Electronic Colloquium on Computational Complexity, Report No. 35 (2002)

A Combinatorial Characterization of Resolution Width

Albert Atserias *
Universitat Politècnica de Catalunya
Barcelona, Spain

Víctor Dalmau †
Universitat Pompeu Fabra
Barcelona, Spain

May 27, 2002

Abstract

We provide a characterization of the resolution width introduced in the context of Propositional Proof Complexity in terms of the existential pebble game introduced in the context of Finite Model Theory. The characterization is tight and purely combinatorial. Our first application of this result is a surprising proof that the minimum space of refuting a 3-CNF formula is always bounded from below by the minimum width of refuting it (minus 3). This solves a well-known open problem. The second application is the unification of several width lower bound arguments, and a new width lower bound for the Dense Linear Order Principle. Since we also show that this principle has Resolution refutations of polynomial size, this provides yet another example showing that the size-width relationship is tight.

* Partially supported by CICYT TIC2001-1577-C03-02, ALCOM-FT IST-99-14186
† Supported by MCyT Program "Ramón y Cajal"

ISSN 1433-8092

1 Introduction

Resolution is one of the most popular proof systems for propositonal logic. Since Haken [15] proved an exponential lower bound for the smallest resolution proofs of the Pigeonhole Principle, its strength has been studied in depth. The focus has been put in two related directions: (1) proving strong lower bounds for interesting tautologies arising from combinatorial principles [21, 10, 6, 8, 3, 18, 19], and (2) the study of the complexity of finding resolution proofs [6, 8, 2, 5]. This research is still ongoing, and we believe that the question of whether Resolution is automatizable or weakly automatizable in reasonable time is one of the most interesting open problems in propositional proof complexity.

A definitive step towards the understanding of the strength of Resolution in a unified way was made by Ben-Sasson and Wigderson [8] with the introduction of the width measure. The width of a resolution refutation is the size of the largest clause in the refutation. The main result of Ben-Sasson and Wigderson, building upon the work of Clegg, Edmonds and Impagliazzo [11] and Beame and Pitassi [6], is the following: If a 3-CNF formula F has a resolution refutation of size S, then F has a resolution refutation of width $O\left(\sqrt{n \log(S)}\right)$. This interesting result relates the size with the width in a form that is suitable to prove size lower bounds. Indeed, if the minimal width of refuting F is w, then every resolution refutation of F requires size $2^{\Omega(w^2/n)}$. Equipped with this result, Ben-Sasson and Wigderson not only re-derived all previously known lower bounds for resolution in an elegant and unified way, but even they managed to show that resolution is automatizable in subexponential time by an extremely simple dynamic programming algorithm. Should we notice however, that the size-width relationship of Ben-Sasson and Wigderson has shown insufficient to prove size lower bounds for some interesting cases such as the Weak Pigeonhole Principle. In fact, Bonet and Galesi [9] proved that the size-width trade-off is tight and therefore the technique cannot be applied to it. The problem about the Weak Pigeonhole Principle was finally solved by Raz [18] using a completely different technique.

Our goal in this paper is to establish a tight connection between the resolution width of Ben-Sasson and Wigderson, and a certain combinatorial game, called existential k-pebble game, first introduced by Kolaitis and Vardi in the context of Finite Model Theory. Research in this direction was initiated by Atserias in [4], in the study of the proof complexity of random formulas.

It is well known that the expressive power of several major logical formalisms, including first-order logic and second-order logic, can be analized using certain combinatorial two-player games (see [12]). Existential k-pebble games were introduced by Kolaitis and Vardi [16, 17] and used to analyze the expressive power of Datalog, a well-known query language in Database Theory. These games are played between two players, the Spoiler and the Duplicator, on two relational structures $\mathbf{A}$ and $\mathbf{B}$ according to the following rules. Each player has a set of k pebbles numbered $\{1, \ldots, k\}$. In each round of the game, the Spoiler can make one of two different moves: either he places a free pebble over an element of the domain of $\mathbf{A}$, or he removes a pebble from a pebbled element of $\mathbf{A}$. To each move of the Spoiler, the Duplicator must respond by placing her corresponding pebble over an element of $\mathbf{B}$, or removing her corresponding pebble from $\mathbf{B}$ respectively. If the Spoiler reaches a round in which the set of pairs of pebbled elements is not a partial homomorphism between $\mathbf{A}$ and $\mathbf{B}$, then he wins the game. Otherwise, we say that the Duplicator wins the game.

The crucial point that relates pebble games to resolution width is the fact, first pointed out by Feder and Vardi [14], that the satisfiability problem of a r-CNF F can be identified with the homomorphism problem on relational structures: given two finite relational structures $\mathbf{A}$ and $\mathbf{B}$ over the same vocabulary, is there a homomorphism from $\mathbf{A}$ to $\mathbf{B}$? Informally, the structure $\mathbf{A}$ represents the variables and the clausules of F, the structure $\mathbf{B}$ represents the truth-values $\{0,1\}$ and the combination of them that are valid assignments for the clauses, and the homomorphisms from $\mathbf{A}$ to $\mathbf{B}$ are precisely the assignments of variables to truth-values satisfying all the clauses of F. Using this reformulation, we show that the concepts of Resolution width and pebble games are intimately related. More specifically, we prove that F does not have a Resolution refutation of width k if and only if the Duplicator wins the existential $(k+1)$-pebble game on $\mathbf{A}$ and $\mathbf{B}$.

