Cardinality Constraints are Hard for Resolution

Ilario Bonacina
UPC Universitat Politècnica de Catalunya, Spain

Jordi Levy
IIIA, CSIC, Spain

Ion Mikel Liberal
IIIA, CSIC, Spain

Abstract

Cardinality constraints are one of the most widely used high-level constraints in SAT-based reasoning. Recently, it has been observed experimentally that the input ordering of cardinality encodings can significantly affect the performance of SAT solvers, sometimes even more than the choice of the encoding itself. In this paper, we study this phenomenon from a proof-complexity perspective, showing that encoding the contradictory pair of constraints $x_1+\cdots+x_n \geq k+1$ and $x_1+\cdots+x_n \leq k$, with totalizers and different input orderings, gives rise to exponentially hard formulas for Resolution.

2012 ACM Subject Classification Theory of computation → Proof complexity; Mathematics of computing

Keywords and phrases proof complexity, cardinality constraints, totalizers, resolution

1 Introduction

Cardinality constraints are among the most widely used high-level constraints in SAT-based reasoning. They express conditions of the form $x_1 + \cdots + x_n \leq k$ or $x_1 + \cdots + x_n \geq k$ where the variables are Boolean, and therefore provide a natural bridge between pseudo-Boolean reasoning, integer programming, and SAT. They are especially important in MaxSAT, where in core-guided algorithms such as OLL [15], SAT solvers are repeatedly called as subroutines and bounds on sets of relaxation variables are commonly represented by cardinality constraints. Beyond optimization, cardinality constraints also arise in scheduling, resource allocation, planning, configuration, and verification [9]. For this reason, their proof complexity is relevant to both the theory of Resolution and the design of effective SAT encodings.

Since SAT solvers operate on CNF formulas, cardinality constraints must be compiled into clauses. Hence, a line of research focuses on developing encodings that try to balance compactness and propagation strength, such as totalizers [4], sequential counters [18], sorting networks [6, 12], and cardinality networks [1].

For a single cardinality constraint, a good (propagation-complete) encoding can make unit propagation essentially as strong as the original high-level constraint [5, 14].

The situation becomes more subtle when several cardinality constraints are present simultaneously. Even if each individual constraint is propagation-complete, the CNF formula obtained by taking the encodings together may not propagate all consequences of the system of constraints. For instance, the auxiliary structure introduced by the encoding may depend strongly on the ordering of the input variables. This is not only a question of formula size or local propagation strength: recent experimental work [16] has shown that the ordering of literals inside cardinality encodings can have a substantial impact on the performance of SAT solvers, sometimes even larger than the choice of the encoding itself. This suggests that different orderings may create auxiliary structures that are easy or hard for Resolution.

Our contributions. In this paper, we study this phenomenon from a proof-complexity perspective. We consider the most basic contradictory system of cardinality constraints

(*Opposite Inequality Principle*),

$$\mathrm{OIP}_{n,\rho,k} := \mathsf{Enc}\big(x_1 + \cdots + x_n \geq k+1\big) \wedge \mathsf{Enc}\big(x_{\rho(1)} + \cdots + x_{\rho(n)} \leq k\big)\ , \tag{1}$$

encoded separately with totalizers and with different orderings of the input variables. More precisely, for the standard ordering and another ordering given by a permutation ρ. Semantically, the formulas $\mathrm{OIP}_{n,\rho,k}$ are trivially inconsistent. Proof-theoretically, however, the difficulty of refuting them can depend dramatically on the permutation ρ. If the two constraints use the same ordering, i.e., $\rho(i) = i$, then the two encodings have the same recursive structure, and Resolution may efficiently identify the corresponding auxiliary variable values (Theorem 3.1). In contrast, if ρ is a uniformly random permutation, then the two recursive decompositions are "misaligned", and we show that Resolution requires w.h.p. size $2^{\Omega(n)}$ to refute $\mathrm{OIP}_{n,\rho,n/2}$ (Theorem 5.2).

The proof uses an intermediate bounded-arity formulation. Given a multigraph $G = (V, E)$ and a labeling of the vertices $\ell \in \mathbb{Z}^V$, we consider the formula

$$\mathrm{Card}(G, \ell) := \bigwedge_{v \in V} \mathsf{CNF}\big(\sum_{e \ni v} x_e = \ell_v\big)\ ,$$

consisting of one variable for each edge and a cardinality constraint for each vertex, encoded without additional variables. In particular, we focus on 4-regular bipartite graphs and labels $\ell = (3, 2, 2, \ldots, 2)$. We prove that if G is a suitable boundary expander, then $\mathrm{Card}(G, \ell)$ requires linear Resolution width (Theorem 4.4) and hence exponential Resolution size (Corollary 4.5). For a random permutation ρ, we associate 4-regular multigraph $G_{\rho,4}$ that with high probability is such an expander (Theorem 2.3), giving a linear width lower bound for $\mathrm{Card}(G_{\rho,4}, \ell)$. Cardinality constraints similar to $\mathrm{Card}(G, \ell)$ but for different ℓ and other proof systems were also studied in [13, 3].

The connection between $\mathrm{OIP}_{n,\rho,n/2}$ and $\mathrm{Card}(G_{\rho,4}, \ell)$ with $\ell = (3, 2, 2, \ldots, 2)$ is established by a restriction argument. We restrict the two totalizers in the encoding of $\mathrm{OIP}_{n,\rho,n/2}$ so that each block of four consecutive input variables is forced to have Hamming weight 2, except for one distinguished block where the weight is 3. After this restriction, the remaining degrees of freedom correspond naturally to the edge variables of $\mathrm{Card}(G_{\rho,4}, \ell)$.

