Space Complexity in Propositional Calculus

Michael Alekhnovich*, Eli Ben-Sasson†
Alexander A. Razborov‡, Avi Wigderson§

October 29, 2001

Abstract

We study space complexity in the framework of propositional proofs. We consider a natural model analogous to Turing machines with a read-only input tape, and such popular propositional proof systems as *resolution*, *polynomial calculus* and *Frege* systems. We propose two different space measures, corresponding to the maximal number of bits, and clauses/monomials that need be kept in the memory simultaneously. We prove a number of lower and upper bounds in these models, as well as some structural results concerning the clause space for resolution and Frege systems.

1 Introduction

Complexity of propositional proofs plays as important a role in the theory of feasible proofs as the role played by the complexity of Boolean circuits in the theory of efficient computations. It is also well recognized that there exists a very productive cross-fertilization of techniques between the two fields. Partly because of this similarity, most of the research in the proof-complexity area concentrated on complexity measures related to *size*, which is the most interesting measure in the circuit complexity framework. In other words, the

*Moscow State University, Moscow, Russia mike@mccme.ru. Supported by INTAS grant # 96-753 and by the Russian Basic Research Foundation

†Institute of Computer Science, Hebrew University, Jerusalem, Israel. elli@cs.huji.ac.il.

‡Steklov Mathematical Institute, Moscow, Russia razborov@genesis.mi.ras.ru. Supported by INTAS grant # 96-753 and by the Russian Basic Research Foundation

§Institute of Computer Science, Hebrew University, Jerusalem, Israel avi@cs.huji.ac.il. This research was supported by grant number 69/96 of the Israel Science Foundation, founded by the Israel Academy for Sciences and Humanities, and by a grant from the Alfred P. Sloan Foundation.

main effort in proof complexity was invested in investigating the amount of *time* (or at least time-like resources) taken by proofs; we recommend the excellent recent survey [BP98] for further reading on this subject.

During the workshop "Complexity Lower Bounds" held at the Fields Institute in Toronto in 1998, A. Haken raised the question whether something intelligent can be said about the amount of *space* taken by propositional proofs. Quite surprisingly, it turned out that this very natural question had been virtually untouched in the past. Apparently, the only early paper devoted to the space of proofs is [Koz77], but it dealt only with *equational* theories involving no propositional connectives.

Recently Esteban and Toran [ET99] proposed a convenient definition of space complexity for resolution which measures the number of clauses to be kept simultaneously in the memory to infer the tautology[1]. This model is analogous to a Turing machine computation, with a special read-only input tape from which the axioms can be downloaded to the working memory when needed, and erased from the working memory as many times as necessary. They showed some upper and lower bounds for clause space (see Section 3) and noticed the connection between the clause complexity for resolution and the pebbling game on the graph of a derivation.

Our goal in this paper is to generalize the natural notion of space complexity to other propositional proof systems and complexity measures, and research its properties. The first arising question is how to measure the memory content at any given moment of time for a specified proof system. Recall (see e.g. [Kra95]) that the most customary measures for size complexity of propositional proofs are the bit size and the number of lines. Of these two, the bit size is by far more important, and can be defined analogously, and naturally, in the context of space complexity. The only simplification we allowed ourselves is in fact customary for the size complexity as well. Namely, instead of the bit space we consider the *variable* space (Definition 3.3) which is the overall number of occurrences of variables. This changes the complexity only by at most a logarithmic factor, but makes things substantially cleaner.

It turns out that the line complexity is less adequate a measure for space complexity than it is a size measure. The reason is quite simple: if the language of the proof system is sufficiently strong and allows unbounded fan-in AND gates, then one gets only trivial results. Specifically, we can prove everything that is provable with just $O(1)$ memory cells, one of them containing a big AND of *all* formulae derived at previous steps.

One notable proof system that is not closed under the AND operation is *resolution*, in which case lines are just clauses. In the current paper we in particular show that the clause complexity, as opposed to the line complexity, makes perfect sense even for rather strong systems, and can be considered as its natural replacement in space-complexity studies.

It turns out that all tautologies can be proven within *polynomial* space for any "reasonable" space measure. Specifically, *every* DNF tautology in

[1] Throughout this paper, all propositional systems will prove that ϕ is a tautology by actually proving that its negation, $\neg\phi$, is unsatisfiable.

n variables has already a resolution proof with the clause space $(n+1)$ [ET99], and this upper bound trivially holds for stronger proof systems. This in itself implies a *quadratic* upper bound on the *variable* space, but for the case of Frege systems we are able to improve it to a *linear* upper bound in the number of variables (Theorem 6.3).

These upper bounds determine the range of parameters in which the whole story develops. We ask which tautologies indeed require that much space, and which can be proved within, say, (quasi)logarithmic space resources. We propose some lower bound techniques that in many cases allow us to answer this question for specific tautologies, proof systems and space measures. It is worth noting that all these techniques are purely semantic in nature and thus can be applied to stronger *semantic* versions of the proof systems in question (see definitions in Section 3.2). Let us also point out that it is not quite clear to which extent semantic versions of propositional proof systems are actually stronger than ordinary ones in the context of space complexity. On the contrary, we show for our weakest proof system (resolution) and for our strongest one (Frege system) that the space complexity differs from its semantic analogue by at most a constant multiplicative factor (Theorem 3.7, Corollary 6.6).

For many good reasons, bounded fan-in CNF's (like Tseitin's tautologies) are always preferred in proving lower bounds or separation results. For tautologies from this class (and in the clause space model) we were able to prove strong lower bounds only for resolution (Theorem 3.18, Corollary 3.27)[2].

Finally, we prove one lower bound in the variable space model that does not follow from our clause space bounds. Our argument applies in parallel to both resolution and polynomial calculus (abbreviated throughout the paper by PC), and this situation is already familiar from the proof *size* complexity. For example, [CEI96] proved that every resolution proof of size S can be transformed into a PC proof of degree $O(\sqrt{n \log S})$, and [IPS97] used essentially the same argument for showing that every PC proof of size S can be also transformed into another PC proof of degree $O(\sqrt{n \log S})$. For that reason we find it very instructive to introduce a natural minimal common extension of Resolution and PC (called PCR), that is at least as efficient as resolution, in terms of proof size and space. The above-cited results [CEI96, IPS97] can then be considered as specifications of one general theorem about PCR which says that the degree of every size S PCR proof can be reduced to $O(\sqrt{n \log S})$. Our quadratic lower bounds for the variable space are also very naturally formulated and proved in terms of this new system (Theorem 5.1).

1.1 Summary of Results

We introduce the clause space and variable space measures for resolution and the polynomial calculus. The *clause space* of a proof is the maximal number of clauses/monomials that need to be kept in the memory during the verification of a proof, and the *variable space* is the maximal number of overall symbols that need to be kept during such a verification.

[2]Corollary 3.27 was also independently proved in [Tor99].

We prove tight lower bounds for resolution clause space for a variety of formulas that includes the *pigeonhole principle, counting principles*, and several other interesting cases. This is done by proving a general lower bound that applies to all these cases. Via a different technique, we present a lower bound for the graph based *Tseitin tautologies*, that is *linear* in the number of variables appearing in this formula, and hence optimal.

For the polynomial calculus we prove nearly optimal (up to a small multiplicative constant) lower bounds for *wide tautologies* that include the pigeonhole principle. For this proof we use more complicated techniques than those used for the case of resolution. We show that these techniques are needed by proving that for some cases, the polynomial calculus is strictly more efficient than resolution.

Using our clause space lower bounds for resolution and the polynomial calculus, we derive nearly optimal (up to a small multiplicative constant) lower bounds for the variable space of wide tautologies, such as the pigeonhole principle.

Finally, we prove *linear*, and hence optimal, *upper* bounds on the variable space of Frege proofs for *any* tautology.

1.2 Paper Organization

Following several general definitions (Section 2) we define the resolution clause space measure and prove lower bounds for it in Section 3. In Section 4 we define the polynomial calculus and its extension to multi-valued logic and prove our clause space lower bounds for this system. The variable space lower bounds for resolution and the polynomial calculus appear in Section 5. Finally, we present optimal upper bounds for Frege variable space in Section 6, and conclude with some interesting open problems (Section 7).

2 General Definitions

Let x be a Boolean variable, i.e. a variable that ranges over the set $\{0,1\}$. Throughout this paper we shall identify **1** with $True$ and **0** with $False$. A *literal* of x is either x (denoted sometimes as x^1) or $\bar{x}$ (denoted sometimes as x^0). A *clause* is a disjunction of literals. We write $x^\epsilon \in C$ iff the clause C contains the literal x^ϵ. A *CNF formula* is a set of clauses.

For any Boolean function $f : \{0,1\}^n \to \{0,1\}$, $Vars(f)$ will denote its set of variables. An *assignment to* f is a mapping $\alpha : Vars(f) \to \{0,1\}$. A *restriction* is a mapping $\rho : Vars(f) \to \{0,1,\star\}$. We denote by $|\rho|$ the number of assigned variables, $|\rho| = |\rho^{-1}(\{0,1\})|$. We say that a restriction ρ' *extends* ρ iff they coincide on $\rho^{-1}(\{0,1\})$.

The restriction of f by ρ, denoted $f|_\rho$, is the Boolean function obtained from f by setting the value of each $x \in \rho^{-1}(\{0,1\})$ to $\rho(x)$, and leaving each $x \in \rho^{-1}(\star)$ as a variable.

We say that an assignment α *satisfies* f, if $f(\alpha) = 1$. For Boolean functions $f_1, \ldots, f_k, g$ we say that $f_1, \ldots, f_k$ *semantically imply* g, $f_1, \ldots, f_k \models g$, if every assignment to $V \stackrel{\text{def}}{=} Vars(f_1) \cup \ldots \cup Vars(f_k) \cup Vars(g)$ satisfying $f_1, \ldots, f_k$, satisfies g as well (i.e. $\forall \alpha \in \{0,1\}^V (f_1(\alpha) = \cdots = f_k(\alpha) = 1 \Rightarrow$

$g(\alpha) = 1)$). For $\mathcal{F}, \mathcal{G}$ two sets of functions, we say that $\mathcal{F}$ implies $\mathcal{G}$ ($\mathcal{F} \models \mathcal{G}$), if for all $g \in \mathcal{G}$, $\mathcal{F} \models g$.

Notation: Throughout this paper, a, b will denote Boolean constants, x, y, z will denote Boolean variables, f, g, h will denote functions, φ, ψ will denote formulas, A, B, C, D will denote clauses, α, β will denote assignments, ρ will denote restrictions. Calligraphic letters, $\mathcal{A}, \mathcal{M}, \mathcal{N}, \mathcal{T}$ will denote sets of formulas. For n, a non-negative integer let $[n] \stackrel{\text{def}}{=} \{1, 2, \ldots, n\}$. For $\mathcal{M}$ a set, we denote by $|\mathcal{M}|$ its cardinality.

3 Resolution Clause Space

In this section we prove lower bounds for resolution clause space for a number of principles which include various modifications of the pigeonhole principle, counting principles and the principle GT_n (the latter was used in the recent work of [BG99] to produce a tautology with large minimal proof width and polynomially bounded proof size). These results follow from a general lower bound for *semi-wide tautologies*, also introduced in this section (Theorem 3.13). We also show how to transform any semi-wide tautology (and, in particular, any of the above mentioned examples) to an equivalent 3-CNF form while preserving clause space hardness (Theorem 3.18).

We will start by giving definitions of the resolution clause space, proceed to show the equivalence of *semantic* and *syntactic* resolution, and then prove the lower bounds.

Notation: *Throughout Section 3 we do not distinguish between a clause C and the Boolean function computed by it.*

3.1 Resolution Clause Space - Definitions

Recall that a CNF formula is a set of clauses. The *resolution rule* is the following derivation rule:

Resolution Rule: Derive $A \vee B$ from $\{A \vee x, B \vee \overline{x}\}$, where A, B are any clauses, and x is any variable.

Let $\mathcal{T} = \{C_1, C_2, \ldots, C_m\}$ be a CNF formula over n variables. A *resolution proof* (or *derivation*) of a clause E from $\mathcal{T}$ is a sequence of clauses $\pi = \{D_1, D_2 \ldots, D_s\}$ such that the last clause is E and each D_i is either some initial clause $C_j \in \mathcal{T}$, or is derived from previous clauses using the resolution rule. A *resolution refutation of* $\mathcal{T}$ is a resolution derivation of the empty clause, $\mathbf{0}$ from $\mathcal{T}$. Notice that by the definition of the resolution rule, all lines in a resolution proof must be clauses. Notice that every refutation gives rise to a labeled directed acyclic graph, called the *refutation DAG*. Each node in this graph is labeled by a clause of the proof. The sources are labeled by $C \in \mathcal{T}$, the single sink by $\mathbf{0}$, and each node in the middle is connected to the two clauses that were used to derive it.

The definition of the resolution clause space was first given in [ET99]. We recast it here in slightly different terms (so that it will be easier for us to generalize this definition for stronger proof systems in the forthcoming sections).

Suppose we are given a resolution proof from $\mathcal{T}$, and wish to verify it using a minimal amount of memory. The proof π, as well as the CNF $\mathcal{T}$, are written on a read-only memory tape. We keep in our *working memory* a subset of the clauses in the proof (starting with the empty set), and at each time step we either add a clause $C \in \mathcal{T}$ to our memory, *or* apply a single resolution derivation to two clauses *in the memory*, and add the resulting clause to it, *or* remove an unnecessary clause from the memory. The *clause space* of the proof π is the maximal number of clauses we need to keep at some time during the verification of the proof. Of course, there are many ways to verify a single proof (e.g. we may keep all clauses in the proof, in which case the space will be $|\pi|$), and we naturally define the space to be the minimal one over all possible verifications of π. Finally, the *resolution clause space* of $\mathcal{T}$ is the minimal space of a refutation π of $\mathcal{T}$ (if such a refutation exists, and ∞ otherwise).

We now present a formal definition of the clause space that captures our intuition, and will be easy to work with rigorously. We start with a different definition of a resolution proof, that exposes the clause space naturally. Comparing this definition with our previous one, we see they are equivalent in size, up to a polynomial factor.

