Electronic Colloquium on Computational Complexity, Report No. 38 (2014)

# Total space in resolution

Ilario Bonacina* Nicola Galesi* Neil Thapen†

March 21, 2014

**Abstract**

We show $\Omega(n^2)$ lower bounds on the total space used in resolution refutations of random $k$-CNFs over $n$ variables, and of the graph pigeonhole principle and the bit pigeonhole principle for $n$ holes. This answers the long-standing open problem of whether there are families of $k$-CNF formulas of size $O(n)$ requiring total space $\Omega(n^2)$ in resolution, and gives the first truly quadratic lower bounds on total space. The results follow from a more general theorem showing that, for formulas satisfying certain conditions, in every resolution refutation there is a memory configuration containing many clauses of large width.

## 1 Introduction

The most common questions in propositional proof complexity concern the *size* of proofs – as is well-known, NP=coNP if and only if there is a proof system in which every tautology has a polynomial size proof [11]. There is a natural analogy between the size of a proof and the size of a circuit, or the time taken by a Turing machine. Developing this analogy, [1, 10, 13] introduced a notion of the *space* used by a propositional proof, similar to the notion of space for Turing machines. Since then, space has been investigated in depth in proof complexity, especially for the resolution proof system [1,2,4–7,12,13,16–18] and more recently for polynomial calculus [9, 14, 15].

Resolution is a well-studied system for refuting formulas in conjunctive normal form (CNFs). Each line in a resolution refutation is a *clause*, that is, a disjunction of literals, and resolution has only one rule: from two clauses $A \vee x$ and $B \vee \neg x$ we may infer the clause $A \vee B$. A CNF is unsatisfiable if and only if the empty clause can be derived from it using this rule.

Intuitively, the space required by a refutation is the amount of information we need to keep simultaneously in memory as we work through the proof and

*Computer Science Department, Sapienza University of Rome, via Salaria 113, 00198 Rome, Italy, {bonacina, galesi}@di.uniroma.it.

†Institute of Mathematics, Academy of Sciences of the Czech Republic, Žitná 25, 115 67 Prague 1, Czech Republic, thapen@math.cas.cz. Research partially supported by the ERC project FEALORA, by grant IAA100190902 of GA AV ČR, and by the Center of Excellence CE-ITI under grant P202/12/G061 of GA ČR and RVO: 67985840.



ISSN 1433-8092

convince ourselves that the original CNF is unsatisfiable. This was made formal for resolution in [13] as follows. A *memory configuration*, or just *configuration*, is a set of clauses. We assume that a resolution refutation of $\varphi$ is given in the form of a sequence $M_1, \ldots, M_t$ of configurations, where $M_1$ is empty, $M_t$ contains the empty clause, and each $M_{i+1}$ is derived from $M_i$ in one of the following three ways:

**Axiom download:** $M_{i+1} = M_i \cup \{C\}$ where $C$ is a clause from $\varphi$

**Erasure:** $M_{i+1} \subseteq M_i$

**Inference:** $M_{i+1} = M_i \cup \{D\}$ where $D$ follows from two clauses in $M_i$ by the resolution rule.

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.

Following [1, 13] the *clause space* used by the refutation is the maximum number of clauses in any configuration $M_i$ in the sequence. The *total space* used is the maximum over $i$ of the total number of symbols needed to write down $M_i$. In other words, it is the total number of instances of variables occurring in $M_i$ (we ignore punctuation and logical connectives).[1]

Clause space and its relation with proof size are by now well-studied [2, 5–7, 17]. But much less is known about total space, despite it capturing more closely the intuitive idea of the memory required by a refutation.

As well as being of theoretical interest, total space is also directly relevant for SAT solving. Memory use is a major problem for SAT solvers and a current goal of research is to understand the resources of time and space in resolution proofs, how they are connected to each other and how they can be optimized in the design of new SAT solvers. Here we are interested in the real amount of memory (bit size) needed while verifying the refutation, so total space is a more useful measure than clause space.

Every unsatisfiable CNF $\varphi$ over $n$ variables can be refuted in resolution in clause space $n + 1$, which is the pebbling number of the brute-force treelike resolution refutation of $\varphi$ [13]. Since every clause in the refutation has width at most $n$, this gives an upper bound of $n(n + 1)$ on the total space of refuting $\varphi$ (where the *width* of a clause is the number of literals in it).

The only previously known lower bounds for total space, other than those following trivially from lower bounds on clause space, are from [1]. There it is shown that the *pigeon hole principle* $\mathrm{PHP}_n$, which is defined over $O(n^2)$ variables, can be refuted in $\Theta(n^2)$ total space. The proof relies on a formulation of $\mathrm{PHP}_n$ as a CNF with only wide clauses. A similar result is shown for the *complete tree* contradiction $\mathrm{CT}_n$, a CNF of exponential size defined by excluding all possible assignments to $n$ variables.

[1] In [1] this is called *variable space*, but we follow [5–7, 16, 17] in calling it *total space* to distinguish it from a different measure in which different occurrences of the same variable are not counted.

Improving these results for resolution has been a long-standing open problem, posed in many works in proof complexity in the last ten years [1,4–7,16,17]. We are able to solve this in essentially an optimal way, showing that some standard families of constant width CNF contradictions, defined over $n$ variables and hence of size $O(n)$, require $\Omega(n^2)$ total space. Our main result is:

**Theorem 1.1.** *Fix $k \geq 4$ and $\Delta > 1$. Then there is a constant $\lambda > 0$ such that for a random $k$-CNF formula $\varphi$ with $n$ variables and $\Delta n$ clauses, with exponentially high probability every resolution refutation of $\varphi$ requires total space $\lambda n^2$.*

We show similar lower bounds for some other CNFs. In particular:

**Theorem 1.2.** *Fix $k \geq 4$ and $\Delta > 1$. Then there is a constant $\lambda > 0$ such that for a random $\mathcal{G}$ chosen from the set of bipartite graphs with left-degree $d$ going from a set of $\Delta n$ pigeons to a set of $n$ holes, with exponentially high probability every resolution refutation of $\mathcal{G}$-PHP requires total space $\lambda n^2$.*

**Theorem 1.3.** *Every resolution refutation of the bit pigeonhole principle $\mathrm{BPHP}_n$ requires total space $n^2/16$.*

In each case we actually prove something stronger, that every refutation of the formula in question must pass through a configuration containing $r$ clauses each of width at least $r$, where $r = \Omega(n)$.

The random formulas and the instances of $\mathcal{G}$-PHP in Theorems 1.1 and 1.2 are $k$-CNFs with $O(n)$ variables, so in both cases our lower bound matches the quadratic upper bound on total space, up to a constant factor. The bit pigeonhole principle $\mathrm{BPHP}_n$ is a $(\log n)$-CNF with $(n+1)\log n$ variables, so our lower bound is only $\Omega(m^2/(\log m)^2)$ in terms of the number $m$ of variables (but the proof is much simpler than for the other two principles).

In the next section we prove a general theorem (Theorem 2.4) from which our results follow. We define the notion of an *$r$-free family* of assignments, and show that if a CNF has such a family then every resolution refutation of it has a configuration containing $r/2$ clauses each of width at least $r/2$.

In Section 3 we give two easy applications of this. One is the total space lower bound for $\mathrm{BPHP}_n$. The other is that from any constant-width CNF $F$ requiring large width to refute, we can construct a constant-width CNF $F[\oplus]$, the "xorification of $F$", which requires large total space to refute (Theorem 3.2). In particular, this gives us a lower bound for certain Tseitin formulas.

