, 8, 16, 15, 11, 10]. This investigation has raised several important foundational questions. Some of these have been solved, while several others are still open and challenging (see [19] for a survey on this topic). Space of proofs concerns the minimal memory occupation of algorithms verifying the correctness of proofs in concrete propositional proof systems, and is thus also relevant in more applied algorithmic contexts. For instance, a major problem in state of the art SAT-solvers is memory consumption. In proof complexity, this resource is modeled by proof space. It is well-known that SAT-solvers used in practice (like CDCL) are based on low-level proof systems such as *Resolution*.

In this work we focus on two well known proof systems that play a central role in proof complexity: *Resolution* [20] and *Polynomial Calculus* [13]. Resolution (RES) is a refutational proof system for unsatisfiable propositional CNF formulas using only one logical rule: $\frac{A \vee x \quad \neg x \vee B}{A \vee B}$. Polynomial calculus is an algebraic refutational proof system for unsatisfiable sets of polynomials (over $\{0, 1\}$ solutions) based on two rules: *linear combination* of polynomials and *multiplication* by
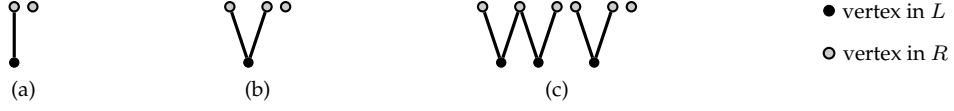
Figure 1: Comparison among (a) $(1,1)$-matchings, (b) $(2,2)$-matchings, (c) $(2,4)$-matchings

variables. In this article, we consider the stronger system *Polynomial Calculus with Resolution* (PCR) which extends both Resolution and Polynomial Calculus [1].

Several different measures for proof space were investigated for these two systems [14, 1, 5, 3, 7, 18, 8, 16, 11, 10]. In this work we focus on *total space* (for RES), which is the maximum number of variables (possibly repeated) to be kept simultaneously in memory while verifying a proof; and *monomial space* (for PCR), which is the maximum number of distinct monomials to be kept simultaneously in memory while verifying a proof. Both measures were introduced in [1], where some preliminary lower and upper bounds were given. However, major open problems about these two measures were solved only recently in [15, 10, 11]. In particular, in [10, 11] it was proved that, for $r \geq 4$, random r-CNFs over n variables require $\Theta(n^2)$ total space in resolution and $\Theta(n)$ monomial space in PCR.

It is an open problem whether there is any family of 3-CNFs requiring large *total space* (in RES) and *monomial space* (in PCR). In this work we solve this problem proving both *total space* (in RES) and *monomial space* (in PCR) lower bounds for the case of random 3-CNFs, a computationally hard class of formulas that are conjectured difficult to prove in very strong proof systems.

Results. Let φ be a random 3-CNF in n variables. We prove that every PCR refutation of φ requires, with high probability, $\Omega(\frac{n}{\log n})$ distinct monomials to be kept simultaneously in memory (Corollary 5.9). Moreover, every RES refutation of φ has, with high probability, $\Omega(\frac{n}{\log n})$ clauses each of width $\Omega(\frac{n}{\log n})$ to be kept at the same time in memory (Corollary 5.9). This gives a $\Omega(n^2 / \log^2 n)$ lower bound for the total space of every RES refutation of φ. These results resolve questions about space complexity of 3-CNFs mentioned in [15, 11, 10, 16].

Both results follow using the framework proposed in [10], where the construction of suitable families of assignments called *k-winning strategies* (Definition 5.1) leads to monomial space lower bounds in PCR (Theorem 5.2). This construction is made possible by a modification of Hall's theorem [17] for matchings to $(2,4)$-matchings. A $(2,4)$-*matching* in a bipartite graph with bipartition (L, R) is a collection of disjoint paths of length at most 4 with both endpoints in R. The notion of (h,k)-matching (Definition 3.1) is a generalization of the standard notion of matching. With this terminology a matching is a $(1,1)$-matching (see Figure 1.(a)), and a *2-matching* (as it is used in [11, 10]) is a $(2,2)$-matching (see Figure 1.(b)). Figure 1.(c) depicts a $(2,4)$-matching.

We can now state our variant of Hall's theorem.

Theorem 1.1 $((2-\epsilon)$-Hall's Theorem). *Let $\epsilon < \frac{1}{23}$. Let G be a bipartite graph with bipartition (L, R) such that the left-degree is at most 3 and for every subset A of L, $|N_G(A)| \geq (2-\epsilon)|A|$. Then there exists a $(2,4)$-matching covering L.*

This theorem and its proof are independent from the proof complexity results and might be usable in other contexts. Note that the converse of Theorem 1.1 does not hold (unlike in Hall's theorem). Hence, in order to apply it as a substitute for Hall's theorem, we had to prove a slightly stronger statement.

Theorem 1.2. *Let $\epsilon < \frac{1}{23}$. Let G be a bipartite graph with bipartition (L, R) such that each vertex in L has degree at most 3 and no pair of degree 3 vertices in L have the same set of neighbours. If $|N_G(L)| \geq$*

$(2 - \epsilon)|L|$, and each proper subset of L can be covered by a $(2, 4)$-matching, then L can be covered by a $(2, 4)$-matching.

Outline of the paper.   Section 2 contains some preliminary notions about proof complexity. In particular, we present the formal definitions of Resolution and Polynomial Calculus with Resolution, the model of space (based on [14, 1]) and the formal definition of total space and monomial space.

In Section 3, we define the notion of (h, k)-matchings (Definition 3.1) and present the proofs of Theorems 1.1 and 1.2 guaranteeing the existence of $(2, 4)$-matchings. The proof of the main theorem of Section 3 relies on a concentration result on the average right-degree and a discharging argument. We also prove a bound for the best possible value of ϵ for which Theorems 1.1 and 1.2 could hold and conjecture that this bound is in fact the optimal value of ϵ.

In Section 4, we define a two player covering game CoverGame, whose aim is to dynamically build a $(2, 4)$-matching inside a fixed bipartite graph G (Definition 4.3). Informally, a player, Choose, queries nodes in the graph G and the other player, Cover, attempts to extend the current $(2, 4)$-matching to also cover the node queried (if not already covered). The main result of Section 4 is Theorem 4.3, where we prove that if the graph G has large left-expansion (i.e. large enough to apply Theorem 1.2 to sufficiently large subgraphs of G), then there is a winning strategy for Cover to force Choose to query a very large portion of the graph G. In the analysis of the game, we use the $(2 - \epsilon)$-Hall's Theorem and $(2, 4)$-matchings in a similar manner to how $(1, 1)$-matchings and $(2, 2)$-matchings were used in RES and PCR [6, 2, 11, 10].