Structure of the paper. Section 2 contains the preliminaries. In Section 3 we give the precise definition of $\mathrm{OIP}_{n,\rho,k}$ and the upper bound on the size of resolution refutations of $\mathrm{OIP}_{n,\rho,k}$ for ρ being the identity permutation (Theorem 3.1). In Section 4, we show width and size lower bounds on the cardinality formulas $\mathrm{Card}(G, \ell)$ (Theorem 4.4 and Corollary 4.5) and, in Section 5, we show the size lower bound $\mathrm{OIP}_{n,\rho,n/2}$ for a random ρ (Theorem 5.2).

2 Preliminaries

Given $n \in \mathbb{N}$, let $[n] = \{1, \ldots, n\}$. Consider the usual Boolean basis $\{\wedge, \vee, \neg, 0, 1\}$ and the corresponding classical interpretation of the symbols. Given a set X of Boolean variables, a *literal* is a variable $x \in X$ or its negation $\neg x$, a *clause* is a finite disjunction of literals, and a *CNF formula* is a finite conjunction of clauses. The *width* of a clause C is the number of literals that appear in it. A k-CNF formula is a CNF with all clauses in it of width at most k. A *(total) assignment* α over the set X is a mapping $\alpha : X \to \{0, 1\}$ that can be extended to formulas using $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y)$, $\alpha(x \vee y) = \alpha(x) \vee \alpha(y)$ and $\alpha(\neg x) = \neg\alpha(x)$, and simplifying using the usual properties of the connectives, such as $F \vee 0 = F$, $F \vee 1 = 1$ etc. An assignment α is *partial* if $\mathrm{dom}(\alpha) \subsetneq X$. A CNF formula F is *satisfiable* if there is an assignment α such that $\alpha(F) = 1$; otherwise, F is *unsatisfiable*.

Resolution. Resolution [10, 17] is a sound and complete propositional proof system and is arguably the most studied propositional proof system due to its connection with practical SAT solving. Given a CNF formula φ, a *resolution derivation* of a clause D from φ is a sequence $C_1, \ldots, C_n$ of clauses such that $C_n = D$ and for every $i \in [n]$ either C_i is a clause in φ (C_i is an *axiom*) or C_i is the result of applying one of the following inference rules with premises that are already in the sequence: $\frac{A \vee x \quad B \vee \neg x}{A \vee B}$ (resolution rule) and $\frac{A}{A \vee B}$ (weakening rule), where A, B are clauses and x is a variable. A *refutation* is a derivation of the empty clause $\bot$.

The *minimum size* of a resolution refutation of φ (denoted $\text{size}(\varphi \vdash \bot)$) is the smallest number of clauses in a resolution refutation of φ. The *minimum width* needed to refute φ in resolution (denoted $\text{width}(\varphi \vdash \bot)$) is the minimum integer w s.t. there is a resolution refutation of φ only containing clauses of width at most w.

One of the fundamental relations between size and width in resolution is the *size-width inequality* [8]: for every unsatisfiable k-CNF formula φ over n variables,

$$\text{size}(\varphi \vdash \bot) \geq 2^{\Omega((\text{width}(\varphi \vdash \bot) - k)^2/n)} \ . \tag{2}$$

Multigraphs and expansion. A *graph* is a pair $G = (V, E)$ of where V is a set of vertices and E is a set of undirected edges between vertices in V. A *multigraph* is a graph $G = (V, E)$ where edges can occur multiple times. A multigraph is *bipartite* if $V = L \dot\cup R$ and for every $\{x, y\} \in E$, $x \in L$ and $y \in R$ or vice versa.

The *degree* $d(x)$ of a vertex x in V is the number of incident edges in x (counted with multiplicity), and the *degree* of a multigraph is the maximum degree among all the vertices. A (multi)graph is *d-regular* if all the vertices have degree d. Notice that, similarly to graphs, a connected multigraph with all degrees even has an Eulerian cycle, i.e., a cycle visiting each edge exactly once.

Given a multigraph $G = (V, E)$ and a subset $U \subseteq V$, the set $N(U)$ of *neighbors* of U is the set $N(U) := \{y \in V : \exists x \in U \ \{x, y\} \in E\}$, and the *boundary* (or *unique neighbors*) of U is the set $\partial(U) := \{y \in V : \exists! \, x \in U \ \{x, y\} \in E\}$. Notice that $N(U)$ and $\partial(U)$ are sets, for example, even when the edge $\{u, v\} \in E$ has multiplicity $d > 1$, $N(u) = \partial(u) = \{v\}$ and $|N(u)| = |\partial(u)| = 1$.

A multigraph $G = (V, E)$ is an (r, c)-*expander* if for every $U \subseteq V$ with $|U| \leq r$ it holds $|N(U)| \geq c|U|$. The multigraph G is an (r, c)-*boundary-expander* if for every $U \subseteq V$ with $|U| \leq r$ it holds $|\partial(U)| \geq c|U|$.