Thus, existential k-pebble games provide a purely combinatorial characterization of Resolution width that allows us to re-derive, in a uniform way, essentially all known width lower bounds. Generally, an increase of insight reverts also in the acquisition of new results. It is not surprising then, that this new characterization can also be used to obtain new width lower bounds. In particular we show that every Resolution refutation of the Dense Linear Order Principle (DLO_n), stating that no finite linear order is dense, has width at least $n/3$, where n is the number of elements of the linear order. It is worth to remark that most of the tautologies studied in the literature, including DLO_n, have large initial width. Consequently, in order to get meaningful width lower bounds it is necessary to convert them into equivalent and short (generally 3-CNF) formulas in a preliminary step. Unfortunately, it is usually the case that the resulting formula looses some of the intuitive appeal of the principle it expresses. Furthermore, in a width lower bound proof, dealing with the auxiliary variables is usually simple but cumbersome and laborious. To simplify this situation we define a variant of the pebble game, called extended pebble game, that can be played directly over formulas with large clauses and that hiddes all the technical details, such as the process of dividing large clauses, the introduction of auxiliary variables and its treatment, inside the proof. In particular, the width lower bound for the DLO_n is obtained this way. We complete the picture about DLO_n by showing that it has polynomial-size Resolution proofs. Thus, the DLO_n principle provides a new example requiring large width but having small Resolution proofs (see [9, 2, 5] for further discussion on this).

Our second application of the combinatorial characterization is a suprising result relating the space and the width in Resolution. The space measure was introduced by Esteban and Torán [13] (see also [1]). Intuitively, the minimal Resolution space of refuting a CNF formula F is the number of clauses that are required to be kept in a blackboard (memory) if we insist that the refutation must be self-contained. In [1], this measure is referred to as the *clause space*. Strong space lower bounds were proved in the literature for well-known tautologies such as the Pigeonhole Principle [20, 1], Tseitin Tautologies [20, 1], Graph Tautologies [1], and Random Formulas [7] to cite some. Our surprising result is that the minimum space of refuting an r-CNF formula is always bigger than the minimum width of refuting F minus r. In symbols, $s(F) \geq w(F) - r$. Thus, for r-CNF formulas with small r, space lower bounds follow at once from width lower bounds. Our result answers the conjecture in [7] in the positive.

2 Preliminaries

Let V be a set of propositional variables. A literal is a variable or the negation of a variable. A clause is a set of literals. If a clause has exactly r literals, we call it a r-clause. An r-CNF formula is a set of r-clauses. Alternatively, clauses may be viewed as disjunctions of literals, and CNF formulas may be viewed as conjunctions of clauses. A partial truth assignment to V is any function $f : V' \to \{0,1\}$ where $V' \subseteq V$. We say that f falsifies a clause C if it sets all literals from C to 0. Dually, we say that f satisfies C if it sets some literal from C to 1. In all other cases we say that f leaves C undecided. Resolution is a refutation system that works with clauses. The only rule is the so-called resolution rule:

$$\frac{C \cup \{x\} \quad D \cup \{\neg x\}}{C \cup D}$$

where C and D are arbitrary clauses and x is a variable. The goal is to derive the empty clause $\{\}$ from a set of initial clauses F.

Let $L = \{R_1, \ldots, R_m\}$ be a finite relational language, that is, a finite set of relation symbols with an associated arity. An L-structure is a tuple $\mathbf{A} = (A, R_1^{\mathbf{A}}, \ldots, R_m^{\mathbf{A}})$ where A is a set called the universe and $R_i^{\mathbf{A}} \subseteq A^{k_i}$ is a k_i-ary relation on A, where k_i is the arity of R_i. Let $\mathbf{A} = (A, R_1^{\mathbf{A}}, \ldots, R_m^{\mathbf{A}})$ and $\mathbf{B} = (B, R_1^{\mathbf{B}}, \ldots, R_m^{\mathbf{B}})$ be L-structures. A partial homomorphism from $\mathbf{A}$ to $\mathbf{B}$ is any function $f : A' \to B$, where $A' \subseteq A$, such that f defines an homomorphism from the substructure of $\mathbf{A}$ with domain A' to the structure $\mathbf{B}$. In other words, f is a function such that for every relation symbol $R \in L$ of arity s and $a_1, \ldots, a_s \in A'$, if $(a_1, \ldots, a_s) \in R^{\mathbf{A}}$ then $(f(a_1), \ldots, f(a_s)) \in R^{\mathbf{B}}$. If f and g are partial homomorphisms, we say that g extends f, denoted by $f \subseteq g$, if $\mathrm{Dom}(f) \subseteq \mathrm{Dom}(g)$ and $f(a) = g(a)$ for every $a \in \mathrm{Dom}(f)$. If $f \subseteq g$, we also say that f is the projection of g to $\mathrm{Dom}(f)$.

The existential k-pebble game on $\mathbf{A}$ and $\mathbf{B}$ is played by two players: the Spoiler and the Duplicator. Each player has a set of k pebbles numbered $\{1, \ldots, k\}$. In each round of the game, the Spoiler can make one of two different moves: either he places a free pebble over an element of the domain of $\mathbf{A}$, or he removes a pebble from a pebbled element of $\mathbf{A}$. To each move of the Spoiler, the Duplicator must respond by placing her corresponding pebble over an element of $\mathbf{B}$, or removing her corresponding pebble from $\mathbf{B}$ respectively. If the Spoiler reaches a round in which the set of pairs of pebbled elements is not a partial homomorphism between $\mathbf{A}$ and $\mathbf{B}$, then he wins the game (note that if two different pebbles are placed on the same element of $\mathbf{A}$ but the two corresponding pebbles are placed over different elements of $\mathbf{B}$, then the set of pairs does not define a partial homomorphism). Otherwise, we say that the Duplicator wins the game. The next definition formalizes this intuitive discussion:

Definition 1 *We say that the Duplicator wins the k-pebble game on $\mathbf{A}$ and $\mathbf{B}$ if there is a nonempty family $\mathcal{H}$ of partial homomorphisms from $\mathbf{A}$ to $\mathbf{B}$ such that*

(i) If $f \in \mathcal{H}$, then $|\mathrm{Dom}(f)| \leq k$.