In Section 5, we present a simplified (but less general) version of the k-winning strategies of [10] (Definition 5.1). These k-winning strategies were used in [10] to prove monomial space lower bounds for PCR. We recall the definition of *r-free family* (Definition 5.3), used in [11] to prove total space lower bounds in RES (Theorem 5.4). We then show that the existence of a k-winning strategy for a formula φ implies the existence of $(k-1)$-free families of assignments for the formula φ (Lemma 5.5)[1]. We prove (Theorem 5.7) that if Cover wins CoverGame on the adjacency graph of a CNF φ (see Section 2 for the definition) guaranteeing $(2, 4)$-matchings of maximal size μ, then there exists a μ-winning strategy for the polynomial encoding of φ. Finally, the monomial space in PCR and the total space in RES for random 3-CNFs (Corollary 5.9) follow from well-known results about expansion of its adjacency graph [12, 4, 9, 6].

2   Preliminaries

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: $C = (\ell_1 \vee \ldots \vee \ell_k)$. The **width** of a clause is the number of literals in it. A formula φ is in *Conjunctive Normal Form* (CNF) if $\varphi = C_1 \wedge \ldots \wedge C_m$ where C_i are clauses. It is a k-CNF if each C_i contains at most k literals. Let φ be a CNF and X be the set of variables appearing in φ. The *adjacency graph of* φ is a bipartite graph G_φ with bipartition (L, R) such that L is the set of clauses of φ, $R = X$, and $(C, x) \in E$ if and only if x or $\neg x$ appears in C. If φ is a k-CNF, then G_φ has left-degree at most k.

We define $\overline{X} = \{\bar{x} : x \in X\}$, which we regard as a set of formal variables with the intended meaning of $\bar{x}$ as $\neg x$. Given a field $\mathbb{F}$, the ring $\mathbb{F}[X, \overline{X}]$ is the ring of polynomials in the variables $X \cup \overline{X}$ with coefficients in $\mathbb{F}$. Following [1], we use the following *standard encoding (tr)* of CNF formulas over X into a set of polynomials in $\mathbb{F}[X, \overline{X}]$: $tr(\varphi) = \{tr(C) : C \in \varphi\} \cup \{x^2 - x, x + \bar{x} - 1 :$

---

[1] Notice that this lemma is not proving a reduction of the notion of r-free families to the full general version of k-winning strategies in [10].

$x \in X\}$, where

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

A set of polynomials P in $\mathbb{F}[X]$ is **contradictory** if and only if 1 is in the ideal generated by P. Notice that a CNF φ is unsatisfiable if and only if $tr(\varphi)$ is a contradictory set of polynomials.

Resolution (RES) [20] is a propositional proof system for refuting unsatisfiable CNFs. Starting from an unsatisfiable CNF φ, RES allows us to derive the empty clause $\bot$ using the following inference rule:

$$\frac{C \vee x \quad D \vee \neg x}{C \vee D}.$$

In order to study space of proofs we follow a model 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 [14].

Given an unsatisfiable CNF formula φ, a RES **refutation** of φ is a sequence $\Pi = \langle \mathfrak{M}_0, \ldots, \mathfrak{M}_\ell \rangle$ of sets of clauses, called **memory configurations**, such that: $\mathfrak{M}_0 = \emptyset$, $\bot \in \mathfrak{M}_\ell$, and for all $i \leq \ell$, $\mathfrak{M}_i$ is obtained by $\mathfrak{M}_{i-1}$ by applying one of the following rules:

  (AXIOM DOWNLOAD) $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{C\}$, where C is a clause of φ;
  (INFERENCE ADDING) $\mathfrak{M}_i = \mathfrak{M}_{i-1} \cup \{C \vee D\}$, where $C \vee x, D \vee \neg x \in \mathfrak{M}_{i-1}$, for some variable x;
  (ERASURE) $\mathfrak{M}_i \subset \mathfrak{M}_{i-1}$.

The **total space** of Π is the maximum over i of the number of literals (counted with repetitions) occurring in $\mathfrak{M}_i$.

Polynomial Calculus with Resolution (PCR) [1] is an algebraic proof system for polynomials in $\mathbb{F}[X, \overline{X}]$. Starting from an initial set of contradictory polynomials P in $\mathbb{F}[X, \overline{X}]$, PCR allows us to derive the polynomial 1 using the following inference rules: for all $p, q \in \mathbb{F}[X, \overline{X}]$

$$\frac{p \qquad q}{\alpha p + \beta q} \forall \alpha, \beta \in \mathbb{F}, \qquad\qquad \frac{p}{vp} \forall v \in X \cup \overline{X}.$$

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

Given a set of contradictory polynomials P, a PCR **refutation** of P is a sequence $\langle \mathfrak{M}_0, \ldots, \mathfrak{M}_\ell \rangle$ of sets of polynomials, called **memory configurations**, such that: $\mathfrak{M}_0 = \emptyset$, $1 \in \mathfrak{M}_\ell$, and for all $i \leq \ell$, $\mathfrak{M}_i$ 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 PCR;
  (ERASURE) $\mathfrak{M}_i \subset \mathfrak{M}_{i-1}$.

The **monomial space** of Π, denoted by $\mathrm{MSpace}(\Pi)$, is the maximum over i of the number of distinct monomials appearing in $\mathfrak{M}_i$.

If in the definition of PCR refutation we substitute the INFERENCE ADDING rule with:

  (SEMANTICAL INFERENCE) $\mathfrak{M}_i$ is contained in the ideal generated by $\mathfrak{M}_{i-1}$,

we have what is called a **semantical** PCR **refutation** of P [1].

2.1 Partial assignments

A *partial assignment* over a set of variables X is a map $\alpha : X \longrightarrow \{0, 1, \star\}$. The *domain* of α is $\mathrm{dom}(\alpha) = \alpha^{-1}(\{0, 1\})$. We denote the partial assignment with empty domain as λ. Given a partial assignment α and a CNF φ we can apply α to φ, obtaining a new formula $\alpha(\varphi)$ in the standard way, substituting each variable x of φ in $\mathrm{dom}(\alpha)$ with the value $\alpha(x)$ and then simplifying the result. We say that α *satisfies* φ, and we write $\alpha \models \varphi$, if $\alpha(\varphi) = 1$. Similarly, for a family F of partial assignments, $F \models \varphi$ means that for each $\alpha \in F$, $\alpha \models \varphi$.