Section 4 is the only really technical part of the paper. We develop the main tools we will need for random $k$-CNFs and $\mathcal{G}$-PHP. These are certain families of substructures of bipartite graphs which we call *$r$-covering families*. We show that in a random bipartite graph such a family exists with high probability.

In Section 5 and 6 we use this to prove our total space lower bounds for random $k$-CNFs and $\mathcal{G}$-PHP.

In Section 7 we discuss *semantic resolution* [1]. We show that resolution can require much more total space than semantic resolution. We prove that if a CNF has an $r$-free family then it requires large total space in a weak version of semantic resolution, in which we can derive a new clause if it is implied by some set of $d$ clauses in memory, where $d$ is fixed (Theorem 7.1). We prove that every $r$-semiwide CNF requires large semantic total space (Theorem 7.3).

Almost all of our total space lower bounds are closely based on constructions used to prove lower bounds on monomial space in the system PCR (polynomial calculus resolution). The notions of an $r$-free family and an $r$-covering family, and their applications to random $k$-CNFs and $\mathcal{G}$-PHP, are inspired by [9]. The lower bound for the bit pigeonhole principle is modelled on [15] and the lower bound for xorifications on [14].

A natural question is whether these lower bounds can be extended to stronger proof systems such as bounded depth Frege, where very little is known about space, or PCR. For unrestricted Frege systems a linear upper bound (in the size of the CNF being refuted) on total space was shown in [1].

Finally, all of our lower bounds are for formulas which are already known to be hard for resolution, in that they have no subexponential size refutations. It is open whether there is a family of CNFs which have short refutations but which still require quadratic, or at least superlinear, total space. By a result of [8], if a CNF has a resolution refutation of size $S$ then it also has a refutation in which every clause has width at most $O(\sqrt{n \log S})$. Hence we cannot hope to use our arguments, which show large space by finding many clauses of large width.

## 2 Main theorem

**Definition 2.1.** *A* piecewise assignment *$\alpha$ to 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 $\alpha$ the *pieces* of $\alpha$. A piecewise assignment gives rise to a partial assignment $\bigcup \alpha$ to $X$ together with a partition of the domain of $\bigcup \alpha$. We could have defined a piecewise assignment in this way instead, as a pair of a partial assignment and a partition of its domain.

For piecewise assignments $\alpha, \beta$ we will write $\alpha \sqsubseteq \beta$ to mean that every piece of $\alpha$ appears in $\beta$. We will write $\|\alpha\|$ to mean the number of pieces in $\alpha$. Note that these are formally exactly the same as $\alpha \subseteq \beta$ and $|\alpha|$, using the definition of $\alpha$ and $\beta$ as sets. In other situations we will often use $\alpha$ to mean the partial assignment $\bigcup \alpha$, for example writing $\alpha(\varphi)$ for the evaluation of $\varphi$ under $\bigcup \alpha$ and $\mathrm{dom}(\alpha)$ for the domain of $\bigcup \alpha$.

**Lemma 2.2.** *Let $\alpha, \beta$ be piecewise assignments with $\alpha \sqsubseteq \beta$. Let $Y \subseteq \mathrm{dom}(\beta)$. Then there exists a piecewise assignment $\beta'$ with $\alpha \sqsubseteq \beta' \sqsubseteq \beta$ such that $Y \subseteq \mathrm{dom}(\beta')$ and $\|\beta'\| \leq \|\alpha\| + |Y|$.* □

**Definition 2.3.** *A non-empty family $\mathcal{H}$ of piecewise assignments is* $r$-free *for a CNF $\varphi$ if it has the following properties.*

*(Consistency) No $\alpha \in \mathcal{H}$ falsifies any clause from $\varphi$.*

*(Retraction) If $\alpha \in \mathcal{H}$, $\beta$ is a piecewise assignment and $\beta \sqsubseteq \alpha$ then $\beta \in \mathcal{H}$.*

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

**Theorem 2.4.** *Let $\varphi$ be an unsatisfiable CNF formula. If there is a family of piecewise assignments which is $r$-free for $\varphi$, then any resolution refutation of $\varphi$ 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 $r^2/4$.*

*Proof.* Suppose that $\varphi$ is an unsatisfiable formula and that $\mathcal{H}$ is a family of piecewise assignments which is $r$-free for $\varphi$. Let $\Pi = (M_1, \ldots, M_s)$ be a resolution refutation of $\varphi$, given as a sequence of memory configurations.

Let $S$ be the set of all clauses which are falsified by some member of $\mathcal{H}$. There is at least one clause in $\Pi \cap S$ with width strictly less than $r/2$, namely the empty clause. Let $M_t$ be the first configuration in $\Pi$ in which a clause of width strictly less than $r/2$ occurs in $M_t \cap S$ and let $C$ be such a clause. Let $\alpha \in \mathcal{H}$ falsify $C$. By Lemma 2.2 we may assume that $\|\alpha\| < r/2$. Our goal now is to show that there is some $i < t$ such that $|M_i \cap S| \geq r/2$. Since for every $i < t$ every clause in $M_i \cap S$ has width at least $r/2$, this will give the theorem.

Suppose for a contradiction that $|M_i \cap S| < r/2$ for each $i < t$. We will inductively construct a sequence of piecewise assignments $\beta_1, \ldots, \beta_t$ in $\mathcal{H}$ such that for each $i \leq t$ we have that $\alpha \sqsubseteq \beta_i$ and that $\beta_i$ satisfies every clause in $M_i \cap S$. This will give a contradiction when we reach $\beta_t$, since $\alpha$ falsifies the clause $C \in M_t \cap S$.

The first configuration $M_1$ is empty, so we can put $\beta_1 = \alpha$. Supposing that $1 \leq i < t$ and that we already have a suitable $\beta_i$, we distinguish three cases.

**Axiom download:** $M_{i+1} = M_i \cup \{D\}$ where $D$ is a clause from $\varphi$. By the consistency property of $\mathcal{H}$, $D$ is not in $S$ and we can simply put $\beta_{i+1} = \beta_i$.

**Erasure:** $M_{i+1} \subseteq M_i$. We put $\beta_{i+1} = \beta_i$.

**Inference:** $M_{i+1} = M_i \cup \{D \vee E\}$ where $D \vee E$ follows by resolution on some variable $x$ from two clauses $D \vee x$ and $E \vee \neg x$ in $M_i$. Using Lemma 2.2, since $\|\alpha\| < r/2$ and $|M_i \cap S| < r/2$ we may assume that $\|\beta_i\| \leq \|\alpha\| + |M_i \cap S| < r$.

If $D \vee E$ contains a variable outside $\mathrm{dom}(\beta_i)$, then by the extension property we can extend $\beta_i$ to some $\beta_{i+1} \in \mathcal{H}$ which satisfies $D \vee E$, as required.