▶ **Lemma 2.1.** *If a degree-d multigraph $G = (V, E)$ is an (r, c)-expander then it is also an $(r, 2c - d)$-boundary-expander.*

▶ **Lemma 2.2.** *Let G be an (r, c)-expander with $c > 1$, then each connected component of G has size at least $r + 1$.*

Multigraphs from permutations. Let $L = \{u_1, \ldots, u_n\}$ and $R = \{v_1, \ldots, v_n\}$. A permutation $\rho \in \mathcal{S}_n$, gives naturally the bipartite graph $G_\rho = (L \dot\cup R, E)$, with edges $E = \{\{u_i, v_{\rho(i)}\} : i \in [n]\}$. For a given k dividing n, we consider the bipartite graph $G_{\rho,k}$ obtained from G_ρ, identifying consecutive vertices in L and R in blocks of size k. This gives a k-regular bipartite *multi*graph. Formally, consider the partition of L as $L = L_1 \dot\cup \cdots \dot\cup L_{n/k}$ where $L_i = \{u_{k(i-1)+j} : j \in [k]\}$. Similarly, partition R into n/k blocks of k consecutive variables $R_1, \ldots, R_{n/k}$. The k-regular bipartite multigraph $G_{\rho,k} = (V, E)$ has vertices

$$V = \{L_1, \ldots, L_{n/k}\} \dot\cup \{R_1, \ldots, R_{n/k}\} \ ,$$

and edges $\{L_i, R_j\}$ with multiplicity given by the number of edges in G_ρ connecting vertices in the partition L_i with vertices in R_j, that is

$$E = \{\{L_i, R_j\} : \exists \ell \in [n]\ u_\ell \in L_i \ \text{ and } v_{\rho(\ell)} \in R_j\}\ ,$$

and the multiplicity of $\{L_i, R_j\}$ is the number of distinct $\ell \in [n]$ verifying the condition.

▶ **Theorem 2.3.** *Let $\rho : [n] \to [n]$ be a permutation chosen with uniform probability, and let k be a constant. For any constant $c < k - 2$, there is a constant γ such that $G_{\rho,k}$ is a $(\gamma n, c)$-boundary-expander with high probability.*

We omit the proof of this result, but the argument is similar to the one used in analogous results on the expansion properties of random k-CNF formulas (see, for instance [7, 11]).

3 The Opposite Inequality Principle

We encode the formula $\mathrm{OIP}_{n,\rho,k}$ using totalizers, that is

$$\begin{aligned}\mathrm{OIP}_{n,\rho,k} &= \mathsf{Enc}\big(x_1 + \cdots + x_n \geq k+1\big) \wedge \mathsf{Enc}\big(x_{\rho(1)} + \cdots + x_{\rho(n)} \leq k\big) \\ &= \mathrm{Tot}(x_1, \ldots, x_n, y_1, \ldots, y_n) \wedge y_{k+1} \ \wedge \\ &\quad \mathrm{Tot}(x_{\rho(1)}, \ldots, x_{\rho(n)}, y'_1, \ldots, y'_n) \wedge \neg y'_{k+1}\ ,\end{aligned}$$

where $k \in \{0, \ldots, n-1\}$, $\rho : [n] \to [n]$ is a permutation and $\mathsf{Enc}(\cdot)$ is a CNF encodings of the given cardinality constraints using a *totalizer* Tot, i.e., a circuit that has n Boolean inputs $\vec{x} = (x_1, \ldots, x_n)$ and n Boolean outputs $\vec{y} = (y_1, \ldots, y_n)$ with the property that for each $i \in [n-1]$, $y_i \geq y_{i+1}$ and the Hamming weight of $\vec{x}$ and $\vec{y}$ are the same. $\mathrm{Tot}(x_{\rho(1)}, \ldots, x_{\rho(n)}, y'_1, \ldots, y'_n)$ is the same as the formula $\mathrm{Tot}(x_1, \ldots, x_n, y_1, \ldots, y_n)$ but with renamed internal and output variables (see Figure 2a for a visual representation of the variables of $\mathrm{OIP}_{n,\rho,k}$).

Following [4], we consider CNF formulas $\mathrm{Tot}(x_1, \ldots, x_n, y_1, \ldots, y_n)$ constructed recursively as follows: when $n = 2$, $\mathrm{Tot}(x_1, x_2, y_1, y_2) = (y_1 \leftrightarrow x_1 \vee x_2) \wedge (y_2 \leftrightarrow x_1 \wedge x_2)$, and for n a power of 2

$$\begin{aligned}\mathrm{Tot}(x_1, \ldots, x_n, y_1, \ldots, y_n) = {} & \mathrm{Tot}(x_1, \ldots, x_{n/2}, r_1, \ldots, r_{n/2}) \wedge \\ & \mathrm{Tot}(x_{n/2+1}, \ldots, x_n, r_{n/2+1}, \ldots, r_n) \wedge \\ & \bigwedge_{i=1}^{n/2} \Big((r_i \vee r_{n/2+i} \to y_i) \wedge (y_{n/2+i} \to r_i \wedge r_{n/2+i})\Big) \wedge \\ & \bigwedge_{i,j=1}^{n/2} \Big((r_i \wedge r_{n/2+j} \to y_{i+j}) \wedge (y_{i+j-1} \to r_i \vee r_{n/2+j})\Big) \qquad (3)\end{aligned}$$

where the r's are fresh auxiliary variables. This encoding of Tot above as a CNF uses $\Theta(n^2)$ clauses over $\mathcal{O}(n \log n)$ variables in total. For n not a power of 2, the definition is similar. For simplicity, we prove all the results of the paper for n being a power of 2.