Definition 3.1 (Syntactical Resolution Derivation) *A* configuration *is a set of clauses. A* proof π *from a CNF* $\mathcal{T}$ *is a sequence of configurations* $\mathcal{M}_0, \ldots, \mathcal{M}_s$ *such that* $\mathcal{M}_0 = \emptyset$ *and for all* $t \in [s]$, $\mathcal{M}_t$ *is obtained from* $\mathcal{M}_{t-1}$ *by one of the following rules:*

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

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

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

We use the notation $\mathcal{M} \rightsquigarrow \mathcal{M}'$ *to mean that* $\mathcal{M}'$ *is the immediate successor of* $\mathcal{M}$ *in a derivation. If* $\mathcal{M}_s = \{\mathbf{0}\}$ *(the empty clause) then the derivation is called a* refutation of $\mathcal{T}$*.*

Definition 3.2 (Clause Space) *The* clause space *of a set of configurations* $\pi = \{\mathcal{M}_0, \ldots, \mathcal{M}_s\}$ *is*

$$CSpace(\pi) \stackrel{\text{def}}{=} \max\{|\mathcal{M}_i| : i \in [s]\}.$$

The resolution clause space *of a CNF* $\mathcal{T}$ *is*

$$CSpace(\mathcal{T}) \stackrel{\text{def}}{=} \min\{CSpace(\pi)\},$$

where the minimum is taken over all refutations of $\mathcal{T}$*, and is defined to be* ∞ *if no such refutation exists (i.e.* $\mathcal{T}$ *is satisfiable).*

Although we will prove variable space lower bounds only in Section 5 (and in this section concentrate on *clause* space lower bounds), we nonetheless present its definition now (for the sake of coherence).

Definition 3.3 (Variable Space) *The* variable space *of a configuration* $\mathcal{M}$ *is* $\sum_{C\in\mathcal{M}}|C|$*, where* $|C|$ *is the number of literals in* C*. The* variable space of a set of configurations $\pi = \{\mathcal{M}_0, \ldots, \mathcal{M}_s\}$ *is*

$$VSpace_R(\pi) \stackrel{\text{def}}{=} \max\{\sum_{C\in\mathcal{M}_i}|C| : i \in [s]\}.$$

The resolution variable space *of a CNF* $\mathcal{T}$ *is*

$$VSpace_R(\mathcal{T}) \stackrel{\text{def}}{=} \min\{VSpace_R(\pi)\},$$

where the minimum is taken over all refutations π *of* $\mathcal{T}$*, and is defined to be* ∞ *if no such refutation exists (i.e.* $\mathcal{T}$ *is satisfiable).*

As we already mentioned, the research of clause space in resolution was started by Esteban and Toran in [ET99]. They in particular defined the following tautologies[3] CT_n:

Definition 3.4 (COMPLETE-TREE tautologies) CT_n *is the following set of axioms:*

$$\{x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_n^{\epsilon_n} \mid \vec{\epsilon} \in \{0,1\}^n\},$$

and showed hardness of their proof in terms of clause space.

They also gave an upper bound for *any* tautology $\mathcal{T}$ over n variables (we state it in our language):

Theorem 3.5 *[ET99] If* $\mathcal{T}$ *is a contradictory set of clauses over* n *variables then* $CSpace(\mathcal{T}) \leq n+1$.

This bound is tight for the principle CT_n.

CT_n contains an exponential number of axioms. In this section we define the class of *semi-wide* tautologies of polynomial size which are hard to refute for resolution in terms of clause space. This class contains such popular principles as PHP_n^m, $onto - PHP_n^m$, $Count_p$, GT_n. We also show via a slightly different approach the space hardness of Tseitin tautologies for expander graphs.

3.2 Equivalence of Syntactic and Semantic Resolution

All our lower bounds in this paper will work for *semantical* proof systems, which are stronger versions of the regular proof systems. In this subsection we define semantical resolution, and then prove that with respect to clause space, syntactical and semantical derivations are equivalent, up to a constant factor.

We start by pointing out that the *inference* rule of Definition 3.1 is *sound*, i.e. if $\mathcal{M}_t$ was derived from $\mathcal{M}_{t-1}$ by an application of this rule, then $\mathcal{M}_{t-1} \models \mathcal{M}_t$. The *semantical resolution proof system* replaces this rule by the following stronger *semantical inference* rule:

[3]Throughout the paper we assume that all tautologies are represented in the negated form of a contradictory CNF $\mathcal{T}$.

SEMANTICAL INFERENCE $\mathcal{M}_t := \mathcal{M}_{t-1} \cup C$, for some C such that $\mathcal{M}_{t-1} \models C$.

The definition of proof space in semantical resolution is analogous to that of the syntactical resolution system. Denote by $CSpace^{sem}(\mathcal{T})$ the clause space of refuting $\mathcal{T}$ in semantical resolution.

The semantical inference rule generalizes the inference rule, and hence any syntactical resolution derivation is also a semantical one. Notice that when it comes to *size*, semantical resolution is much stronger than syntactical resolution, because once $\mathcal{M}_t$ is unsatisfiable, we can derive $\mathbf{0}$ in a single step. We will now prove that with respect to space, there is no big difference between the two, and they are equivalent up to a constant factor.

A CNF formula is *minimal unsatisfiable* if it is unsatisfiable and removing any clause from it will make it satisfiable. We will need a very useful theorem, due to M. Tarsi [Tar], which can be originally found in [AL86].

Theorem 3.6 [Tarsi's Theorem] *If $\mathcal{T}$ is a minimal unsatisfiable CNF formula on n variables and m clauses, then $m > n$.*

Proof: Consider the following bipartite graph on $\mathcal{T} \times Vars(\mathcal{T})$: a clause C is connected to a variable x iff x appears in C (either as a positive or negative literal). Clearly, there is no matching from $\mathcal{T}$ to $Vars(\mathcal{T})$ in this graph, because the formula is unsatisfiable. Hence, by Hall's theorem, there must be some set $S \subset \mathcal{T}$ such that $|N(S)| < |S|$. Let S be such a set of maximal size. By the maximality of S, for any $V \subseteq \mathcal{T} - S$ we have $|N(V) - N(S)| \geq |V|$. Thus there is a matching from $\mathcal{T} - S$ into $Vars(\mathcal{T}) - N(S)$. By the minimal unsatisfiability of $\mathcal{T}$, if $S \neq \mathcal{T}$ then S is satisfiable, and $\mathcal{T} - S$ is satisfiable by its matching into $Vars(\mathcal{T}) - N(S)$. Thus we conclude that $S = \mathcal{T}$ and hence $m = |S| = |\mathcal{T}| > |N(S)| = |Vars(\mathcal{T})| = n$. □

The main theorem of this subsection is the following.

Theorem 3.7 *For any unsatisfiable CNF $\mathcal{T}$,*

$$CSpace^{sem}(\mathcal{T}) \leq CSpace(\mathcal{T}) \leq 2 \cdot CSpace^{sem}(\mathcal{T}).$$

Proof: The first inequality is trivial, because a syntactical resolution derivation is also a legitimate semantical one. Let π be a semantical refutation of $\mathcal{T}$ with clause space s. We wish to show that $\mathcal{T}$ has a clause space $2s$ syntactical refutation. The only difference between the two systems is in the inference rule, so we focus on this rule. Suppose $\mathcal{M}_{t+1}$ was inferred from $\mathcal{M}_t$ by the semantic inference rule ($\mathcal{M}_{t+1} := \mathcal{M}_t \cup \{C\}$, $\mathcal{M}_t \models C$), where $|\mathcal{M}_t|, |\mathcal{M}_{t+1}| \leq s$.

Let ρ be the unique minimal size restriction on the variables of C such that $C|_\rho = 0$. Now we use the soundness of the step to claim that $\mathcal{M}_t|_\rho$ must be unsatisfiable. $\mathcal{M}_t|_\rho$ contains a minimal unsatisfiable sub-formula $\mathcal{M}'$, which, by Tarsi's theorem, has at most $s-1$ variables. By Theorem 3.5, the contradictory set of clauses $\mathcal{M}'$ can be refuted in space s. It is an easy exercise to adjust this proof and derive C from $\mathcal{M}_t$ with the same clause space s.

We need a space of s cells for saving $\mathcal{M}_t$. Additionally, we use s cells to derive $C \in \mathcal{M}_{t+1}$ from $\mathcal{M}_t$. □

3.3 Lower Bounds for Semi-Wide Tautologies

We are ready to prove our lower bounds for the clause space of semantical resolution proofs. The main idea is the following. Consider a derivation that keeps at most k clauses in the memory. We shall show that for some classes of tautologies (called *semi-wide*, see Definition 3.10) we can inductively construct restrictions of maximal size k, that satisfy the memory content. Thus, there can be no space k refutation, because the empty clause cannot be satisfied.

Although this proof technique is very simple, we will use similar ideas when proving lower bounds for stronger proof systems. Also, these results will be useful for proving lower bounds for the variable space complexity. For this reason we present our proof method in a somewhat fancy style.

The main idea of our lower bounds is to come up with some set of memory-configurations $\mathbb{A}$ ("$\mathbb{A}$" stands for "admissible") such that:

- it does not contain contradictory configurations;
- any memory-configuration achievable in small memory is the semantical corollary of some configuration from $\mathbb{A}$.

Notice that we do *not* require $\mathbb{A}$ to contain all the formulas which can be derived using small space. We only require that for any such formula φ, there exists a memory configuration $\mathcal{M} \in \mathbb{A}$ implying φ.

In all our cases these "dominating" memory-configurations will be CNF's of a very simple nature, namely, sets of *disjoint* clauses:

$$\mathcal{M} \in \mathbb{A} \Rightarrow \mathcal{M} = \left\{ \bigvee_{j \in J_i} x_j^{\epsilon_j} \mid 1 \le i \le k \right\},$$

where $J_i \cap J_{i'} = \emptyset$ for different i, i'. Moreover, in this section we will be interested only in the following partial case of this definition naturally corresponding to ordinary restrictions:

Definition 3.8 (Proper 1-CNF's) *$\mathcal{M}$ is called a* proper 1-CNF *if it is a set of pairwise distinct literals, i.e.*

$$\mathcal{M} = \{x_{j_1}^{\epsilon_1}, x_{j_2}^{\epsilon_2}, \ldots, x_{j_k}^{\epsilon_k}\},$$

and $j_{i_1} \neq j_{i_2}$ for different i_1, i_2.

The heart of our lower bounds for clause space for resolution is the following (trivial) locality lemma which informally claims that small 1-CNF's are enough to imply any small space consequence of the axioms. Later on we shall present an analogous locality lemma 4.14 for the polynomial calculus, which will be less trivial.

Lemma 3.9 (Locality lemma for resolution) *Let $\mathcal{M}$ be a proper 1-CNF. Suppose that $\mathcal{M}_1$ is the semantical resolution corollary of $\mathcal{M}$ (i.e. $\mathcal{M}_1$ is a set of clauses and $\mathcal{M} \models \mathcal{M}_1$), let $|\mathcal{M}_1| = s$. Then there exists $\mathcal{M}_1^{-1} \subseteq \mathcal{M}$ such that $\mathcal{M}_1^{-1} \models \mathcal{M}_1$ and $|\mathcal{M}_1^{-1}| \le s$.*

Proof: Suppose $\mathcal{M}_1 = \{C_1, C_2, \ldots, C_s\}$. For any clause C_i which is the semantical corollary of $\mathcal{M}$ there exists some $x_{j_i}^{\epsilon_i} \in \mathcal{M} \cap C_i$. Thus $\mathcal{M}_1$ is the semantical corollary of the configuration $\mathcal{M}_1^{-1} = \{x_{j_1}^{\epsilon_1}, x_{j_2}^{\epsilon_2}, \ldots, x_{j_s}^{\epsilon_s}\}$. $\square$

A contradictory set of clauses is called *n-wide* if all its axioms have width (= the number of literals) $\geq n$. [ET99] proved that every n-wide tautology has clause space $> n$. In Section 4.4 we shall prove PC lower bounds for these tautologies. In the case of the weaker resolution system, we can prove lower bounds for a bigger class of *semi-wide* tautologies.

Definition 3.10 (Semi-Wide Tautologies) *Suppose that $\mathcal{T}$ is a contradictory set of clauses which is divided into two groups: $\mathcal{T} = \mathcal{P} \dot{\cup} \mathcal{R}$, where $\mathcal{P}$ is satisfiable.*

For $\mathcal{M}$ a proper 1-CNF, we say that $\mathcal{M}$ is $\mathcal{P}$-consistent *iff $\mathcal{P} \cup \mathcal{M}$ is consistent. Equivalently, $\mathcal{M}$ is $\mathcal{P}$-consistent iff it can be extended to a proper 1-CNF which implies all axioms of $\mathcal{P}$ ($\exists \mathcal{M}' \supseteq \mathcal{M}$ $(\mathcal{M}' \models \mathcal{P})$).*

Finally, $\mathcal{T}$ is n-semi-wide iff there exists a partition $\mathcal{T} = \mathcal{P} \dot{\cup} \mathcal{R}$ such that $\mathcal{P}$ is satisfiable and for every axiom $C \in \mathcal{R}$, for every $\mathcal{P}$-consistent proper 1-CNF $\mathcal{M}$ with $|\mathcal{M}| < n$, it can be extended to a $\mathcal{P}$-consistent proper 1-CNF $\mathcal{M}' \supseteq \mathcal{M}$ such that $\mathcal{M}' \models C$.

Before we show that n-semi-wide tautologies demand clause space at least $n+1$ to be refuted, we give several natural examples.

It is obvious that every n-wide tautology is also n-semi-wide: we let $\mathcal{P} = \emptyset$, and if we fix the values of $n-1$ variables by a proper 1-CNF $\mathcal{M}$, any clause $C = x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_N^{\epsilon_N}$ with $N \geq n$ can be satisfied by fixing some unassigned variable (i.e., the variable which isn't contained in $\mathcal{M}$) x_j. In particular, the COMPLETE-TREE tautology CT_n is n-semi-wide.

Another example is the pigeonhole principle with m pigeons and n holes PHP_n^m which states that there is no 1-1 map from $[m]$ to $[n]$, as long as $m > n$. The propositional formulation of this principle has received much consideration in proof complexity, and is one the major test cases for comparing different proof systems. In particular, our $(n+1)$ lower bound on the clause space of refuting PHP_n^m was independently proved in [Tor99].

We discuss here only the onto-version of this principle which constrains 1-1 maps to be onto. One can easily extend our arguments to other PHP-like principles and $Count_p$.