Suppose that all variables in $D \vee E$ are set by $\beta_i$. If $x \in \mathrm{dom}(\beta_i)$ let $\beta_{i+1} = \beta_i$, and otherwise let $\beta_{i+1} \in \mathcal{H}$ be any extension of $\beta_i$ which assigns a value to $x$. Then $\beta_{i+1}$ sets all variables in both $D \vee x$ and $E \vee \neg x$. It cannot falsify either clause, since that would imply that that clause is in $S$ and thus is already satisfied by $\beta_i$. Therefore it must satisfy both clauses and thus also satisfy $D \vee E$. □

Informally, we can think of each element $C$ of $S$ as identified with a minimal assignment $\alpha_C$ in $\mathcal{H}$ which falsifies it. Then $S$ contains the empty assignment and, by the extension property of $\mathcal{H}$, has a rich structure. In particular, if a clause $C$ in $\Pi \cap S$ has width less than $r$ and was derived by resolution on a variable outside $\mathrm{dom}(\alpha_C)$, then *both* parents of $C$ in $\Pi$ are in $S$. The proof of Theorem 2.4 then uses an idea from [1], taking the first clause $C$ in $S$ with small width and applying the usual clause space lower-bound argument to the substructure of $S$ which derives $C$.

# 3 Two simple applications

Let $n = 2^k$ for $k \in \mathbb{N}$. The formula $\mathrm{BPHP}_n$, the *bit pigeonhole principle on $n$ holes*, is an unsatisfiable CNF with variables $\{x_j^u : u \in [n+1], j \in [k]\}$. It asserts that for all distinct $u, v \in [n+1]$, the length-$k$ binary strings $x_1^u \dots x_k^u$ and $x_1^v \dots x_k^v$ are distinct. We think of each element of $[n+1]$ as a pigeon and of the string $x_1^u \dots x_k^u$ as the address, in binary, of the hole in $[n]$ that pigeon $u$ is mapped to. Understood in this way, $\mathrm{BPHP}_n$ asserts that there is an injective mapping of $n+1$ pigeons into $n$ holes. Formally the principle consists of the clauses

$$\bigvee_{j=1}^{k} (x_j^u \neq h_j) \vee \bigvee_{j=1}^{k} (x_j^v \neq h_j)$$

for each $u, v \in [n+1]$ with $u < v$ and each binary string $h_1 \dots h_k \in \{0,1\}^k$.

**Theorem 3.1.** *Any resolution refutation of* $\mathrm{BPHP}_n$ *passes through a configuration containing $n/4$ clauses of width at least $n/4$.*

*Proof.* By Theorem 2.4 it is enough to exhibit a family of piecewise assignments which is $n/2$-free.

For any partial matching $f$ of pigeons into holes, let $\alpha_f$ be the piecewise assignment that, for each pigeon $u$ in $\mathrm{dom}(f)$, assigns to the variables $x_1^u \dots x_k^u$ the binary string corresponding to the hole $f(u)$. The pieces of $\alpha_f$ correspond to the sets of variables $\{x_1^u, \dots, x_k^u\}$ belonging to each pigeon. Let $\mathcal{H}$ be the family of all piecewise assignments arising in this way.

Clearly $\mathcal{H}$ is non-empty and has the consistency and retraction properties. For the extension property, suppose we are given $\alpha_f \in \mathcal{H}$ and a variable $x_j^u$, with $\|\alpha_f\| < n/2$ and $x_j^u \notin \mathrm{dom}(\alpha_f)$. Then $|\mathrm{ran}(f)| < n/2 = 2^{k-1}$ and $u \notin \mathrm{dom}(f)$, and it is sufficient to find two holes $h_1 \dots h_k$ and $h'_1 \dots h'_k$ in $\{0,1\}^k \setminus \mathrm{ran}(f)$ with $h_j = 0$ and $h'_j = 1$. But there are exactly $2^{k-1}$ holes $h$ with $h_j = 0$, so there must be at least one such hole outside $\mathrm{ran}(f)$. A similar argument works for $h'$. $\square$

As a second application, we show that a CNF requiring large total space in resolution can be constructed from any CNF which requires large width. This is closely modelled on a similar result in [14] for monomial space in PCR.

Let $\varphi$ be a CNF over a set of variables $X$. Let $X'$ be a new set of variables containing a disjoint pair $\{x^1, x^2\}$ of variables for each $x \in X$. Following [14], for each clause $C$ in $\varphi$, let $C[\oplus]$ be the formula over $X'$ obtained by replacing each occurrence of $x_i$ in $C$ with the expression $(x_i^1 \oplus x_i^2)$ and then converting the result back into conjunctive normal form. Let $\varphi[\oplus]$ be the conjunction of all the CNFs $C[\oplus]$.

The *width* of a resolution refutation is the maximum width of any clause in it. The *refution width* of a CNF $\varphi$ in resolution is the minimal width of any refutation of $\varphi$.

**Theorem 3.2.** *Let $\varphi$ be a CNF and let $w$ the minimal refutation width of $\varphi$ in resolution. Then any resolution refutation of $\varphi[\oplus]$ passes through a configuration containing $w/2$ clauses of width at least $w/2$.*

*Proof.* Using the characterization of width in resolution by Atserias and Dalmau [2], we know that there is a $w$-winning strategy for the Duplicator in the Spoiler-Duplicator game on $\varphi$. That is, there is a nonempty family $\mathcal{K}$ of partial truth assignments such that:

1. if $f \in \mathcal{K}$ then $f$ does not falsify any clause from $\varphi$
2. if $f \in \mathcal{K}$ and $g \subseteq f$, then $g \in \mathcal{F}$
3. if $f \in \mathcal{K}$, $|\operatorname{dom}(f)| < w$ and $x$ is any variable, then there is some $g \in \mathcal{K}$ such that $f \subseteq g$ and $x \in \operatorname{dom}(g)$.

We will use $\mathcal{K}$ to build an $w$-free family $\mathcal{H}$ of piecewise assignments for $\varphi[\oplus]$. The result then follows by our main theorem.

Consider an assignment $f \in \mathcal{K}$. For each variable $x \in \operatorname{dom}(f)$, let $\alpha_x^0$ be the partial assignment $(x^1, x^2) \mapsto (0, f(x))$ and let $\alpha_x^1$ be the partial assignment $(x^1, x^2) \mapsto (1, f(x) \oplus 1)$, so that for $b = 0, 1$ we have $\alpha_x^b(x^1) \oplus \alpha_x^b(x^2) = f(x)$ and for $i = 1, 2$ at least one of the partial assignments $\alpha_x^0, \alpha_x^1$ sets $x^i$ to 0 and at least one sets $x^i$ to 1. For any map $\delta : \operatorname{dom}(f) \to \{0, 1\}$ let $\alpha_f^\delta$ be the piecewise assignment $\{\alpha_x^{\delta(x)} : x \in \operatorname{dom}(f)\}$. Notice that for each clause $C$ in $\varphi$, $\alpha_f^\delta$ falsifies $C[\oplus]$ if and only if $f$ falsifies $C$.

Let $\mathcal{H}$ contain the piecewise assignment $\alpha_f^\delta$ for each $f \in \mathcal{K}$ and each possible map $\delta : \operatorname{dom}(f) \to \{0, 1\}$. Consistency and retraction for $\mathcal{H}$ follow from properties 1 and 2 of $\mathcal{K}$. For the extension property, suppose $\alpha \in \mathcal{H}$ and $x^i$ is a variable in $X'$ such that $\|\alpha\| < r$ and $x^i \notin \operatorname{dom}(\alpha)$. Then $\alpha$ must arise from some $f \in K$, with $|f| < r$ and $x \notin \operatorname{dom}(f)$. By property 3 of $\mathcal{K}$, there is an extension $g \supseteq f$ in $\mathcal{K}$ with $x \in \operatorname{dom}(g)$. By the construction of $\mathcal{H}$ there exist piecewise assignments $\beta_0$ and $\beta_1$ arising from $g$ and extending $\alpha$ such that $\beta_0(x^i) = 0$ and $\beta_1(x^i) = 1$. □

In particular this result is interesting when $\varphi$ is a Tseitin formula over some graph $G$. In this case $\varphi[\oplus]$ can be seen as a Tseitin formula over the graph $G'$ formed by replacing each edge in $G$ with a double edge.