▶ **Theorem 3.1.** *When ρ is the identity permutation, the formula $\mathrm{OIP}_{n,\rho,k}$ has a $\mathcal{O}(n^2)$-size resolution refutation.*

Proof sketch. It is not too hard to see that the encoding of Tot above has the property that there are derivations of the clauses $y_i \leftrightarrow y'_i$ from $\mathrm{Tot}(x_1, \ldots, x_n, y_1, \ldots, y_n) \wedge \mathrm{Tot}(x_1, \ldots, x_n, y'_1, \ldots, y'_n)$ in resolution size $\mathcal{O}(n^2)$. The refutation of $\mathrm{OIP}_{n,\rho,k}$ proceeds by

induction, proving $r_i^j \leftrightarrow r_i'^j$ for every layer j and every pair of auxiliary variables in the same position (i, j) of both totalizers. Once obtained the clauses $y_{k+1} \leftrightarrow y'_{k+1}$, cutting with y_{k+1} and $\neg y'_{k+1}$ gives immediately the empty clause. An analysis (omitted here) shows that every clause, say $r_{i_1}^j \wedge r_{i_2}^j \to r_{i_3}^{j+1}$, of the totalizer encoding is used only once in the derivation, in this case, in the derivation of $r_{i_3}'^{j+1} \to r_{i_3}^{j+1}$. This allows us to conclude that the proof is linear in the size of the formula. ◀

4 Cardinality Formulas

Given a multigraph $G = (V, E)$ and a labeling $\ell \in \mathbb{Z}^V$, let the *Cardinality Formula* over G and ℓ be the following CNF:

$$\mathrm{Card}(G, \ell) := \bigwedge_{v \in V} \mathsf{CNF}\Big(\sum_{e \ni v} x_e = \ell_v\Big) \ , \tag{4}$$

where the CNF encoding of the cardinality constraint is the natural one that does not use new variables. Notice that, when $\ell = (1, 1, \ldots, 1)$ and $G = (V, E)$ is a graph with $|V|$ odd, this is known as the *Perfect Matching Principle* on G (see for instance [13, 3]).

▶ Remark 4.1. When e is an edge with multiplicity m, technically we would need variables $x_{e,1}, \ldots, x_{e,m}$ to distinguish between difference occurrences of the edge e. To ease the notation we omit the reference to the multiplicity.

We consider $\mathrm{Card}(G, \ell)$ when G is a 4-regular multigraph and $\ell = (2, 2, \ldots, 2)$ or $\ell = (3, 2, 2, \ldots, 2)$. Despite some similarity with the Perfect Matching Principle, the combinatorics of $\mathrm{Card}(G, \ell)$ for $\ell = (2, \ldots, 2)$ and $\ell = (3, 2, \ldots, 2)$ is quite different, as the next two observations show.

▶ **Observation 4.2.** *Let $G = (L \cup R, E)$ be a 4-regular bipartite multigraph and $\ell = (2, \ldots, 2)$. Then, the formula $\mathrm{Card}(G, \ell)$ is satisfiable.*

Proof. Since G is 4-regular, for each connected component of G, there is an Eulerian cycle visiting all edges of the component. For each cycle $v_0, v_1, \ldots, v_k, v_{k+1}$, with $v_{k+1} = v_0$, map $x_{v_i, v_{i+1}}$ to 0 if $v_i \in R$ and $v_{i+1} \in L$, and to 1 otherwise. It is easy to see that this assignment satisfies $\mathrm{Card}(G, \ell)$. ◀

With a similar argument as the above, but negating the assignment of part of the Eulerian path in the connected component of the vertex with label 3, we can also prove the following observation.

▶ **Observation 4.3.** *Let $G = (L \cup R, E)$ be a 4-regular bipartite multigraph, $\ell = (3, 2, \ldots, 2)$ and let $w \in R$ be the vertex with label 3. Then, for every vertex $v \in L$ in the connected component of w, there is an assignment α, satisfying all constraints in $\mathrm{Card}(G, \ell)$, except the one for v, where $\sum_{e \ni v} \alpha(x_e) = 3$.*

▶ **Theorem 4.4** (width l.b. for $\mathrm{Card}(G, \ell)$)**.** *Let $G = (L \cup R, E)$ be a 4-regular bipartite multigraph, $\ell = (3, 2, \ldots, 2)$. If G is a (r, c)-boundary-expander with $c > 1$, then $\mathrm{width}(\mathrm{Card}(G, \ell) \vdash \bot) \geq r(c-1)/8$.*

Proof. Without loss of generality, let R be the set containing the vertex with label 3. Let C be a clause in the variables of $\mathrm{Card}(G, \ell)$. We call a total assignment α *critical* if it satisfies all constraints in $\mathrm{Card}(G, \ell)$ except the cardinality constraint for a single $v \in L$ where $\sum_{e \ni v} \alpha(x_e) = 3$. Recall that by assumption the vertex with label 3 is not in L.

Given a set of vertices $S \subseteq L$, we write that $S \models C$ if every total *critical* assignment satisfying $\bigwedge_{v \in S \cup R} \mathsf{CNF}\big(\sum_{e \ni v} x_e = \ell_v\big)$ also satisfies C. Consider the following complexity measure $\mu(C) = \min_{S \subseteq L} \{|S| : S \models C\}$.

It is immediate to see that for every clause $C \in \mathrm{Card}(G, \ell)$, $\mu(C) \leq 1$ and that μ is sub-additive along resolution steps, that is $\mu(C \vee D) \leq \mu(C \vee x) + \mu(D \vee \neg x)$. We also have that $\mu(\bot) > r$. To prove this, it is enough to show that for every $S \subseteq L$ with $|S| \leq r$,

$$\bigwedge_{v \in S \cup R} \mathsf{CNF}\Big(\sum_{e \ni v} x_e = \ell_v\Big) \tag{5}$$

is satisfiable. By Observation 4.2, every connected component in S with constant labeling 2 is satisfiable. By Lemma 2.2, the connected component of the vertex with label 3 has size at least $r + 1$, and by Observation 4.3, that connected component can be satisfied only violating one cardinality constraint that can be anywhere in the connected component. Since $|S| \leq r$ we can choose the violated cardinality constraint in L but outside S and hence (5) is satisfiable.