Definition 3.11 (Onto-Pigeonhole Principle) *$Onto - PHP_n^m$ is the union of the following four groups of axioms:*

(i) $P_i \stackrel{\text{def}}{=} \bigvee_{1 \leq j \leq n} x_{ij}$ *$(i \in [m])$;*

(ii) $H_j \stackrel{\text{def}}{=} \bigvee_{1 \leq i \leq n} x_{ij}$ *$(j \in [n])$;*

(iii) $Q_{i_1,i_2;j} \stackrel{\text{def}}{=} \bar{x}_{i_1 j} \vee \bar{x}_{i_2 j}$ *$(i_1, i_2 \in [m],\ i_1 \neq i_2;\ j \in [n])$;*

(iv) $Q_{i;j_1,j_2} \stackrel{\text{def}}{=} \bar{x}_{ij_1} \vee \bar{x}_{ij_2}$ *$(i \in [m];\ j_1, j_2 \in [n],\ j_1 \neq j_2)$.*

One can see that $onto - PHP_n^m$ is n-semi-wide by taking the partition $\mathcal{P} \dot\cup \mathcal{R}$ with $\mathcal{P} = \{Q_{i_1,i_2;j} \mid i_1, i_2, j\} \cup \{Q_{i;j_1,j_2} \mid i, j_1, j_2\}$ and $\mathcal{R} = \{P_i \mid i\} \cup \{H_j \mid j\}$. The proper 1-CNF $\mathcal{M}$ is $\mathcal{P}$-consistent iff it doesn't put either two pigeons to the same hole (i.e., contains the literals $x_{i_1 j}, x_{i_2 j}$) or one pigeon in two different holes (i.e., contains the literals x_{ij_1}, x_{ij_2}), in other words iff positive literals in $\mathcal{M}$ form a partial matching. Now if $n-1$ variables are fixed then when we take the axiom P_i we can put ith pigeon to some unassigned hole (that is, to add the corresponding positive literal). Dually, if we take the axiom H_j we can put some unassigned pigeon to jth hole. Thus we can always satisfy an axiom from $\mathcal{R}$ with some extended $\mathcal{P}$-consistent proper 1-CNF.

Another principle, GT_n, states that in every transitive directed graph which doesn't contain cycles of size two, there must exist a source node with no incoming edges. This principle, formulated in [Kri85], was shown to have a proof of polynomial size [Sta96]. Recently, [BG99] used this principle to produce a tautology of polynomial proof size and large minimal proof width.

Quite surprisingly, this very same principle also shows that large clause space complexity does not imply large proof size.

Definition 3.12 *GT_n is the following contradictory set of axioms over $n(n-1)$ variables x_{ij} $(i, j \in [n], i \neq j)$ consisting of three groups:*

(i) $T_{ijk} \stackrel{\text{def}}{=} (x_{ij} \wedge x_{jk}) \to x_{ik}$ $(i, j, k \in [n], i \neq j \neq k)$;

(ii) $C_{ij} \stackrel{\text{def}}{=} \bar{x}_{ij} \vee \bar{x}_{ji}$ $(i, j \in [n], i \neq j)$;

(iii) $S_j \stackrel{\text{def}}{=} \bigvee_{k \neq j} x_{kj}$ $(j \in [n])$.

The first group of axioms says that the graph is transitive. The second group states that there are no cycles of size two. The axiom S_j says that j is not the source node. Clearly this set of axioms is contradictory. To see that it is $\frac{n}{2}$-semi-wide take the partition $\mathcal{T} = \mathcal{P} \dot\cup \mathcal{R}$ where $\mathcal{P}$ consists of the axioms of the first and second groups. Then the proper 1-CNF $\mathcal{M}$ is $\mathcal{P}$-consistent iff it doesn't contain a cycle of positive literals (i.e. chains like $x_{i_1 i_2}, x_{i_2 i_3}, \ldots, x_{i_k i_1}$) and it doesn't contain a chain $x_{i_1 i_2}, x_{i_2 i_3}, \ldots, x_{i_{k-1} i_k}$ together with the literal $\bar{x}_{i_1 i_k}$. Suppose now that $\mathcal{M}$ is $\mathcal{P}$-consistent and assigns not more than $\frac{n}{2} - 1$ variables and we are to extend it to satisfy some axiom $S_j \in \mathcal{R}$. We can choose the index $k \neq j$ such that no variables $x_{ki}, x_{ik}, i \in [n]$ are contained in $\mathcal{M}$ and let $\mathcal{M}' = \mathcal{M} \cup \{x_{kj}\}$. Thus GT_n is $\frac{n}{2}$-semi-wide.

In the next theorem, which is the main result of this section, we show that semi-wide tautologies are hard for resolution in terms of clause space. The intuition of the proof is simple: we show inductively that a configuration of $k < n$ clauses can be satisfied by a restriction that sets $\leq k$ variables.

Theorem 3.13 *For any n-semi-wide tautology $\mathcal{T}$:*

$$CSpace^{sem}(\mathcal{T}) > n.$$

Proof: Fix the partition $\mathcal{T} = \mathcal{P} \dot{\cup} \mathcal{R}$ in accordance with Definition 3.10.

Definition 3.14 (Admissible configurations for $\mathcal{T}$) *We call* $\mathcal{M}$ admissible *iff* $\mathcal{M}$ *is a* $\mathcal{P}$*-consistent proper* 1*-CNF and* $|\mathcal{M}| \leq n$.

Consider the set $\mathbb{A}$ of all admissible configurations. We claim that the following holds: for each configuration $\mathcal{M}$, derivable in space $\leq n$, there exists a configuration $\mathcal{M}^{-1} \in \mathbb{A}$ such that $\mathcal{M}^{-1} \models \mathcal{M}$ and $|\mathcal{M}^{-1}| \leq |\mathcal{M}|$. This is obviously enough to prove the theorem since $\mathbb{A}$ doesn't contain contradictory configurations.

We prove it by induction. The basis is trivial: in the beginning of the derivation the memory contains an empty set. To check the induction step suppose that $\mathcal{M}_t \rightsquigarrow \mathcal{M}_{t+1}$, and that there exists $\mathcal{M}_t^{-1} \in \mathbb{A}$ such that $\mathcal{M}_t^{-1} \models \mathcal{M}_t,\ |\mathcal{M}_t^{-1}| \leq |\mathcal{M}_t|$.

Let us consider the three cases corresponding to the possible derivation steps: axiom download, semantic inference step and memory erasing.

Axiom Download ($\mathcal{M}_{t+1} := \mathcal{M}_t \cup \{C\},\ C \in \mathcal{T}$): In this case $|\mathcal{M}_t| \leq n-1$ (since there is free space for the new axiom). Thus $|\mathcal{M}_t^{-1}| \leq n-1$, hence it can be extended to $\mathcal{P}$-consistent proper 1-CNF $\mathcal{M}_{t+1}^{-1}$ which satisfies C (if $C \in \mathcal{R}$ this follows from the definition of semi-wide tautology, and if $C \in \mathcal{P}$ it is obvious). Since C is a clause we can satisfy it by fixing just one variable. Thus we can assume w.l.o.g. that $|\mathcal{M}_{t+1}^{-1}| \leq |\mathcal{M}_t^{-1}| + 1$.

Clearly, $\mathcal{M}_{t+1}^{-1} \in \mathbb{A}$ and $\mathcal{M}_{t+1}^{-1} \models \mathcal{M}_{t+1}$. Also, $|\mathcal{M}_{t+1}^{-1}| \leq |\mathcal{M}_t^{-1}| + 1 \leq |\mathcal{M}_t| + 1 = |\mathcal{M}_{t+1}|$.

Semantical Inference ($\mathcal{M}_{t+1} := \mathcal{M}_t \cup \{C\},\ \mathcal{M}_t \models C$): In this case $\mathcal{M}_t^{-1} \models \mathcal{M}_{t+1}$. By the locality lemma 3.9 there exists $\mathcal{M}_{t+1}^{-1} \subseteq \mathcal{M}_t^{-1}$ such that $\mathcal{M}_{t+1}^{-1} \models \mathcal{M}_{t+1}$ and $|\mathcal{M}_{t+1}^{-1}| \leq |\mathcal{M}_{t+1}|$.

Memory Erasing ($\mathcal{M}_{t+1} := \mathcal{M}_t - \mathcal{M}' \subseteq \mathcal{M}_t$) : Analogous to the case of inference step.

Theorem 3.13 follows. □

So far we have strongly used the existence of axioms of width n to show that a given tautology is semi-wide and thus prove a lower bound of n on the clause space. We now go one step further to show that we can transform any semi-wide tautology to the following 3-CNF version which requires essentially the same space as the "standard" version.

Definition 3.15 (Strong Nondeterministic Extensions) *For* $C(\vec{x})$ *a clause, a* strong nondeterministic extension of C *is any Boolean function* $f(\vec{x}, \vec{y})$ *such that:*

- *if* $C(\vec{\alpha}) = 0$ *then* $f(\vec{\alpha}, \vec{y}) \equiv 0$*;*
- *if* $x_j^\epsilon \in C$ *then there exists an assignment* $\vec{\beta}$ *to* $\vec{y}$ *such that setting* x_j *to* ϵ *and* $\vec{y}$ *to* $\vec{\beta}$ *fixes* f *to* 1*. Formally:*

$$f\left[\epsilon/x_j,\ \vec{\beta}/\vec{y}\right] \equiv 1.$$

Example 3.16 *One standard strong nondeterministic extension of a clause* $C = x_1 \vee x_2 \vee \ldots \vee x_n$ *is the function represented by the following 3-CNF family over* $n+2$ *clauses and* $2n+1$ *variables:*

$$\{\bar{y}_0\} \cup \{y_{j-1} \vee x_j \vee \bar{y}_j \mid 1 \leq j \leq n\} \cup \{y_n\}.$$

Definition 3.17 (Extended version of $\mathcal{T}$) *An* extended version of the tautology $\mathcal{T}$, *denoted* $\widetilde{\mathcal{T}}$ *is derived by replacing every axiom* C_i *with some CNF set of clauses* $\mathcal{EC}_i$ *representing a strong nondeterministic extension of* C_i, *such that distinct* $\mathcal{EC}_i$ *use distinct extension variables* $\vec{y}_i = \langle y_{i1}, y_{i2}, \ldots, y_{ik_i} \rangle$.

Theorem 3.18 *If* $\mathcal{T}$ *is* n*-semi-wide, and* $\widetilde{\mathcal{T}}$ *is some extended version of it, then*

$$CSpace^{sem}(\widetilde{\mathcal{T}}) > n.$$

Proof:

As in the proof of Theorem 3.13, we are going to define the set of admissible configurations $\mathbb{A}$. After that the proof will be very similar to that of Theorem 3.13. Let, as before, the partition $\mathcal{T} = \mathcal{P} \dot{\cup} \mathcal{R}$ be chosen according to Definition 3.10. For every clause $C_i \in \mathcal{T}$ and every $x_j^\epsilon \in C_i$ we *rigidly fix once and for all* an arbitrary assignment $\vec{\beta}_{ij}$ to the variables $\vec{y}_i$ such that the restriction which sends x_j to ϵ and sends $\vec{y}_i$ to $\vec{\beta}_{ij}$ forces to 1 all clauses from $\mathcal{EC}_i$.

Definition 3.19 (Admissible configurations for $\widetilde{\mathcal{T}}$) *We call a proper* 1*-CNF* $\mathcal{M}$ *admissible for* $\widetilde{\mathcal{T}}$ *iff there exists a* $\mathcal{T}$*-admissible configuration* $\widehat{\mathcal{M}}$ *(in ordinary variables* $\vec{x}$*) such that:*

- *for every original variable* $x_j^\epsilon \in \mathcal{M}$, *we also have* $x_j^\epsilon \in \widehat{\mathcal{M}}$;
- *if* $\mathcal{M}$ *contains at least one auxiliary variable from* $\vec{y}_i$, *then there exists* $x_j^\epsilon \in \widehat{\mathcal{M}}$ *such that the values of* all *auxiliary variables in* $\vec{y}_i$ *belonging to* $\mathcal{M}$ *are consistent with* $\vec{\beta}_{ij}$.

Consider the set $\mathbb{A}$ of all configurations admissible for $\widetilde{\mathcal{T}}$. We claim that the following holds: for each configuration $\mathcal{M}$ derivable in space n, there exists a configuration $\mathcal{M}^{-1} \in \mathbb{A}$ such that $\mathcal{M}^{-1} \models \mathcal{M}$ and $|\mathcal{M}^{-1}| \leq |\mathcal{M}|$. This is obviously enough to prove the theorem since $\mathbb{A}$ doesn't contain contradictory configurations.

We prove it by induction. The basis, inference step and memory erasing can be handled with the help of the locality lemma 3.9, as in Theorem 3.13.

Consider the axiom download. Let $\mathcal{M}_{t+1} \leftarrow \mathcal{M}_t \cup \{C\}$, $C \in \mathcal{EC}_i$. By the induction hypothesis there exist configurations $\mathcal{M}_t^{-1}, \widehat{\mathcal{M}}_t^{-1}$ with properties described in Definition 3.19, and such that $\mathcal{M}_t^{-1} \models \mathcal{M}_t$ and $|\mathcal{M}_t^{-1}| \leq |\mathcal{M}_t|$.
Case 1: $\mathcal{M}_t^{-1}$ already contains some auxiliary variable from $\mathcal{EC}_i$.

Then we have already assigned in $\widehat{\mathcal{M}}_t^{-1}$ some variable x_j with $x_j^\epsilon \in C_i$ to ϵ such that the values of all auxiliary variables $\vec{y}_i$ in $\mathcal{M}_t^{-1}$ are consistent with $\vec{\beta}_{ij}$. Either $x_j^\epsilon \in C$ or $y_{i\ell}^{\beta_{ij\ell}} \in C$ for some $\ell \leq k_i$. In the first case we let

$\mathcal{M}_{t+1}^{-1} \stackrel{\text{def}}{=} \mathcal{M}_t^{-1} \cup \{x_j^\epsilon\}$, and in the second case we let $\mathcal{M}_{t+1}^{-1} \stackrel{\text{def}}{=} \mathcal{M}_t^{-1} \cup \{y_{i\ell}^{\beta_{ij\ell}}\}$. Put also $\widehat{\mathcal{M}}_{t+1}^{-1} \stackrel{\text{def}}{=} \widehat{\mathcal{M}}_t^{-1}$.

Case 2: $\mathcal{M}_t^{-1}$ doesn't contain any auxiliary variables from $\mathcal{EC}_i$.

W.l.o.g. we can assume that $|\widehat{\mathcal{M}}_t^{-1}| \leq |\mathcal{M}_t^{-1}|$ (simply leave in $\widehat{\mathcal{M}}_t^{-1}$ only those x_j^ϵ which are really used for fulfilling the two conditions in Definition 3.19). Since $\widehat{\mathcal{M}}_t^{-1}$ is $\mathcal{T}$-admissible and $|\widehat{\mathcal{M}}_t^{-1}| \leq |\mathcal{M}_t^{-1}| \leq |\mathcal{M}_t| < n$, arguing as in the proof of Theorem 3.13, we can find some $x_j^\epsilon \in C_i$ such that $\widehat{\mathcal{M}}_t^{-1} \cup \{x_j^\epsilon\}$ is still $\mathcal{T}$-admissible. Arguing as in Case 1 above, we can extend $\mathcal{M}_t^{-1}$ with either x_j^ϵ itself, or with some $y_{i\ell}^{\beta_{ij\ell}}$ to get $\mathcal{M}_{t+1}^{-1}$ with $\mathcal{M}_{t+1}^{-1} \models C$.

