Electronic Colloquium on Computational Complexity, Report No. 31 (2001)

Space Complexity of Random Formulae in Resolution

Eli Ben-Sasson*
Institute of Computer Science
Hebrew University
Jerusalem, Israel
e-mail: elli@cs.huji.ac.il

Nicola Galesi†
School of Mathematics
Institute for Advanced Study
Princeton, New Jersey, USA
e-mail: galesi@ias.edu

April 5, 2001

Abstract

We study the space complexity of refuting unsatisfiable random k-CNFs in the Resolution proof system. We prove that for any large enough Δ, with high probability a random k-CNF over n variables and Δn clauses requires resolution clause space of $\Omega(n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}})$, for any $0 < \epsilon < 1/2$. For constant Δ, this gives us linear, optimal, lower bounds on the clause space.

A nice consequence of this lower bound is the first lower bound for size of treelike resolution refutations of random 3-CNFs with clause density $\Delta >> \sqrt{n}$. This bound is nearly tight. Specifically, we show that with high probability, a random 3-CNF with Δn clauses requires treelike refutation size of $\exp(\Omega(n/\Delta^{\frac{1+\epsilon}{1-\epsilon}}))$, for any $0 < \epsilon < 1/2$.

Our space lower bound is the consequence of three main contributions.

1. We introduce a 2-player Matching Game on bipartite graphs G to prove that there are no perfect matchings in G.
2. We reduce lower bounds for the clause space of a formula F in Resolution to lower bounds for the complexity of the game played on the bipartite graph $G(F)$ associated with F.
3. We prove that the complexity of the game is large whenever G is an expander graph.

Finally, a simple probabilistic analysis shows that for a random formula F, with high probability $G(F)$ is an expander.

We also extend our result to the case of $G-PHP$, a generalization of the pigeonhole Principle based on bipartite graphs G. We prove that the clause space for $G - PHP$ can be reduced to the game complexity on G.

*Supported by the Clore Foundation Doctoral Scholarship
†Supported by the NSF grant n. CCR-9987845

ISSN 1433-8092

1 Introduction

1.1 Proof Space Complexity

The importance of Proof Complexity comes from the close relationship between its fundamental questions and long-standing open problems in Complexity Theory. In its more general setting a Propositional Proof System can be defined as a polynomial time computable function that is onto the set of tautologies [CR79]. In similarity with Circuit Complexity, we have very little knowledge of the properties of arbitrary proof systems, and thus usually we restrict our attention to some simple concrete proof systems. The system receiving most attention by far is the Resolution system. The attention arises from several reasons. Resolution has a single rule, that is relatively simple to analyze. Resolution is used heavily in practice for Automated Theorem Proving. In the last 15 years several fundamental works have analyzed the complexity of proofs in Resolution, showing that many tautologies require exponentially long refutations in Resolution [Hak85, Urq87, CS88, BP96, BW98].

As it is well known, the complexity of an algorithm is measured not only in terms of the running time but also in terms of the *memory consumption*. The *space* not only is a natural measure for the complexity of algorithms, but, as for the time measure, is also widely studied in Complexity Theory.

The proof complexity measure related to the *time* complexity measure is the *size* of a proof, that is the number of *symbols* used in the proof, or when polynomially related, the number of formulas used. Recently [ET99, ABRW00] introduced and studied a new complexity measure for propositional proof systems, analogous to the *space* complexity measure for circuits. For the Resolution system, Esteban and Torán [ET99] proposed to consider as measure for the Resolution space complexity, the number of different clauses that must be simultaneously available (that is *kept in memory*) to obtain the empty clause. Alekhnovich *et al.* [ABRW00] generalized under several aspects, the work [ET99]. First of all they extend the definition of clause space complexity in a natural way to all important propositional proof system such as Frege Systems or Polynomial Calculus. Moreover to measure the memory content in a given moment during a proof they also considered *the variable space*, that is the overall number of variables used, as well as the total number of symbols needed, *the bit space*.

In spite of its recent introduction several non trivial upper and lower bounds for space complexity are already known. Torán in [Tor99] gave lower bounds for clause space in Resolution. He considered two well-known tautologies, for which several lower bounds for the *size* are known: the PHP_n and the so-called Tseitin Tautologies. Alekhnovich *et. al.* [ABRW00] devised a general technique to give non trivial lower bounds for the clause space in Resolution, and in other proof systems. Using this method they obtain non trivial clause space lower bounds in Resolution for class of formulas like PHP_n, GT_n and CT_n.

1.2 Random CNFs

It is well-known that in circuit complexity simple counting arguments show that a random function is hard to compute. In studying the complexity of a given proof system it is natural to ask what is the proof complexity of a tautology taken at random. However we don't have a definition of what is a random tautology. Still, in some cases, if we restrict our attention only to certain kinds of tautologies we can deduce informations on their random behaviour. An easy calculation shows that for a high enough constant Δ, with high probability (i.e. with probability $1 - o(1)$). a random 3-CNF formula with n variables and Δn clauses is unsatisfiable (Δ is called the *clause density*). Let us introduce the definition of a random CNF and the satisfiability threshold.

Definition 1.1 (Random CNFs) *Let $\mathbb{F}_m^{k,n}$ be the probability distribution obtained by selecting m clauses uniformly at random from the set of all $2^k \cdot \binom{n}{k}$ clauses of size k over n variables. $\mathcal{F} \sim \mathbb{F}_m^{k,n}$, means that $\mathcal{F}$ is selected at random from this distribution. A random k-CNF formula is a formula $\mathcal{F} \sim \mathbb{F}_m^{k,n}$.*

Definition 1.2 (Satisfiability Threshold) *Let θ_k be the satisfiability threshold for k-CNFs, i.e. θ_k is the minimal constant such that as $n \to \infty$, whp $\mathcal{F} \sim \mathbb{F}_{\theta \cdot n}^{k,n}$ is unsatisfiable.*[1]

Size proof complexity of unsatisfiable random CNFs has been widely studied. Chvatál and Szmerédi in their seminal paper [CS88] showed that with high probability, any random 3-CNF over n variables and Δn clauses for $\Delta = O(1)$, requires exponentially long Resolution proofs to be refuted. The importance of their work was in showing that in fact Resolution is a very weak proof system, because in some sense almost all unsatisfiable 3-CNF require exponential size proofs to be refuted. Their lower bound was later improved and simplified by Beame and Pitassi in [BP96], and finally improved up to a ratio $\Delta = o(\sqrt{n})$ by Beame, Karp, Pitassi and Saks in [BKPS98], and reformulated in terms of a general technique based on the *width* by Ben-Sasson and Wigderson in [BW98] . All these results, as well as the results presented in this paper can be generalized to k-CNFs for arbitrary constant $k > 3$.