(ii) If $f \in \mathcal{H}$ and $g \subseteq f$, then $g \in \mathcal{H}$.

(iii) If $f \in \mathcal{H}$, $|\mathrm{Dom}(f)| < k$, and $a \in A$, then there is some $g \in \mathcal{H}$ such that $f \subseteq g$ and $a \in \mathrm{Dom}(g)$.

We say that $\mathcal{H}$ is a winning strategy for the Duplicator.

Intuitively, each partial homomorphism $g \in \mathcal{H}$ is a winning position for the Duplicator in the game. For the interested reader, we mention that the existential k-pebble game is know to characterize definability in the k-variable fragment of the infinitary logic $\exists\mathcal{L}_{\infty\omega}$ that is obtained by closing the set of atomic formulas under arbitrary conjunctions and disjunctions and existential quantification (see [16, 17] for more information).

3 Combinatorial characterization as games

It is well know that r-CNF formulas may be encoded as finite relational structures. Indeed, let $L = \{P_0, P_1, \ldots, P_r\}$ be the finite relational language that consists of $r+1$ relations of arity r each. An r-CNF formula F over the propositional variables $v_1, \ldots, v_n$ is encoded as an L-structure $\mathbf{M}(F)$ as follows. The domain of $\mathbf{M}(F)$ is the set of variables $\{v_1, \ldots, v_n\}$. For each $s \in \{0, \ldots, r\}$, the relation P_s encodes the set of clauses of F with exactly s negated variables. More precisely, the interpretation of P_s consists of all r-tuples of the form

$$(v_{i_1}, \ldots, v_{i_s}, v_{i_{s+1}}, \ldots, v_{i_r}) \in \{v_1, \ldots, v_n\}^r$$

such that $\{\neg v_{i_1}, \ldots, \neg v_{i_s}, v_{i_{s+1}}, \ldots, v_{i_r}\}$ is a clause of F. Next we define a particular r-CNF formula T_r whose encoding $\mathbf{M}(T_r)$ is of our interest. The clauses of T_r are all the r-clauses on the variables v_0 and v_1 that are satisfied by the truth assignment that maps v_0 to 0, and v_1 to 1.

We will consider the particular case of the existential k-pebble game that is played on the structures $\mathbf{M}(F)$ and $\mathbf{M}(T_r)$. Observe that each partial homomorphism from $\mathbf{M}(F)$ to $\mathbf{M}(T_r)$ may be viewed as a partial truth assignment to the variables of F that does not falsify any clause from F. Thus, the existential k-pebble game on $\mathbf{M}(F)$ and $\mathbf{M}(T_r)$ may be reformulated as follows.

Definition 2 *Let F be an r-CNF formula. We say that the Duplicator wins the Boolean existential k-pebble game on F if there is a nonempty family $\mathcal{H}$ of partial truth assignments that do not falsify any clause from F such that*

(i) If $f \in \mathcal{H}$, then $|\mathrm{Dom}(f)| \leq k$.

(ii) If $f \in \mathcal{H}$ and $g \subseteq f$, then $g \in \mathcal{H}$.

(iii) If $f \in \mathcal{H}$, $|\mathrm{Dom}(f)| < k$, and x is a variable, then there is some $g \in \mathcal{H}$ such that $f \subseteq g$ and $x \in \mathrm{Dom}(g)$.

We say that $\mathcal{H}$ is a winning strategy for the Duplicator.

We stress on the fact that this definition is only a particular case of the definition of winning strategy for the existential k-pebble game defined in Section 2.

Lemma 1 *If there is no resolution refutation of F of width k, then the Duplicator wins the existential $(k+1)$-pebble game on F.*

Proof: Let $\mathcal{C} = \{C_1, \ldots, C_m\}$ be all clauses generated by resolution of width at most k from F. Let $\mathcal{H}$ be the set of all partial truth assignments with domain of size at most $k+1$ that do not falsify any clause in $\mathcal{C}$. We will see that $\mathcal{H}$ is a winning strategy. Clearly $\mathcal{H}$ is not empty since it contains the partial truth assignment with empty domain (note that $C_1, \ldots, C_m$ does not contain the empty clause). Clearly, $\mathcal{H}$ is closed under projections. Now, let f be any partial truth assignment in $\mathcal{H}$

with $|\mathrm{Dom}(f)| \leq k$, and let x be any variable not in $\mathrm{Dom}(f)$. Let us assume that there does not exist a valid extension of f to x in $\mathcal{H}$. In this case let $C \in \mathcal{C}$ be the clause falsified by the extension of f that maps x to 0. Clearly $C = C' \cup \{x\}$ since otherwise f would falsify C. Analogously there exits some $D \in \mathcal{C}$ of the form $D' \cup \{\neg x\}$ that is falsified by the extension of f that maps x to 1. Thus, f falsifies $C' \cup D'$. However, $C' \cup D'$ has width at most k since all its variables are in $\mathrm{Dom}(f)$. □

Lemma 2 *If the Duplicator wins the existential $(k+1)$-pebble game on F, then there is no resolution refutation of F of width k.*