We recall briefly what a *Tseitin formula* is. Let $G = (V, E)$ be a connected graph of degree $d$ over $n$ vertices. For each edge $e \in E$ define a variable $x_e$. Fix an *odd-weight* function $\sigma : V \to \{0, 1\}$, that is, a function $\sigma$ such that $\sum_{v \in V} \sigma(v) \equiv 1 \pmod 2$. For each $v \in V$ define $\text{PARITY}_v$ as a CNF expressing

$$\sum_{e \ni v} x_e \equiv \sigma(v) \pmod 2.$$

The Tseitin formula $T(G, \sigma)$ is then the conjunction $\bigwedge_{v \in V} \mathrm{PARITY}_v$. It is well known that refutation width of $T(G, \sigma)$ is at least the connectivity expansion of $G$ (see for example [1]).

**Corollary 3.3.** *Let $G = (V, E)$ be a 3-regular expander graph over $n$ vertices. Let $G'$ be $G$ with each edge replaced with a double edge. Then for any odd weight function $\sigma : V \to \{0, 1\}$ the total space needed to refute $T(G', \sigma)$ is at least $\Omega(n^2)$.* $\square$

Here $T(G', \sigma)$ is a 6-CNF. This corollary is a partial answer to the question posed in open problem 2 of [1] about the space needed to refute $T(G, \sigma)$ when $G$ is a 3-regular expander graph.

# 4 Bipartite expanders and 2-matchings

The goal of this section is to define certain families of substructures of bipartite graphs, which we call *$r$-covering families*, and to show that in a random bipartite graph such a family exists with high probability. See Definitions 4.10 and 4.11 and Corollary 4.14 at the end of the section. We will need such families in our lower bounds for random formulas and for the graph pigeonhole principle. The constructions in this section are adapted from [9], which in turn is based on [4]. Our main innovation is Lemma 4.8.

We first introduce some notation. Let $\mathcal{G} = (U \cup V, E)$ be a bipartite graph. For a node $a$ in $\mathcal{G}$ we will write $N(a)$ for the set of neighbours of $a$, and for a set of nodes $A$ in $\mathcal{G}$ we will write $N(A)$ for $\bigcup_{a \in A} N(a)$.

For sets $A \subseteq U$ and $B \subseteq V$, a *2-matching $\sigma$ of $A$ into $B$* is a subset of the edge relation $E$ such that each element of $A$ has as neighbours under $\sigma$ exactly two elements of $B$, and no two elements of $A$ share a neighbour under $\sigma$. We will sometimes use functional notation for 2-matchings, as follows: for $a \in A$ we will write $\sigma(a)$ for the pair of neighbours of $a$; for $X \subseteq A$ we will write $\sigma(X)$ for the set of all neighbours of $X$; we will write $\mathrm{dom}(\sigma)$ for $A$ and $\mathrm{ran}(\sigma)$ for $\sigma(A)$. A *fork* in $\mathcal{G}$ is a 2-matching with a domain of size one.

**Definition 4.1.** *Let $\mathcal{G} = (U \cup V, E)$ be a bipartite graph. For $\gamma > 1$, we say that $\mathcal{G}$ is an $(s, \gamma)$-*expander* if*

$$\forall A \subseteq U,\ |A| \leq s \to |N(A)| \geq \gamma |A|.$$

We will usually be interested in $(s, 2 + \epsilon)$-expanders, for some $\epsilon > 0$. On subgraphs of such graphs we can apply the following corollary of Hall's Theorem, proved in [1].

**Lemma 4.2.** *Let $\mathcal{G} = (U \cup V, E)$ be a bipartite graph. If $|N(A)| \geq 2|A|$ for every set $A \subseteq U$, then there is a 2-matching of $U$ into $V$.* $\square$

For the rest of this section (until Theorem 4.13), fix integers $d$ and $s$ and a real number $\epsilon > 0$. Let $\mathcal{G} = (U \cup V, E)$ be a fixed bipartite graph of left-degree $d$ which is an $(s, 2 + \epsilon)$-expander.

**Definition 4.3.** *Given two sets $A \subseteq U$ and $B \subseteq V$, we say that $(A, B)$* has the double-matching property *if for every $C \subseteq U \setminus A$, if $|A| + |C| \leq s$ then there exists a 2-matching of $C$ into $V \setminus B$.*

We have the following useful lemma, which applies the expansion property of $\mathcal{G}$ to bound the size of a minimal witness $C$ that the double-matching property fails.

**Lemma 4.4.** *Let $A \subseteq U$ and $B \subseteq V$ be such that $(A, B)$ does not have the double-matching property. Then there is a set $C \subseteq U \setminus A$ with $|C| < \frac{1}{\epsilon}|B|$ such that there is no 2-matching of $C$ into $V \setminus B$.*

*Proof.* Let $C \subseteq U \setminus A$ be minimal such that $|C| \leq s - |A|$ and there is no 2-matching of $C$ into $V \setminus B$. Then for every $D \subsetneq C$, there is a 2-matching of $D$ into $V \setminus B$, so in particular $|N(D) \setminus B| \geq 2|D|$. Hence we must have $|N(C) \setminus B| < 2|C|$, since otherwise there would be a 2-matching of $C$ into $V \setminus B$ by Lemma 4.2. On the other hand, by expansion, since $|C| \leq s$ we have that $|N(C)| \geq (2 + \epsilon)|C|$.

Combining these, we get

$$(2 + \epsilon)|C| \leq |N(C)| \leq |N(C) \setminus B| + |B| < 2|C| + |B|$$

and hence $|C| < \frac{1}{\epsilon}|B|$. $\square$

**Lemma 4.5.** *The pair $(\emptyset, \emptyset)$ has the double-matching property.*

*Proof.* This follows directly from Lemma 4.2, since $\mathcal{G}$ is a $(s, 2+\epsilon)$ expander. $\square$

**Lemma 4.6.** *(Left extension.) Let $A \subseteq U$ and $B \subseteq V$ be such that $(A, B)$ has the double-matching property and $\frac{d(d-1)}{\epsilon}(|B| + 2) + |A| + 1 \leq s$. Then for each $u \in U \setminus A$ there is a 2-matching $\pi$ of $u$ into $V \setminus B$ such that $(A \cup \{u\}, B \cup \pi(u))$ has the double-matching property.*

*Proof.* Let $\Pi$ be the set of all 2-matchings $\pi$ of $u$ into $V \setminus B$. Since $|A| + 1 \leq s$ and $(A, B)$ has the double-matching property, we know that $\Pi$ is non-empty. Suppose for a contradiction that for every $\pi \in \Pi$, the pair $(A \cup \{u\}, B \cup \pi(u))$ does not have the double-matching property. By Lemma 4.4, for every $\pi \in \Pi$ there is a set $C_\pi \subseteq U \setminus (A \cup \{u\})$ with $|C_\pi| < \frac{1}{\epsilon}|B \cup \pi(u)|$ such that there is no 2-matching of $C_\pi$ into $V \setminus (B \cup \pi(u))$.