Theorem 3.18 follows. □

3.4 Tseitin Tautologies

A Tseitin tautology is an unsatisfiable CNF capturing the basic combinatorial principle that for every graph, the sum of degrees of all vertices is even. These tautologies were originally used by Tseitin [Tse68] to present the first super-polynomial lower bounds on proof size for a certain restricted form of resolution (regular resolution).

The main theorem in this subsection is Theorem 3.24 that presents a linear lower bound on the clause space of Tseitin formulas. This result was independently obtained in [Tor99].

Definition 3.20 (Tseitin Formulas) *Fix G a finite connected graph, with $|V(G)| = n$. $\sigma : V(G) \to \{0,1\}$ is said to have* odd-weight *if $\Sigma_{v \in V(G)} \sigma(v) \equiv 1 \pmod 2$. Denote by $d_G(v)$ the degree of v in G. Fix σ an odd-weight function. Assign a distinct variable x_e to each edge $e \in E(G)$. For $v \in V(G)$ define $PARITY_{v,\sigma} \stackrel{\text{def}}{=} (\bigoplus_{e \ni v} x_e \equiv \sigma(v) (\text{mod } 2))$. The* Tseitin formula *of G and σ is:*

$$T(G,\sigma) \stackrel{\text{def}}{=} \bigwedge_{v \in V(G)} PARITY_{v,\sigma}.$$

If the maximal degree of G is constant, then the initial size and width of $T(G,\sigma)$ are small as well:

Lemma 3.21 *If d is the maximal degree of G, then $T(G,\sigma)$ is a d-CNF with at most $n \cdot 2^{d-1}$ clauses, and at most $nd/2$ variables.*

We shall need the following lemma from [Urq95]:

Lemma 3.22 *[Urq95] If G is connected, then $T(G,\sigma)$ is contradictory iff σ is an odd weight function. Moreover, for any $v \in V(G)$ there is an assignment satisfying all axioms from $\{ PARITY_{u,\sigma} \mid u \neq v \}$.*

The space lower bound on Tseitin formulas will be directly connected to the following notion of expansion:

Definition 3.23 (Connectivity Expansion) *For G a connected graph on n vertices, let $c(G)$ be the minimal number of edges that one must remove from G in order to obtain a graph in which all connected components have size $\leq n/2$.*

Theorem 3.24 *For G a graph of maximal degree d,*

$$CSpace^{sem}(T(G,\sigma)) > c(G) - d.$$

Proof: Our invariant will be a specially tailored sequence of restrictions, defined hereby:

Definition 3.25 (Admissible configurations for $T(G,\sigma)$) *Suppose that $\mathcal{M}$ is a proper 1-CNF with $|\mathcal{M}| < c(G)$. Let $E(\mathcal{M}) \subseteq E(G)$ be the subset of edges corresponding to the variables of $\mathcal{M}$. Then $G \setminus E(\mathcal{M})$ (the graph G after removing the edges $E(\mathcal{M})$) has an uniquely defined maximal connected component $V_{max}(\mathcal{M})$ with $|V_{max}(\mathcal{M})| > n/2$.*

We call the proper 1-CNF $\mathcal{M}$ with $|\mathcal{M}| < c(G)$ admissible *for $T(G,\sigma)$ if there exists a proper 1-CNF $\mathcal{M}'$ such that $\mathcal{M}' \supseteq \mathcal{M}$ and $\mathcal{M}' \models PARITY_{v,\sigma}$ for any $v \notin V_{max}(\mathcal{M})$ (in other words, $\mathcal{M}$ is consistent with $\{ PARITY_{v,\sigma} \mid v \notin V_{max}(\mathcal{M}) \}$).*

Remark: It is important to notice the following *monotonicity property*: if $\mathcal{M}$ is admissible and $\mathcal{M}' \subseteq \mathcal{M}$, then $V_{max}(\mathcal{M}') \supseteq V_{max}(\mathcal{M})$ and $\mathcal{M}'$ is admissible, too. That's exactly what we need the condition $|\mathcal{M}| < c(G)$ for.

Lemma 3.26 *Suppose that $\mathcal{M}$ is admissible for $T(G,\sigma)$. Then for any $v_0 \in V_{max}(\mathcal{M})$ there exists a proper 1-CNF $\mathcal{M}' \supseteq \mathcal{M}$ such that $\forall v \neq v_0$ $\mathcal{M}' \models PARITY_{v,\sigma}$ (in other words we can extend the assignment $\mathcal{M}$ to satisfy all axioms except that of v_0).*

Proof: Let us consider the restriction ρ which corresponds to $\mathcal{M}$ ($\rho(x_e) = \epsilon$ iff $x_e^\epsilon \in \mathcal{M}$). If we apply this restriction to the tautology $T(G,\sigma)$ it will be partitioned to the independent formulas: $T^i = \bigwedge_{v \in V_i} PARITY_{v,\sigma'}$ for different connected components V_i of the graph $(G \setminus E(\mathcal{M}))$, where

$$\sigma'(v) \stackrel{\text{def}}{=} \sigma(v) \oplus \bigoplus_{\substack{e \ni v \\ \rho(x_e) \neq *}} \rho(x_e).$$

$V_{max}(\mathcal{M})$ is the component with maximal size. By the definition of admissible configurations, all T^i are satisfiable for $V_i \neq V_{max}(\mathcal{M})$. By Lemma 3.22 there exists an assignment to the edges in $V_{max}(\mathcal{M})$ which satisfies all axioms except $PARITY_{v_0,\sigma'}$. The lemma follows. □

Let us now finish the proof of Theorem 3.24. Let $\mathbb{A}$ be the set of configurations admissible for $T(G,\sigma)$. As usual we claim that for each configuration $\mathcal{M}$, derivable in space $c(G) - d$, there exists a configuration $\mathcal{M}^{-1} \in \mathbb{A}$ such that $\mathcal{M}^{-1} \models \mathcal{M}$ and $|\mathcal{M}^{-1}| \leq |\mathcal{M}|$. We prove it by induction. The basis, inference step and memory erasing can be handled with help of the locality lemma 3.9 just as in Theorems 3.13, 3.18.

Consider the axiom download. Let $\mathcal{M}_{t+1} := \mathcal{M}_t \cup \{C\}$, $C \in PARITY_{v,\sigma}$ for some vertex v. The proof splits into two cases.

Case 1: $v \notin V_{max}(\mathcal{M}_t^{-1})$. Since $\mathcal{M}_t^{-1}$ is admissible, there exists $\mathcal{M}_t' \supseteq \mathcal{M}_t^{-1}$ such that $\forall v \notin V_{max}(\mathcal{M}_t^{-1})$, $\mathcal{M}_t' \models PARITY_{v,\sigma}$ (and in particular $\mathcal{M}_t' \models C$). Let $x_e^\epsilon \in \mathcal{M}_t'$ be a literal which forces C to true (i.e. $x_e^\epsilon \in C$). Let

$\mathcal{M}_{t+1}^{-1} = \mathcal{M}_t^{-1} \cup \{x_e^\epsilon\}$. It is clear that $V_{max}(\mathcal{M}_{t+1}^{-1}) = V_{max}(\mathcal{M}_t^{-1})$ (since $e \ni v$) and $\mathcal{M}_{t+1}^{-1} \in \mathbb{A}$.

Case 2: $v \in V_{max}(\mathcal{M}_t^{-1})$. Let us add to $E(\mathcal{M}_t^{-1})$ all the edges adjacent to v: $E' = E(\mathcal{M}_t^{-1}) \cup E(v)$. By the induction hypothesis, $|\mathcal{M}_t^{-1}| \leq c(G) - d - 1$ (there's one free memory cell for axiom download) hence $|E'| < c(G)$. Let V'_{max} be the maximal connected component in $G \setminus E'$. By our remark on the monotonicity, $V'_{max} \subseteq V_{max}(\mathcal{M}_t^{-1})$. Fix any $v_0 \in V'_{max}$ and let $\mathcal{M}'$ be the proper extension of $\mathcal{M}_t^{-1}$ from Lemma 3.26 such that $\forall u \neq v_0\ \mathcal{M}' \models PARITY_{u,\sigma}$. Let $x_e^\epsilon \in \mathcal{M}'$ be a literal which forces C to true (i.e. $x_e^\epsilon \in C$). Let $\mathcal{M}_{t+1}^{-1} = \mathcal{M}_t^{-1} \cup \{x_e^\epsilon\}$. It is clear that $V_{max}(\mathcal{M}_{t+1}^{-1}) \supseteq V'_{max} \ni v_0$, hence $\mathcal{M}_{t+1}^{-1} \in \mathbb{A}$.

Theorem 3.24 follows.

□

If G is an expander, then the clause space of refuting $T(G, \sigma)$ is linear in the input size, and we get:

Corollary 3.27 *There exist arbitrarily large unsatisfiable* 3*-CNF formulas* $\mathcal{T}$ *with*

$$CSpace^{sem}(\mathcal{T}) = \Omega(|\mathcal{T}|).$$

Proof: Let G be a 3-regular expander with expansion $\epsilon > 0$ (i.e., $\forall(V' \subset V)(|V'| \leq n/2 \Rightarrow |E(G) \cap (V' \times (V \setminus V'))| \geq \epsilon|V'|)$). Let σ be an odd-weight function on $V(G)$. Let $\mathcal{T} = T(G, \sigma)$. By Lemma 3.21, $\mathcal{T}$ is an unsatisfiable 3-CNF formula with $O(|V|)$ clauses and variables. On the other hand, it is easy to verify that $c(G) = \Omega(|V|)$. □

4 Clause Space in the Polynomial Calculus

In this section we give definitions of the clause space in the stronger proof system called the *polynomial calculus* (PC). We then show that the proof techniques of the previous section are not good enough for the polynomial calculus, by proving an upper bound of $\frac{2}{3}n + O(1)$ on the clause space of CT_n. Finally, we generalize our proof systems to *multi-valued logic*, since our lower bounds will be presented more naturally in this setting. The lower bound itself appears in the next section.

4.1 The Polynomial Calculus

In the polynomial calculus we work within a fixed field $\mathbb{F}$. A line in a PC derivation is a polynomial over $\mathbb{F}$, represented as a sum of monomials[4]. With every polynomial $P(x_1, \ldots, x_n)$ we associate the Boolean function $||P||$, called the *interpretation* of P, which is the characteristic function of the set of its roots in $\{0,1\}^n$, i.e.

$$||P||(\alpha) = 1 \quad \text{iff} \quad P(\alpha) = 0.$$

[4]Since all our results apply to any field $\mathbb{F}$, we do not mention it in our future definitions and statements, and simply assume $\mathbb{F}$ is some fixed field.

For $\mathcal{P}$ a set of polynomials, $||\mathcal{P}|| \stackrel{\text{def}}{=} \{||P|| : P \in \mathcal{P}\}$.

Notation: *Throughout this section we sometimes identify a polynomial P with its interpretation $||P||$ as a Boolean function, and it will be clear from the context which of the two we mean. In particular, for $\mathcal{P}$ a set of polynomials, and $\mathcal{M}$ a set of Boolean functions, we will use the notation $\mathcal{M} \models \mathcal{P}$, ($\mathcal{P} \models \mathcal{M}$ resp.) to denote $\mathcal{M} \models ||\mathcal{P}||$ ($||\mathcal{P}|| \models \mathcal{M}$ resp.)*

The natural representation of the clause $\bigvee_{i=1}^{n} x_i$ as a polynomial is by $\prod_{i=1}^{n}(1 - x_i)$. Notice that this polynomial has 2^n monomials, and since we will define the clause space of a polynomial to be the number of monomials appearing in it, this representation makes the polynomial calculus much weaker than resolution. For this reason we use an augmented version of the polynomial calculus that is strictly stronger than resolution, with respect to space as well as size. We denote this augmented system by PCR (*polynomial calculus augmented with resolution*). In this system, we introduce a distinct *variable* for every *literal*, and add some axioms forcing x_i and $\bar{x}_i$ to have distinct values in $\{0, 1\}$. Thus, a line in PCR is a polynomial over the variable set $x_1, \bar{x}_1, x_2, \bar{x}_2, \ldots$, and the following inference rules are used.

> DEFAULT AXIOMS $x(1-x)$ for all variables x (forcing $\{0,1\}$ solutions), and $x + \bar{x} = 1$ for all pairs of distinct variables $x, \bar{x}$ (forcing x to be the negation of $\bar{x}$).
>
> SCALAR ADDITION Derive $\alpha P_1 + \beta P_2$ from P_1, P_2, for α, β scalars in $\mathbb{F}$, and P_1, P_2 any polynomials over $\mathbb{F}$.
>
> VARIABLE MULTIPLICATION Derive $x \cdot P$ from P, for x any variable and P any polynomial over $\mathbb{F}$.

A PCR derivation of a polynomial Q from a set of polynomials $\mathcal{P} = \{P_1, \ldots, P_m\}$ is a sequence of configurations $\pi = \{\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_s\}$, where $\mathcal{M}_0 = \emptyset$, $\mathcal{M}_s = \{Q\}$, and for $1 \leq t \leq s$, $\mathcal{M}_t$ must be one of the following:

> Axiom Download $\mathcal{M}_t := \mathcal{M}_{t-1} \cup \{P\}$ for some axiom $P \in \mathcal{P}$ or some default axiom P.
>
> Memory Erasing $\mathcal{M}_t := \mathcal{M}_{t-1} - \mathcal{M}'$, for some subset of polynomials $\mathcal{M}' \subseteq \mathcal{M}_{t-1}$.
>
> Inference $\mathcal{M}_t := \mathcal{M}_{t-1} \cup \{P\}$, for P inferred from some subset $\mathcal{M}' \subseteq \mathcal{M}_{t-1}$ by a single application of scalar addition or variable multiplication rules.

Just like in resolution, our lower bounds will apply to the *semantical* version of the polynomial calculus. In this system, we replace the inference step of the above definition with the following semantical inference step:

> Semantical Inference $\mathcal{M}_t := \mathcal{M}_{t-1} \cup \{P\}$, for P such that $||\mathcal{M}_{t-1}|| \models ||P||$.

The clause and variable space of a PCR derivation are the natural analogs of the same measures in resolution. Namely, a *configuration* is a set of polynomials, and its clause space is the number of *distinct* monomials that appear in the polynomials (notice that a certain monomial may appear in

several polynomials, but we count it only once). The variable space of a configuration is the sum of degrees of these distinct monomials.