By a standard medium complexity clause argument, there must exist a clause C in the refutation of $\mathrm{Card}(G, \ell)$ with $r/2 < \mu(C) \leq r$. Let $S \subseteq L$ be the witness of the fact that $r/2 < \mu(C) \leq r$, that is $r/2 < |S| \leq r$ and $S \models C$.

We call a vertex u in S *good* if there are at least two distinct vertices v_1, v_2 in $\partial(S)$ s.t. $\{u, v_1\} \in E$ and $\{u, v_2\} \in E$. Let U be the set of all good vertices in S.

First, let's give a lower bound on $|U|$. We have the following chain of inequalities

$$\begin{aligned}
|S| + 4|U| &\geq |S \setminus U| + 4|U| \\
&= |N(S \setminus U) \cap \partial(S)| + 4|U| && \text{[for each } v \in S \setminus U,\ |N(v) \cap \partial(S)| = 1\text{]} \\
&\geq |N(S \setminus U) \cap \partial(S)| + |N(U) \cap \partial(S)| && \text{[}G \text{ is 4-regular]} \\
&= |\partial(S)| \geq c|S| \ . && \text{[by expansion since } |S| \leq r\text{]}
\end{aligned}$$

Which gives $|U| \geq (c-1)|S|/4$. To conclude we only need to show that the width of C is at least $|U|$. This together with $|U| \geq (c-1)|S|/4$ and $|S| > r/2$ gives the width lower bound.

To show that the width of C is at least $|U|$ is enough to show that for every $u \in U$, the clause C must contain a variable x_e for some $e \ni u$ or some $e \ni v_1$, $e \ni v_2$ where v_1, v_2 are the vertices in $\partial(S)$ witnessing the fact that $u \in U$.

Suppose, towards a contradiction, that there is $u \in U$ and distinct v_1, v_2 in $\partial(S)$ s.t. $\{u, v_1\} \in E$ and $\{u, v_2\} \in E$ such that C does not contain variables x_e with $e \ni u$ or $e \ni v_1$ or $e \ni v_2$.

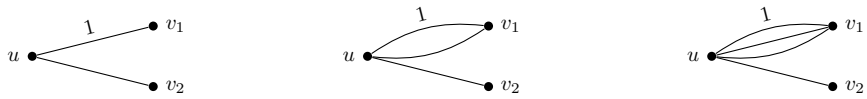
By minimality of S, there is an assignment α such that $\alpha(C) = 0$, α satisfies

$$\bigwedge_{v \in S \setminus \{u\} \cup R} \mathsf{CNF}\Big(\sum_{e \ni v} x_e = \ell_v\Big) \ , \tag{6}$$

and $\sum_{e \ni u} \alpha(x_e) = 3$. We have few cases to consider but in all of them the strategy is the same: show that there is always an $i \in \{1, 2\}$ s.t. $\alpha(x_{u,v_i}) = 1$ and $\alpha(x_{v',v_i}) = 0$ with $v' \notin S$. We flip the values of those variables, getting a new critical assignment α'. Since neither x_{u,v_i} nor x_{v',v_i} appear in C, $\alpha(C) = \alpha'(C) = 0$, but $\sum_{e \ni u} \alpha'(x_e) = 2$ and therefore α' satisfies

$$\bigwedge_{v \in S \cup R} \mathsf{CNF}\Big(\sum_{e \ni v} x_e = \ell_v\Big) \ , \tag{7}$$

contradicting the assumption that $S \models C$. To conclude we need to show that there is always an $i \in \{1, 2\}$ s.t. $\alpha(x_{u,v_i}) = 1$ and $\alpha(x_{v',v_i}) = 0$ with $v' \notin S$. Since $\sum_{e \ni u} \alpha(x_e) = 3$, it is not



(a) $\{u, v_1\}$ has multiplicity 1 **(b)** $\{u, v_1\}$ has multiplicity 2 **(c)** $\{u, v_1\}$ has multiplicity 3

Figure 1 Possible cases to consider according to the multiplicity of the edge $\{u, v_1\}$. The multiplicity of the edge $\{u, v_2\}$ is not drawn.

possible that $\alpha(x_{u,v_1}) = \alpha(x_{u,v_2}) = 0$. W.l.o.g. let v_1 be the vertex that we are guaranteed has $\alpha(x_{u,v_1}) = 1$. The edge $\{u, v_1\}$ can have multiplicity 1, 2, or 3 (see Figure 1) but not 4.
Case 1 ($\{u, v_1\}$ has multiplicity 1, see Figure 1a). Since v_1 has degree 4 and $v_1 \in \partial(S)$, there are three edges e_1, e_2, e_3 connecting v_1 with vertices outside S. The assignment α cannot map all variables $x_{e_1}, x_{e_2}, x_{e_3}$ to 1 otherwise $\sum_{e \ni v_1} \alpha(x_e) = 4$, while we know that α satisfies the cardinality constraint in v_1. Thus, we know that $\sum_{e \ni v_1} \alpha(x_e) \leq 3$ and therefore there is an e_i s.t. $\alpha(x_{e_i}) = 0$.
Case 2 ($\{u, v_1\}$ has multiplicity 2, see Figure 1b). Since v_1 has degree 4 and $v_1 \in \partial(S)$, there are two edges e_1, e_2 connecting v_1 with vertices outside S. If the assignment α maps all variables x_{e_1}, x_{e_2} to 1, $\sum_{e \ni v_1} \alpha(x_e) \geq 3$, if the label of v_1 was 2 this gives a contradiction. If the label of v_1 is 3, then the other edge connecting u with v_1 must be mapped to 0, and hence the edge $\{u, v_2\}$ must be mapped to 1 (and v_2 has label 2), hence we can argue as in the previous case. It is not possible that all edges adjacent to v_2 have label 1.
Case 3 ($\{u, v_1\}$ has multiplicity 3, see Figure 1c). The similar argument is left to the reader.