Proof: Let $\mathcal{H}$ be a winning strategy for the Duplicator for the existential $(k+1)$-pebble game on F. We will show by induction in the resolution proof of width k that no partial truth assignment in $\mathcal{H}$ falsifies a clause of the proof. Thus, the proof cannot be a refutation. The statement is clearly satisfied by the initial clauses since we are dealing with partial truth assignments that do not falsify any clause of F. Let $C \cup \{x\}$ and $D \cup \{\neg x\}$ be clauses of the proof, and let $C \cup D$ be the result of applying the resolution rule. Let f be any partial truth assignment in $\mathcal{H}$. If the domain of f does not include all the variables in $C \cup D$ then we are done since it cannot falsify it. Otherwise consider the projection g of f to the variables in $C \cup D$. We will show that g (and hence f) does not falsify $C \cup D$. Since the width of $C \cup D$ is at most k, the domain of g has size at most k. Therefore, there exists some extension h of g to x such that h is in $\mathcal{H}$. By induction hypothesis h does not falsify any of $C \cup \{x\}$ and $D \cup \{\neg x\}$. Consequently, since h falsifies x or $\neg x$, h cannot falsify $C \cup D$ either. □

Combining these two lemmas we obtain the main result of this section. We say that the Spoiler wins the existential k-pebble game on F if the Duplicator does not win the existential $(k+1)$-pebble game on F.

Theorem 1 *Let F be an r-CNF formula. Then, F has a Resolution refutation of width k if and only if the Spoiler wins the Boolean existential $(k+1)$-pebble game on F.*

We note that the existential k-pebble game does not talk about resolution at all. Thus, this provides a purely combinatorial characterization of resolution width.

4 Application: Width bounds space from below

In this section we show that the resolution space introduced by Esteban and Torán [13] and by Alekhnovich, Ben-Sasson, Razborov and Wigderson [1] is tighly related to the width. Indeed, for an r-CNF formula F, the minimal space $s(F)$ of refuting F, is always bounded from below by $w(F) - r$, where $w(F)$ is the minimal width of refuting F. This solves an open problem in [20, 1, 7].

We start with some definitions. Let F be an r-CNF formula. A configuration is a set of clauses. A sequence of configurations $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_r$ is a self-contained resolution proof if $\mathcal{C}_0 = \emptyset$ and for $i > 0$, the configutarion $\mathcal{C}_i$ is obtained from $\mathcal{C}_{i-1}$ by one of the following rules:

(i) Axiom Download: $\mathcal{C}_i = \mathcal{C}_{i-1} \cup \{C\}$ for some $C \in F$,

(ii) Erasure: $\mathcal{C}_i = \mathcal{C}_{i-1} - \{C\}$ for some $C \in \mathcal{C}_{i-1}$,

(iii) Inference: $\mathcal{C}_i = \mathcal{C}_{i-1} \cup \{C\}$ for some C that is obtained from an application of the resolution rule on two clauses from $\mathcal{C}_{i-1}$.

The space of a self-contained resolution proof $\mathcal{C}_0, \dots, \mathcal{C}_r$ is the maximum of $|\mathcal{C}_i|$ for $i = 0, \dots, r$. A self-contained resolution refutation is a self-contained resolution proof whose last configuration is $\{\Box\}$. The minimal space of refuting an unsatisfiable formula F, denoted by $s(F)$, is the minimal space of all self-contained resolution refutations of F. We will need the following easy lemma.

Lemma 3 (Locality Lemma [1]) *Let f be a partial truth assignment and let $\mathcal{C}$ be a set of clauses. If f satisfies $\mathcal{C}$, then there exists a restriction $g \subseteq f$ such that $|\mathrm{Dom}(g)| \leq |\mathcal{C}|$ and g still satisfies $\mathcal{C}$.*

Proof: For every $C \in \mathcal{C}$, let $l_C \in C$ be a literal that is satisfied by f. For every l_C, let x_C be the underlying variable. Finally, let g be the projection of f to $\{x_C : C \in \mathcal{C}\}$. $\Box$

Lemma 4 *Let F be an unsatisfiable r-CNF formula, and let $k \geq 1$. If the Duplicator wins the Boolean existential $(k + r - 1)$-pebble game on F, then the minimal space of refuting F is at least k.*

Proof: Let $\mathcal{H}$ be a winning strategy for the Duplicator in the existential $(k + r - 1)$-pebble game on F. We show that if $\mathcal{C}_0, \dots, \mathcal{C}_m$ is a self-contained resolution proof of space less than k, then every $\mathcal{C}_i$ is satisfiable. This will prove that F cannot have a resolution refutation of space less than k. We build, by induction on i, a sequence of partial truth assignments $f_i \in \mathcal{H}$ such that f_i satisfies $\mathcal{C}_i$ and $|\mathrm{Dom}(f_i)| \leq |\mathcal{C}_i|$. In the following, let $s_i = |\mathcal{C}_i|$. Let $f_0 = \emptyset$. In order to define f_i for $i > 0$, suppose that f_{i-1} has already been defined. We consider the three possible scenarios for $\mathcal{C}_i$. Case 1: $\mathcal{C}_i = \mathcal{C}_{i-1} \cup \{C\}$ by an axiom download for $C \in F$. Let $f \in \mathcal{H}$ be an extension of f_{i-1} such that all variables in C are in $\mathrm{Dom}(f)$. Since $|\mathrm{Dom}(f_{i-1})| \leq s_{i-1} < k$, $f_{i-1} \in \mathcal{H}$ and C is an r-clause, such an f exists in $\mathcal{H}$. Moreover, since f does not falsify any clause from F, and since all variables in C are defined, f satisfies C. Therefore, f satisfies $\mathcal{C}_i$. Now, by the Locality Lemma, there exists some restriction $g \subseteq f$ such that $|\mathrm{Dom}(g)| \leq s_i$ and still g satisfies $\mathcal{C}_i$ and belongs to $\mathcal{H}$. Let $f_i = g$. Case 2: $\mathcal{C}_i = \mathcal{C}_{i-1} \cup \{C\}$ by an inference. In this case set $f_i = f_{i-1}$. The soundness of the resolution rule guarantees that f_i satisfies $\mathcal{C}_i$. Of course, $|\mathrm{Dom}(f_i)| \leq s_{i-1} \leq s_i$ and $f_i \in \mathcal{H}$. Case 3: $\mathcal{C}_i = \mathcal{C}_{i-1} - \{C\}$ by a memory erasure. Obviously, f_{i-1} still satisfies $\mathcal{C}_i$ since it satisfies $\mathcal{C}_{i-1}$. Now, by the Locality Lemma, there is a restriction g of f_{i-1} such that $|\mathrm{Dom}(g)| \leq s_i$ and still g satisfies $\mathcal{C}_i$ and belongs to $\mathcal{H}$. Let $f_i = g$. $\Box$