A *refutation of* $\mathcal{P}$ is a derivation of the polynomial 1 from $\mathcal{P}$. The *clause space of a derivation* is the maximal clause space of a configuration in it, and the clause space of $\mathcal{P}$, denoted $MSpace(\mathcal{P})$ is the minimal clause space of a refutation of $\mathcal{P}$, if it exists, and ∞ otherwise (we use the letter M, for *monomial space*, to distinguish it from resolution clause space). The variable space of $\mathcal{P}$, denoted $VSpace_{PCR}(\mathcal{P})$, and the semantical clause space of a PCR proof, denoted $MSpace^{sem}(\mathcal{P})$, are analogously defined.

Remark: A polynomial is a linear combination of clauses. It is worth noting that the clause space lower bounds of Section 4.4 apply to any sound calculus that uses lines that are *arbitrary* Boolean functions of clauses (the linearity, however, will be important in the next section 5 for the *variable* space lower bounds). The strongest such system is the *functional calculus*, which has as lines any Boolean function over clauses, and has the single semantical inference rule that allows to derive any function g from $\mathcal{M}$ whenever $\mathcal{M} \models g$. A definition of this system and its clause space appear in Appendix.

We end this section by noting that PCR is at least as efficient as resolution with respect to variable and clause space. The proof of the following lemma follows from the fact that PCR can efficiently simulate a resolution derivation.

Lemma 4.1 *For $\mathcal{T}$ a contradictory set of clauses, and $\mathcal{P}$ its natural formulation as a set of polynomials:*

- $MSpace(\mathcal{P}) \leq CSpace(\mathcal{T}) + O(1)$.
- $VSpace_{PCR}(\mathcal{P}) \leq 2 \cdot VSpace_{R}(\mathcal{T})$.

4.2 PCR upper bounds for CT_n

We now show that $MSpace(CT_n)$ is substantially smaller than $CSpace^{sem}(CT_n)$. This result shows the necessity of using more complicated techniques than those in Section 3 to prove PCR lower bounds (recall that $CSpace^{sem}(CT_n) = n$).

Theorem 4.2 $MSpace(CT_n) \leq 2n/3 + 6$.

Proof:

Definition 4.3 *We say that a PCR proof π has k* temporary memory cells *if whenever the transition $\mathcal{M}_{t-1} \rightsquigarrow \mathcal{M}_t$ is an axiom download then $MSpace(\mathcal{M}_{t-1}) \leq MSpace(\pi) - k$ (Informally, distinct monomials appearing in the current configuration $\mathcal{M}_t$ are stored in distinct "memory cells". The definition says that whenever we start downloading an axiom, there exist at least k (out of $MSpace(\pi)$) free memory cells).*

We prove by induction the following claim saying that if we can refute CT_n in small space, we can also refute $CT_{\ell \cdot n}$ in small space.

Claim 4.4 (Amplification) *If there exists a PCR refutation π of CT_n with*

$$MSpace(\pi) \leq s + k$$

such that π has k temporary cells then for all integers $\ell \geq 1$

$$MSpace(CT_{\ell \cdot n}) \leq \ell \cdot s + k.$$

Moreover the corresponding refutation also has k temporary memory cells.

Proof: By induction on $\ell \geq 1$. For the induction step, suppose π_ℓ is a refutation of $CT_{\ell \cdot n}$ with $MSpace(\pi_\ell) \leq \ell \cdot s + k$ which has k temporary cells. We shall use π_ℓ to refute $CT_{(\ell+1)\cdot n}$. We only have to show how to derive an axiom $A \in CT_{\ell \cdot n}$ from $CT_{(\ell+1)\cdot n}$ using small memory, because if we can derive any axiom of $CT_{\ell \cdot n}$ in small space, we can use π_ℓ directly, replacing each axiom download in π_ℓ with our small space derivation.

Suppose the t'th step of π_ℓ is an axiom download of $A \in CT_{\ell \cdot n}$. $A = \bigvee_{j=1}^{\ell n} x_j^{\epsilon_j}$, for some $\vec{\epsilon} = \{\epsilon_1, \ldots, \epsilon_{\ell n}\} \in \{0,1\}^{\ell n}$. By the induction hypothesis, $MSpace(\mathcal{M}_{t-1}) \leq \ell \cdot s$, because $\mathcal{M}_{t-1}$ has k empty memory cells. We use these empty memory cells, and additional s memory cells to derive A from all axioms $B \in CT_{(\ell+1)\cdot n}$ that agree with A on all variables of A (i.e. $B = A \vee \bigvee_{j=\ell n+1}^{(\ell+1)n} x_j^{\epsilon_j}$, for some $\epsilon_{\ell n+1}, \ldots, \epsilon_{(\ell+1)n} \in \{0,1\}$). The total memory of the new proof is $MSpace(CT_{\ell \cdot n}) + s$. It also has k temporary memory cells since it downloads axioms only during the emulation of the proof of CT_n. □

To prove Theorem 4.2 it is sufficient to produce a PCR refutation of CT_3 with clause space six and four temporary memory cells ($s = 2, k = 4$). At the beginning of this refutation we infer the configuration $\{x_1, x_2\}$ in the obvious way. After that the proof proceeds as follows (we omit straightforward intermediate transitions):

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} x_1 \\ x_2 \\ \text{Axiom: } \bar{x}_1\bar{x}_2x_3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} x_1 \\ x_2 \\ \bar{x}_2x_3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1-\bar{x}_1 \\ 1-\bar{x}_2 \\ 1-\bar{x}_3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1-\bar{x}_1 \\ \bar{x}_1-\bar{x}_1\bar{x}_2 \\ \bar{x}_1\bar{x}_2-\bar{x}_1\bar{x}_2\bar{x}_3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1-\bar{x}_1\bar{x}_2\bar{x}_3 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1-\bar{x}_1\bar{x}_2\bar{x}_3 \\ \text{Axiom: } \bar{x}_1\bar{x}_2\bar{x}_3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 \end{pmatrix}.$$

All the configurations explicitly displayed here have at most four clauses. Two more temporary clauses are needed to keep intermediate polynomials. □

Remark: For the stronger system called the *functional calculus*, we get better upper bounds than those of the previous theorem (namely, CT_n can be refuted in clause space $n/2 + 2$). For a definition of this proof system, and a proof of this and related results, see Appendix.

4.3 PCR over multi-valued logic

In this subsection we extend our proof systems to work with multi-valued variables. The motivation is the usual one: in many cases, the multi-valued logic is a natural vista to view lower bounds for the Boolean case which is our true interest. For example, [RWY97] used R-way (read-once) branching programs to formulate and prove some partial results about the resolution (size) complexity of the weak (i.e., when $m \gg n$) pigeonhole principle PHP_n^m. Crucial to their results are two dual interpretations of PHP_n^m in terms of multi-valued logic; here we are interested only in one of them, the *Column Model*. In this model, the pigeonhole principle has the following form: suppose $x_1, \ldots, x_n$ are variables of m-valued logic, where $m > n$ ("$x_j = i$" has the intended meaning "the i'th pigeon sits in the j'th hole"). Then there exists $i \in [m]$ which is not in the set $\{x_1, \ldots, x_n\}$.

In the proofs of our remaining lower bounds, it will be also very convenient to treat PHP_n^m in this way. In particular, this will allow us to formulate our bounds in terms of a simple, uniform and concise criterion fulfilled by both CT_n and PHP_n^m (Definition 4.12 below).

We need to generalize some previous definitions.

Definition 4.5 *Let us fix some finite domain D. Instead of Boolean variables, we use* multi-valued variables x_j *ranging over the domain D. A* multi-valued Boolean function $f(x_1, \ldots, x_n)$ *is a mapping from D^n to $\{0,1\}$, where, as before, we identify 1 with $True$ and 0 with $False$. The notions of* a (multi-valued) satisfying assignment $a \in D^n$ *and* semantical implication $f_1, \ldots, f_k \models g$ *are generalized to the case of multi-valued logic straightforwardly.*

Thus, the only remaining thing we still need to define is the set of allowable lines.

Definition 4.6 (Multi-valued clauses) *Suppose that D is some finite domain. A* multi-valued literal *is the formal expression x_j^π, where π is some non-constant function $\pi : D \to \{0,1\}$.*

A multi-valued clause *is a disjunction of multi-valued literals corresponding to distinct variables*

$$C = x_{j_1}^{\pi_1} \vee x_{j_2}^{\pi_2} \vee \ldots \vee x_{j_w}^{\pi_w},\ k \neq l \to j_k \neq j_l,$$

with the straightforward interpretation $||C||(\alpha) \stackrel{\text{def}}{=} \pi_1(\alpha_{j_1}) \vee \ldots \vee \pi_w(\alpha_{j_w})$.

The width *of a multi-valued clause is the number of multi-valued literals in it.*

Definition 4.7 *Denote by x_j^i the multi-valued literal $x_j^{\chi_i}$, where χ_i is the characteristic function of i ($\chi_i(i') = 1$ iff $i' = i$).*

We are ready to define multi-valued semantical resolution and PCR:

Definition 4.8 (Multi-valued resolution) Multi-valued semantical resolution over domain D *is the system analogous to semantical resolution which works with multi-valued clauses instead of usual ones.*

The clause and variable complexity are analogous to that of semantical resolution. Denote by $CSpace_D^{sem}(\mathcal{T})$ the clause space of refuting $\mathcal{T}$ in semantical resolution over domain D.

Definition 4.9 (Multi-valued PCR) *Suppose that $\mathbb{F}$ is a field.* Multi-valued semantical PCR over domain D *is the semantical system which keeps in memory polynomials over $\mathbb{F}$ with literals x_j^π for all possible j, π as their variables. As in the Boolean case, the interpretation is given by the characteristic function of the set of roots:*

$$||P||(\alpha_1, \ldots, \alpha_n) = 1 \quad \textit{iff} \quad P[\pi(\alpha_j)/x_j^\pi] = 0$$

in the field $\mathbb{F}$. The clause and variable complexity are analogous to that of semantical PCR. Denote by $MSpace_D^{sem}(\mathcal{P})$ the clause space of refuting $\mathcal{P}$ in semantical resolution over domain D.

We conclude this subsection with one possible translation from multi-valued systems to ordinary ones. This straightforward translation preserves the variable and clause space lower bounds.

Definition 4.10 *Suppose that P is some multi-valued proof system over domain D, $\mathcal{T}$ is a contradictory set of axioms. Replace each multi-valued variable x_j with the tuple $x_{1j}, x_{2j}, \ldots, x_{mj}$, where $m = |D|$. The intuitive meaning of x_{ij} is "$x_j = i$", i.e., the same as of the multi-valued literal x_j^i.*

Let us denote by $PR_D(\mathcal{T})$ the following set of axioms over Boolean variables x_{ij}:

- $\bar{x}_{i_1 j} \vee \bar{x}_{i_2 j}$, *for* $i_1 \neq i_2$;
- $\phi\left[\bigvee_{i \in \pi^{-1}(1)} x_{ij}/x_j^\pi\right]$ *for all* $\phi \in \mathcal{T}$.

It is clear that each refutation of $PR_D(\mathcal{T})$ can be transformed into the refutation of $\mathcal{T}$ without increase in either variables or clauses. Thus we have the following trivial proposition which shows how to use multi-valued systems for proving Boolean lower bounds:

Proposition 4.11 *For $\mathcal{T}$ a contradictory set of multi-valued clauses over domain D,*

$$CSpace_D^{sem}(\mathcal{T}) \leq CSpace(PR_D(\mathcal{T})).$$

For $\mathcal{P}$ a contradictory set of polynomials over domain D,

$$MSpace_D^{sem}(\mathcal{P}) \leq MSpace(PR_D(\mathcal{P})).$$

4.4 Wide Tautologies and Lower Bounds for PCR

In this section we define a natural class of *wide* tautologies which turn out to be hard for PCR in terms of clause complexity. In Section 5 we will also show that wide tautologies are hard for PCR (and hence for resolution as well) in terms of *variable* complexity. The previous upper bound on the clause space of CT_n (Theorem 4.2) shows that selecting *one* variable per clause in the memory, and using this variable to satisfy our clause, will not work for PCR. Surprisingly, we show that selecting *two* variables per clause does the job.

Definition 4.12 (Multi-valued wide tautology) *A family of multi-valued clauses $\mathcal{T}$ over multi-valued variables $x_1, \ldots, x_n$ is* wide *iff every clause in it has maximal possible width n.*

One obvious example of a (Boolean) wide family is CT_n. The second example, and our main motivation, is PHP_n^m. Namely, suppose that $|D| = m > n$, and let $\mathcal{T} \stackrel{def}{=} \left\{ x_1^i \vee x_2^i \vee \ldots \vee x_n^i \mid i \in [m] \right\}$. Then $PR_D(\mathcal{T}) = PHP_n^m$. By Proposition 4.11, lower bounds for the space complexity of this multi-valued version imply lower bounds for the space complexity of the ordinary (Boolean) pigeonhole principle.

Now we show that wide tautologies are hard. The heart of our lower bounds for PCR is the locality lemma 4.14.

Definition 4.13 (Proper 2-CNF's) *$\mathcal{M}$ is called a* proper 2-CNF *iff*

$$\mathcal{M} = \{x_{j_1^1}^{i_1^1} \vee x_{j_1^2}^{i_1^2},\ x_{j_2^1}^{i_2^1} \vee x_{j_2^2}^{i_2^2}, \ldots, x_{j_k^1}^{i_k^1} \vee x_{j_k^2}^{i_k^2}\},$$

where $j_1^1, j_1^2, j_2^1, \ldots, j_k^2$ are pairwise distinct indices and $i_1^1, \ldots, i_k^2 \in [m]$ (not necessarily distinct). (In other words, the proper 2-CNF says that for every $\ell \in [k]$ either $x_{j_\ell^1} = i_\ell^1$ or $x_{j_\ell^2} = i_\ell^2$).