The case analysis above shows that there is always an $i \in \{1, 2\}$ s.t. $\alpha(x_{u,v_i}) = 1$ and $\alpha(x_{v',v_i}) = 0$ with $v' \notin S$, concluding the proof. ◀

Theorem 4.4 above and Theorem 2.3 imply that $\text{width}(\text{Card}(G_{\rho,4}, \ell) \vdash \bot) = \Omega(n)$ when ρ is a random permutation, and the size-width inequality in (2) implies the following corollary.

▶ **Corollary 4.5.** *For a random permutation $\rho : [n] \to [n]$ and $\ell = (3, 2, \ldots, 2)$, with high probability,* $\text{Card}(G_{\rho,4}, \ell)$ *requires resolution proofs of size at least* $2^{\Omega(n)}$.

5 Lower bound on the Opposite Inequality Principle

In this section we assume n to be a multiple of 4. We first show that a width lower bound for $\text{Card}(G_{\rho,4}, \ell)$ for $\ell = (3, 2, \ldots, 2)$ implies a width lower bound for a restriction σ of $\text{OIP}_{n,\rho,n/2}$ (Lemma 5.1). The restriction σ gives a value to all variables of $\text{OIP}_{n,\rho,n/2}$ except the input variables and the variables in Tot and Tot$'$ immediately above the variables. The values given by σ are enforcing only assignments that are consistent with $x_1 + x_2 + x_3 + x_4 = 3$, $x_5 + \cdots + x_8 = \cdots = x_{n-3} + \cdots + x_n = 2$ and $x_{\rho(1)} + x_{\rho(2)} + x_{\rho(3)} + x_{\rho(4)} = \cdots = x_{\rho(n-3)} + \cdots + x_{\rho(n)} = 2$ (see Figure 2b). In particular, σ does not falsifies $\text{OIP}_{n,\rho,n/2}$.

The connection between $G_{\rho,4}$ and $\text{OIP}_{n,\rho,n/2}|_\sigma$ is that $G_{\rho,4}$ imposes essentially the same constraints of $\text{OIP}_{n,\rho,n/2}|_\sigma$ by identifying the vertices in $\{x_1, x_2, x_3, x_4\}$, $\{x_5, x_6, x_7, x_8\}$, $\ldots$, $\{x_{n-3}, x_{n-2}, x_{n-1}, x_n\}$, and in the permuted sets, and imposing cardinality constraints analogous to the ones in $\text{OIP}_{n,\rho,n/2}|_\sigma$ (see Figure 2c for the $G_{\rho,4}$ associated to Figure 2b).

▶ **Lemma 5.1.** *Let $\rho : [n] \to [n]$ be a permutation and $\ell = (3, 2, \ldots, 2)$. We have that* $\text{width}(\text{OIP}_{n,\rho,n/2}\big|_\sigma \vdash \bot) \geq \frac{1}{2}\,\text{width}(\text{Card}(G_{\rho,4}, \ell) \vdash \bot) - 1$.

Proof. To show this, we use the characterization of the resolution width as a game [2]:

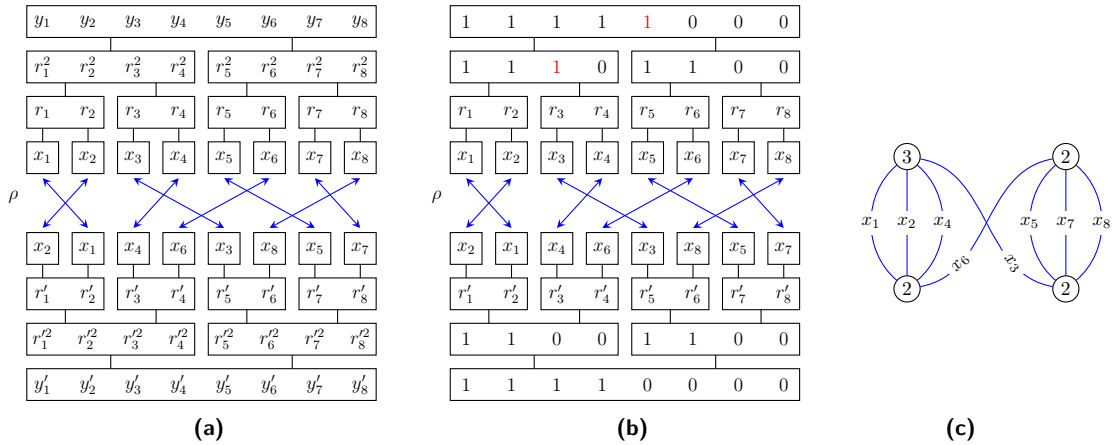


Figure 2 In (a) we give a graphical representation of the variables of $\mathrm{OIP}_{8,\rho,4}$ with the permutation $\rho = (1\ 2)(3\ 5\ 7\ 8\ 6\ 4)$; in (b) The restriction σ; and in (c) the graph $G_{\rho,4}$ and labelling ℓ associated to $\mathrm{OIP}_{8,\rho,4}|_\sigma$.