Theorem 2 *Let F be an unsatisfiable r-CNF formula. Then, $s(F) \geq w(F) - r$ where $s(F)$ is the minimal space of refuting F in resolution, and w is the minimal width of refuting F in resolution.*

We note that this theorem can be used to derive space lower bounds for all formulas for which width lower bounds are known such as the Pigeonhole Principle, Tseitin Formulas, Random Formulas, and so on.

5 Application: Unified width lower bounds

The new characterization of the width can be used to obtain width lower bounds in a simpler and unified way. For CNF formulas whose clauses are already small, the width lower bound is obtained directly by exhibiting a winning strategy for the Duplicator. We illustrate this point with the encoding of the Pigeonhole Principle into an unsatisfiable 3-CNF formula by means of auxiliary variables (the so-called standard non-deterministic extension).

We will consider the 3-CNF formula $EPHP_n^{n+1}$ encoding the negation of the Pigeonhole Principle. For every $i \in \{1, \ldots, n+1\}$ and $j \in \{1, \ldots, n\}$, let $p_{i,j}$ be a propositional variable meaning that pigeon i sits in hole j. For every $i \in \{1, \ldots, n+1\}$ and $j \in \{0, \ldots, n\}$, let $y_{i,j}$ be a new propositional variable. The following 3-CNF formula EP_i expresses that pigeon i sits in some hole:

$$EP_i \equiv \neg y_{i,0} \wedge \bigwedge_{j=1}^{n} (y_{i,j-1} \vee p_{i,j} \vee \neg y_{i,j}) \wedge y_{i,n}.$$

Finally, the 3-CNF formula $EPHP_n^{n+1}$ expressing the negation of the Pigeonhole Principle is the conjunction of all EP_i and all clauses $H_k^{i,j} \equiv \neg p_{i,k} \vee \neg p_{j,k}$ for $i, j \in \{1, \ldots, n+1\}$, $i \neq j$ and $k \in \{1, \ldots, n\}$.

Lemma 5 *The Duplicator wins the Boolean existential n-pebble game on $EPHP_n^{n+1}$.*

Proof: Let $\mathcal{B}$ be the set of all one-to-one partial functions from $\{1, \ldots, n+1\}$ into $\{1, \ldots, n\}$. For every $a \in \mathcal{B}$, define a partial truth assignment h_a as follows:

(i) $h_a(p_{i,j}) = 1$ if $f(i)$ is defined and $f(i) = j$,

(ii) $h_a(p_{i,j}) = 0$ if $f(i)$ is defined and $f(i) \neq j$,

(iii) $h_a(y_{i,j}) = 0$ if $f(i)$ is defined and $f(i) > j$,

(iv) $h_a(y_{i,j}) = 1$ if $f(i)$ is defined and $f(i) \leq j$.

Let $\mathcal{F} = \{h_a : a \in \mathcal{B}\}$, and let $\mathcal{H}$ be the set of restrictions of assignments of $\mathcal{F}$ to all sets of at most n variables[1]. It is straightforward to check that $\mathcal{H}$ is a winning strategy for the Duplicator. □

We claim that all width lower bounds in the literature can be easily re-derived by exhibiting a winning strategy for the Duplicator. For example, [4] provided a winning strategy for the Duplicator for random formulas, and thus width lower bounds are also derived for them.

Our next twist is an attempt to systematize the use of the extension variables such as the $y_{i,j}$'s in $EPHP_n^{n+1}$. The point is that we would like to play games on CNF formulas with arbitrarily long clauses, and derive meaningful width lower bounds for their standard non-deterministic extensions. For an arbitrary CNF formula F without any restriction on the length of its clauses, let us define an equivalent r-CNF formula for $r \geq 3$. Such a formula is called the *standard non-deterministic extension of* F in [1]. For every clause C of length at most r, let $E_r(C) = C$. For every clause

[1]We note, by the way, that the set $\mathcal{F}$ is what is commonly known as the set of critical truth assignments for the pigeonhole principle.

$C = \{l_1, \ldots, l_w\}$ of length $w > r$, let $y_{C,0}, \ldots, y_{C,w}$ be a collection of new variables. Then we define $E_r(C)$ as follows:

$$E_r(C) \equiv \neg y_{C,0} \wedge \bigwedge_{j=1}^{w} (y_{C,j-1} \vee l_i \vee \neg y_{C,j}) \wedge y_{C,w}.$$

Then, $E_r(F)$ is the conjunction of all $E_r(C)$. Note that $E_r(F)$ is now an r-CNF formula and it is unsatisfiable if and only if F is.