1.3 Our Results

Lower bounds for the clause space of unsatisfiable random 3-CNF didn't follow from any of the techniques devised in the previous works on space complexity [ET99, ABRW00, Tor99]. In fact this was left as an open problem in both [Tor99] and [ABRW00].

In this paper we study the clause space complexity of refuting unsatisfiable random CNF in Resolution. Our main result is the following.

Theorem 1.3 *For any $k \geq 3$, any $0 < \epsilon \leq 1/2$ and any $\Delta > \theta_k$, with high probability refuting a random k-CNF with n variables and $\Delta \cdot n$ clauses requires Clause Space $\Omega\left(n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}}\right)$*

For instance, setting Δ to be a constant we get linear lower bounds. Since [ET99] showed that the clause space of any formula is at most $n+1$, this lower bound is optimal up to a multiplicative constant.

Corollary 1.4 [Constant Δ] *For any constant $\Delta > \theta_k$, a random k-CNF with n variables and Δn clauses requires $\Omega(n)$ clause space to refute.*

Another interesting corollary is for large clause density, which we state for concreteness for $k = 3$.

Corollary 1.5 *For any constant $1 > \delta > 0$, there exists an $\epsilon > 0$ such that with high probability, a random 3-CNF with n variables and $n^{2-\delta}$ clauses requires clause space $\Omega(n^{\epsilon})$ to refute.*

This lower bound which applies for clause density greater than $\sqrt{n}$, is in contrast with the known lower bounds for *size* of proofs within this density range: our best size lower bounds become trivial when the clause density reaches $\sqrt{n}$. Indeed, one corollary of our space lower bound is the first exponential lower bound on the minimal size of a *treelike* refutation, for clause density greater than $\sqrt{n}$ (theorem 5.5).This bound is nearly tight. Previously such lower bounds were known only for special types of treelike proofs, formed by a *Ordered DLL* algorithm [BKPS98].

[1] Currently, the best lower bound on θ_3 is $3.145 \leq \theta_3$ of [A00] and the best upper bound is $\theta_3 \leq 4.5793$ [JSY00] and a recent $\theta_3 \leq 4.506$ claimed by [DBM00].

1.4 Proof Outline

A 3-CNF has an obvious interpretation in terms of bipartite graphs. Under this intepretation, a matching in the graph $G(F)$ associated with F corresponds to a partial assignment satisfying part of the formula F.

In order to prove clause space lower bounds on F, we define a 2-player game (*The Matching Game*) to be played on the bipartite graph $G(F)$, associated with F. The aim of the first player is to prove that there is no perfect matching. The second player is an opponent which instead tries to force a perfect matching. The first player should complete his task "remembering" as few as possible of his moves in the game.

We prove two main properties. First that the clause space of refuting a 3-CNF can be reduced to the natural complexity measure for the game (i.e the minimal number of moves Player I needs to remember to win). Then we prove that when the graph is an expander, the first player needs to remember a large number of moves, where the size is correlated to the expansion parameters of the graph.

It turns out that our characterization of clause space is quite general. Indeed we can extend our result also to the case of another tautology based on bipartite graphs G, the $G-PHP$, introduced by [BW98]. We prove that clause space for $G-PHP$ can be reduced to the game complexity of the Matching Game played on G.

The paper is organized as follows. In Section 2 we give some preliminary definitions. Section 3 is dedicated to the definition of the Matching Game and its relationship with the clause space. In Section 4 we prove a lower bound for the Matching Game played on graphs from the class of (r,ϵ)-bipartite expanders. In Section 5 we prove a Lemma studying under which parameters $r=r(n)$ and $\epsilon=\epsilon(n)$, a random k-CNF over n variables defines an (r,ϵ)-bipartite expander. This result joint with results from previous sections gives the lower bound for resolution. Finally in Section 6 we show that the Matching Game applies also to the $G-PHP$.

2 Definitions

Let V be finite set of boolean variables. A *literal* l is either a variable $x \in V$ or its negation $\bar{x}$. A *clause* is a disjunction (eventually empty) of literals. A *CNF formula* is a conjunction of clauses and it will be convenient to see it as a set of clauses. We use calligraphic letters (e.g. $\mathcal{F}, \mathcal{C}$) for denoting CNF formulas, and capital letters for denoting clauses. A 3-CNF formula is a CNF formula in which all the clauses have exactly 3 literals.

For $\mathcal{F}$ a formula, $Vars(\mathcal{F})$ is the set of variables appearing in $\mathcal{F}$. A *restriction* on $\mathcal{F}$ is a partial function $\rho : Vars(\mathcal{F}) \to \{0,1\}$. $\mathcal{F}_\rho$ denotes the CNF formula obtained from $\mathcal{F}$ after applying ρ in the standard way: if a literal ℓ is set to 1 by ρ, then all clauses C of $\mathcal{F}$ such that $\ell \in C$ disappear in $\mathcal{F}|_\rho$; all clauses C in $\mathcal{F}$ such that $C = \bar{\ell} \vee D$ become D in $\mathcal{F}_\rho$. We say $\rho(x) = \star$ when $x \notin Domain(\rho)$. The size of a restriction, $|\rho|$, is $|Domain(\rho)|$.

2.1 Clause Space in Resolution

Resolution is a refutation proof system for unsatisfiable CNF formulas based on the following propositional *resolution rule*:

$$\frac{D_1 \cup \{x\} \qquad D_2 \cup \{\bar{x}\}}{D_1 \cup D_2}$$

We define a *space complexity measure* following the definitions of [ABRW00]. Let $[n]$ be the set $\{1, \ldots, n\}$.