For each partial assignment α over $X \cup \overline{X}$ we assume that it respects 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 an assignment α and a polynomial p in $\mathbb{F}[X, \overline{X}]$, we can apply α to p, obtaining a new polynomial $\alpha(p)$ in the standard way, substituting each variable x of p in $\mathrm{dom}(\alpha)$ with the value $\alpha(x)$ and then simplifying the result. The notation $\alpha \models p$ means that $\alpha(p) = 0$. If F is a family of partial assignments and P a set of polynomials, we write $F \models P$ if $\alpha \models p$ for each $\alpha \in F$ and $p \in P$. Notice that if φ is a CNF and α is a partial assignment then $\alpha \models \varphi$ if and only if $\alpha(tr(\varphi)) = 0$.

3 A $(2 - \epsilon)$-Hall's Theorem

We begin with the definition of (h, k)-matching.

Definition 3.1 ((h, k)-matching). *Let $k \geq h$ be positive integers and G a bipartite graph with bipartition (L, R). An (h, k)-matching in G is a subgraph F of G such that*

1. *each connected component of F is a tree with at most k edges;*

2. *each vertex in $V(F) \cap L$ has degree exactly h in F.*

An (h, k)-matching F covers a set of vertices S if $S \subseteq V(F)$. Define $\ell(F) = V(F) \cap L$ and $r(F) = V(F) \cap R$.

We now proceed with the proof of Theorem 1.2; we will see afterwards that Theorem 1.1 follows easily.

Restated Theorem 1.2. *Let $\epsilon < \frac{1}{23}$. Let G be a bipartite graph with bipartition (L, R) such that each vertex in L has degree at most 3 and no pair of degree 3 vertices in L have the same set of neighbours. If $|N_G(L)| \geq (2 - \epsilon)|L|$, and each proper subset of L can be covered by a $(2, 4)$-matching, then L can be covered by a $(2, 4)$-matching.*

Proof. Define the hypergraph $\mathcal{H} = (V, E)$ with $V = N_G(L)$ and $E = \{N_G(x) : x \in L\}$. Observe that each vertex v in L has degree 2 or 3, otherwise v could not be covered by a $(2, 4)$-matching. Similarly, no degree 2 vertices in L have the same neighbourhood. By assumption, no degree 3 vertices have the same neighbourhood. Therefore, $N_G : L \to E$ is a bijection and $|V| \geq (2-\epsilon)|L| = (2 - \epsilon)|E|$. Recall that the degree of a vertex v in $\mathcal{H}$ is the number of distinct edges which contain v.

Let $L' \subseteq L$ and let $E' = \{N_G(x) : x \in L'\}$. The existence of a $(2, 4)$-matching in G covering $L' \subseteq L$ is equivalent to the existence of an injective function $f : E' \to \{\{x, y\} : x, y \in N_G(L')\}$ such that for every $e \in E'$, $f(e) \subseteq \binom{e}{2}$ and for each triple of distinct hyperedges $e_1, e_2, e_3 \in E'$, it is not the case that $f(e_1)$ intersects $f(e_2)$ and $f(e_2)$ intersects $f(e_3)$. We call a function f with these properties a 2-*path cover* of E' in $\mathcal{H}$.

Observe that all the configurations of hyperedges shown in Figure 2 have a 2-path cover using only degree 1 and 2 vertices of $\mathcal{H}$. If any of these configurations appear in $\mathcal{H}$, we can by assumption find a 2-path cover f of the remaining hyperedges, and then extend f to a 2-path cover of $\mathcal{H}$. Therefore, we may assume that no configuration from Figure 2 appears in $\mathcal{H}$.
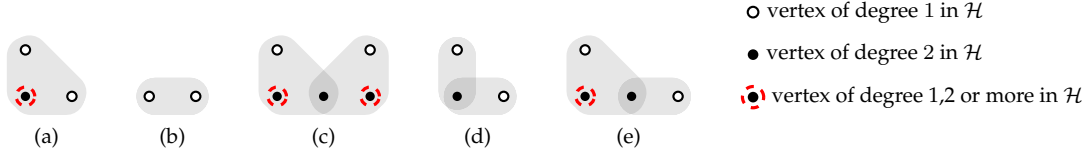
Figure 2: A set of reducible configurations for $\mathcal{H}$

Let d be the average degree in $\mathcal{H}$. Observe that

$$3|E| \geq \sum_{v \in V} \deg_{\mathcal{H}}(v) = d|V| \geq d(2 - \epsilon)|E|,$$

where the last inequality follows from the hypothesis that $|V| \geq (2 - \epsilon)|E|$. Thus, $d \leq \frac{3}{2-\epsilon}$.

Let D be the set of vertices of $\mathcal{H}$ of degree 1, and $\mathcal{D}$ be the set of hyperedges which contain a vertex in D. Note that $|D| = |\mathcal{D}|$, since the configurations (a), (b) of Figure 2 do not appear in $\mathcal{H}$. We now prove a concentration result for $|D|$. An upper bound follows immediately from the following chain of inequalities

$$|D| = |\mathcal{D}| \leq |E| \leq \frac{1}{2-\epsilon}|V|.$$

For the lower bound suppose $\frac{1-2\epsilon}{2-\epsilon}|V| > |D|$. Then,

$$\frac{3}{2-\epsilon}|V| \geq d|V| = \sum_{v \in D} \deg_{\mathcal{H}}(v) + \sum_{v \in V \setminus D} \deg_{\mathcal{H}}(v)$$

$$\geq |D| + 2|V \setminus D| > \frac{1-2\epsilon}{2-\epsilon}|V| + 2(1 - \frac{1-2\epsilon}{2-\epsilon})|V| = \frac{3}{2-\epsilon}|V|,$$

which is a contradiction. Hence we have that $\frac{1-2\epsilon}{2-\epsilon}|V| \leq |D| \leq \frac{1}{2-\epsilon}|V|$.

We finish the proof with a discharging argument. Each vertex v of $\mathcal{H}$ receives a charge of $\deg_{\mathcal{H}}(v)$. Let E_2 be the set of hyperedges in E of size 2 and $\mathcal{D}_2$ be $\mathcal{D} \cap E_2$. Clearly $|\mathcal{D}_2| \leq |E_2|$. The edges in $\mathcal{D}_2$ receive a charge of -2, the edges in $\mathcal{D} \setminus \mathcal{D}_2$ receive charge -3. The edges not in $\mathcal{D}$ receive no charge.

We now perform the following discharging rule. Each hyperedge e in $\mathcal{D}$ gives a charge of -1 to each vertex in e. After discharging, every hyperedge has charge 0, and every vertex has non-negative charge. Let Z be the set of vertices with charge 0 after discharging. Observe that a vertex x is in Z if and only if every hyperedge containing x also contains a degree 1 vertex.