Let $C = \bigcup_{\pi \in \Pi} C_\pi$. Then $|C| < \frac{d(d-1)}{\epsilon}(|B| + 2)$, since $|\Pi| \leq d(d-1)$. Hence, by our assumption about the sizes of $|A|$ and $|B|$, we have that $|C \cup \{u\}| \leq s - |A|$. Furthermore $C \cup \{u\} \subseteq U \setminus A$, so by the double-matching property for $(A, B)$ there is a 2-matching $\sigma$ of $C \cup \{u\}$ into $V \setminus B$.

There must be some $\pi \in \Pi$ such that $\pi(u) = \sigma(u)$. Let $\sigma'$ be $\sigma$ with the fork $u \mapsto \pi(u)$ removed. Then $\sigma'$ is a 2-matching of $C$ into $V \setminus (B \cup \pi(u))$, and in particular contains a 2-matching of $C_\pi$ into $V \setminus (B \cup \pi(u))$, contradicting the choice of $C_\pi$. $\square$

**Lemma 4.7.** *(Left retraction.) Let $A \subseteq U$ and $B \subseteq V$ be such that $(A, B)$ has the double-matching property and $\frac{1}{\epsilon}|B| + |A| \leq s$. Suppose that $u \in A$ and there is a 2-matching $\pi$ of $u$ into $B$. Then $(A \setminus \{u\}, B \setminus \pi(u))$ has the double-matching property.*

*Proof.* Let $C \subseteq (U \setminus A) \cup \{u\}$ with $|C| \leq s - |A \setminus \{u\}|$. We want to show that there is a 2-matching of $C$ into $(V \setminus B) \cup \pi(u)$. By Lemma 4.4, it is enough to consider only sets $C$ with $|C| < \frac{1}{\epsilon}|B \setminus \pi(u)|$.

If $u \in C$, then $|C \setminus \{u\}| \leq s - |A|$ so by the double-matching property for $(A, B)$ there is a 2-matching $\sigma$ of $C \setminus \{u\}$ into $V \setminus B$. Hence $\sigma \cup \pi$ is a 2-matching of $C$ into $(V \setminus B) \cup \pi(u)$.

If $u \notin C$, then $|C| \leq s - |A|$ by our assumption about the sizes of $|A|$ and $|B|$, so by the double-matching property for $(A, B)$ there is a 2-matching of $C$ into $V \setminus B$. $\square$

**Lemma 4.8.** *(Right extension.) Let $A \subseteq U$ and $B \subseteq V$ be such that $(A, B)$ has the double-matching property. Let $v \in V \setminus B$ have degree $e$, and suppose that $\frac{d(d-1)}{\epsilon}(|B| + 2e) + |A| + e \leq s$. Then either*

1. *for some $u \in U \setminus A$ there is a 2-matching $\pi$ of $u$ into $V \setminus B$ such that $v \in \pi(u)$ and $(A \cup \{u\}, B \cup \pi(u))$ has the double-matching property, or*

2. *$(A, B \cup \{v\})$ has the double-matching property.*

*Proof.* Let $D$ be $N(v) \setminus A$, so that $|D| \leq e$. By applying Lemma 4.6 $|D|$ many times, we can find a 2-matching $\sigma$ of $D$ into $V \setminus B$ such that $(A \cup D, B \cup \sigma(D))$ has the double-matching property. Notice that $\frac{1}{\epsilon}(|B| + |\sigma(D)|) + |A| + |D| \leq s$ so that, by Lemma 4.7, the double-matching property is preserved if we remove any number of elements from $D$ and the corresponding forks from $\sigma$.

There are now two cases. In the first case, there is $u \in D$ and a corresponding fork $\pi$ in $\sigma$ such that $v \in \pi(u)$. In this case we may remove all other elements from $D$ and all other forks from $\sigma$ and thus satisfy condition 1 of the lemma.

In the second case, $v \notin \sigma(D)$. Then the double-matching property for $(A \cup D, B \cup \sigma(D))$ implies the double-matching property for $(A \cup D, B \cup \sigma(D) \cup \{v\})$, since no neighbours of $v$ remain in $U \setminus (A \cup D)$. As in the previous case, it follows by Lemma 4.7 that $(A, B \cup \{v\})$ has the double-matching property, satisfying condition 2. $\square$

**Lemma 4.9.** *(Right retraction.) Let $A \subseteq U$ and $B \subseteq V$ be such that $(A, B)$ has the double-matching property. For each $v \in V$, the pair $(A, B \setminus \{v\})$ has the double-matching property.*

*Proof.* This is trivial from the definition of the double-matching property. $\square$

We can now describe the objects we will need for our lower bounds.

**Definition 4.10.** *A* 2-structure *$\kappa$ in $\mathcal{G}$ is a pair $(\sigma, S)$ where $\sigma$ is a 2-matching and $S \subseteq V \setminus \mathrm{ran}(\sigma)$. We think of $\kappa$ as consisting of a set of* forks *(the forks in $\sigma$) and a disjoint set of* singletons *(the elements of $S$).*

*The* size *of a 2-structure $\kappa$ is defined to be $|\kappa| = |\operatorname{dom}(\sigma)| + |S|$, that is, the number of forks plus the number of singletons. Given two 2-structures $\kappa = (\sigma, S)$ and $\lambda = (\sigma', S')$ we say that $\lambda$* extends *$\kappa$, written $\kappa \subseteq \lambda$, if $\sigma \subseteq \sigma'$ and $S \subseteq S'$. We say that the 2-structure $\kappa$* covers *a node $w \in \mathcal{G}$ if $w \in \operatorname{dom}(\sigma) \cup \operatorname{ran}(\sigma) \cup S$.*

**Definition 4.11.** *A non-empty set $\mathcal{F}$ of 2-structures in $\mathcal{G}$ is called an $r$-*covering family *if it has the following two properties.*

*(Retraction) If $\kappa \in \mathcal{F}$ and $\lambda$ is a 2-structure in $\mathcal{G}$ with $\lambda \subseteq \kappa$, then $\lambda \in \mathcal{F}$.*

*(Extension) If $\kappa \in \mathcal{F}$ with $|\kappa| < r$ and $w$ is any node of $\mathcal{G}$, then $\kappa$ can be extended to a 2-structure in $\mathcal{F}$ which covers $w$.*

**Lemma 4.12.** *Let $r = s\epsilon/6d^2$. Suppose that no node in $V$ has degree more than $r$. Then an $r$-covering family $\mathcal{F}$ of 2-structures exists on $\mathcal{G}$.*

*Proof.* For a 2-structure $\kappa$, let $A_\kappa = \operatorname{dom}(\sigma)$ and $B_\kappa = \operatorname{ran}(\sigma) \cup S$. We take $\mathcal{F}$ to be the set of all 2-structures $\kappa$ in $\mathcal{G}$ for which $(A_\kappa, B_\kappa)$ has the double-matching property and $\frac{1}{\epsilon}|B_\kappa| + |A_\kappa| \leq s$.