Definition 2.1 *A* configuration *is a set of clauses. A* refutation π *of a CNF* $\mathcal{F}$*, is a sequence of configurations* $\mathcal{C}_0, \ldots, \mathcal{C}_s$ *such that* $\mathcal{C}_0 = \emptyset$*,* $\mathcal{C}_s = \{\blacksquare\}$ *(the empty clause) and for all* $t \in [s]$*,* $\mathcal{C}_t$ *is obtained from* $\mathcal{C}_{t-1}$ *by one of the following rules:*

AXIOM DOWNLOAD $\mathcal{C}_t := \mathcal{C}_{t-1} \cup C$ *for some clause* $C \in \mathcal{F}$*;*

MEMORY ERASING $\mathcal{C}_t := \mathcal{C}_{t-1} - \mathcal{C}'$ *for some* $\mathcal{C}' \subseteq \mathcal{C}_{t-1}$*;*

INFERENCE ADDING $\mathcal{C}_t := \mathcal{C}_{t-1} \cup C$*, for some* C *obtained by a single application of the resolution rule to two clauses in* $\mathcal{C}_{t-1}$*.*

The following definitions define the measure for the resolution space: the *clause space*. Let $\pi_F \vdash F$ denote that π_F is a resolution derivation (in the form of sequence of configurations) of F.

Definition 2.2 (Clause Space) *For* $\mathcal{C}$ *a set of clauses,* $|\mathcal{C}|$ *is the number of clauses in* $\mathcal{C}$*. The* space *of a set of configurations* $\pi = \{\mathcal{C}_0, \ldots, \mathcal{C}_s\}$ *is the maximal number of clauses in a configuration of* π*.*

The clause space *of refuting an unsatisfiable CNF* $\mathcal{F}$*, denoted* $CSpace(\mathcal{F})$*, is the minimal space of a resolution refutation of* $\mathcal{F}$*.*

Definition 2.3 (Width) $|C|$ *(also denoted by* $w(C)$ *- the* width *of* C*) is the number of literals in the clause* C*. The width of a set of clauses* $\mathcal{F}$ *is the width of the largest clause in* $\mathcal{F}$*. The width of a resolution refuation of* $\mathcal{F}$ *is the width of the largest clause in the refutation. Finally, the width of refuting an unsatisfibale set of clauses* $\mathcal{F}$*, denoted by* $w(\vdash \mathcal{F})$ *is the minimal width taken over all refutations of* $\mathcal{F}$*.*

3 The Matching Game

We wish to reduce the space required to refute a CNF formula to a natural combinatorial game played on a bipartite graph. We shall prove lower bounds for this game whenever the bipartite graph is an expander.

Definition 3.1 Bipartite Expanders *A bipartite graph* $G =< V \cup U, E >$ *is called an* (r, ϵ)-bipartite expander *if*

$$\forall V' \subset V \quad |V'| \leq r, \quad |N(V')| \geq (1+\epsilon)|V'|,$$

where $N(V')$ *is the set of neighbors of* V'*.*

3.1 Proving there is no Perfect Matching

For $G =< (V \cup U), E >$ a bipartite graph, if $|V| > |U|$ then there is no matching of V into U. We wish to prove this claim, using "limited space". For this purpose let us define a two player game. The players are Pete (Prover) and Dana (Disprover). Pete tries to prove that there is no matching from V to U, and Dana tries to prove that such a matching exists. Pete has k fingers, numbered $\{1, \ldots, k\}$, and Dana has k fingers, numbered identically. We start with all vertices of G uncovered, and on each round one of the following occurs:

1. Pete Places a finger j on some uncovered $v \in V$, and Dana must answer by placing her finger j on some uncovered $u \in U$ that is a neighbor of v.

2. Pete removes a finger j from a covered $v \in V$, and Dana answers by removing her finger j from its covered neighbor $u \in U$.

Notice that the set of fingers placed on the graph corresponds naturally to a partial matching in G : each v covered by a finger j of Pete is matched to the u that is covered by Dana's finger j in reply. Pete wins the game when he places a finger on some vertex such that all its neighbors are already covered by Dana. If Pete cannot win the game, then Dana wins. We define $MSpace(G)$ (Matching Space) to be the minimal number of fingers that Pete needs in order to win the game. Clearly $MSpace(G) \leq |U| + 1$.

3.2 Reducing Clause Space to Matching Space

Definition 3.2 *For $\mathcal{C}$ a CNF formula, define $G(\mathcal{C})$ to be the following bipartite graph:*

1. *V is the set of clauses.*

2. *U is the set of variables.*

3. *$(C, x) \in E(G)$ iff the variable x appears in the clause C (we do not care whether x appears as a positive or negative literal).*

The main claim of this section is:

Theorem 3.3 $CSpace(\mathcal{C}) \geq MSpace(G(\mathcal{C}))$.

Proof: For $m = \{(C_{i_1}, x_{i_1}), \ldots (C_{i_k}, x_{i_k})\}$ a partial matching in $G(\mathcal{C})$ of size k, define $\rho(m)$ to be the restriction of size k that sets the variable x_{i_j} to the value that satisfies the clause C_{i_j}, for $j = 1 \ldots k$, and leaves all other variables unassigned.

Assume Dana has a winning strategy when the matching game is played on $G(\mathcal{C})$ using k fingers. We will use this strategy to show that every set of clauses derivable in clause space k is satisfiable. Let $\mathcal{C}_0, \ldots \mathcal{C}_\ell$ be a derivation from $\mathcal{C}$, of space k. We construct inductively a sequence of partial matchings in $G(\mathcal{C})$, $m_0, \ldots m_\ell \quad m_t \subset E \quad t = 0 \ldots \ell$, that maintains the following properties for all $t = 0 \ldots \ell$:

1. m_t is the matching obtained by playing the matching game with k fingers for $t' \leq t$ rounds.

2. $|m_t| \leq |\mathcal{C}_t|$.

3. $\mathcal{C}_t|_{\rho(m_t)} = 1$

m_0 is the empty matching. For the induction step, we prove the claim according to the type of rule used at time t:

1. **Axiom Download:** If the new axiom C is satisfied by the restriction, we do nothing, and clearly all properties are maintained. Otherwise, the number of fingers Pete has at time $t-1$ is at most $|C_{t-1}| \leq k - 1$, and thus, when Pete places a finger on C in $G(\mathcal{C})$, Dana can respond by placing a finger on some uncovered x appearing in C. We set $m_t = m_{t-1} \cup \{(C, x)\}$. All properties are maintained: the new matching corresponds to playing one more round of the matching game. The memory size and the matching size are both incremented by one. $\mathcal{C}_t|_{\rho(m_t)} = 1$, because $\mathcal{C}_{t-1}|_{\rho(m_{t-1})} = 1$, and $C|_{\rho(\{(C,x)\})} = 1$.