Let C denote the total charge. Then,

$$C = 3|E| - |E_2| - 3|\mathcal{D}| + |\mathcal{D}_2| \leq 3|E| - 3|D| \leq \frac{3}{2-\epsilon}|V| - 3\frac{1-2\epsilon}{2-\epsilon}|V| = \frac{6\epsilon}{2-\epsilon}|V|.$$

It follows that $|Z| \geq \frac{2-7\epsilon}{2-\epsilon}|V|$. Since $D \subseteq Z$ and $|D| \leq \frac{|V|}{2-\epsilon}$, we conclude that $|Z \setminus D| \geq \frac{1-7\epsilon}{2-\epsilon}|V|$. Because the configurations $(c), (d), (e)$ of Figure 2 do not appear in $\mathcal{H}$, every vertex in $Z \setminus D$ has degree at least 3. Thus,

$$\frac{3}{2-\epsilon}|V| \geq d|V| \geq \sum_{v \in D} \deg_{\mathcal{H}}(v) + \sum_{v \in Z \setminus D} \deg_{\mathcal{H}}(v) \geq |D| + 3|Z \setminus D|$$

$$\geq \frac{1-2\epsilon}{2-\epsilon}|V| + 3\frac{1-7\epsilon}{2-\epsilon}|V| = \frac{4-23\epsilon}{2-\epsilon}|V|.$$

Therefore, $3 \geq 4 - 23\epsilon$, which is a contradiction as $\epsilon < \frac{1}{23}$. $\qquad\square$

We now quickly derive Theorem 1.1.

Restated Theorem 1.1 (($2-\epsilon$)-Hall's Theorem). *Let $\epsilon < \frac{1}{23}$. Let G be a bipartite graph with bipartition (L, R) such that the left-degree is at most 3 and for every subset A of L, $|N_G(A)| \geq (2-\epsilon)|A|$. Then there exists a $(2, 4)$-matching covering L.*

Proof. Assume the theorem is false, and pick a counterexample G with $|V(G)|$ minimum. For every proper subset $L' \subseteq L$, the subgraph of G induced by L' and $N_G(L')$ has a $(2, 4)$-matching covering L' by the minimality of G. But now, Theorem 1.2 implies that there is a $(2, 4)$-matching covering L, and so G is not a counterexample. $\square$

We end this section with a comment on the parameter ϵ.

Theorem 3.2. *For all $\epsilon > \frac{1}{3}$ there exists a bipartite graph G_ϵ with bipartition (L, R) such that each vertex in L has degree at most 3 and no pair of degree 3 vertices in L have the same set of neighbours. Moreover, $|N_{G_\epsilon}(L)| \geq (2-\epsilon)|L|$ and each proper subset of L can be covered by a $(2, 4)$-matching but L cannot be covered by a $(2, 4)$-matching.*

We conjecture that Theorem 1.2 is true for $\epsilon \leq \frac{1}{3}$. Theorem 3.2 shows that this would be best possible.

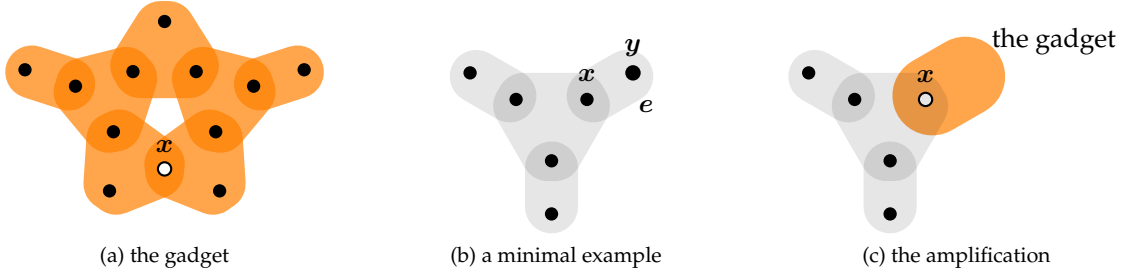We now prove Theorem 3.2, here rephrased in terms of hypergraphs.

(a) the gadget   (b) a minimal example   (c) the amplification

Figure 3: The construction

Theorem 3.3. *For every $\epsilon > \frac{1}{3}$, there exists a hypergraph $\mathcal{H}_\epsilon$ such that $\mathcal{H}_\epsilon$ has no isolated vertices, each hyperedge of $\mathcal{H}_\epsilon$ has size 2 or 3, $|V(\mathcal{H})| \geq (2-\epsilon)|E(\mathcal{H})|$, every proper subset of $E(\mathcal{H}_\epsilon)$ has a 2-path cover, but $\mathcal{H}_\epsilon$ does not have a 2-path cover.*

Proof. Let $\epsilon > \frac{1}{3}$ and consider the gadget $\mathcal{G}$ shown in Figure 3.(a). It is easy to verify that every 2-path cover of $\mathcal{G}$ must cover the vertex x. Next note that the hypergraph $\mathcal{H}$ shown in Figure 3.(b) is obviously not 2-path coverable, but every proper subset of $E(\mathcal{H})$ is 2-path coverable. We have $\frac{|V(\mathcal{H})|}{|E(\mathcal{H})|} = \frac{6}{4}$. However, we can increase this ratio via the amplification trick shown in Figure 3.(c).

That is, let e be a hyperedge of $\mathcal{H}$ of size 2. Label the vertices of e as x and y, where y has degree 1. Let $\mathcal{H}_1$ be the hypergraph obtained from $\mathcal{H}$ by deleting y and then gluing $\mathcal{G}$ to $\mathcal{H} - y$ along x. Since every 2-path cover of $\mathcal{G}$ must use the vertex x, $\mathcal{H}_1$ does not have a 2-path cover. On the other hand, since every proper subset of $E(\mathcal{G})$ has a 2-path cover avoiding x, it follows that every proper subset of $E(\mathcal{H}_1)$ has a 2-path cover. Note that this amplification trick increases the number of vertices of $\mathcal{H}$ by 10 and the number of edges of $\mathcal{H}$ by 6. Moreover, we can repeat this amplification trick arbitrarily many times since $\mathcal{G}$ also has pendent edges of size 2. So, choose n such that $\frac{6+10n}{4+6n} \geq 2 - \epsilon$ and take $\mathcal{H}_\epsilon$ to be the graph obtained from $\mathcal{H}$ by performing the amplification trick n times. $\square$

4 A cover game over bipartite graphs

As an application, we use the previous result to build a winning strategy for a game played on bipartite graphs.