This family is non-empty by Lemma 4.5 and has the retraction property by Lemmas 4.7 and 4.9. For the extension property, suppose that $|\kappa| < r$, that is, $|\operatorname{dom}(\sigma)| + |S| < r$. Then $|A_\kappa| < r$ and $|B_\kappa| = 2|\operatorname{dom}(\sigma)| + |S| < 2r$. Since $\mathcal{G}$ is an $(s, 2+\epsilon)$-expander we must have $\epsilon < d$, so $r < s/6$. Thus

$$\frac{d(d-1)}{\epsilon}\left(|B_\kappa| + 2r\right) + |A_\kappa| + r < \frac{4d^2 r}{\epsilon} + 2r < \frac{4s}{6} + \frac{2s}{6} = s.$$

Hence the requirements on the sizes of $A_\kappa$ and $B_\kappa$ for Lemmas 4.6 and 4.8 are satisfied. Now given $v \in V$, applying Lemma 4.8 we can extend $\kappa$ to a 2-structure $\kappa'$ which covers $v$, by either adding one more fork or one more singleton. In either case, $(A_{\kappa'}, B_{\kappa'})$ still has the double-matching property and $\frac{1}{\epsilon}|B_{\kappa'}| + |A_{\kappa'}| \leq s$, so we remain within $\mathcal{F}$. Similarly, given $u \in U$ we can apply Lemma 4.6 to extend $\kappa$ to $\kappa' \in \mathcal{F}$ covering $u$. $\square$

We will say that a graph $\mathcal{G}$ is a $(n, d, \Delta)$-*random bipartite graph* if it is chosen uniformly at random from the set of bipartite graphs $(U \cup V, E)$ of left-degree $d$ with $|U| = \Delta n$ and $|V| = n$.

**Theorem 4.13.** *Choose constants $d \geq 4$, $\Delta > 1$ and $\epsilon \in (0, 1/2)$. Then there is a strictly positive constant $\gamma = \gamma_{d,\epsilon,\Delta}$ such that, for large $n$, if $\mathcal{G}$ is a $(n, d, \Delta)$-random bipartite graph then with exponentially high probability $\mathcal{G}$ is a $(\gamma n, 2+\epsilon)$-expander.*

*Proof.* This is standard and can be found for example in [3]. $\square$

**Lemma 4.14.** *Choose constants $d \geq 4$ and $\Delta > 1$. There is a constant $\delta > 0$ such that, for large $n$, if $\mathcal{G}$ is a $(n, d, \Delta)$-random bipartite graph then with exponentially high probability there exists a $\delta n$-covering family of 2-structures on $\mathcal{G}$.*

*Proof.* Fix $\epsilon \in (0, 1/2)$ arbitrarily. Let $\gamma$ be the constant $\gamma_{d,\epsilon,\Delta}$ from Theorem 4.13 and let $\delta = \gamma\epsilon/6d^2$. With exponentially high probability, $\mathcal{G}$ is a $(\gamma n, 2+\epsilon)$-expander. To show that $\mathcal{G}$ has a $\delta n$-covering family, by Lemma 4.12 it is enough to show that every node in $V$ has degree at most $\delta n$. The degree is the sum of independent Boolean random variables and has expected value $\Delta d$, so this is true with exponentially high probability by the Chernoff bound. $\square$

# 5 Random $k$-CNFs

A *random $k$-CNF* with $n$ variables and clause density $\Delta$ is a CNF picked uniformly at random from the set of all formulas in variables $\{x_1, \ldots, x_n\}$ which consist of exactly $\Delta n$ clauses, with each clause containing exactly $k$ literals, with no variable appearing twice in a clause. As is well-known, there is a constant $\theta_k$ such that if $\Delta > \theta_k$ then such a $\varphi$ is unsatisfiable with high probability for large $n$.

**Theorem 5.1.** *Let $k \geq 4$ and $\Delta > 1$. There is a constant $c > 0$ such that, for large $n$, if $\varphi$ is a random $k$-CNF with $n$ variables and clause density $\Delta$ then with exponentially high probability any resolution refutation of $\varphi$ passes through a configuration containing $cn$ clauses of width at least $cn$.*

*Proof.* We associate with $\varphi$ the bipartite graph $\mathcal{G} = (U \cup V, E)$, where $U$ is the set of clauses of $\varphi$, $V$ is the set $\{x_1, \ldots, x_n\}$ of variables, and an edge exists between a clause $C$ in $U$ and a variable $x$ in $V$ if $x$ appears in $C$ (either positively or negatively). Then $\mathcal{G}$ is an $(n, k, \Delta)$-random bipartite graph. Hence by Lemma 4.14 there is a constant $\delta$ such that with exponentially high probability there exists a $\delta n$-covering family $\mathcal{F}$ of 2-structures on $\mathcal{G}$. We will show how such a family $\mathcal{F}$ can be used to construct a family $\mathcal{H}$ of piecewise assignments that is $\delta n$-free for $\varphi$. The theorem follows by Theorem 2.4, with $c = \delta/2$.

Let $\kappa = (\sigma, S)$ be any 2-structure in $\mathcal{F}$ and consider the following way of labeling the forks and singletons of $\kappa$ with partial assignments.

- Let $\pi : u \mapsto \{x_i, x_j\}$ be a fork in $\kappa$ with $i < j$. Label $\pi$ with an assignment to $\{x_i, x_j\}$ chosen as follows: either set $x_i$ to satisfy the clause $u$ and set $x_j$ arbitrarily, or set $x_j$ to satisfy the clause $u$ and set $x_i$ arbitrarily.
- Label each singleton $x_i$ in $\kappa$ with an arbitrary assignment to $x_i$.

Notice that, in both cases, for every variable $x_i$ covered there is at least one possible label which sets $x_i \mapsto 1$ and one label which sets $x_i \mapsto 0$.

Let $L$ be an assignment of such a label to every fork and singleton in $\kappa$. All the labels in $L$ have disjoint domains. Hence we can use $L$ to define a piecewise assignment $\alpha$ as the set of all labels chosen for the forks in $\kappa$ together with all labels chosen for the singletons of $\kappa$. Then in particular $\|\alpha\| = |\kappa|$ and $\alpha$ satisfies every clause $C$ covered by $\kappa$. We take $\mathcal{H}$ to consist of every piecewise assignment $\alpha$ which arises in this way from a 2-structure $\kappa \in \mathcal{F}$ and a labeling $L$ of $\kappa$.

We now need to show that $\mathcal{H}$ satisfies Definition 2.1. It is clearly non-empty. For the retraction property, observe that given two piecewise assignments $\beta \sqsubseteq \alpha$, if $\alpha \in \mathcal{H}$ then there is some $\kappa \in \mathcal{F}$ such that $\alpha$ is a labeling of $\kappa$. We can obtain $\beta$ from $\alpha$ by removing some pieces from $\alpha$. Let $\kappa'$ be the 2-structure obtained by removing the corresponding forks and singletons from $\kappa$. Then $\beta$ is a labeling of $\kappa'$ and $\kappa' \in \mathcal{F}$ by the retraction property for $\mathcal{F}$. Hence $\beta \in \mathcal{H}$.

For the consistency property, suppose for a contradiction that some $\alpha \in \mathcal{H}$ falsifies a clause $C$ of $\varphi$. By the retraction property of $\mathcal{H}$ proved above, we may assume without loss of generality that $\|\alpha\| \leq k$ by removing any pieces of $\alpha$ which do not mention a variable in $C$ and remembering that $|C| = k$. The piecewise assignment $\alpha$ arises as a labeling of some 2-structure $\kappa \in \mathcal{F}$ which cannot cover $C$, since otherwise $\alpha$ by construction would satisfy $C$. Since $|\kappa| = \|\alpha\| \leq k < \delta n$ for large $n$, by the extension property for $\mathcal{F}$ we can extend $\kappa$ to a 2-structure $\kappa'$ in $\mathcal{F}$ which does cover $C$ and thus contains some fork $\pi : C \mapsto \{x_i, x_j\}$. Then in particular the variable $x_i$ appears in $C$ but is not in the domain of $\alpha$, contradicting the assumption that $\alpha$ falsifies $C$.