2. **Inference:** Set $m_t = m_{t-1}$. By the soundness of resolution, we know that $\mathcal{C}_{t-1} \models \mathcal{C}_t$ and hence $\mathcal{C}_t|_{\rho(m_t)} = \mathcal{C}_t|_{\rho(m_{t-1})} = 1$. Since $|\mathcal{C}_t| > |\mathcal{C}_{t-1}|$ it also follows that $|m_t| \leq |\mathcal{C}_t|$.

3. **Memory Erasure:** $\mathcal{C}_t = \mathcal{C}_{t-1} - C'$ for some clauses C'. Any assignment satisfying $\mathcal{C}_{t-1}$ also satisfies $\mathcal{C}_t$. We set $m_t \subseteq m_{t-1}$ to be some minimal size submatching such that $\mathcal{C}_t|_{\rho(m_t)} = 1$. Since $\rho(m)$ is in 1-1 correspondence with m, for any m, we have that $|m_t| \leq |\mathcal{C}_t|$ using the locality lemma for Resolution from [ABRW00].

   Lemma 3.4 (Locality lemma) *[ABRW00] Let ρ be a restriction and $\mathcal{C}$ be a set of clauses, such that $(\bigwedge_{C\in\mathcal{C}} C|_\rho) \equiv 1$. Then there exists a sub-restriction ρ' of ρ, such that $(\bigwedge_{C\in\mathcal{C}} C|_{\rho'}) \equiv 1$, and $|\rho'| \leq |\mathcal{C}|$.*

Thus we get that the clause space required to refute $\mathcal{C}$ is at least $MSpace(G(\mathcal{C}))$ and the theorem is proved. □

4 Lower Bound on the Matching Game

We shall now prove lower bounds on the Matching Space when G is a good expander. In the proof we extensively use Hall's theorem:

Theorem 4.1 (Hall's Matching Theorem) *For a bipartite graph $G =< V \cup U, E >$, there exists a perfect matching of $V' \subseteq V$ into U iff $\forall V'' \subseteq V', |N(V'')| \geq |V''|$.*

We call V' *minimal unmatchable* into U' if V' is unmatchable into U', and any proper subset of V' is matchable into U'. By Hall's theorem, this occurs iff $|N(V')| < |V'|$ but for all $V'' \subset V'$ $|N(V'')| \geq |V''|$.

Theorem 4.2 (Matching Space Lower Bound) *If a graph $G =< (V \cup U), E >$ is an (r, ϵ)-bipartite expander, then*

$$MSpace(G) > \frac{\epsilon \cdot r}{2 + \epsilon}$$

Proof: Suppose the game is played until at time T, Pete wins. Thus, at time $0 \leq t < T$ the set of covered vertices corresponds to a partial matching in G. For any $0 \leq t < T$, let $E_t \subseteq E$ be the matching at time t, let $s_t = |E_t|$ be the matching space at time t, and let V_t (resp. U_t) be the set of uncovered vertices in V (resp. U). We define a strategy for Dana.

Strategy 4.3 *Answer trying to maintain the property:*

$$\forall V' \subseteq V_t, |V'| \leq r - s_t,\ V' \text{ can be matched into } U_t. \tag{1}$$

At $t = 0$ $s_t = 0$, and the property holds, by the definition of expansion and Hall's theorem. Let t be the first time property (1) does not hold. We claim that $s_t \geq \frac{\epsilon r}{2+\epsilon}$. The proof of this claim is divided into two cases, according to the step taken at time t.

1. **Pete removes a finger from v:** Let u be the vertex matched to v at time $t-1$ (i.e. $(v, u) \in E_{t-1}$). $V_t = V_{t-1} \cup \{v\}$, $U_t = U_{t-1} \cup \{u\}$ and $s_t = s_{t-1} - 1$. There exists some $V' \subset V_t$ of size at most $r - s_t$, that is minimal unmatchable into U_t.

   Claim 4.4 $|V'| = r - s_t$.

Proof: By definition, $|V'| \leq r - s_t$. Assume, for the sake of contradiction, that $|V'| < r - s_t$. By the minimality of t, every set of size $(r - s_t) - 1 = r - s_{t-1}$ which *does not* include v, is matchable into U_t because it is even matchable into $U_{t-1} \subset U_t$. A set of size $r - s_{t-1}$ which *does* includes v can be matched into U_t in the following way: match v to u, and use the matching of the remaining set (of size $r - s_{t-1} - 1$) into U_{t-1}, which must exist, by the minimality of t. We conclude that V' is matchable into U_t, contradiction. Thus $|V'| \geq r - s_t$. □

Let us calculate the size of the set of neighbors of V' in the original graph G. On the one hand, $|V'| \leq r$, and hence by the definition of expansion:

$$|N(V')| \geq (1 + \epsilon)|V'| \tag{2}$$

On the other hand, V' is *minimal* unmatchable into U_t, and hence by Hall's matching theorem $|V'| > |N(V') \cap U_t|$. The only other possible neighbors of V' in G are in the matching E_t, which has size s_t. Thus we get

$$|V'| + s_t > |N(V')| \tag{3}$$

Combining the two inequalities and setting $|V'| = r - s_t$ we get:

$$|V'| + s_t > (1 + \epsilon)|V'| \quad \Rightarrow \tag{4}$$

$$s_t > \epsilon \cdot |V'| \quad \Rightarrow \tag{5}$$

$$s_t > \frac{\epsilon \cdot r}{1 + \epsilon} > \frac{\epsilon \cdot r}{2 + \epsilon} \tag{6}$$

Case 1 is proven.

2. **Pete places a finger on v:** Let $u_1, \ldots u_d$ be the neighbors of v in U_{t-1} (for some $d > 0$). For any choice u_i that Dana makes, there is some $V^i \subset V_t$, $|V^i| \leq r - s_t$ that is minimally unmatchable into $U_{t-1} \setminus \{u_i\}$.