Given a CNF formula φ and $w \in \mathbb{N}$, $\mathrm{width}(\varphi \vdash \bot) \geq w$ *if and only if there exists a non-empty set of partial assignments $\mathcal{H}$ s.t., for all $\alpha \in \mathcal{H}$,*

1. $\alpha(\varphi) \neq \bot$,
2. *for all $\beta \subseteq \alpha$, $\beta \in \mathcal{H}$, and*
3. *if $|\mathrm{dom}(\alpha)| < w$ and $x \notin \mathrm{dom}(\alpha)$, then exists $\beta \in \mathcal{H}$ s.t. $\beta \supseteq \alpha$ and $x \in \mathrm{dom}(\beta)$.*

Let $w = \mathrm{width}(\mathrm{Card}(G_{\rho,4}, \ell) \vdash \bot)$, X the set of variables of $\mathrm{Card}(G_{\rho,4}, \ell)$ and $X \cup R \cup R'$ the set of variables of $\mathrm{OIP}_{n,\rho,n/2}|_\sigma$. By the characterization above there exists a family $\mathcal{H}$ of partial truth assignments on X satisfying the conditions 1–3 above with $\varphi = \mathrm{Card}(G_{\rho,4}, \ell)$. To show that $\mathrm{width}(\mathrm{OIP}_{n,\rho,n/2}|_\sigma \vdash \bot) \geq \frac{1}{2}w - 1$ we use the other implication in the characterization.

By the construction of the totalizer (see Figure 2b) we have that, for $i \in [n]$ odd, $r_i \leftrightarrow x_i \vee x_{i+1}$, and for $i \in [n]$ even, $r_i \leftrightarrow x_i \wedge x_{i-1}$, and similarly for r'_i. This means that every assignment α over the X-variables, can be extended to an assignment α^+ on $X \cup R \cup R'$ in the following way: on variables of X, α coincides with α^+, and if i odd and *both* $x_i, x_{i+1} \in \mathrm{dom}(\alpha)$, then $\alpha^+(r_i) = \alpha(x_i) \vee \alpha(x_{i+1})$. If i even and *both* $x_{i-1}, x_i \in \mathrm{dom}(\alpha)$, then $\alpha^+(r_i) = \alpha(x_{i-1}) \wedge \alpha(x_i)$. On the r'_is α^+ is defined similarly.

Consider the family of assignments $\mathcal{H}' := \{\alpha' : \exists \alpha \in \mathcal{H} \quad \alpha' \subseteq \alpha^+\}$. Clearly $\mathcal{H}'$ is non-empty and if $\beta' \subseteq \alpha'$ and $\alpha \in \mathcal{H}'$, then $\beta' \in \mathcal{H}'$. Moreover, since no partial assignment in $\mathcal{H}$ falsifies $\mathrm{Card}(G_{\rho,4}, \ell)$, then, by construction, no assignment in $\mathcal{H}'$ falsifies $\mathrm{OIP}_{\rho,n/2}|_\sigma$.

Now given $\alpha' \in \mathcal{H}'$ with $|\mathrm{dom}(\alpha')| \leq \frac{w}{2} - 1$ and $v \in (X \cup R \cup R') \setminus \mathrm{dom}(\alpha')$ we want to show that there exists $\beta' \in \mathcal{H}'$ s.t. $\beta' \supseteq \alpha'$ and $v \in \mathrm{dom}(\beta')$. Let $\alpha \in \mathcal{H}$ s.t. $\alpha' \subseteq \alpha^+$ and let α be of minimal domain. Clearly $|\mathrm{dom}(\alpha)| \leq |\mathrm{dom}(\alpha^+)|$, and, by minimality, $|\mathrm{dom}(\alpha^+)| \leq 2|\mathrm{dom}(\alpha')|$ which in turn is at most $w - 2$ by the assumption on $|\mathrm{dom}(\alpha')|$.
Case 1 ($v \in X$). By the properties of $\mathcal{H}$ there exists $\beta \in \mathcal{H}$ s.t. $\beta \supseteq \alpha$ and $v \in \mathrm{dom}(\beta)$.
Case 2 ($v \in R \cup R'$). Assume w.l.o.g. that $v \in R$. Then, $v \leftrightarrow x_i \vee x_{i+1}$ or $v \leftrightarrow x_{i-1} \wedge x_i$. Since the argument is very similar in both cases, we just consider $v \leftrightarrow x_i \vee x_{i+1}$. Since $v \notin \mathrm{dom}(\alpha')$, by the minimality of α^+, x_i and x_{i+1} are not in $\mathrm{dom}(\alpha^+)$. Since $|\mathrm{dom}(\alpha^+)| \leq w - 2$, there exists $\beta \in \mathcal{H}$ s.t. $\beta \supseteq \alpha$ and $x_i, x_{i+1} \in \mathrm{dom}(\beta)$.

In both cases take $\beta' = \beta^+$. By definition $\beta^+ \in \mathcal{H}'$ and since $\alpha \subseteq \beta$ then $\alpha^+ \subseteq \beta^+$ and hence $\beta^+ \supseteq \alpha'$ and by construction $v \in \mathrm{dom}(\beta^+)$. ◀

▶ **Theorem 5.2.** *Let n be a multiple of 4 and $\rho : [n] \to [n]$ a uniformly random permutation. With high probability,* $\mathrm{size}(\mathrm{OIP}_{n,\rho,n/2} \vdash \bot) = 2^{\Omega(n)}$.