Definition 4.1 (Cover Game). *The **Cover Game** $\mathsf{CoverGame}_{(h,k)}(G,\mu)$ is a game between two players, Choose and Cover, on a bipartite graph G. At each step i of the game the players maintain an (h,k)-matching F_i in G. At step $i+1$ Choose can*

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 and challenge Cover to find another (h,k)-matching F_{i+1} in G such that*

   (a) *F_{i+1} extends F_i. That is, 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 $\mathsf{CoverGame}_{(h,k)}(G,\mu)$ if at some point she cannot answer a challenge by Choose. Otherwise, Cover wins.*

Definition 4.2 ((s,δ)-bipartite expander). *Let s be a positive integer and δ be a positive real number. A bipartite graph G with bipartition (L,R) is an $(\boldsymbol{s,\delta})$-**bipartite expander** if all subsets $X \subseteq L$ of size at most s satisfy $|N_G(X)| \geq \delta|X|$.*

The next theorem shows that Cover has a winning strategy for the game $\mathsf{CoverGame}_{(2,4)}(G,\mu)$ for expander graphs G with appropriately chosen parameters.

Theorem 4.3. *Let G be a bipartite graph with bipartition (L,R), s,d be two integers, and $\epsilon < \frac{1}{23}$ be a real number. If each vertex in L has degree 3, each vertex in R has degree at most d, and G is an $(s, 2 - \frac{\epsilon}{2})$-bipartite expander, then Cover wins the cover game $\mathsf{CoverGame}_{(2,4)}(G,\mu)$ with $\mu = \frac{\epsilon s}{72d+2\epsilon} - d$.*

The proof of this result is similar to constructions that can be found for example in [6, 2, 11]. The proof we give is modeled following [11]. The main difference is the use of our variant of Hall's Theorem (Theorem 1.1), suitable for bipartite graphs of left-degree at most 3.

For the rest of this section, fix a bipartite graph G with bipartition (L,R), integers s,d and a real number $\epsilon < \frac{1}{23}$ such that G is an $(s, 2 - \frac{\epsilon}{2})$-expander, each vertex in L has degree 3 and each vertex in R has degree at most d.

Given $A \subseteq L$ and $B \subseteq R$, we denote with $G_{A,B}$ the subgraph of G induced by $(L \cup R) \setminus (A \cup B)$.

Definition 4.4 (robust). *Given two sets $A \subseteq L$ and $B \subseteq R$, we say that the pair (A,B) is **robust**, if for every $C \subseteq L \setminus A$ with $|A| + |C| \leq s$, there exists a $(2,4)$-matching F in $G_{A,B}$ covering C.*

Lemma 4.5. *The pair $(\emptyset, \emptyset)$ is robust.*

Proof. This follows from Theorem 1.1 since G is an $(s, 2 - \frac{\epsilon}{2})$-expander. $\qquad\square$

Lemma 4.6. *Let $A \subseteq L$ and $B \subseteq R$ be such that the pair (A,B) is not robust. Then there exists a set $C \subseteq L \setminus A$ such that no $(2,4)$-matching in $G_{A,B}$ covers C and $|C| < \frac{2}{\epsilon}|B|$.*

Proof. Take $C \subseteq L \setminus A$ of minimal size such that no $(2,4)$-matching in $G_{A,B}$ covers C. By minimality of C and Theorem 1.2 it follows that

$$|N_{G_{A,B}}(C)| < (2 - \epsilon)|C|.$$

But, by hypothesis on G, $(2 - \frac{\epsilon}{2})|C| \leq |N_G(C)|$. Therefore,

$$(2 - \frac{\epsilon}{2})|C| \leq |N_G(C)| \leq |N_{G_{A,B}}(C)| + |B| < (2 - \epsilon)|C| + |B|.$$

Hence $|C| < \frac{2}{\epsilon}|B|$, as required. $\qquad\square$

Lemma 4.7 (component removal). *Let $A \subseteq L$ and $B \subseteq R$ be such that the pair (A, B) is robust and $\frac{2}{\epsilon}|B| + |A| \leq s$. Then for each $(2, 4)$-matching F over the vertices $A \cup B$, $(A \setminus \ell(F), B \setminus r(F))$ is robust.*

Proof. Let $A' = A \setminus \ell(F)$ and $B' = B \setminus r(F)$ and suppose, by contradiction, that (A', B') is not robust. By Lemma 4.6, it is sufficient to prove that for each set $C \subseteq L \setminus A'$ with $|C| < \frac{2}{\epsilon}|B'|$, there is a $(2, 4)$-matching in $G_{A',B'}$ covering C. Let $C' = C \cap \ell(F)$ and $C'' = C \setminus C'$. By construction, F is a $(2, 4)$-matching such that $\ell(F) \subseteq A$, $r(F) \subseteq B$ and F covers C'. Moreover, we have that

$$|C''| + |A| \leq |C| + |A| < \frac{2}{\epsilon}|B'| + |A| < \frac{2}{\epsilon}|B| + |A| \overset{(\star)}{\leq} s,$$

where the inequality $(\star)$ is by hypothesis. Hence there exists a $(2, 4)$-matching F'' of C'' in $G_{A,B}$, and so $F \cup F''$ is a $(2, 4)$-matching covering C in $G_{A',B'}$. $\qquad\square$

Lemma 4.8 (left vertex-covering). *Let $A \subseteq L$ and $B \subseteq R$ be such that the pair (A, B) is robust and $\frac{24d}{\epsilon}(|B| + 3) + |A| + 1 \leq s$. Then for each vertex v in $L \setminus A$, there is a $(2, 4)$-matching F in $G_{A,B}$ covering v and such that $(A \cup \ell(F), B \cup r(F))$ is robust.*

Proof. Fix $v \in L \setminus A$ and let Π be the set of all $(2, 4)$-matchings F in $G_{A,B}$, covering v and such that F is connected.

Since $|A| + 1 \leq s$ and (A, B) is robust, we know that Π is non-empty. For every $F \in \Pi$, let (A_F, B_F) be the pair $(A \cup \ell(F), B \cup r(F))$, and suppose for a contradiction that for every $F \in \Pi$, (A_F, B_F) is not robust. By Lemma 4.6, for every $F \in \Pi$ there is a set $C_F \subseteq L \setminus A_F$ with $|C_F| < \frac{2}{\epsilon}|B_F|$ and such that there is no $(2, 4)$-matching of C_F in G_{A_F,B_F}.

Let $C = \bigcup_{F \in \Pi} C_F$. Then $|C| < \frac{24d}{\epsilon}(|B|+3)$, since $|\Pi| \leq 3 + 3 \cdot 2 \cdot (d-1) \cdot 2 \leq 12d$ and $|r(F)| \leq 3$. Hence, by our assumption about the sizes of $|A|$ and $|B|$, we have that $|C \cup \{v\}| + |A| \leq s$. Furthermore, $C \cup \{v\} \subseteq L \setminus A$, so by the fact that (A, B) is robust, there is a $(2, 4)$-matching F' covering $C \cup \{v\}$ in $G_{A,B}$.