Claim 4.5 *There is no matching of $\tilde{V} = \cup_{i=1}^{d} V_i \cup \{v\}$ into U_{t-1}.*

Proof: Assume for the sake of contradiction that $\tilde{V}$ is matchable into U_{t-1}, and fix such a matching. Let $U^i \subset U_{t-1}$ be the image of V^i under this matching. Recalling that V^i is minimal unmatchable into $U_{t-1} \setminus \{u_i\}$, we conclude that $u_i \in U^i$. This is true for any $i = 1 \ldots d$, and hence all neighbors of v are already taken by the matching on $\cup_{i=1}^{d} V^i$. Thus v cannot be matched, contradiction. □

By the claim, and the minimality of t, $|\tilde{V}| > r - s_{t-1}$, and since $s_t = s_{t-1} + 1$, we get $|\cup_{i=1}^{d} V^i| > r - s_t$.

Claim 4.6 *For $i = 1 \ldots d$, $|N(V^i) \cap U_{t-1}| = |V^i|$.*

Proof: $|V^i| \leq r - s_t < r - s_{t-1}$, so V^i is matchable into U_{t-1}, and hence $|N(V^i) \cap U_{t-1}| \geq |V^i|$. V^i is minimal unmatchable into $U_{t-1} \setminus \{u_i\}$, so $|N(V^i) \cap U_{t-1} \setminus \{u_i\}| < |V^i|$, and hence $|N(V^i) \cap U_{t-1}| \leq |V^i|$ □

For all i, $|V_i| \leq r - s_t$, whereas, $|\cup_{i=1}^{d} V^i| > r - s_t$. There must exist some subset $I \subseteq [d]$ such that $\frac{r - s_t}{2} < |\cup_{i \in I} V^i| \leq r - s_t$. Fix such an I, and denote $V' = \cup_{i \in I} V^i$.

Claim 4.7 *Suppose $V^1, \ldots V^d$ are sets such that for all $i \in [d]$*

(a) $|N(V^i)| = |V^i|$.

(b) V^i *is matchable into* U.

Then $|N(\cup_{i\in[d]} V^i)| \leq |\cup_{i\in[d]} V^i|$.

Proof: By induction on d. For $d = 1$ the claim is simply condition a. Let $V^d_{NEW} = V^d \setminus (\cup_{i=1}^{d-1} V^i)$ be the set of "new" vertices added by V^d, and $V^d_{OLD} = V^d \setminus V^d_{NEW}$. If $V^d_{NEW} = \emptyset$ there is nothing to prove. Otherwise, assume for the sake of contradiction that $|N(V^d_{NEW}) \setminus N(\cup_{i=1}^{d-1} V^i)| > |V^d_{NEW}|$, i.e. V^d adds more neighbors than its size, when it is added to $\cup_{i=1}^{d-1} V^i$. By property 2 we know that $|N(V^d_{OLD})| \geq |V^d_{OLD}|$. Thus

$$\begin{aligned} |N(V^d)| &= |N(V^d_{OLD})| + |N(V^d_{NEW}) \setminus N(V^d_{OLD})| \\ &\geq |N(V^d_{OLD})| + |N(V^d_{NEW}) \setminus N(\cup_{i=1}^{d-1} V^i)| \\ &> |V^d_{OLD}| + |V^d_{NEW}| \\ &> |V^d| \end{aligned}$$

The second inequality follows from the fact that $V^d_{OLD} \subseteq \cup_{i=1}^{d-1} V^i$. We have reached a contradiction to property (a), and the claim is proven. □

Let us calculate once again the size of the set of neighbors of V' in the initial graph G. On the one side $s_{t-1} + |N(V') \cap U_{t-1}| \geq |N(V')|$. Applying claims 4.6, 4.7 to $\{V^i\}_{i\in I}$ gives us

$$s_{t-1} + |V'| \geq |N(V')|.$$

On the other hand, the expansion property and the fact $|V'| \leq r$ give us

$$|N(V')| \geq (1+\epsilon)|V'|.$$

Combining the two together, we get:

$$\begin{aligned} |V'| + s_{t-1} &\geq (1+\epsilon)|V'| \quad \Rightarrow \quad (s_t > s_t - 1) \\ s_t &> \epsilon|V'| \quad \Rightarrow \quad (|V'| \geq \frac{r - s_t}{2}) \\ s_t &> \frac{\epsilon \cdot r}{2+\epsilon} \end{aligned}$$

Case 2 is proven, and with it the theorem. □

5 Proof of the Theorem 1.3

In this section we complete the proof of the main theorem 1.3.

Proof of Theorem 1.3: By the following lemma 5.1, with high probability $\mathcal{F} \sim \mathbb{F}^{k,n}_{\Delta\cdot n}$ is an $\left(\Omega(n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}}), \epsilon\right)$-bipartite expander. By theorem 4.2 the matching game played on $G(\mathcal{F})$ requires space $\left(\Omega(n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}})\right)$, and finally by theorem 3.3 the clause space is at least $\left(\Omega(n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}})\right)$. □

The rest of this section is devoted to analyzing the expansion parameters of a random $G(\mathcal{F})$, using a union bound.

Lemma 5.1 *For each integer $k \geq 3$ and $0 < \epsilon < 1/2$, there exists a constant $\kappa = \kappa(k, \epsilon)$ such that the following holds. For $\mathcal{F} \sim \mathbb{F}^{k,n}_{\Delta \cdot n}$, with probability tending to 1 as n tends to ∞, $G(\mathcal{F})$ is an $\left(\kappa \cdot n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}}, \epsilon\right)$-bipartite expander.*

Proof: Let $\mathcal{F} \sim \mathbb{F}^{k,n}_{\Delta \cdot n}$ a k-CNF and let $G(\mathcal{F})$ be the bipartite graph associated with $\mathcal{F}$. Let $r = \kappa n \Delta - \frac{1+\epsilon}{k-2-\epsilon}$, where the constant κ will be determined later. Let BAD be the event that $G(\mathcal{F})$ is not an (r, ϵ)-bipartite expander. We prove that the $\Pr[BAD]$ tends to 0 as n grows. We bound the probability of BAD by the probability that there exists a set $V' \subseteq V$, with $1 \leq |V'| \leq r$, such that $|N(V')| < (1+\epsilon)|V'|$ and then we use the union bound to upper bound this probability.