Proof. Let $1 < c < 2$ and $\ell = (3, 2, \ldots, 2)$ and consider the restriction σ. By Theorem 2.3, there exists a constant γ such that the multigraph $G_{\rho,4}$ is with high probability a $(\gamma n, c)$-boundary-expander, hence, by Theorem 4.4 $\mathrm{width}(\mathrm{Card}(G_{\rho,4}, \ell) \vdash \bot) = \Omega(n)$, and, by Lemma 5.1, $\mathrm{width}(\mathrm{OIP}_{n,\rho,n/2}\big|_\sigma \vdash \bot) = \Omega(n)$. Hence by the size-width inequality in (2), $\mathrm{size}(\mathrm{OIP}_{n,\rho,n/2}\big|_\sigma \vdash \bot) = 2^{\Omega(n)}$. Since restrictions do not increase resolution proofs, $\mathrm{size}(\mathrm{OIP}_{n,\rho,n/2} \vdash \bot) = 2^{\Omega(n)}$. ◀

References

1 Roberto Asín, Robert Nieuwenhuis, Albert Oliveras, and Enric Rodríguez-Carbonell. Cardinality networks: a theoretical and empirical study. *Constraints An Int. J.*, 16(2):195–221, 2011. doi:10.1007/S10601-010-9105-0. Cited on page(s): 1

2 Albert Atserias and Víctor Dalmau. A combinatorial characterization of resolution width. *Journal of Computer and System Sciences*, 74(3):323–334, 2008. Cited on page(s): 7

3 Per Austrin and Kilian Risse. Perfect matching in random graphs is as hard as Tseitin. *TheoretiCS*, Volume 1, 2022. doi:10.46298/theoretics.22.2. Cited on page(s): 2, 5

4 Olivier Bailleux and Yacine Boufkhad. Efficient CNF Encoding of Boolean Cardinality Constraints. In *Principles and Practice of Constraint Programming (CP)*, pages 108–122. Springer, 2003. doi:10.1007/978-3-540-45193-8_8. Cited on page(s): 1, 4

5 Olivier Bailleux, Yacine Boufkhad, and Olivier Roussel. A translation of pseudo-boolean constraints to SAT. *Journal on Satisfiability, Boolean Modeling and Computation*, 2(1–4):191–200, 2006. doi:10.3233/SAT190021. Cited on page(s): 1

6 K. E. Batcher. Sorting networks and their applications. In *Proceedings of the April 30–May 2, 1968, Spring Joint Computer Conference*, AFIPS '68 (Spring), page 307314, New York, NY, USA, 1968. Association for Computing Machinery. doi:10.1145/1468075.1468121. Cited on page(s): 1

7 Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. *Random Structures & Algorithms*, 23(1):92–109, 2003. doi:10.1002/rsa.10089. Cited on page(s): 4

8 Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *J. ACM*, 48(2):149–169, March 2001. doi:10.1145/375827.375835. Cited on page(s): 3

9 Miquel Bofill, Jordi Coll, Peter Nightingale, Josep Suy, Felix Ulrich-Oltean, and Mateu Villaret. SAT encodings for pseudo-boolean constraints together with at-most-one constraints. *Artificial Intelligence*, 302:103604, 2022. doi:10.1016/j.artint.2021.103604. Cited on page(s): 1

10 Martin Davis and Hilary Putnam. A computing procedure for quantification theory. *Journal of the ACM*, 7(3):201–215, 1960. doi:10.1145/321033.321034. Cited on page(s): 3

11 Susanna F. de Rezende, Jakob Nordström, Kilian Risse, and Dmitry Sokolov. Exponential resolution lower bounds for weak pigeonhole principle and perfect matching formulas over sparse graphs. In *35th Computational Complexity Conference (CCC 2020)*, volume 169, pages 28:1–28:24, 2020. doi:10.4230/LIPIcs.CCC.2020.28. Cited on page(s): 4

12 Niklas Eén and Niklas Sörensson. Translating pseudo-boolean constraints into SAT. *J. Satisf. Boolean Model. Comput.*, 2(1-4):1–26, 2006. doi:10.3233/sat190014. Cited on page(s): 1

13 Dmitry Itsykson, Vsevolod Oparin, Mikhail Slabodkin, and Dmitry Sokolov. Tight lower bounds on the resolution complexity of perfect matching principles. *Fundamenta Informaticae*, 145(3):229–242, 2016. doi:10.3233/FI-2016-1358. Cited on page(s): 2, 5

14 João Marques-Silva and Inês Lynce. Towards robust CNF encodings of cardinality constraints. In *Principles and Practice of Constraint Programming (CP)*, volume 4741, pages 483–497, 2007. doi:10.1007/978-3-540-74970-7_35. Cited on page(s): 1

15 Antonio Morgado, Carmine Dodaro, and Joao Marques-Silva. Core-guided MaxSAT with soft cardinality constraints. In *Principles and Practice of Constraint Programming (CP)*, pages 564–573, 2014. Cited on page(s): 1

16 Joseph E. Reeves, João Filipe, Min-Chien Hsu, Ruben Martins, and Marijn J. H. Heule. The impact of literal sorting on cardinality constraint encodings. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 39, 2025. doi:10.1609/aaai.v39i11.33232. Cited on page(s): 1

17 John Alan Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, 1965. doi:10.1145/321250.321253. Cited on page(s): 3

18 Carsten Sinz. Towards an optimal CNF encoding of boolean cardinality constraints. In Peter van Beek, editor, *Principles and Practice of Constraint Programming (CP)*, pages 827–831. Springer, 2005. doi:10.1007/11564751_73. Cited on page(s): 1