The aim of the following definitions is to formalize a variation on the existential k-pebble game that is tailored for the non-deterministic extensions that we just introduced. Let F be a CNF formula without any restriction on the length of its clauses. Let V be the set of propositional variables of F. An extended partial truth assignment a is a pair (D, f) where $D \subseteq V \times (F \cup \{1\})$ and f is partial truth assignment. Moreover, if $D = \{(x_1, C_1), \ldots, (x_r, C_r)\}$, then $\mathrm{Dom}(f) = \{x_1, \ldots, x_r\}$ and clause C_i is satisfied by setting x_i to $f(x_i)$ (note that 1 is always satisfied). If $a = (D, f)$ and $b = (E, g)$ are extended partial truth assignments, we say that b is an extension of a, denoted by $a \subseteq b$, if $D \subseteq E$ and $f \subseteq g$. We also say that a is a projection of b. We say that an extended partial truth assignment (D, f) does not falsify a clause if f does not falsify it.

Definition 3 *We say that the Duplicator wins the extended (r, k)-game on F if there is a nonempty family $\mathcal{A}$ of extended partial truth assignments that do not falsify any clause of F such that*

- *(i) If $(D, f) \in \mathcal{A}$, then $|D| \leq k$.*
- *(ii) If $(D, f) \in \mathcal{A}$ and $E \subseteq D$, then there is some $g \subseteq f$ such that $(E, g) \in \mathcal{A}$.*
- *(iii) If $(D, f) \in \mathcal{A}$, $|D| < k$, and $x \in V$, then there is some g such that $f \subseteq g$ and $(D \cup \{(x, 1)\}, g) \in \mathcal{A}$.*
- *(iv) If $(D, f) \in \mathcal{A}$, $|D| < k$, and $C \in F$ has length at least $r + 1$, then there is some g and some $x \in V$ such that $f \subseteq g$ and $(D \cup \{(x, C)\}, g) \in \mathcal{A}$.*

The main result about this new game is the following lemma.

Lemma 6 *If the Duplicator wins the extended (r, k)-game on F, then the Duplicator wins the Boolean existential k-pebble game on $E_r(F)$.*

Proof: Let $\mathcal{A}$ be a winning strategy for the (r, k)-game on F. We first claim that we may assume without loss of generality that every extended partial truth assignment (D, f) in $\mathcal{A}$ is such that if $(x, C) \in D$ and $(y, C) \in D$ for some $C \neq 1$, then $x = y$. Indeed, let $\mathcal{A}'$ be the set of all extended partial truth assignments that are obtained from those in $\mathcal{A}$ in the following way: Given a partial truth assignment $a = (D, h)$, where

$$D = \{(x_{1,1}, C_1), \ldots, (x_{1,r_1}, C_1), \ldots, (x_{s,1}, C_s), \ldots, (x_{s,r_s}, C_s), (x_1, 1), \ldots, (x_q, 1)\}$$

with $C_1, \ldots, C_s \neq 1$, obtain an extended partial truth assignment $a' = (D', h)$ for each choice of $D' = \{(x_{1,i_1}, C_1), \ldots, (x_{s,i_s}, C_s), (x_1, 1), \ldots, (x_q, 1)\}$ and put all of them in $\mathcal{A}'$. It is not hard to see that $\mathcal{A}'$ is also a winning strategy for the (r, k)-game on F.

Now, let $a = (D, f)$ be an extended partial truth assignment. We define an ordinary partial truth assignment t_a as follows:

(i) The domain of t_a is the set of all $x \in V$ such that $(x, C) \in D$ for some $C \in F \cup \{1\}$, together with all variables $y_{C,j}$ such that $(x, C) \in D$ for some $x \in V$ and $C \in F$.

(ii) If $(x, C) \in D$ for some $C \in F \cup \{1\}$, then $t_a(x) = f(x)$.

(iii) If $(x, C) \in D$ for some $C \in F$, let l_i be the literal of $C = \{l_1, \ldots, l_w\}$ corresponding to variable x and set $t_a(y_{C,j}) = 0$ if $j < i$ and $t_a(y_{C,j}) = 1$ if $j \geq i$ (here is where we use the assumption about the uniqueness of x).

First notice that each t_a is a partial truth assignment to the variables of $E_r(F)$ that does not falsify any clause from $E_r(F)$. Moreover, if $a \subseteq b$, then $t_a \subseteq t_b$. Now, we construct our winning strategy $\mathcal{H}$ by including, for every $a \in \mathcal{A}$, every partial truth assignment f such that $f \subseteq t_a$ and $|\mathrm{Dom}(f)| \leq k$. Conditions (i) and (ii) in Definition 2 are obviously satisfied. Let us consider condition (iii). Let $f \in \mathcal{H}$ be such that $|\mathrm{Dom}(f)| \leq k - 1$. Then, there exists $a \in \mathcal{A}$ such that $f \subseteq t_a$. Since $|\mathrm{Dom}(f)| \leq k - 1$, there exists a projection $b \subseteq a$ such that $|\mathrm{Dom}(b)| \leq k - 1$ and $f \subseteq t_b$. Let $b = (D, g)$. Let x be an initial variable. By the extended forth property there is an h such that $g \subseteq h$ and $(D \cup \{(x, 1)\}, h) \in \mathcal{A}$. Thus $f \subseteq t_b \subseteq t_c$ where $c = (D \cup \{(x, 1)\}, h)$. Then, the projection of t_c to the variables in $\mathrm{Dom}(f) \cup \{x\}$ is an extension of f that belongs to $\mathcal{H}$ and has x in its domain. Now let $y_{C,j}$ be an extension variable of clause C with $|C| > r$. We have to consider two cases: (1) $(x, C) \in D$ for some x, and (2) otherwise. In case (1), the projection of t_b to the variables in $\mathrm{Dom}(f) \cup \{y_{C,j}\}$ is an extension of f that belongs to $\mathcal{H}$ and has $y_{C,j}$ in its domain. In case (2), there exists some variable x and h such that $g \subseteq h$ and $(D \cup \{(x, C)\}, h) \in \mathcal{H}$. This time $f \subseteq t_c$ where $c = (D \cup \{(x, C)\}, h)$, and the projection of t_c to the variables in $\mathrm{Dom}(f) \cup \{y_{C,j}\}$ is an extension of f that belongs to $\mathcal{H}$ and has $y_{C,j}$ in its domain. □