Observe that there are $\binom{\Delta n}{i}$ possible sets $V' \subseteq V$ of size i, and there are $\binom{n}{(1+\epsilon)i}$ possible small sets of neighbors of V'. For a given set V' of size i, and a given set U' of size $(1+\epsilon)i$, the probability that $N(V') \subseteq U'$ is

$$P_i = \left(\frac{\binom{(1+\epsilon)i}{k}}{\binom{n}{k}}\right)^i \leq \left(\frac{(1+\epsilon)i}{n}\right)^{ki}$$

Let us bound the probability of the BAD event:

$$\begin{aligned}
\Pr[BAD] &\leq \sum_{i=1}^{r} \binom{\Delta n}{i} \cdot \binom{n}{(1+\epsilon)i} \cdot P_i \\
&\leq \sum_{i=1}^{r} \left(\frac{e\Delta n}{i}\right)^i \cdot \left(\frac{en}{(1+\epsilon)i}\right)^{(1+\epsilon)i} \cdot \left(\frac{(1+\epsilon)i}{n}\right)^{ki} \\
&\leq \sum_{i=1}^{r} \left[c \cdot \Delta \cdot \left(\frac{i}{n}\right)^{(k-2-\epsilon)}\right]^i \qquad (7)
\end{aligned}$$

The first inequality uses the well-known estimation $\binom{a}{b} \leq \left(\frac{ea}{b}\right)^b$, and the second is true for the constant $c = c(k, \epsilon) = e^{2+\epsilon} \cdot (1+\epsilon)^{k-1-\epsilon}$ (recall that $0 \leq \epsilon \leq 1/2$).

We now split the proof into cases:

Case 1: $\Delta \geq n^{1/10}$

$$\begin{aligned}
\Pr[BAD] &\leq \sum_{i=1}^{r} \left[c \cdot \Delta \cdot \left(\frac{i}{n}\right)^{(k-2-\epsilon)}\right]^i \\
&\leq \sum_{i=1}^{r} \left[c \cdot \Delta \cdot \left(\frac{r}{n}\right)^{(k-2-\epsilon)}\right]^i \\
&\leq \sum_{i=1}^{r} \left[\frac{1}{2} \cdot \Delta^{-\epsilon}\right]^i
\end{aligned}$$

This geometric sum vanishes as n goes to ∞, because $\Delta > n^{1/10}$.

Case 2: $\Delta < n^{1/10}$

Notice that since $\Delta < n^{1/10}$, $k \geq 3$, and $\epsilon \leq 1/2$, then $r \geq n^{7/10}$. We split the sum of equation (7) into two:

$$\Pr[BAD] \leq \sum_{i=1}^{r}[c\cdot\Delta\cdot(\frac{i}{n})^{(k-2-\epsilon)}]^i \quad (8)$$

$$\leq \sum_{i=1}^{\sqrt{n}}[c\cdot\Delta\cdot(\frac{i}{n})^{(k-2-\epsilon)}]^i \quad (9)$$

$$+ \sum_{i=\sqrt{n}}^{r}[c\cdot\Delta\cdot(\frac{i}{n})^{(k-2-\epsilon)}]^i \quad (10)$$

We bound the first sum by the geometric sum

$$(9) \leq \sum_{i=1}^{\sqrt{n}}[c\cdot n^{1/10}\cdot n^{-\frac{1}{2}(k-2-\epsilon)}]^i$$

$$\leq \sum_{i=1}^{\sqrt{n}}[c\cdot n^{1/10-1/4}]^i$$

$$\leq \sum_{i=1}^{\sqrt{n}}[c\cdot n^{-1/4}]^i$$

As for the second sum, setting $\kappa(k,\epsilon) = \left(\frac{1}{2c(k,\epsilon)}\right)^{\frac{1}{k-2-\epsilon}}$, we get that $(\frac{r}{n})^{k-2-\epsilon} = \frac{1}{2c\Delta^{1+\epsilon}}$. Recalling $\Delta > \theta_k > 1$ we get:

$$(10) \leq \sum_{i=\sqrt{n}}^{r}[c\cdot\Delta\cdot(\frac{r}{n})^{(k-2-\epsilon)}]^{\sqrt{n}}$$

$$\leq \sum_{i=\sqrt{n}}^{r}[\frac{c\cdot\Delta}{2c\Delta^{1+\epsilon}}]^{\sqrt{n}} \leq n\cdot 2^{-\sqrt{n}}$$

Clearly, both sums vanish as n approaches ∞. lemma 5.1 is proven. □

5.1 Lower Bounds for Treelike Resolution Size

One nice consequence of the Space lower bound of theorem 1.3 is a new lower bound for minimal size of treelike resolution refutations for high clause density ($\Delta > \sqrt{n}$). A treelike resolution proof is a proof in which every derived clause can be used at most once in resolution inference. [BKPS98] proved the following upper bound for the minimal size of tree-like resolution proofs for random CNFs.

Theorem 5.2 *[BKPS98] Let $k \geq 3$, and $\Delta > \theta_k$. With high probability the size of a minimal tree-like resolution refutation of a random k-CNF with n variables and Δn clauses, is $2^{O(n/\Delta^{1/(k-2)})}n^{O(1)}$.*

This upper bound is achieved by a satisfiability algorithm called *ordered DLL*, which produces a treelike resolution proof. Moreover, [BKPS98] proved a matching lower bound for this algorithm.

The question of existence of short arbitrary treelike resolution proofs has been open for $\Delta \geq \sqrt{n}$, and the best previous lower bounds were those of [BKPS98, BW98], which followed essentially from width lower bounds (for simplicity we cite only the case of 3-CNF):

Theorem 5.3 *[BKPS98, BW98] For any $0 < \epsilon < 1/2$, if $\Delta = n^{1/2-\epsilon}$, then with high probability, a random 3-CNF with n variables and Δn clauses requires treelike resolution size of* $\exp\left(\Omega(n/\Delta^{\frac{2}{1-\epsilon}})\right)$.

We can now improve the lower bound using the following theorem of [ET99].