For the extension property, suppose that $\alpha \in \mathcal{H}$ is a labeling of $\kappa \in \mathcal{F}$ with $|\kappa| < \delta n$, and let $x_i$ be any variable not in the domain of $\alpha$. Then $x_i$ is not covered by $\kappa$. By the extension property for $\mathcal{F}$, we can extend $\kappa$ to a 2-structure $\kappa' \in \mathcal{F}$ by adding either a fork or a singleton which covers $x_i$, and by the properties of our labelings we can extend $\alpha$ to a labeling $\alpha'$ of $\kappa'$ which sets $x_i$ to whichever value we choose. $\square$

# 6 The graph pigeonhole principle

Let $\mathcal{G} = (U \cup V, E)$ be a bipartite graph with $|U| > |V|$. We think of $U$ is a set of pigeons and $V$ as a set of holes. The formula $\mathcal{G}$-PHP, the *graph pigeonhole principle for* $\mathcal{G}$, is an unsatisfiable CNF in variables $\{x_{uv} : (u, v) \in E\}$. It asserts that the variables describe a map, given by a subset of the edges of $\mathcal{G}$, in which each pigeon gets mapped to at least one hole but no hole receives two pigeons. Formally, it is a conjunction of all clauses

1. $\bigvee\{x_{uv} : (u, v) \in E\}$ for each $u \in U$
2. $\neg x_{uv} \vee \neg x_{u'v}$ for each distinct pair of edges $(u, v)$ and $(u', v)$ in $E$.

We will call these clauses respectively the pigeon axioms and the hole axioms. Notice that if $\mathcal{G}$ has left-degree $d$ then $\mathcal{G}$-PHP is a $d$-CNF. We will write $X_v$ for the set of variables representing the edges touching the hole $v$.

**Theorem 6.1.** *Let $d \geq 4$ and $\Delta > 1$. There is a constant $c > 0$ such that, for large $n$, if $\mathcal{G}$ is a $(n, d, \Delta)$-random bipartite graph then with exponentially high probability any resolution refutation of $\mathcal{G}$-PHP passes through a configuration containing $cn$ clauses of width at least $cn$.*

*Proof.* The proof of this result closely follows the pattern of the proof of Theorem 5.1. By Lemma 4.14 there is a constant $\delta$ such that with exponentially high probability there exists a $\delta n$-covering family $\mathcal{F}$ of 2-structures on $\mathcal{G}$. We will construct from such an $\mathcal{F}$ a family $\mathcal{H}$ of piecewise assignments that is $\delta n$-free for $\mathcal{G}$-PHP. The result follows by Theorem 2.4.

Let $\kappa = (\sigma, S)$ be any 2-structure in $\mathcal{F}$ and consider the following way of labelling the forks and singletons of $\kappa$.

- Label each fork $\pi : u \mapsto \{v, v'\}$ in $\kappa$ with an assignment $\alpha_\pi$ to $X_v \cup X_{v'}$ chosen as follows: order the holes $v, v'$ arbitrarily as $v_1, v_2$. Map pigeon $u$ to hole $v_1$ and set the remaining variables in $X_{v_1}$ to zero. Either choose any pigeon $u' \in N(v_2)$ and map it to hole $v_2$ (we allow $u' = u$), setting the remaining variables in $X_{v_2}$ to zero, or simply set all variables in $X_{v_2}$ to zero.

- Label each singleton $v$ in $\kappa$ with an assignment $\alpha_v$ to $X_v$ chosen as follows: either choose any pigeon $u \in N(v)$ and map it to $v$, setting all other variables in $X_v$ to zero, or simply set all variables in $X_v$ to zero.

Notice that in both cases, for every pigeon $v$ covered and every variable $x \in X_v$, there is at least one label which sets $x \mapsto 1$ and one label which sets $x \mapsto 0$.

As in the proof of Theorem 6.1, we can label $\kappa$ with a piecewise assignment $\alpha$ arising from our choice $L$ of labels for the parts of $\kappa$. Notice that $\|\alpha\| = |\kappa|$, that $\alpha$ does not violate any hole axiom, and that $\alpha$ satisfies the pigeon axiom for each pigeon $u$ covered by $\kappa$. We take $\mathcal{H}$ to consist of every piecewise assignment $\alpha$ which arises in this way from any $\kappa \in \mathcal{F}$ and any labeling $L$ of $\kappa$. We now need to show that $\mathcal{H}$ satisfies Definition 2.1.

Clearly $\mathcal{H}$ is non-empty. The retraction and consistency properties follow exactly as in Theorem 5.1, using the observation that no $\alpha \in \mathcal{H}$ falsifies any hole axiom. For the extension property, suppose that $\alpha \in \mathcal{H}$ is a labeling of some 2-structure $\kappa \in \mathcal{F}$ with $\|\alpha\| = |\kappa| < r$, and let $x$ be any variable not in the domain of $\alpha$. Then $x$ must be in $X_v$ for some hole $v$ which is not covered by $\kappa$. By the extension property for $\mathcal{F}$, we can extend $\kappa$ to a 2-structure $\kappa' \in \mathcal{F}$ by adding either a fork or a singleton which covers $v$. By the freedom in our choice of labelings, there is an extension $\beta_0$ of $\alpha$ to a labeling of $\kappa'$ which sets $x$ to zero, and another such extension $\beta_1$ which sets $x$ to one. $\square$

An alternative version of this theorem would be to show a total space lower bound for $\mathcal{G}$-PHP for all bipartite expanders of left-degree $d$ with a suitable bound on the right-degree (rather than for random graphs), applying Lemma 4.12 directly to get the covering family of 2-structures.

# 7 Semantic total space

In this section we address a question raised in [1]. The space bounds in that paper hold not only for the usual versions of the proof systems considered, but also for *semantic* versions of the systems. In particular a *semantic resolution* refutation of a CNF $\varphi$ is a sequence of configurations where, at each step in the refutation, we can either add an axiom from $\varphi$ to the current configuration $M_i$, or we can replace $M_i$ with *any* configuration $M_{i+1}$ with the property that every clause in $M_{i+1}$ is implied by $M_i$.

In [1] the authors show that, for any unsatisfiable CNF $\varphi$, the clause space required to refute $\varphi$ in resolution is no more than twice the clause space required in semantic resolution, and ask whether the same thing is true for total space.

It follows from our lower bounds that, for total space, resolution can require quadratically more space than semantic resolution. In particular, let $\varphi$ be an unsatisfiable random $k$-CNF with $n$ variables and clause density $\Delta$, where $n$ is large. We can refute $\varphi$ in semantic resolution by simply writing down all the clauses of $\varphi$ and then deriving the empty clause in one step. This uses total space $\Delta kn$, the size of $\varphi$. But by Theorem 5.1, a resolution refutation of $\varphi$ typically requires total space $\Omega(n^2)$.

On the other hand, the proof of Theorem 2.4 does not depend very much on the details of the syntax of the resolution rule. The theorem generalizes easily to give lower bounds for a weak form of semantic resolution, with the following inference rule: from a configuration $M_i$ we can move to a configuration $M_i \cup \{C\}$, where the clause $C$ is implied by some set of at most $d$ clauses in $M_i$, for a fixed integer $d$. Calling this system *$d$-bounded semantic resolution*, we have:

**Theorem 7.1.** *Let $\varphi$ be an unsatisfiable CNF formula and suppose $d \leq r$. If there is a family of piecewise assignments which is $r$-free for $\varphi$, then any $d$-bounded semantic resolution refutation of $\varphi$ must pass through a configuration containing at least $(r-d)/2$ clauses each of width at least $(r-d)/2$.*

*Proof.* The proof is the same as for Theorem 2.4, except that we replace the bound $r/2$ with $(r-d)/2$ and use a different argument for the inference case, as follows. Suppose $M_{i+1} = M_i \cup \{E\}$ where $E$ is implied by clauses $D_1, \ldots, D_d \in M_i$. Since $\|\alpha\| < (r-d)/2$ and $|M_i \cap S| < (r-d)/2$ we may assume that $\|\beta_i\| \leq \|\alpha\| + |M_i \cap S| < r - d$.