There must be some $F \in \Pi$ such that F is a connected component of F'. Let F'' be F' with the component F removed. Then F'' is a $(2, 4)$-matching in G_{A_F,B_F} and F'' covers C_F, contradicting the choice of C_F. $\qquad\square$

Lemma 4.9 (right vertex-covering). *Let $A \subseteq L$ and $B \subseteq R$ be such that the pair (A, B) is robust and $\frac{24d}{\epsilon}(|B| + 3d) + |A| + 2d \leq s$. Then for each vertex v in $R \setminus B$, there is a $(2, 4)$-matching F in $G_{A,B}$ covering v and such that $(A \cup \ell(F), B \cup r(F))$ is robust.*

Proof. Fix $v \in R \setminus B$ and let D be $N_G(v) \setminus A$. By hypothesis $|D| \leq d$ and, by the cardinality constraints on A and B, we can apply Lemma 4.8 $|D|$ times obtaining a $(2, 4)$-matching F in $G_{A,B}$ covering D and such that $(A \cup \ell(F), B \cup r(F))$ is robust. Now, since $N_G(v) \subseteq A \cup \ell(F)$, we have that $(A \cup \ell(F), B \cup r(F) \cup \{v\})$ is robust. Either v is covered by F, or it is possible to add $\{v\}$ as a new connected component to F while still maintaining the property of being a $(2, 4)$-matching in $G_{A,B}$. $\qquad\square$

Proof of Theorem 4.3. We now use the previous lemmas to describe a winning strategy $\mathscr{L}$ for Cover to win $\mathsf{CoverGame}_{(2,4)}(G, \mu)$. Take $\mathscr{L}$ to be the set of all $(2, 4)$-matchings F in G such that

1. $(\ell(F), r(F))$ is robust, and

2. $\frac{2}{\epsilon}|r(F)| + |\ell(F)| \le s$.

This family is non-empty by Lemma 4.5 and is closed under removing connected components by Lemma 4.7. Suppose now that at step $i+1$ of the game Choose picks a vertex v in G and that F_i has strictly less than $\mu = \frac{\epsilon s}{72d + 2\epsilon} - d$ components. Then, $(\ell(F_i), r(F_i))$ satisfies the hypotheses of Lemma 4.8 and Lemma 4.9:

$$\frac{24d}{\epsilon}(|r(F_i)| + 3d) + |\ell(F_i)| + 2d \le \frac{24d}{\epsilon}(3\mu + 3d) + 2\mu + 2d = (\mu + d)(\frac{72d}{\epsilon} + 2) =$$
$$= (\frac{\epsilon s}{72d + 2\epsilon})(\frac{72d}{\epsilon} + 2) = s.$$

Hence by Lemma 4.8 and Lemma 4.9, there exists a $(2, 4)$-matching F_{i+1} extending F_i and covering v such that $(\ell(F_{i+1}), r(F_{i+1}))$ is robust. From the previous chain of inequalities, it follows easily that the pair $(\ell(F_{i+1}), r(F_{i+1}))$ satisfies the cardinality condition $\frac{2}{\epsilon}|r(F_{i+1})| + |\ell(F_{i+1})| \le s$. $\square$

5 Space lower bounds for random 3-CNFs in RES and PCR

To prove a space lower bound for random 3-CNFs, we use the techniques developed in [10, 11]. Using the Cover Game on $(2, 4)$-matchings, we provide families of assignments that define k-*winning strategies* (for the monomial space in PCR) [10] and r-*free families* (for the total space in Resolution) [11]. We start with some preliminaries, and then prove that k-*winning strategies* alone are sufficient. Finally, we prove the main results, which together with the main Theorem in [11] will imply the two results on space bounds.

5.1 Flippable assignments from $(2, 4)$-matchings

Let A be a family of partial assignments, and let $\operatorname{dom}(A)$ be the union of the domains of the assignments in A. We say that a set of partial assignments A is **flippable** if and only if for all $x \in \operatorname{dom}(A)$ there exist $\alpha, \beta \in A$ such that $\alpha(x) = 1 - \beta(x)$. Two families of partial assignments A and A' are **domain-disjoint** if $\operatorname{dom}(\alpha)$ and $\operatorname{dom}(\alpha')$ are disjoint for all $\alpha \in A$ and $\alpha' \in A'$. Given non-empty and pairwise domain-disjoint sets of assignments[2] $H_1, \ldots, H_t$, the **product-family** $\mathcal{H} = H_1 \otimes \ldots \otimes H_t$ is the following set of assignments

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

or, if $t = 0$, $\mathcal{H} = \{\lambda\}$, where λ is the partial assignment of the empty domain. Note $\operatorname{dom}(\mathcal{H}) = \bigcup_i \operatorname{dom}(H_i)$. We call the H_i the **factors** of $\mathcal{H}$. For a product-family $\mathcal{H} = H_1 \otimes \ldots \otimes H_t$, the **rank** of $\mathcal{H}$, denoted $\|\mathcal{H}\|$, 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 every $\mathcal{H}$.

A family of flippable product-families is called a **strategy** and denoted by $\mathscr{L}$. We now present a definition of suitable families of flippable products: the k-*winning strategies* [10][3].

Definition 5.1 (k-winning strategy [10]). *Let P be a set of polynomials in the ring $\mathbb{F}[X, \overline{X}]$. A non-empty strategy $\mathscr{L}$ is a **k-winning strategy** if and only if for every $\mathcal{H} \in \mathscr{L}$ the following conditions hold:*

---

[2]We always suppose that the partial assignments are respecting the intended meaning of the variables in $\overline{X}$. That is, if $x \in \operatorname{dom}(\alpha)$, then $\alpha(\bar{x}) = 1 - \alpha(x)$; hence a variable x is in $\operatorname{dom}(H_i)$ if and only if $\bar{x}$ is in $\operatorname{dom}(H_i)$.

[3]This definition correspond to a particular case of the definition of k-*winning strategy* in the [10]. In [10] the definition of k-winning strategy depend on the choice of some particular proper ideal I in $\mathbb{F}[X, \overline{X}]$. Here we just state the simplified case where $I = \{0\}$.

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

(EXTENSION) *if $\|\mathcal{H}\| < k$, then for each $p \in P$ there exists a flippable product-family $\mathcal{H}' \in \mathscr{L}$ such that $\mathcal{H}' \sqsupseteq \mathcal{H}$ and $\mathcal{H}' \models p$.*

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

Theorem 5.2 ([10]). *Let P be a contradictory set of polynomials in $\mathbb{F}[X, \overline{X}]$ and $k \geq 1$ an integer. If there exists a non-empty k-winning strategy $\mathscr{L}$ for P, then for every semantical PCR refutation Π of P, $\mathrm{MSpace}(\Pi) \geq k/4$.*

5.2   Total space lower bounds via k-winning strategies

In this section we recall some definitions and theorems from [11] and we show that in order to prove total space lower bounds in RES it suffices to show the existence of k-winning strategies.