Theorem 5.4 *[ET99] Let ϕ be an unsatisfiable CNF formula with tree-like resolution refutations of size S. Then ϕ has a resolution refutation of space $\lceil \log S \rceil + 1$.*

Plugging in theorem 1.3 we get the following lower bound, which nearly reaches the upper bound of [BKPS98] mentioned previously.

Theorem 5.5 *For any $k \geq 3$, any $0 < \epsilon \leq 1/2$, and any $\Delta > \theta_k$, with high probability refuting a random k-CNF with n variables and $\Delta \cdot n$ clauses requires treelike resolution size of* $\exp\left(\Omega\left(n \cdot \Delta^{-\frac{1+\epsilon}{k-2-\epsilon}}\right)\right)$.

We give the explicit result for 3-CNFs with high clause density.

Theorem 5.6 *For any $0 < \epsilon \leq 1/2$, there exists a $\delta > 0$ such that with high probability, refuting a random 3-CNF with n variables and $n^{2-\epsilon}$ clauses requires treelike refutation size of* $\exp\left(\Omega(n^{\delta})\right)$.

For general resolution, we do not have any lower bounds for $\Delta \geq \sqrt{n}$. This is in contrast with the space and the minimal treelike size, for which we have nearly optimal lower bounds.

It would be interesting to understand the space complexity around the range $\Delta = n$ and observe whether passing this point causes formulas to have constant space refutations, as well as understanding in general whether our lower bounds for space are tight.

6 Space Lower Bounds for $G - PHP$

An Optimal Space lower bound for refutation of the pigeonhole principle in Resolution was proved by [ET99], and even extended to the Polynomial Calculus by [ABRW00]. The Graph Pigeonhole Principle, $G - PHP$, was introduced by [BW98] as a generalization for which size lower bounds still apply. The idea is to restrict the number of holes that a pigeon may go to, according to some underlying graph G. We prove that the space complexity of refuting the $G - PHP$ to the matching game, in a generalization of theorem 3.3.

Definition 6.1 (G – PHP) *Let $G = ((V \cup U), E)$ be a bipartite graph, $|V| = m$, $|U| = n$. Assign each edge a distinct variable x_e. $G - PHP$ is the conjunction of the following clauses:*

$P_v \stackrel{\text{def}}{=} \bigvee_{v \in e} x_e$ *for* $v \in V$.

$H^u_{v,v'} \stackrel{\text{def}}{=} \bar{x}_e \vee \bar{x}_{e'}$ *for* $e = (v,u), e' = (v',u)$, $v, v' \in V$, $v \neq v'$, $u \in U$.

Denote by $\mathcal{H}$ the conjunction of $H^u_{v,v'}$, for all $e=(v,u), e'=(v',u),\ \ v,v'\in V,\ \ v\neq v',\ \ u\in U$. For $\mathcal{C}$ a set of clauses over $Vars(G-PHP)$, and ρ a partial restriction that does not falsify $\mathcal{H}$, we say $\mathcal{C}|_\rho \equiv 1 (\text{mod } \mathcal{H})$ if $\mathcal{H} \models \mathcal{C}|_\rho$, i.e. any assignment that satisfies $\mathcal{H}$, satisfies $\mathcal{C}|_\rho$ as well.

Lemma 6.2 *A restriction falsifies $\mathcal{H}$ iff there exist a pair of edges $e_1=(v,u)$, $e_2=(v',u)$ such that $v\neq v'$ and $e_1,e_2\in\{e : x_e|_\rho = 1\}$.*

Theorem 6.3 *For any graph G, $CS(G-PHP)\geq Space(G)$.*

Proof: For $m=\{(v_{i_1},u_{i_1}),\ldots(v_{i_k},u_{i_k})\}$ a partial matching in G of size k, we define its corresponding restriction to set 1's to all edges in m, 0's to all edges (v,u) such that u is in matched in m to some $v'\neq v$, and leave all other variables unassigned. Formally:

$$x_{(v,u)}|_{\rho(m)} = \begin{cases} 1 & (v,u)\in m \\ 0 & (v,u)\notin m \text{ And } \exists v'\in V \ \ (v',u)\in m \\ \star & \text{otherwise} \end{cases}$$

As in the proof of theorem 3.3, suppose Dana can win when the matching game over G is played with k pebbles. Let $\mathcal{C}_0,\ldots\mathcal{C}_\ell$ be a derivation from $G-PHP$ (in the form of sequence of configurations) of space k. We construct inductively a sequence of matchings $m_0,\ldots m_\ell$ that maintains the following properties for all $t=0\ldots\ell$:

1. $|m_t|\leq|\mathcal{C}_t|$.
2. $\mathcal{C}_t|_{\rho(m_t)}\equiv 1 \text{ (mod } \mathcal{H})$.

Notice that for a matching m, $\rho(m)$ does not falsify $\mathcal{H}$, and can be easily extended to an assignment that satisfies $\mathcal{H}$ (by setting all unassigned variables to 0). Thus, condition 2 implies that $\mathcal{C}_t$ is satisfiable for all $t=0\ldots\ell$.

m_0 is the empty matching. For the induction step, we prove the claim according to the type of step taken:

1. **Axiom Download:** Suppose we download the axiom C. If $C\in\mathcal{H}$, we set $m_t=m_{t-1}$, and it is easy to see that both conditions are maintained. If $C=P_v$, Pete places a blue pebble on v in the graph G, and Dana places a red pebble on some $u\in N(v)$ (this is possible because $|m_{t-1}|<k$ and Dana wins when the game is played with k pebbles). We set $m_t=m_{t-1}\cup\{(v,u)\}$, and once again, it is easy to verify that both conditions are maintained.
2. **Inference:** By the soundness of resolution, $\mathcal{C}_{t-1}\models\mathcal{C}$, and hence $\mathcal{C}_t|_{\rho(m_{t-1})}\equiv 1 \pmod{\mathcal{H}}$. Additionally, $|\mathcal{C}_t|=|\mathcal{C}_{t-1}|+1$, so setting $m_t=m_{t-1}$ maintains both conditions.
3. **Memory Erasure:** Follows from the following locality claim, which is similar to the locality lemma of [ABRW00]