There is a strong reason to claim that the definition of the (r, k)-game is not arbitrary. Indeed, a sharp converse to Lemma 6 holds as one can easily see: if the Duplicator wins the Boolean existential $(k + 2)$-pebble game on $E_r(F)$, then the Duplicator wins the (r, k)-game on F. Thus, we loose essentially nothing in restricting ourselves to playing the modified game on $E_r(F)$. We illustrate its use for the set of clauses expressing the Dense Linear Order Principle which says that a finite linear order cannot be dense.

For every $i, j \in \{1, \ldots, n\}$, let $x_{i,j}$ be a propositional variable whose intended meaning is that i is smaller than j in the linear ordering. For every $i, j, k \in \{1, \ldots, n\}$, let $z_{i,j,k}$ be a propositional variable whose intended meaning is that i is smaller than j, and j is smaller than k in the linear ordering. The clauses of DLO_n are the following:

(1)	$\neg x_{i,j} \vee \neg x_{j,i}$	(5)	$\neg z_{i,j,k} \vee x_{i,j}$	
(2)	$x_{i,j} \vee x_{j,i}$	(6)	$\neg z_{i,j,k} \vee x_{j,k}$	
(3)	$\neg x_{i,j} \vee \neg x_{j,k} \vee x_{i,k}$	(7)	$\neg x_{i,k} \vee z_{i,1,k} \vee \cdots \vee z_{i,n,k}$	$(D_{i,k})$
(4)	$\neg x_{i,j} \vee \neg x_{j,k} \vee z_{i,j,k}$			

where $i, j, k \in \{1, \ldots, n\}$ and $i \neq j$ in (2). Since DLO_n has large clauses, we employ the (r, k)-game introduced above.

Lemma 7 *The Duplicator wins the extended $(3, n/3)$-game on DLO_n, and therefore, every Resolution refutation of $E_3(DLO_n)$ requires width $n/3$.*

Proof: For every linear ordering $<_a$ on $\{1,\dots,n\}$, let $f_a = (D,h)$ be the extended partial truth assignment with domain $D = D_1 \cup D_2 \cup D_3 \cup D_4$ where $D_1 = \{(x_{i,j},1) : 1 \le i,j \le n\}$, $D_2 = \{(z_{i,j,k},1) : 1 \le i,j,k \le n\}$, $D_3 = \{(x_{i,j}, D_{i,j}) : j <_a i\}$, and $D_4 = \{(z_{i,j,k}, D_{i,k}) : i <_a j <_a k\}$. The mapping h is defined as $h(x_{i,j}) = 1$ if $i <_a j$ and 0 otherwise and $h(z_{i,j,k}) = 1$ if $i <_a j <_a k$ and 0 otherwise. By the way it is defined, f_a is an extended partial truth assignment.

We define our winning strategy $\mathcal{A}$ as the set containg every $f \subseteq f_a$ for some linear ordering $<_a$ on $\{1,\dots,n\}$ such that $|\mathrm{Dom}(f)| \le n/3$. Thus, $\mathcal{A}$ satisfies conditions (i) and (ii) of extended winning strategy. We will show that condition (iii) is also satisfied. Let $(D,h) \subseteq f_a$ be any element of $\mathcal{A}$ with $|D| < n/3$. For any $x_{i,j}$, $(x_{i,j},1)$ is in the domain of f_a, and, in consequence, the projection of f_a with domain $D \cup \{(x_{i,j},1)\}$ belongs to $\mathcal{A}$. Analogoulsy, for every $z_{i,j,k}$, $(z_{i,j,k},1)$ is in $\mathrm{Dom}(f_a)$ and consequently, the projection of f_a with domain $D \cup \{(z_{i,j,k},1)\}$ is also in $\mathcal{A}$.

Let us consider now condition (iv). Let N be a subset of $\{1,\dots,n\}$ containing all the indices in $\{1,\dots,n\}$ referenced in D. That is, N contains i and j if $(x_{i,j},C)$ is in D for some C, and N contains i, j, and k if $(z_{i,j,k},C)$ is in D for some C. Since $|D| < n/3$ then $N \le n-3$. Let $1 \le i,j \le n$ be an arbitrary pair of indices on $\{1,\dots,n\}$. We will show that there exists a linear order $<_b$ on $\{1,\dots,n\}$ such that (1) $<_a$ and $<_b$ coincide on N, i.e., for every $i',j' \in N$, $i' <_a j'$ iff $i' <_b j'$, and (2) the domain of f_b contains $(x, D_{i,j})$ for some x. Thus, the projection of f_b to $D \cup \{(x,D_{i,j})\}$ belongs to $\mathcal{A}$. To construct $<_b$ we do the following: if i and k belong to N and $i <_a k$ then we fix $<_b$ to be a linear ordering that coincides with $<_a$ on N and such that $i <_b j <_b k$ for some j not in N. It is immediate to see that such $<_b$ allways exists and that $(z_{i,j,k}, D_{i,k}) \in \mathrm{Dom}(f_b)$. Otherwise, we can find some linear ordering $<_b$ that coincides with $<_a$ on N and such that $k <_b i$. In this case $(x_{i,k}, D_{i,k}) \in \mathrm{Dom}(f_b)$. □

We stress on the fact that the introduction of the new game was motivated by an attempt to generalize the construction of winning strategies in the presence of auxiliary variables. A winning strategy for the Duplicator in the original game on the non-deterministic extension $E_3(DLO_n)$ could also be easily found directly.