A *piecewise (p.w.) assignment* α of a set of variables X is a set of non-empty partial assignments to X with pairwise disjoint domains. We will sometimes call the elements of α the *pieces* of α. A piecewise assignment gives rise to a partial assignment $\bigcup \alpha$ to X together with a partition of the domain of $\bigcup \alpha$.

For piecewise assignments α, β we will write $\alpha \sqsubseteq \beta$ to mean that every piece of α appears in β. We will write $\|\alpha\|$ to mean the number of pieces in α. Note that these are formally exactly the same as $\alpha \subseteq \beta$ and $|\alpha|$, using the definition of α and β as sets.

Definition 5.3 (r-free [11]). *A non-empty family $\mathscr{F}$ of p.w. assignments is r-free for a CNF φ if it has the following properties.*

(CONSISTENCY) *No $\alpha \in \mathscr{F}$ falsifies any clause from φ.*

(RETRACTION) *If $\alpha \in \mathscr{F}$, β is a p.w. assignment and $\beta \sqsubseteq \alpha$, then $\beta \in \mathscr{F}$.*

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

Theorem 5.4 ([11]). *Let φ be an unsatisfiable CNF formula. If there is a family of p.w. assignments which is r-free for φ, then any resolution refutation of φ must pass through a memory configuration containing at least $r/2$ clauses each of width at least $r/2$. In particular, the refutation requires total space at least $r^2/4$.*

The next lemma establishes a connection between Definition 5.1 and Definition 5.3.

Lemma 5.5. *Let φ be an unsatisfiable CNF and let $P_\varphi = tr(\varphi)$ be the standard polynomial encoding of φ. If there exists a k-winning strategy for P_φ, then there exists a $(k-1)$-free family for φ.*

Proof. Let $\mathscr{L}$ be the k-winning strategy. Define the $(k-1)$-free family $\mathscr{F}$ as follows: $\alpha \in \mathscr{F}$ if and only if there exists $H_1 \otimes \ldots \otimes H_t \in \mathscr{L}$ such that $\alpha = \alpha_1 \cup \ldots \cup \alpha_t$ with $\alpha_i \in H_i$ and $t \leq k-1$. The p.w. structure of α is inherited from the domain-disjointness of $H_1 \otimes \ldots \otimes H_t$; in particular, $\|\alpha\| = \|H_1 \otimes \ldots \otimes H_t\|$. The *retraction property* of $\mathscr{F}$ is immediate from the corresponding property of $\mathscr{L}$.

To prove the *consistency property* of $\mathscr{F}$ assume, by contradiction, that there is an $\alpha \in \mathscr{F}$ such that α falsifies some clause $C \in \varphi$. Since $\|\alpha\| \leq k-1 < k$, there exists $\mathcal{H} = H_1 \otimes \ldots \otimes H_t \in \mathscr{L}$ such that $\alpha \in \mathcal{H}$ and $\|\alpha\| = \|\mathcal{H}\|$. By the extension property of $\mathscr{L}$, there is an $\mathcal{H}' \sqsupseteq \mathcal{H}$ such that $\mathcal{H}' \models tr(C)$. In particular there exists some partial assignment $\beta \supseteq \alpha$ such that $\beta \models tr(C)$. By construction, for every assignment γ, $\gamma \models tr(C)$ if and only if $\gamma \models C$. Thus $\beta \models C$, which is impossible since α falsifies C.
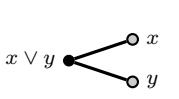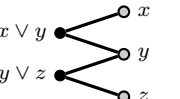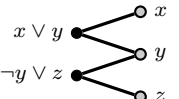
For the *extension property* let $\alpha \in \mathscr{F}$, with $\|\alpha\| < k-1$ and let x be a variable of φ not in $\mathrm{dom}(\alpha)$. By construction, there exists some $\mathcal{H} \in \mathscr{L}$ such that $\alpha \in \mathcal{H}$, $\|\alpha\| = \|\mathcal{H}\|$ and $\mathrm{dom}(\alpha) = \mathrm{dom}(\mathcal{H})$. By

the extension property of $\mathscr{F}$ there exists some flippable $\mathcal{H}' \in \mathscr{L}$ such that $\mathcal{H}' \sqsupseteq \mathcal{H}$ and $\mathcal{H}' \models x^2 - x$. By taking restrictions in $\mathscr{L}$ we can suppose that $\|\mathcal{H}'\| = \|\mathcal{H}\| + 1$. Hence there exist $\beta_0, \beta_1 \in \mathscr{F}$ extending α, setting x respectively to 0 and 1 and such that $\|\beta_0\| = \|\beta_1\| = \|\alpha\| + 1 \leq k - 1$. $\qquad\square$

To avoid confusion, we want to emphasize that this reduction from k-winning strategies to $(k-1)$-free families does not hold for the full general definition of k-winning strategies as in [10].

5.3 Space lower bounds via CoverGames on $(2,4)$-matchings

Table 1: From $(2,4)$-matchings to flippable assignments

x	$x \vee y \rightarrow x$, y	$x \vee y$, $y \vee z \rightarrow x$, y, z	$x \vee y$, $\neg y \vee z \rightarrow x$, y, z
$x \mapsto 0$	$(x,y) \mapsto (0,1)$	$(x,y,z) \mapsto (0,1,0)$	$(x,y,z) \mapsto (0,1,1)$
$x \mapsto 1$	$(x,y) \mapsto (1,0)$	$(x,y,z) \mapsto (1,0,1)$	$(x,y,z) \mapsto (1,0,0)$

Lemma 5.6. *Let φ be a CNF and G_φ be the adjacency graph of φ. For every $(2,4)$-matching F in G_φ, there exists a flippable product-family of assignments H_F such that $H_F \models \ell(F)$, $\mathrm{dom}(H_F) = r(F)$, and $\|H_F\|$ is the number of connected components of F.*

Proof. We prove the result by induction on the number of connected components of F. If F is the union of two disjoint $(2,4)$-matchings F', F'' then by hypothesis $H_{F'} \models \ell(F')$, $\mathrm{dom}(H_{F'}) = r(F')$ and $\|H_{F'}\|$ is the number of connected components of F'. And analogously for F''. Then, since $r(F')$ and $r(F'')$ are disjoint, $H_F = H_{F'} \otimes H_{F''}$ is well-defined. We immediately see that $H_F \models \ell(F)$, $\mathrm{dom}(H_F) = r(F)$ and $\|H_F\|$ is the number of connected components of F.