Lemma 4.14 (Locality lemma for PCR) *Let $\mathcal{M}$ be a proper 2-CNF, and $\mathcal{M}_1$ be a set of polynomials such that $\mathcal{M} \models \mathcal{M}_1$. Then there exists a proper 2-CNF $\mathcal{M}_1^{-1}$ such that $\mathcal{M}_1^{-1} \models \mathcal{M}_1$ and $|\mathcal{M}_1^{-1}| \leq 2 \cdot MSpace_D^{sem}(\mathcal{M}_1)$.*

Remark: Notice that $\mathcal{M}_1^{-1}$ is not necessarily a proper sub-formula of $\mathcal{M}$.
Proof: In our proof we will use the following corollary of Hall's Matching Theorem:

Lemma 4.15 (Hall's Theorem) *For a family of sets $V_1, \ldots, V_k$ (not necessarily distinct), if for all index sets $I \subseteq [k]$*

$$|\bigcup_{i \in I} V_i| \geq |I|,$$

then the family $V_1, \ldots, V_k$ has a system of distinct representatives. *That is, there exist $v_i \in V_i$ such that $\{v_1, \ldots, v_k\}$ are pairwise distinct.*

Corollary 4.16 *For a family of sets $V_1, \ldots, V_k$, if for all index sets $I \subseteq [k]$*

$$|\bigcup_{i \in I} V_i| \geq 2 \cdot |I|,$$

then we can assign to each V_i two *distinct representatives $v_{i1}, v_{i2} \in V_i$ such that all $2k$ elements $v_{11}, v_{12}, \ldots, v_{k1}, v_{k2}$ are pairwise distinct.*

Proof: Just apply Hall's matching theorem to the system

$$V_1, V_1, V_2, V_2, \ldots, V_k, V_k.$$

□

Let us now prove Lemma 4.14. Note that $||\mathcal{M}_1|| = g(C_1, \ldots, C_s)$, where $s = MSpace_D^{sem}(\mathcal{M}_1)$, $C_1, \ldots, C_s$ are multi-valued clauses, and g is some Boolean function. Let us gradually construct the required proper 2-CNF $\mathcal{M}_1^{-1}$. Suppose w.l.o.g. that $\mathcal{M} = \{x_{1,1}^0 \vee x_{1,2}^0,\ x_{2,1}^0 \vee x_{2,2}^0, \ldots, x_{k,1}^0 \vee x_{k,2}^0\}$.

For a clause C denote by $V(C) \subseteq [k]$ the index set of those axioms $x_{j,1}^0 \vee x_{j,2}^0$ of $\mathcal{M}$ for which C contains at least one variable $x_{j,1}, x_{j,2}$ (formally, $V(C) \stackrel{\text{def}}{=} \left\{ j \;\middle|\; \exists \epsilon \in \{1,2\}\ \exists \pi (x_{j,\epsilon}^{\pi} \in C) \right\}$). For $\Gamma \subseteq [s]$, let us denote $\bar{\Gamma} = [s] \setminus \Gamma$, $V(\Gamma) = \bigcup_{\gamma \in \Gamma} V(C_\gamma)$. Let Γ be any maximal subset $\Gamma \subseteq [s]$ with the property

$$|V(\Gamma)| \leq 2 \cdot |\Gamma|.$$

Then for any $I \subseteq \bar{\Gamma}$,

$$|V(I) \setminus V(\Gamma)| > 2 \cdot |I|$$

(otherwise we could add the set I to Γ, contradicting the maximality of Γ). Hence, by Corollary 4.16, for any clause C_γ with $\gamma \in \bar{\Gamma}$ we can choose two unique *representative indices* $j_1, j_2 \in V(C_\gamma)$ such that $j_1, j_2 \notin V(\Gamma)$. Let $x_{rep_1(C_\gamma)}, x_{rep_2(C_\gamma)}$ be two corresponding *representative variables* from C_γ which lie in the intersection with axioms numbers j_1, j_2 of $\mathcal{M}$. Denote by $sat_\epsilon(C_\gamma)$ the value of $x_{rep_\epsilon(C_\gamma)}$ which forces C_γ to *True*. Such a value must exist because C_γ is a clause in which $x_{rep_\epsilon(C_\gamma)}^{\pi}$ appears for some *non-constant* π (see Definition 4.6).

Let

$$\mathcal{M}_1^{-1} = \left\{ x_{j,1}^0 \vee x_{j,2}^0 \,|\, j \in V(\Gamma) \right\} \cup \left\{ x_{rep_1(C_\gamma)}^{sat_1(C_\gamma)} \vee x_{rep_2(C_\gamma)}^{sat_2(C_\gamma)} \,|\, \gamma \in \bar{\Gamma} \right\}.$$

Clearly, $\mathcal{M}_1^{-1}$ is a proper 2-CNF. Let us estimate the size of $\mathcal{M}_1^{-1}$:

$$|\mathcal{M}_1^{-1}| = |V(\Gamma)| + |\bar{\Gamma}| \leq 2 \cdot |\Gamma| + |\bar{\Gamma}| \leq 2 \cdot s.$$

Claim 4.17 $\mathcal{M}_1^{-1} \models \mathcal{M}_1$.

Proof: We need to show that every assignment α satisfying $\mathcal{M}_1^{-1}$ satisfies $g(C_1, C_2, \ldots, C_s)$ as well. Suppose that α satisfies all the clauses of $\mathcal{M}_1^{-1}$. Notice that $\forall \gamma \in \bar{\Gamma}\ C_\gamma(\alpha) = 1$ (since α satisfies $\mathcal{M}_1^{-1}$, it satisfies $x_{rep_1(C_\gamma)}^{sat_1(C_\gamma)} \vee x_{rep_2(C_\gamma)}^{sat_2(C_\gamma)}$ and every one of these representative variables from C_γ forces C_γ to *True*).

We are going to show that α can be changed in such a way that it will still preserve the value of all clauses $C_1, \ldots, C_s$ (and, hence, of g) but at the same time will satisfy $\mathcal{M}$. For an axiom $x_{j,1}^0 \vee x_{j,2}^0$ of $\mathcal{M}$ either $j \in V(\Gamma)$ – in this case the axiom is satisfied since it also appears in $\mathcal{M}_1^{-1}$, or we can choose the variable $x_{j,\epsilon}$ which is *not* a representative variable of any clause C_γ with $\gamma \in \bar{\Gamma}$ (notice that different clauses can not have representatives from the same axiom). In the latter case we just set $x_{j,\epsilon}$ to zero. This doesn't change the values of clauses $C_1, \ldots, C_s$, but the axioms of $\mathcal{M}$ get satisfied.

Thus we can get the new assignment α' which satisfies $\mathcal{M}$ and such that $C_i(\alpha) = C_i(\alpha')$ for all i. Since $||\mathcal{M}|| \models g(C_1, \ldots, C_s)$, we have

$$g(C_1(\alpha), \ldots, C_s(\alpha)) = g(C_1(\alpha'), \ldots, C_s(\alpha')) = 1.$$

Lemma 4.14 follows. □

We are now ready to prove our main theorem:

Theorem 4.18 *For any wide tautology $\mathcal{T}$ over n variables with domain D, $MSpace_D^{sem}(\mathcal{T}) \geq \frac{n}{4}$.*

Remark: The same lower bound, with the same proof, applies to the much stronger *functional calculus*, in which each line is an arbitrary Boolean function, and all derivations rule are purely semantical. For a definition of this system and related results see Appendix.

Proof: The proof is quite analogous to the proof of Theorem 3.13. Let us denote by $\mathbb{A}$ the set of all proper 2-CNF's of size $\leq \frac{n}{2}$. As in the previous cases we claim that for any configuration $\mathcal{M}$, achievable in space $\frac{n}{4}$, there exists a configuration $\mathcal{M}^{-1} \in \mathbb{A}$ such that $|\mathcal{M}^{-1}| \leq 2 \cdot MSpace_D^{sem}(\mathcal{M})$ and $\mathcal{M}^{-1} \models \mathcal{M}$. We prove it by induction.

The inference step can be treated with help of locality lemma 4.14. Namely, if $\mathcal{M}_t \models \mathcal{M}_{t+1}$, take first $\mathcal{M}_t^{-1}$ as $\mathcal{M}_{t+1}^{-1}$, and then shrink it to the required size $2 \cdot MSpace_D^{sem}(\mathcal{M}_{t+1})$ by applying Lemma 4.14.

The axiom download is also straightforward. Suppose that $\mathcal{M}_{t+1} \leftarrow \mathcal{M}_t \cup \{C\}$, $C \in \mathcal{T}$. Take $\mathcal{M}_t^{-1}$ and choose two literals $x_{j_1}^{\pi_1}, x_{j_2}^{\pi_2} \in C$ such that x_{j_1} and x_{j_2} are not contained in $\mathcal{M}_t^{-1}$. Such a pair of literals must exist because C has width n and $|\mathcal{M}_t| < n/4$, and hence $|\mathcal{M}_t^{-1}| \leq n/2$. Then let $\mathcal{M}_{t+1}^{-1} = \mathcal{M}_t^{-1} \cup \{x_{j_1}^{i_1} \vee x_{j_2}^{i_2}\}$, for i_1, i_2 satisfying $\pi_1(i_1) = \pi_2(i_2) = 1$.

Theorem 4.18 follows. □

Corollary 4.19 $MSpace^{sem}(CT_n) \geq MSpace_D^{sem}(CT_n) \geq n/4$.

As said previously, a lower bound on multi-valued logic is also a lower bound on two-valued, Boolean logic, and thus we get:

Corollary 4.20 *For all $m > n$,*

$$MSpace^{sem}(PHP_n^m) \geq MSpace_D^{sem}(PHP_n^m) \geq n/4.$$

5 Variable Complexity for PCR

The variable space is a very natural space measure as it is tightly connected to the bit space, which is the actual number of bits needed to write down a memory configuration. If each variable index is written in binary notation, then the bit space is linear in $\log n$ times the variable space. As follows from Theorem 3.5, every (Boolean) proof system which simulates resolution has variable space upper bounded by n^2. In this section we show that any PCR proof (over an arbitrary field) of any wide tautology requires variable space $\Omega(n^2)$. This bound is tight for both CT_n and PHP_n^m.

Theorem 5.1 *For any wide tautology $\mathcal{T}$ over n variables with domain D and any ground field $\mathbb{F}$, $VSpace_{PCR}^{sem}(\mathcal{T}) = \Omega(n^2)$.*

To understand the intuition of the proof, and see how heavily it depends on our previous clause space lower bounds, we prove first the following (easy) special case of our theorem.

Lemma 5.2 $VSpace_R^{sem}(CT_n) \geq \frac{1}{4}n^2$.

Proof: By Theorem 3.13, $CSpace^{sem}(CT_n) > n$. Let $\pi = \{\mathcal{M}_0 \dots \mathcal{M}_s\}$ be a semantical resolution refutation of CT_n, and let t be the first time there is some clause $C \in \mathcal{M}_t$ of width $\lceil n/2 \rceil$. Such a t must exist, because by the definition of the resolution rule, the width of a clause may decrease by at most 1 in every step, all axioms have width n, and the empty clause has width 0. Let ρ be the minimal size restriction that sets C to 0. $|\rho| = |C| = \lceil n/2 \rceil$, and it is easy to see that $CT_n|_\rho$ is simply $CT_{\lfloor n/2 \rfloor}$, and $\pi|_\rho$ is a legitimate proof of it. Applying Theorem 3.13 once again, $CSpace^{sem}(CT_{\lfloor n/2 \rfloor}) > \lfloor n/2 \rfloor$, meaning there is some $t' < t$ such that $|\mathcal{M}_{t'}| > \lfloor n/2 \rfloor$. By the definition of t, all clauses of $\mathcal{M}_{t'}$ have width larger than than $\lceil n/2 \rceil$, and the lemma is proved. □

Proof [Theorem 5.1]: First we need to define some notation. A term $x_{j_1}^{\pi_1} \cdot \ldots \cdot x_{j_d}^{\pi_d}$ is *multi-linear* if all $j_1, \dots, j_d$ are pairwise distinct. A *multi-linear monomial* is an expression $a \cdot t$, where $a \in F^*$ and t is a multi-linear term. Finally, a *multi-linear polynomial* is a sum of multi-linear monomials. Since we are interested only in the semantical version of PCR, and because of the identity $x_j^\pi \cdot x_j^{\pi'} = x_j^{(\pi\pi')}$, we will assume w.l.o.g. that all our multi-valued terms, monomials and polynomials are multi-linear. Also, throughout the proof of Theorem 5.1 all the terms, monomials and polynomials are multi-valued, thus we omit this word, too. For a term t, let $Supp(t)$ be the set of all j for which x_j^π appears in t for some π. For a polynomial P, $Supp(P) \stackrel{\text{def}}{=} \bigcup_{t \in P} Supp(t)$.

There is a natural correspondence between subsets of the set of terms of a polynomial P and its subpolynomials, thus we sometimes write $t \in P$ when the term t is contained in P, and $P_1 \subseteq P$ which means that P_1 is a subpolynomial of P. $|P|$ is the number of terms in P.

For $\rho : \{x_1, \dots, x_n\} \to D \cup \{*\}$ a restriction and P a polynomial, $\rho(P)$ is the polynomial produced after the substitution of the literals x_j^π, $j \in \rho^{-1}(D)$ with $\pi(\rho(x_j))$ and cancellation of terms. Notice that there can be many different polynomials corresponding to the same multi-valued function $f : D^n \to \{0, 1\}$. We say that such polynomials are *semantically equivalent* and write $P_1 \sim P_2$. For example, $x \sim 1 - \bar{x}$ in case of Boolean PCR.

Our proof will consist of several stages. The heart of it will be the following construction based on Hall's theorem (we already used a similar idea in proving Theorem 4.18).

Lemma 5.3 (Matching Lemma) *Suppose that P is a polynomial, and t is some term (not necessarily from P). Then there exists a subpolynomial $\Gamma \subseteq P$ and a restriction ρ, such that ρ doesn't assign the variables of $Supp(t) \cup Supp(\Gamma)$ and ρ maps all terms of $P \setminus \Gamma$ to zero (thus, in particular, $\rho(t) = t$ and $\rho(P) = \Gamma$). Moreover, $|Supp(t) \cup Supp(\Gamma)| + |\rho| \leq |P| + \deg t$.*

Proof: Let Γ be any maximal subpolynomial of P with the property

$$|Supp(t) \cup Supp(\Gamma)| \leq |\Gamma| + \deg t.$$

Denote $V = Supp(t) \cup Supp(\Gamma)$. Then for any subset of terms $S \subseteq P \setminus \Gamma$, $|Supp(S) \setminus V| > |S|$ (otherwise we could add S to Γ and Γ would not be maximal). Thus by Hall's theorem there exists a matching

$$\mu : [\text{terms of } P \setminus \Gamma] \to Supp(P) \setminus V$$

which gives each term from $P \setminus \Gamma$ its *unique representative* from $Supp(P) \setminus V$. Now we define the restriction ρ as follows. It maps these unique representatives to the values which force the corresponding terms to 0. Thus ρ doesn't touch the variables from V and $|Supp(t) \cup Supp(\Gamma)| + |\rho| \leq \deg t + |\Gamma| + |P \setminus \Gamma| = \deg t + |P|$. □

Let us now prove Theorem 5.1. Suppose that we have some PCR refutation $\{\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_s\}$ of $\mathcal{T}$. W.l.o.g. we can assume that all polynomials in the memory do not contain non-zero subpolynomials semantically equivalent to zero (there's no sense in keeping such subpolynomials). Let us fix the first moment q when some polynomial from $\mathcal{M}_q$ contains a (multi-linear!) term with degree less or equal $\frac{n}{2}$. Let t be any such term which has the smallest possible degree (in particular, $\deg t \leq \frac{n}{2}$), and let $P \in \mathcal{M}_q$ be any polynomial which contains t. Our proof splits into two cases.