To complete this section, in view of the width lower bound that we just proved, it is quite interesting that DLO_n has a Resolution refutation of polynomial size as we show next.

Theorem 3 *The set of clauses DLO_n, and therefore $E_3(DLO_n)$, has a Resolution refutation of size $O(n^3)$.*

Proof: The idea of the proof is to derive the clauses $D_k(i) = \neg x_{1,i} \vee z_{1,1,i} \vee \cdots \vee z_{1,k,i}$ for every $k \in \{1,\dots,n\}$ and $i \in \{1,\dots,n\}$. Once this is done, from $D_1(i)$ we obtain $\neg x_{1,i}$ for every $i \in \{1,\dots,n\}$ by a cut with $\neg z_{1,1,i}$ which is derived from $\neg x_{1,1}$ and (5) (observe that $\neg x_{1,1}$ is simply (1) in the particular case $i = j = 1$). Then we obtain $x_{i,1}$ for every $i \in \{1,\dots,n\}$ by a cut with (2), and $\neg z_{i,1,k}$ for every $i,k \in \{1,\dots,n\}$ by a cut with (6). Then we eliminate all occurrences of all variables $x_{i,1}$, $x_{1,i}$ in DLO_n, and $z_{i,1,k}$ from (7). The resulting formula would contain a copy of DLO_{n-1} up to renaming of indices.

In order to derive $D_k(i)$, observe that each $D_n(i)$ is an initial clause. Observe too that $D_{k-1}(k)$ is derived at once from $D_k(k)$ and the initial clauses since $z_{1,k,k}$ cannot be true. To derive $D_{k-1}(i)$ from $D_k(i)$ for $i \neq k$, cut $D_k(i)$ and (6) on $z_{1,k,i}$ to obtain $D_{k-1}(i) \vee x_{k,i}$. Then combine this with $D_{k-1}(k)$ and the initial clauses (3) expressing transitivity to obtain $D_{k-1}(i)$. □

Therefore, the Dense Linear Order Principle is another example of a tautology witnessing the impossibility of improving the size-width relationship of Ben-Sasson and Wigderson. We note that the width lower bound for GT_n (the Minimum Principle) due to Bonet and Galesi could also be derived using Lemma 6 and a game theoretic argument.

References

[1] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Space complexity in propositional calculus. *SIAM Journal of Computing*, 31(4):1184–1211, 2002. A preliminary version appeared in STOC'00.

[2] M. Alekhnovich and A. A. Razborov. Resolution is not automatizable unless W[P] is tractable. In *42nd Annual IEEE Symposium on Foundations of Computer Science*, 2001.

[3] M. Alekhovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof systems. In *41st Annual IEEE Symposium on Foundations of Computer Science*, 2000.

[4] A. Atserias. Unsatisfiable random formulas are hard to certify. In *17th IEEE Symposium on Logic in Computer Science*, 2002. To appear.

[5] A. Atserias and M. L. Bonet. On the automatizability of resolution and related propositional proof systems. ECCC TR02-010, 2002.

[6] P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *37th Annual IEEE Symposium on Foundations of Computer Science*, pages 274–282, 1996.

[7] E. Ben-Sasson and N. Galesi. Space complexity of random formulas in resolution. In *16th IEEE Conference in Computational Complexity*, 2001.

[8] E. Ben-Sasson and A. Wigderson. Short proofs are narrow–resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

[9] M. L. Bonet and N. Galesi. Optimality of size-width trade-offs for resolution. *Journal of Computational Complexity*, 2001. To appear. A preliminary version appeared in FOCS'99.

[10] V. Chvátal and E. Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35(4):759–768, 1988.

[11] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *27th Annual ACM Symposium on the Theory of Computing*, 1995.

[12] H. Ebbinghaus and J. Flum. *Finite Model Theory*. Springer-Verlag, 1995.

[13] J. L. Esteban and J. Torán. Space bounds for Resolution. In *16th International Symposium on Theoretical Aspects of Computer Science*, pages 530–539, 1999.

[14] T. Feder and M. Y. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory. *SIAM Journal of Computing*, 28(1):57–104, 1998.

[15] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[16] Ph. G. Kolaitis and M. Y. Vardi. On the expressive power of Datalog: tools and a case study. *Journal of Computer and System Sciences*, 51:110–134, 1995.

[17] Ph. G. Kolaitis and M. Y. Vardi. Conjunctive-query containment and constraint satisfaction. *Journal of Computer and System Sciences*, 61(2):302–332, 2000.

[18] R. Raz. Resolution lower bounds for the weak pigeonhole principle. In *34th Annual ACM Symposium on the Theory of Computing*, 2002. To appear.

[19] A. A. Razborov. Resolution lower bounds for perfect matching principles. In *34th Annual ACM Symposium on the Theory of Computing*, 2002. To appear.

[20] J. Torán. Lower bounds for space in Resolution. In *Computer Science Logic '1999, 13th Annual Conference of the EACSL*, Lecture Notes in Computer Science. Springer-Verlag, 1999.

[21] A. Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, 1987.

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