   Lemma 6.4 *Let $\mathcal{C}$ be a set of clauses over $Vars(G-PHP)$, satisfiable $\pmod{\mathcal{H}}$. For all matching m in G such that $\mathcal{C}|_{\rho(m)}\equiv 1 \pmod{\mathcal{H}}$ and for all clauses $C\in\mathcal{C}$, there exists an edge $e_C\in m$, such that*

   - *$C|_{\rho(\{e_C\})}\equiv 1 \pmod{\mathcal{H}}$ and*
   - *for all $C'\in\mathcal{C}$, $C'\neq C$ $C'|_{\rho(\{e_{C'}\})}\not\equiv 0 \pmod{\mathcal{H}}$.*

Proof: Fix any $C \in \mathcal{C}$. Let m be a matching in G such that $\mathcal{C}|_{\rho(m)} \equiv 1 \pmod{\mathcal{H}}$. We have that in particular $C|_{\rho(m)} \equiv 1 \pmod{\mathcal{H}}$. Now look at C. If $\rho(m)$ makes C true fixing some positive literal x_e, then we fix $e_C = e$. Obviously $C|_\rho(\{e_C\}) \equiv 1 \pmod{\mathcal{H}}$ and $\rho(\{e_C\})$ cannot falsify any other clauses in $\mathcal{C}$ since $e \in m$.

Otherwise $\rho(m)$ makes true C satisfying some negated literals $\bar{x}_e$. Assume $e = (v, u)$, then by definition of $\rho(m)$, there is a $v' \in V$ such that $e' = (v'u) \in m$. Fix $e_C = e'$. As before this edge is good to prove our claim. □

Thus if $\mathcal{C}_t \subset \mathcal{C}_{t-1}$ we pick from m_{t-1} according to the previous lemma one edge per clause in $\mathcal{C}_t$, and get m_t that satisfies both properties. □

7 Open Questions

1. The *variable space* of a CNF formula $\mathcal{C}$ is $VSp(\mathcal{C}) \stackrel{\text{def}}{=} \sum_{C \in \mathcal{C}} w(C)$, the variable space of a proof is the maximal variable space of a configuration in the proof, and the variable space of refuting a formula is the minimal variable space of a proof. For any $\mathcal{F}$ over n variables, $VSpace(\mathcal{F}) \leq n^2$, because $CSpace(\mathcal{F}) \leq n$. [ABRW00] proved $\Omega(n^2)$ lower bounds for a certain formula with initial width n. Can one find a 3 CNF for which $VSpace(\mathcal{F}) = \Omega(n^2)$? Is this true for a random 3-CNF with Δn clauses (constant Δ) ? We believe the answer is positive.

2. What is the clause space complexity of refuting a random CNF formula in the Polynomial Calculus ? We suspect that one should get essentially the same lower bounds as for resolution.

3. For many hard tautologies we get linear lower bounds on the *width* and on the *clause space*. This is true for Tseitin graph formulas, the Pigeonhole principle, and random formulas. Notice that width is also a space measure : it is the maximal space of a single clause in the proof. What is the relationship between the two measures ? At least in one aspect width is "harder" than space. A width lower bound yields a size lower bound for treelike *and* general resolution, whereas a space lower bound yields a size lower bound only for treelike resolution. For this reason we conjecture that $CSpace(\mathcal{C}) \geq width(\mathcal{C})$. Is this true ? can one find a counter example ?

4. The following question was raised by Ron Lavi. One may view the graph matching game as an online problem. Let G be a fixed bipartite graph, with $|V| > |U|$. One receives "matching requests" online, and wishes to keep the set matched. The strategy we presented for Dana requires her to compute on each request the matching properties for an exponential number of subsets of V, and doing this in the trivial is inefficient. Can one find a polynomial time algorithm that would operate as well as Dana's strategy ?

8 Acknowledgements

We thank Avi Wigderson, Alexander A. Razborov and Michael Alekhnovich for helpful discussions and Michele Zito for remarks about the satisfiability threshold.

References

[A00] D. Achlioptas. Setting 2 variables at time yields a new lower bound for random 3-SAT. *In Proceedings of 32th STOC*. pp. 28-37 (2000).

[ABRW00] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, A. Wigderson. Space complexity in propositional calculus. In *Proceedings of the* 32*nd STOC*, pages 358–367, 2000.

[BKPS98] P. Beame, R. Karp, T. Pitassi, M. Saks. The efficiency of resolution and Davis Putnam procedures. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC-98)*, pages 561–571, New York, May 23–26 1998. ACM Press.

[BP96] P. Beame, T. Pitassi. Simplified and Improved Resolution Lower Bound. *FOCS'96*, pp. 274-282, 1996.

[BW98] E. Ben-Sasson, A. Wigderson. Short Proofs are Narrow - Resolution made Simple. In *Proceedings of the* 31*st STOC*, pages 517–526, 1999.

[CS88] V. Chvátal, E. Szemerédi. Many hard examples for resolutions. *Journal of the ACM* **35** pp. 759-768 (1988).

[CR79] S. A. Cook, R. Reckhow. The relative efficiency of propositional proof systems. In *J. of Symbolic Logic*, Vol. 44 (1979), pp. 36-50.

[DBM00] O. Dubois, Y. Boufkhad, J. Mandler. Typical random 3-SAT formulae and the satisfiability problem. *In 11-th SODA* pp. 126-127 (2000).

[ET99] J. L. Esteban, J. Toran. Space bounds for Resolution. In *Proceedings of the* 16*th* STACS, pages 530–539, 1999.

[Hak85] A. Haken. The intractability of resolution. *Theoretical Computer Science* **35** pp. 297-308 (1985).

[JSY00] S. Janson, Y.C. Stamatiou, M. Vamvakari. Bounding the unsatisfiability threshold for 3-SAT. *Random Structure and Algorithms* (17) 2 pp.118-116 (2000).

[Koz77] D. Kozen. Lower bounds for natural proof systems. In *Proceedings of the* 18*th IEEE FOCS*, pages 254–266, 1977.

[Tor99] J. Torán. Lower Bounds for Space in Resolution. In *Proceedings of CSL 1999*, pages 362–373. 1999.

[Urq87] A. Urquhart. Hard Examples for Resolution. *Journal of the ACM* **34** pp. 209-219 (1987).

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'