Case 1: $\deg t \geq \frac{n}{4}$.

In this case we can assume that $|P| \leq \frac{n}{8}$ since otherwise $VS(P)$ is already greater than $\frac{n^2}{32}$ (recall that t is the smallest degree monomial from $\mathcal{M}_q$), and we are done.

Lemma 5.4 *Suppose that P is a polynomial with no subpolynomials semantically equivalent to zero, and that t is a term of P. Then there exists a restriction ρ which forces P to a non-zero constant c from F^*, and assigns at most $|\rho| \leq \deg t + |P|$ variables.*

Proof: We apply our Matching Lemma 5.3 to the polynomial P and the term t. We get the subpolynomial Γ and the restriction ρ which kills all the monomials from $P \setminus \Gamma$.

Notice that $\Gamma \neq \emptyset$ since it must contain t. Thus by our assumption, $\Gamma \not\sim 0$, and we can choose an assignment α to $Supp(\Gamma)$ which maps it to some constant $c \in F^*$. Let us extend our restriction ρ to the restriction ρ' by α (this is possible because ρ and α assign to disjoint sets of variables). Then $\rho'(P) = c$ and $|\rho'| \leq |\rho| + |Supp(\Gamma)| \leq |P| + \deg t$. □

The rest of Case 1 is simple. Hitting the first $(q+1)$ lines of the original refutation with the restriction ρ from Lemma 5.4, we get a new valid refutation $\{\rho(\mathcal{M}_0), \rho(\mathcal{M}_1), \ldots, \rho(\mathcal{M}_q)\}$ of the principle $\rho(\mathcal{T})$ (since $c \in \rho(\mathcal{M}_q)$ and $c \neq 0$).

Notice that since $|\rho| \leq \deg t + |P|$ we have $|\rho| \leq \frac{5n}{8}$, so $\rho(\mathcal{T})$ is a wide tautology over $\geq \frac{3n}{8}$ variables. Thus by Theorem 4.18 there exists $j < q$ such that $\rho(\mathcal{M}_j)$ (and, hence, $\mathcal{M}_j$) contains at least $\frac{3n}{32}$ monomials. Each monomial of $\mathcal{M}_j$ had degree $> \frac{n}{2}$ before applying ρ', therefore $VS(\mathcal{M}_j) \geq \frac{3n^2}{64}$.

Case 2: $\deg t \leq \frac{n}{4}$.

Definition 5.5 *We say that a polynomial P is* d-minimal *iff it doesn't contain a non-zero subpolynomial semantically equivalent to a polynomial of degree* $\leq d$.

Since $t \in P$, P is not $\frac{n}{4}$-minimal. Let us represent $P = P_0 + P_1$, where P_1 is $\frac{n}{4}$-minimal and $P_0 \sim P_0'$ with $\deg P_0' \leq \frac{n}{4}$ (we can construct such a representation by consecutively moving subpolynomials semantically equivalent to polynomials of degree $\leq \frac{n}{4}$ from P_1 to P_0).

P does not contain non-zero subpolynomials semantically equivalent to zero; in particular, $P_0 \not\sim 0$. However, there still can be several non-zero polynomials $P_0' \sim P_0$ with $\deg P_0' \leq \frac{n}{4}$. Let P_0' be the polynomial of the smallest degree semantically equivalent to P_0. If there are several such polynomials we choose arbitrarily one with the smallest number of monomials of highest degree. Let s be some maximal-degree term of P_0'.

Let us now apply our Matching Lemma 5.3 to the polynomial P_1 and the term s. It will yield $\Gamma \subseteq P_1$ and the restriction ρ which kills the terms from $P_1 \setminus \Gamma$.

All terms in P_1 are of degree $\geq \frac{n}{4}$, therefore, similarly to Case 1, we can assume that $|P_1| \leq \frac{n}{8}$. Hence, $|Supp(s) \cup Supp(\Gamma)| + |\rho| \leq \deg s + |P_1| \leq \frac{3n}{8}$.

Now we use the fact that $\mathcal{M}_q$ is the *first* configuration when a term t of degree $\leq \frac{n}{2}$ appears. It is clear that the step $\mathcal{M}_{q-1} \rightsquigarrow \mathcal{M}_q$ is a semantical inference (it can't be axiom download because all axioms have degree n). Notice that all terms of polynomials from $\mathcal{M}_{q-1}$ have degree greater than $\frac{n}{2}$. Assume also that $CS(\mathcal{M}_{q-1}) \leq \frac{n}{8}$ (otherwise $VS(\mathcal{M}_{q-1}) \geq \frac{n^2}{16}$). Now we are going to arrive at a contradiction from all these assumptions.

First we claim that ρ can be extended to a restriction ρ_1 that doesn't assign the variables in $|Supp(s) \cup Supp(\Gamma)|$, and kills (= sets to zero) all the terms of $\mathcal{M}_{q-1}$. To see this notice that ρ has assigned $|\rho|$ variables and we should keep unassigned $|Supp(s) \cup Supp(\Gamma)|$ variables, their sum is $|\rho| + |Supp(s) \cup Supp(\Gamma)| \leq |P_1| + \deg s \leq \frac{3n}{8}$ and we need to kill at most $\frac{n}{8}$ terms in $\mathcal{M}_{q-1}$, of degree $\geq n/2$ each. We consecutively kill terms $t \in \mathcal{M}_{q-1}$ by choosing a free unassigned variable from $Supp(t) \setminus (Supp(s) \cup Supp(\Gamma) \cup \rho^{-1}(D))$.

Since $\mathcal{M}_{q-1} \models P$ we have $\rho_1(P) \sim 0$. Thus $\rho_1(P_0 + P_1) \sim 0$ and $\rho_1(P_0' + P_1) \sim 0$ and $\rho_1(P_0') + \Gamma \sim 0$ (because $\rho(P_1 - \Gamma) = 0$, and ρ_1 does not touch variables from $Supp(\Gamma)$). Since $\deg(\rho_1(P_0')) \leq \deg(P_0') \leq n/4$ and P_1 is $n/4$-minimal, Γ should be in fact identically zero.

We proved that $\rho_1(P_0') \sim 0$. Let $d = \deg s = \deg(P_0')$. Notice that every term of degree d in $\rho_1(P_0')$ is also contained in P_0' (because a restriction either decreases the degree of a term, or kills it, or doesn't change it at all). Additionally $\rho_1(P_0')$ contains s, because $\rho_1(s) = s$. Thus we get a polynomial $P_0'' = P_0' - \rho_1(P_0')$ such that $P_0'' \sim P_0$, $\deg(P_0'') \leq d$ and P_0'' contains fewer terms of degree d than P_0'. This contradicts to our choice of P_0' as the polynomial of smallest degree with smallest number of monomials of highest degree. Thus this situation can not take place. Theorem 5.1 follows. □

As direct corollaries, we obtain the following tight bounds:

Corollary 5.6 $VSpace_R(CT_n) \geq VSpace^{sem}_{PCR}(CT_n) \geq \Omega(n^2)$.

Corollary 5.7 $VSpace_R(PHP^m_n) \geq VSpace^{sem}_{PCR}(PHP^m_n) \geq \Omega(n^2)$.

6 Upper Bounds for Frege Systems

In this section we show that the variable space complexity of CT_n is upper bounded by $O(n)$ for Frege systems. It will imply several nice corollaries and in particular the equivalence of semantical and syntactical versions for Frege proofs. We start by defining Frege proof systems and the variable space measure for them.

Definition 6.1 (Frege proof systems) *A* Frege proof system *works with arbitrary propositional formulas. A* line *in a derivation is an arbitrary formula φ over some complete basis. Every inference rule is specified by a* scheme

$$\frac{A_1, \ldots, A_k}{B},$$

where A_i, B are propositional formulas, and altogether there are only finitely many of them. A formula ψ is derived from formulas $\varphi_1, \ldots, \varphi_k$ using this inference rule if there is a set of substitutions σ of formulas for the variables appearing in the scheme such that $\varphi_i = A_i^\sigma$ for $i = 1, \ldots, k$ and $\psi = B^\sigma$. We use the notation $\varphi_1, \ldots, \varphi_k \vdash \psi$ to denote that ψ was derived from $\varphi_1, \ldots, \varphi_k$ using a single rule.

The notions of a Frege proof (derivation) and refutation are analogous to those of resolution and the polynomial calculus. The notion of a semantical Frege proof is the natural extension of semantical systems to Frege. Finally, we give the definition of variable space of a Frege proof:

Definition 6.2 (Frege Variable Space) *For $\mathcal{M}$ a configuration, the* variable space of $\mathcal{M}$ *is $VSpace_F(\mathcal{M}) \stackrel{\text{def}}{=} \sum_{\phi \in \mathcal{M}} VSpace_F(\phi)$ where $VSpace_F(\phi)$ is the number of occurrences of variables in ϕ. The* Frege variable space of a set of configurations $\pi = \{\mathcal{M}_0, \ldots, \mathcal{M}_s\}$ *is*

$$VSpace_F(\pi) \stackrel{\text{def}}{=} \max\{VSpace_F(\mathcal{M}_i) : i \in [s]\},$$

and the Frege variable space *of a CNF $\mathcal{T}$ is*

$$VSpace_F(\mathcal{T}) \stackrel{\text{def}}{=} \min\{VSpace_F(\pi)\},$$

where the minimum is taken over all Frege refutations π of $\mathcal{T}$.

To prove our main result we essentially use the compact rule of representing information analogous to Horner's scheme for quick evaluation of the polynomial P at a given point x:

$$P(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \cdots)).$$

Let us begin with the case when the language of our Frege system $\mathcal{F}$ consists of the standard connectives $\neg, \wedge, \vee, \rightarrow$ and the constant $\mathbf{0}$ (at the end of the section we will show how to modify our proofs to embrace the case of Frege systems in other languages). It is easy to see that the standard simulation of one Frege system by another Frege system in the same language [CR79] also preserves variable space up to a constant multiplicative factor. Therefore,

in the following theorem (which is our main result about variable space for Frege) we can unambiguously use the notation $VSpace_F(\mathcal{T})$, and we can assume in its proof that $\mathcal{F}$ contains any prescribed finite set of sound inference rules.

Theorem 6.3 $VSpace_F(CT_n) = O(n)$.

Proof:

We describe an algorithm for refuting CT_n. Let us call a proof *k-linear* if every line in the proof is derived from k axioms, and at most one line that is not an axiom. A k-linear proof gives rise to a proof DAG that looks like a line, and hence the name. Clearly, if every formula in a k-linear proof has small variable space, then so does the whole proof. We shall present a 2-linear proof of CT_n, such that all intermediate lines have $O(n)$ variable space.

To this end we define the sequence of read-once formulas $\varphi_0, \ldots, \varphi_{2^{(n-1)}-1}$ such that $\varphi_0 = (x_1 \vee x_2 \vee \ldots \vee x_n)$ and $\varphi_{2^{(n-1)}-1} = (x_1 \wedge x_2 \wedge \ldots \wedge x_n)$, and show how to infer φ_{t+1} from φ_t within $O(n)$ variable space, using only two initial clauses from CT_n. The line φ_t encodes in linear space the following claim: *Any satisfying assignment for CT_n, when viewed as a number in binary representation, must be greater than $2 \cdot t$.*

Fix $0 \leq t < 2^{n-1}$, and let $a_1 a_2 \ldots a_{n-1}$ be its binary representation. We let

$$\varphi_t \stackrel{\text{def}}{=} x_1 *_1 (x_2 *_2 (x_3 *_3 (\ldots (x_{n-1} *_{n-1} x_n)))),$$

where $*_i = \wedge$ if $a_i = 1$ and $*_i = \vee$ if $a_i = 0$. Notice that indeed, any assignment satisfying φ_t, when viewed as a binary number, must have value greater than $2 \cdot t$. Notice that all assignments in $\{0,1\}^n$ that satisfy φ_t, satisfy φ_{t+1} as well, *except* for the two assignments that are the binary representation of the numbers $2t+1$ and $2t+2$. Thus, since φ_t "almost" implies φ_{t+1}, we have room for hope that we can derive the latter from the former in small space. We now show that this is indeed the case.

In order to show how to infer φ_{t+1} from φ_t and the initial axioms we need to define one more intermediate formula ψ_t. Let $0 \leq m < n$ be the largest index such that $a_m = 0$ (thus, $t = a_1 a_2 \ldots a_{m-1} 011 \ldots 1$), and let

$$\psi_t \stackrel{\text{def}}{=} x_1 *_1 (x_2 *_2 (x_3 *_3 (\ldots (x_{m-1} *_{m-1} x_m)))).$$

In other words, ψ_t is obtained from φ_t by cutting off the maximal suffix consisting entirely of $\wedge$s and encodes that "the satisfying assignment for CT_n must be greater than $2t+1$".

Define two clauses, corresponding to the binary representations of the numbers $2t+1, 2t+2$, respectively.

$$A_t = x_1^{a_1} \vee x_2^{a_2} \vee \ldots \vee x_{m-1}^{a_{m-1}} \vee x_m \vee \bar{x}_{m+1} \vee \ldots \vee \bar{x}_n$$

and

$$B_t = x_1^{a_1} \vee x_2^{a_2} \vee \ldots \vee x_{m-1}^{a_{m-1}} \vee \bar{x}_m \vee x_{m+1} \vee \ldots \vee x_n.$$

It is obvious from the semantics of φ_t, ψ_t described above that $\{\varphi_t, A_t\} \models \psi_t$ and $\{\psi_t, B_t\} \models \varphi_{t+1}$. The question is how to produce compact syntactic inferences.

As we noticed before, we can assume w.l.o.g. that $\mathcal{F}$ contains any prescribed finite set of inference rules, and in particular we can assume that $\mathcal{F}$ contains modus ponens. Therefore, it is sufficient to produce inferences of the tautological formulas $(\varphi_t \wedge A_t) \to \psi_t$ and $(\psi_t \wedge B_t) \to \varphi_{t+1}$ that use $O(n)$ variable space. We will consider only the first formula; the second proof is analogous.

For $1 \leq \ell \leq n$, let $\varphi_t^{(\ell)}, A_t^{(\ell)}, \psi_t^{(\ell)}$ be the suffixes of φ_t, A_t, ψ_t respectively that are obtained by crossing out the variables $x_1, \ldots, x_{\ell-1}$ (and we let $\psi_t^{(\ell)} \stackrel{\text{def}}{=} \bot$ if $\ell > m$). We are going to infer (in linear variable space) all the formulas $(\varphi_t^{(\ell)} \wedge A_t^{(\ell)}) \to \psi_t^{(\ell)}$ by induction on $\ell = n, n-1, \ldots, 1$.