It remains to prove the case when the $(2,4)$-matching F is just one connected component. It is easy to see that all the possibilities can be reduced to those in Table 1. $\qquad\square$

Theorem 5.7. *Let φ be an unsatisfiable 3-CNF and G_φ its adjacency graph. If Cover wins the cover game $\mathsf{CoverGame}_{(2,4)}(G_\varphi, \mu)$, then there is a μ-winning strategy $\mathscr{L}$ for $tr(\varphi)$.*

Proof. It is straightforward to see that a winning strategy for Cover in $\mathsf{CoverGame}_{(2,4)}(G_\varphi, \mu)$ defines, using Lemma 5.6, a family $\mathscr{L}$ of flippable product-families such that for all $\mathcal{H} \in \mathscr{L}$

1. for each $\mathcal{H}' \sqsubseteq \mathcal{H}$, $\mathcal{H}' \in \mathscr{L}$;

2. if $\|\mathcal{H}\| < \mu$, then: (a) for each $C \in \varphi$, there exists a flippable product-family $\mathcal{H}' \in \mathscr{L}$ such that $\mathcal{H}' \models C$ and $\mathcal{H}' \sqsupseteq \mathcal{H}$; and (b) for each variable $x \notin \mathrm{dom}(\mathcal{H})$, there exists a flippable family $\mathcal{H}' \in \mathscr{L}$ such that $\mathcal{H}' \sqsupseteq \mathcal{H}$.

We claim that $\mathscr{L}$ is a μ-winning strategy. The *size property* and the *restriction property* are immediate. For the *extension property* we use the properties in (2) above: if we have to extend to something in $\mathscr{L}$ that satisfies a boolean axiom we use property 2.(b), otherwise for all other polynomials in $tr(\varphi)$ we use property 2.(a). $\qquad\square$

Corollary 5.8. *Let φ be an unsatisfiable 3-CNF and G_φ its adjacency graph. If Cover wins the cover game $\mathsf{CoverGame}_{(2,4)}(G_\varphi, \mu)$, then for every semantical PCR refutation Π of $tr(\varphi)$, $\mathrm{MSpace}(\Pi) \geq \mu/4$. Moreover, every RES refutation of φ must pass through a memory configuration containing at least $\mu/2$ clauses each of width at least $\mu/2$. In particular, the refutation requires total space at least $\mu^2/4$.*

Proof. The result follows from Theorem 5.7, Theorem 5.2, Lemma 5.5, and Theorem 5.4. $\qquad\square$

Let $n, \Delta \in \mathbb{N}$ and let $X = \{x_1, \ldots, x_n\}$ be a set of n variables. The probability distribution $\mathcal{R}(n, \Delta, 3)$ is obtained by the following experiment: choose independently uniformly at random Δn clauses from the set of all possible clauses with 3 literals over X. It is well-known that when Δ exceeds a certain constant θ_3, φ is almost surely unsatisfiable. Hence we always consider $\varphi \sim \mathcal{R}(n, \Delta, 3)$, where Δ is a constant bigger than θ_3, which implies that φ is unsatisfiable with high probability.

Corollary 5.9. *Let $\Delta > \theta_3$ and $\varphi \sim \mathcal{R}(n, \Delta, 3)$. Then with high probability, for every semantical* PCR *refutation Π of $tr(\varphi)$, $\mathrm{MSpace}(\Pi) \geq \Omega(n/\log n)$. Moreover, every* RES *refutation of φ must pass through a memory configuration containing $\Omega(n/\log n)$ clauses each of width $\Omega(n/\log n)$. In particular, each refutation of φ requires total space $\Omega(n^2/\log^2 n)$.*

Proof. Let G_φ be the adjacency graph of φ. By Chernoff's bound it follows that with high probability the right-degree of G_φ is at most $\log n$ and it is well known that G_φ is a $(\gamma n, 2 - \delta)$-bipartite expander, for every $\delta > 0$ [12, 4, 9, 6]. Hence in particular for $0 < \delta < \frac{1}{23}$, we can apply Theorem 4.3: Cover wins the cover game $\mathrm{CoverGame}_{(2,4)}(G_\varphi, \mu)$ for $\mu = \Omega(n/\log n)$. The result then follows using Corollary 5.8. $\qquad\square$

For every unsatisfiable CNF in n variables, there is a trivial $O(n)$ upper bound on monomial space in PCR and a trivial $O(n^2)$ upper bound on total space in RES. It is an open question whether our lower bounds are tight.

References

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

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

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

[4] Paul Beame and Toniann Pitassi. Simplified and improved resolution lower bounds. In *FOCS*, pages 274–282. IEEE Computer Society, 1996.

[5] Eli Ben-Sasson. Size space tradeoffs for resolution. In John H. Reif, editor, *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*, pages 457–464. ACM, 2002.

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

[7] Eli Ben-Sasson and Jakob Nordström. Short proofs may be spacious: An optimal separation of space and length in resolution. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 709–718. IEEE Computer Society, 2008.

[8] Eli Ben-Sasson and Jakob Nordström. Understanding space in proof complexity: Separations and trade-offs via substitutions. In Bernard Chazelle, editor, *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*, pages 401–416. Tsinghua University Press, 2011.

[9] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001.

[10] Ilario Bonacina and Nicola Galesi. A framework for space complexity in algebraic proof systems. *J. ACM*, to appear. Manuscript available at `http://wwwusers.di.uniroma1.it/~galesi/jacm.pdf`. A preliminary version appeared as: *Pseudo-partitions, transversality and locality: a combinatorial characterization for the space measure in algebraic proof systems*. In ITCS, pages 455–472, 2013.

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

[12] Vasek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988.

[13] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the groebner basis algorithm to find proofs of unsatisfiability. In Gary L. Miller, editor, *STOC*, pages 174–183. ACM, 1996.

[14] Juan Luis Esteban and Jacobo Torán. Space bounds for resolution. *Inf. Comput.*, 171(1):84–97, 2001.

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

[16] Yuval Filmus, Massimo Lauria, Jakob Nordström, Neil Thapen, and Noga Ron-Zewi. Space complexity in polynomial calculus. In *Proceedings of the 27th Conference on Computational Complexity, CCC 2012, Porto, Portugal, June 26-29, 2012*, pages 334–344. IEEE, 2012.

[17] P. Hall. On representatives of subsets. *Journal of the London Mathematical Society*, s1-10(1):26–30, 1935.

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

[19] Jakob Nordström. Pebble games, proof complexity, and time-space trade-offs. *Logical Methods in Computer Science*, 9(3), 2013.

[20] J. A. Robinson. A machine-oriented logic based on the resolution principle. *J. ACM*, 12(1):23–41, January 1965.