Either $D_1$ is satisfied by $\beta_i$ or it is not. If it is, let $\gamma_1 = \beta_i$. If not, then $D_1$ cannot be in $S$, since $\beta_i$ satisfies all members of $M_i \cap S$. It follows that $D_1$ is not falsified by $\beta_i$ either, and thus must contain some literal not set by $\beta_i$. In this case let $\gamma_1 \in \mathcal{H}$ be a minimal extension of $\beta_i$ which satisfies this literal.

We have found $\gamma_1 \in \mathcal{H}$ which satisfies $D_1$ with $\beta_i \sqsubseteq \gamma_1$ and $\|\gamma_1\| < r-d+1$. Applying the same reasoning to $D_2, \ldots, D_d$ in turn, we can build a sequence of extensions $\gamma_1 \sqsubseteq \gamma_2 \sqsubseteq \cdots \sqsubseteq \gamma_d$ in $\mathcal{H}$, finishing with $\gamma_d$ which satisfies each of $D_1, \ldots, D_d$ and thus also satisfies $E$. We put $\beta_{i+1} = \gamma_d$. □

Finally, in [1] the notion of an *$r$-semiwide* formula is defined, and it is shown that any such formula requires clause space $r$ in semantic resolution. We can strengthen this, to show that such a formula also requires total space $r^2/4$ in semantic resolution, by a straightforward generalization of the total space lower bounds in [1] for $\mathrm{PHP}_n$ and $\mathrm{CT}_n$. For a CNF $Z$ and a partial assignment $\alpha$, we say that $\alpha$ is *$Z$-consistent* if $\alpha$ can be extended to satisfy $Z$.

**Definition 7.2.** *A CNF formula $\varphi$ is* $r$-semiwide *if it is the conjunction of a CNF $Z$ and a CNF $W$, where $Z$ is satisfiable, and for each $Z$-consistent partial* *assignment $\alpha$ and each clause $C$ from $W$, if $|\alpha| < r$ then $\alpha$ can be extended to a $Z$-consistent assignment which satisfies $C$.*

**Theorem 7.3.** *Let $\varphi$ be an unsatisfiable $r$-semiwide formula. Then every semantic resolution refutation of $\varphi$ must pass through a configuration containing $r/2$ clauses each of width at least $r/2$.*

*Proof.* Let $\varphi = Z \wedge W$ as in Definition 7.2 and let $\Pi = (M_1, \ldots, M_s)$ be a refutation of $\varphi$. Let $M_i^* = \{C \in M_i \ : \ Z \not\models C\}$. Take the first $t$ such that there exists a clause $C \in M_t^*$ of width strictly less than $r/2$. Fix such a clause $C$ and let $\alpha$ be the minimal partial assignment falsifying $\alpha$. Then $\alpha$ is $Z$-consistent and $|\operatorname{dom}(\alpha)| = |C| < r/2$.

It is now enough to show that $|M_i^*| \geq r/2$ for some $i < t$, since for $i < t$ every clause in $|M_i^*|$ has width at least $r/2$. So suppose for a contradiction that $|M_i^*| < r/2$ for all $i < t$. We prove by induction that for each $i = 1, \ldots, t$ there exists some $Z$-consistent $\beta_i \supseteq \alpha$ such that $\beta_i \models M_i^*$. This leads immediately to a contradiction when $i = t$.

For the erasure case we trivially put $\beta_{i+1} = \beta_i$. For semantic inference, that is, $M_i \models M_{i+1}$, we let $\beta_{i+1}$ be an extension of $\beta_i$ which satisfies $Z$. Then from the fact that $\beta_{i+1} \models M_i^* \wedge Z$ it follows that $\beta_{i+1} \models M_i$ and hence $\beta_{i+1} \models M_{i+1}$. For axiom download, suppose $M_{i+1} = M_i \cup \{D\}$ with $D$ a clause from $W$. We may assume without loss of generality that $|\operatorname{dom}(\beta)| \leq |\operatorname{dom}(\alpha)| + |M_i^*| < r$. Hence by $r$-semiwideness there is a $Z$-consistent $\beta_{i+1} \supseteq \beta_i$ such that $\beta_{i+1} \models D$. □

**Acknowledgements.** The authors are grateful to Jakob Nordström for helpful discussions about this work and about resolution space in general.

# References

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

[2] Albert Atserias and Víctor Dalmau. A combinatorial characterization of resolution width. *Journal of Computer and System Sciences*, 74(3):323–334, 2008.

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

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

[5] Eli Ben-Sasson and Jakob Nordström. A space hierarchy for $k$-DNF resolution. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:47, 2009.

[6] Eli Ben-Sasson and Jakob Nordström. Understanding space in resolution: Optimal lower bounds and exponential trade-offs. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:34, 2009.

[7] Eli Ben-Sasson and Jakob Nordström. Understanding space in proof complexity: Separations and trade-offs via substitutions. In *Proc. 2nd Symposium on Innovations in Computer Science (ICS)*, pages 401–416, 2011.

[8] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. In *Proc. 31st Annual ACM Symposium on Theory of Computing (STOC)*, pages 517–526, 1999.

[9] Ilario Bonacina and Nicola Galesi. Pseudo-partitions, transversality and locality: a combinatorial characterization for the space measure in algebraic proof systems. In *Proc. 4th Conf. on Innovations in Theoretical Computer Science*, pages 455–472. ACM, 2013.

[10] H. Kleine Büning and T. Lettmann. *Propositional Logic - Deduction and Algorithms*. Cambridge University Press, 1999.

[11] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[12] Juan Luis Esteban, Nicola Galesi, and Jochen Messner. On the complexity of resolution with bounded conjunctions. *Theoretical Computer Science*, 321(2-3):347–370, 2004.

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

[14] Yuval Filmus, Massimo Lauria, Mladen Mikša, Jakob Nordström, and Marc Vinyals. Towards an understanding of polynomial calculus: new separations and lower bounds. In *Proc. 40th International Colloquium on Automata, Languages and Programming (ICALP)*, pages 437–448, 2013.

[15] Yuval Filmus, Massimo Lauria, Jakob Nordström, Neil Thapen, and Noga Ron-Zewi. Space complexity in polynomial calculus. In *Proc. 27th Annual IEEE Conference on Computational Complexity*, pages 334–344, 2012.

[16] Jakob Nordström. Narrow proofs may be spacious: separating space and width in resolution. In *Proc. 38th Annual ACM Symposium on Theory of Computing (STOC)*, pages 507–516, 2006.

[17] Jakob Nordström. Pebble games, proof complexity, and time-space trade-offs. *Logical Methods in Computer Science*, 9(3):15, 2013.

[18] Jakob Nordström and Johan Håstad. Towards an optimal separation of space and length in resolution. *Theory of Computing*, 9(14):471–557, 2013.




ECCC ISSN 1433-8092

http://eccc.hpi-web.de