In the base case $\ell = n$ we have $\varphi_t^{(n)} = x_n$, $A_t^{(n)} = \bar{x}_n$, and we get a substitutional instance of the axiom $(A \wedge \bar{A} \to B)$.

In order to infer $(\varphi_t^{(\ell)} \wedge A_t^{(\ell)}) \to \psi_t^{(\ell)}$ from $(\varphi_t^{(\ell+1)} \wedge A_t^{(\ell+1)}) \to \psi_t^{(\ell+1)}$, we use the rule

$$\frac{A \wedge B \to C}{(D \vee A) \wedge (D \vee B) \to (D \vee C)}$$

if $a_\ell = 0$, and the rule

$$\frac{A \wedge B \to C}{(D \wedge A) \wedge (\bar{D} \vee B) \to (D \wedge C)}$$

if $a_\ell = 1$.

We showed how to make the transition from φ_t to φ_{t+1}. At the end we get $\varphi_{2^{(n-1)}-1} = x_1 \wedge x_2 \wedge \ldots \wedge x_n$, which together with $\bar{x}_1 \vee \bar{x}_2 \vee \ldots \vee \bar{x}_n$ implies contradiction. Theorem 6.3 is proved. □

Corollary 6.4 *Any tautological formula φ can be inferred from the empty set of axioms $\mathcal{T} = \emptyset$ in variable space $O(VSpace_F(\varphi))$.*

Proof: W.l.o.g. assume that $\{x_1, \ldots, x_n\}$ is the complete list of variables appearing in φ. By induction on the logical complexity of a formula ψ (not necessarily tautological) we produce, for any $\epsilon \in \{0,1\}^n$, an inference of $x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_n^{\epsilon_n} \vee \psi^{\psi(\bar{\epsilon}_1, \ldots, \bar{\epsilon}_n)}(x_1, \ldots, x_n)$ (where, naturally, $\psi^1 \stackrel{\text{def}}{=} \psi$ and $\psi^0 \stackrel{\text{def}}{=} \bar{\psi}$) that has variable space $O(VSpace_F(\psi))$. Since φ is a tautology, this in particular gives, for any $\epsilon \in \{0,1\}^n$, an inference of $x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_n^{\epsilon_n} \vee \varphi(x_1, \ldots, x_n)$ with variable space $O(VSpace_F(\varphi))$. Now we only have to modify the proof of CT_n from Theorem 6.3 by replacing every formula ψ in it with $(\psi \vee \varphi)$, and modifying inference rules accordingly. □

Corollary 6.5 *For any tautology $\mathcal{T}$ over n variables*

$$VSpace_F(\mathcal{T}) = O(n + \max_{\varphi \in \mathcal{T}} VSpace_F(\varphi)).$$

Proof: similar to the proof of Corollary 6.4. Namely, for every $\epsilon \in \{0,1\}^n$ we can find $\varphi_\epsilon \in \mathcal{T}$ such that $\varphi_\epsilon \to (x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_n^{\epsilon_n})$ is a tautology. When we need the axiom $x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_n^{\epsilon_n}$ from CT_n, we download this φ_ϵ, infer $\varphi_\epsilon \to (x_1^{\epsilon_1} \vee x_2^{\epsilon_2} \vee \ldots \vee x_n^{\epsilon_n})$ and apply modus ponens. □

Let $VSpace_F^{sem}(\mathcal{T})$ denote the *semantical* Frege variable space of refuting $\mathcal{T}$.

Corollary 6.6 *Semantic and syntactic versions of Frege systems are equivalent in the variable space model:*

$$VSpace_F^{sem}(\mathcal{T}) \leq VSpace_F(\mathcal{T}) \leq O(VSpace_F^{sem}(\mathcal{T})).$$

Proof: As in the proof of Theorem 3.7, we show how to emulate the semantic inference π by a syntactic one. The only difference between semantical and syntactical versions is in the inference step. Assume that $\{\varphi_1, \varphi_2, \ldots, \varphi_k\} \vdash \psi$. Then we can produce the syntactic proof of the tautology $\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_k \rightarrow \psi$ according to Corollary 6.4 and repeatedly apply modus ponens. □

At the end we briefly discuss how to generalize these results to the case of Frege systems $\mathcal{F}$ in arbitrary complete language L. The problem with the general translation is that the sizes of the resulting formulas may grow very rapidly. However, at least it is not a problem with the logical constant **0**: it can be trivially replaced with $x \wedge \bar{x}$.

Quite fortunately, the specific language that consists of the remaining connectives $\{\neg, \wedge, \vee, \rightarrow\}$ is known to be the weakest in the sense that it can be modeled in any other complete language with only *linear* blow-up in the variable space. More exactly, the following holds:

Lemma 6.7 (Reckhow [Rec76]) *If $\mathcal{F}$ is a Frege system over any complete language L then there are L-formulas $NOT(x,z)$, $AND(x,y,z)$, $OR(x,y,z)$, and $IMP(x,y,z)$ such that*

(1) *$NOT(x,z)$ contains one occurrence of x, and $AND(x,y,z)$, $OR(x,y,z)$, and $IMP(x,y,z)$ contain exactly one occurrence of each of x and y.*

(2) *The four formulas represent the Boolean functions $\neg x$, $(x \wedge y)$, $(x \vee y)$ and $(x \rightarrow y)$; in particular, the truth values of the formulas are independent of the truth value of z.*

Thus we can rewrite the proof of Theorem 6.3 and its corollaries almost literally replacing our standard connectives with $NOT(x,z)$, $AND(x,y,z)$, $OR(x,y,z)$, and $IMP(x,y,z)$.

7 Open questions

We conclude this paper with a short list of interesting open questions:

1. Is there any way to capture the notion of propositional space complexity in the uniform framework of first-order theories of Bounded Arithmetic?

2. Find an unsatisfiable CNF $\mathcal{T}$ in n variables such that $VSpace_R(\mathcal{T}) \geq \omega(n)$ and $\mathcal{T}$ has only polynomially many clauses (CT_n has exponentially many clauses, and the bound in Corollary 5.7 is only linear in the overall number of variables mn). We conjecture that $VSpace_R(T(G,\sigma)) \geq \Omega(n^2)$ if G is a 3-regular expander graph, and even that

   $$VSpace_{PCR}(T(G,\sigma)) \geq \Omega(n^2)$$

   when $char(F) \neq 2$.

3. Are there any other interesting fragments of Frege systems, not contained in PCR, for which the notion of variable space makes sense? (perhaps Cutting Planes, depth 2 Frege, etc.) Can one prove non-trivial lower bounds for these systems?

4. Can we prove the analogue of Theorem 3.7 for variable space? What can be said about the relation between the syntactical and semantical versions of other proof systems, w.r.t. either clause or variable space?

5. Is it possible to prove super-constant clause space lower bounds for PCR-proofs of any bounded fan-in tautology or of $Count_p$? Once more, we conjecture that Corollary 3.27 can be extended to PCR over any field with $char(F) \neq 2$.

6. [ET99] Is it possible to find some strong connection between the clause complexity of a tautology and its minimal proof width for resolution?

8 Acknowledgement

We are grateful to Jan Krajíček for several useful remarks.

References

[AL86] R. Aharoni, N. Linial. Minimal Non-Two-Colorable Hypergraphs and Minimal Unsatisfiable Formulas. In *J. of Combinatorial Theory*, Series A, Vol. 43, No. 2, (1986) pp 196-204.

[BP98] P. Beame and T. Pitassi. Propositional proof complexity: Past, present and future. Bulletin of the EATCS. See also: Technical Report TR98-067, Electronic Colloquium on Computational Complexity, 1998.

[BG99] M.L. Bonet, N. Galesi. A Study of Proof Search Algorithms for Resolution and Polynomial Calculus. Manuscript, 1999.

[CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the* 28*th ACM STOC*, pages 174–183, 1996.

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

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

[HPV77] J. Hopcroft, W. Paul, L. Valiant. On Time vs. Space. In *J. of ACM*, Vol. 24 (1977), pp. 332-337.

[IPS97] R. Impagliazzo, P. Pudlák, and J. Sgall. Lower bounds for the polynomial calculus and the Groebner basis algorithm. In *Computational Complexity*, Vol. 8 (1999), pp. 127-144.

[Juk97] S. Jukna. Exponential lower bounds for semantic resolution. In P. Beame and S. Buss, editors, *Proof Complexity and Feasible Arithmetics: DIMACS workshop, April* 21-24, 1996*, DIMACS Series in Dicrete Mathematics and Theoretical Computer Science, vol.* 39, pages 163–172. American Math. Soc., 1997.

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

[Kra95] J. Krajíček. *Bounded arithmetic, propositional logic and complexity theory.* Cambridge University Press, 1995.

[Kra97a] J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic*, Vol. 62, No 2 (1997), pp. 457–486.

[Kra97b] J. Krajíček. Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over polynomial calculus. In P. Ružička I.Prívara, editor, *Proceedings of the* 22*nd International Symposium on the Mathematical Foundations of Computer Science* (*Bratislava, August* '97)*, Lecture Notes in Computer Science* 1295, pages 85–90. Springer-Verlag, 1997.

[Kri85] B. Krishnamurthy. Short Proofs for Tricky Formulas. In *Acta Informatica*, Vol. 22 (1985), pp. 253-275.

[RWY97] A. Razborov, A. Wigderson, and A. Yao. Read-once branching programs, rectangular proofs of the pigeonhole principle and the transversal calculus. In *Proceedings of the* 29*th ACM Symposium on Theory of Computing*, pages 739–748, 1997.

[Rec76] R. A. Reckhow. On the Lengths of Proofs in the Propositional Calculus. *PhD thesis*, Department of Computer Science, University of Toronto, 1976. Technical Report #87.

[Sta96] G.Stalmark. Short Resolution Proofs for a Sequence of Tricky Formulas. In *Acta Informatica*, Vol. 33 (1996), pp. 277-280.

[Tar] M. Tarsi. Personal Communication

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

[Tse68] G.S. Tseitin. On the Complexity of Derivation in Propositional Calculus. In *Studies in Constructive Mathematics and Mathematical Logic*, Part 2. Consultants Bureau, New-York-London, 1968, pp. 115-125.

[Urq95] A. Urquhart. The Complexity of Propositional Proofs. In *The Bulletin of Symbolic Logic*, Vol. 1, No. 4 (1995), pp. 425-467.

Appendix

The purely semantical system called the *functional calculus* (FC), works with *arbitrary* Boolean functions, regardless of their syntactical representation complexity. In fact our space complexity for FC defined below will simply minimize over all such representations. Although this system is not natural, the clause space lower bound for the polynomial calculus applies to it as well, and it is a useful tool for proving lower bounds when an abstraction from particulars of a given syntactical system is desirable and instructive.

The line of an FC derivation is an arbitrary Boolean function. The single inference rule is the semantical one, i.e. derive g from $f_1, f_2, \ldots, f_k$ whenever $f_1, f_2, \ldots, f_k \models g$. The definitions of derivations and refutations are analogous to those of resolution and PC.

When defining the clause space for FC, we must overcome the following problem. A line in FC is an *arbitrary* Boolean function f. Clearly, f can be represented by many circuits over some complete Boolean basis, each with a different amount of clauses. The natural way to solve this problem is to define the clause space to be the minimal number of clauses in any such representation.

Definition 8.1 (Clause Space for FC) *For $\mathcal{M}$ a set of Boolean functions over $x_1, \ldots, x_n$, the* clause space *of $\mathcal{M}$ in FC, denoted $FCSpace(\mathcal{M})$, is the minimal s such that we can choose s clauses with the property that every $f \in \mathcal{M}$ can be represented as a Boolean function over the chosen clauses. Formally:*

$$\begin{aligned} FCSpace(\mathcal{M}) \stackrel{\text{def}}{=} \min \{ s \mid \exists (C_1(x_1, \ldots, x_n), C_2(x_1, \ldots, x_n), \ldots, \\ C_s(x_1, \ldots, x_n)) \forall (f(x_1, \ldots, x_n) \in \mathcal{M}) \exists g(y_1, \ldots, y_s) \\ (f \equiv g(C_1, \ldots, C_s)) \} , \end{aligned}$$

where C_i are clauses, and g runs over arbitrary Boolean functions in s variables.

We can also define multi-valued FC over the domain D in a natural way.

Definition 8.2 (Multi-valued functional calculus) Functional Calculus over the domain D *(FC(D)) is the purely semantical system which keeps in memory arbitrary functions $f(x_1, \ldots, x_n) : D^n \to \{0, 1\}$. The inference rule is the semantical one.*

The clause space measure $FCSpace_D(\mathcal{M})$ of a set of such functions $\mathcal{M}$ is the minimal s such that we can choose s multi-valued clauses with the property that every $f \in \mathcal{M}$ can be represented as an (ordinary!) Boolean function over the chosen multi-valued clauses.

We now prove our main theorems for FC. The first is a better upper bound on clause space of CT_n, which is proved using the method of Theorem 4.2.

Theorem 8.3 $FCSpace(CT_n) \leq n/2 + 2$.

Proof: By Claim 4.4 (that applies to FC just as well), we need only analyze the base case and show that $FCSpace(CT_2) \leq 2$ ($s = k = 1$):

$$\left(\begin{array}{c}\text{Axiom: } x_1 \vee x_2\\ \text{Axiom: } x_1 \vee \bar{x}_2\end{array}\right) \rightsquigarrow \left(\ x_1\ \right) \rightsquigarrow \left(\begin{array}{c} x_1\\ \text{Axiom: } \bar{x}_1 \vee x_2\end{array}\right)$$
$$\rightsquigarrow \left(\ \neg(\bar{x}_1 \vee \bar{x}_2)\ \right) \rightsquigarrow \left(\begin{array}{c}\neg(\bar{x}_1 \vee \bar{x}_2)\\ \text{Axiom: } \bar{x}_1 \vee \bar{x}_2\end{array}\right) \rightsquigarrow \left(\ \bot\ \right).$$

□

Although FC is much stronger than PCR, it turns out Theorem 4.18 applies equally well to the functional calculus.

Theorem 8.4 *For any wide tautology $\mathcal{T}$ over n variables with domain D, $FCSpace(\mathcal{T}) \geq \frac{n}{4}$.*

Proof: Identical to the proof of Theorem 4.18 (notice that in the proof of Lemma 4.14 we used the fact $s = MSpace_D^{sem}(\mathcal{M}_1)$ *only* to write down the representation $||\mathcal{M}_1|| = g(C_1, \ldots, C_s)$ for an *unspecified* Boolean function g, and this transition works perfectly well in the context of the functional calculus). □