On Minimal Unsatisfiability and Time-Space Trade-offs for k-DNF Resolution

Jakob Nordström[1] and Alexander Razborov[2]

[1] KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[2] Department of Computer Science, University of Chicago, Chicago, IL 60637, USA

Abstract. A well-known theorem by Tarsi states that a minimally unsatisfiable CNF formula with m clauses can have at most $m-1$ variables, and this bound is exact. In the context of proving lower bounds on proof space in k-DNF resolution, [Ben-Sasson and Nordström 2009] extended the concept of minimal unsatisfiability to sets of k-DNF formulas and proved that a minimally unsatisfiable k-DNF set with m formulas can have at most $(mk)^{k+1}$ variables. This result is far from tight, however, since they could only present explicit constructions of minimally unsatisfiable sets with $\Omega(mk^2)$ variables.

In the current paper, we revisit this combinatorial problem and significantly improve the lower bound to $(\Omega(m))^k$, which almost matches the upper bound above. Furthermore, using similar ideas we show that the analysis of the technique in [Ben-Sasson and Nordström 2009] for proving time-space separations and trade-offs for k-DNF resolution is almost tight. This means that although it is possible, or even plausible, that stronger results than in [Ben-Sasson and Nordström 2009] should hold, a fundamentally different approach would be needed to obtain such results.

1 Introduction

A formula in conjunctive normal form, or *CNF formula*, is said to be *minimally unsatisfiable* if it is unsatisfiable but deleting any clause makes it satisfiable. A well-known result by Tarsi [1], reproven several times by various authors (see, for instance, [6, 12, 15]), says that the number of variables in any such CNF formula is always at most $m-1$, where m is the number of clauses.

Motivated by problems in proof complexity related to the space measure in the *k-DNF resolution* proof systems introduced by Krajíček [14], Ben-Sasson and Nordström generalized this concept in [9]. In that paper, later published as part of [10], they studied the minimal unsatisfiability of conjunctions of formulas in disjunctive normal form where all terms in the disjunctions have size at most k, henceforth *k-DNF formulas*. We begin by reviewing their definition.

Assume that $\mathbb{D} = \{D_1, \ldots, D_m\}$ is the set of k-DNF formulas appearing in our conjunction, and that $\mathbb{D}$ itself is unsatisfiable. What should it mean that $\mathbb{D}$ is *minimally* unsatisfiable?

The first, naive, attempt at a definition would be to require, by analogy with the $k = 1$ case, that $\mathbb{D}$ becomes satisfiable after removing any D_i from it.

However, the following simple example of two 2-DNF formulas

$$\{(x \wedge y_1) \vee \ldots \vee (x \wedge y_n),\ (\bar{x} \wedge y_1) \vee \ldots \vee (\bar{x} \wedge y_n)\} \tag{1}$$

that is minimally unsatisfiable in this sense shows that we can not hope to get any meaningful analogue of Tarsi's lemma under this assumption only.

The reason for this is that the 2-DNF set (1) is *not* minimally unsatisfiable in the following sense: even if we "weaken" a formula in the set (i.e., make it easier to satisfy) by removing any, or even all, y-variables, what remains is still an unsatisfiable set. This leads us to the stronger (and arguably more natural) notion that the formula set should be minimally unsatisfiable not only with respect to removing DNF formulas but also with respect to shrinking terms (i.e., conjunctions) in these formulas. Fortunately, this also turns out to be just the right notion for the proof complexity applications given in [10]. Therefore, following [10], we say that a set $\mathbb{D}$ of k-DNF formulas is *minimally unsatisfiable* if weakening any single term (i.e., removing from it any literal) appearing in a k-DNF formula from $\mathbb{D}$ will make the "weaker" set of formulas satisfiable. This raises the following combinatorial question:

> *How many variables* (as *a function of* k *and* m) *can appear in a minimally unsatisfiable set* $\{D_1, \ldots, D_m\}$ *of* k*-DNF formulas?*

Tarsi's lemma states that for $k = 1$ the answer is $m - 1$. This result has a relatively elementary proof based on Hall's marriage theorem, but its importance to obtaining lower bounds on resolution length and space is hard to overemphasize. For instance, the seminal lower bound on refutation length of random CNF formulas in [12] makes crucial use of it, as does the proof of the "size-width trade-off" in [11]. Examples of applications of this theorem in resolution space lower bounds include [3, 7, 8, 10, 16, 18].

To the best of our knowledge, the case $k \geq 2$ had not been studied prior to [10]. That paper established an $(mk)^{k+1}$ upper bound and an $\Omega\big(mk^2\big)$ lower bound on the number of variables. The gap is large, and, as one of their open questions, the authors asked to narrow it.

In this paper, we almost completely resolve this problem by proving an $(\Omega(m))^k$ lower bound on the number of variables. Our construction is given in Section 3, following some preliminaries in Section 2. In Section 4, we show how a similar construction proves that in order to improve on the space complexity bounds from [10] a different approach would be needed. The paper is concluded with a few remarks and open problems in Section 5.

2 Preliminaries

Recall that a DNF formula is a disjunction of terms, or conjunctions, of literals, i.e., unnegated or negated variables. If all terms have size at most k, then the formula is referred to as a *k-DNF formula* (where k should be thought of as some arbitrary but fixed constant).

Definition 1 ([10]). *A set of DNF formulas* $\mathbb{D}$ *is* minimally unsatisfiable *if it is unsatisfiable but replacing any single term* T *appearing in any DNF formula* $D \in \mathbb{D}$ *with any proper subterm of* T *makes the resulting set satisfiable.*

Note that this indeed generalizes the well-known notion of minimally unsatisfiable CNF formulas, where a "proper subterm" of a literal is the empty term 1 that is always true and "weakening" a clause hence corresponds to removing it from the formula.

We are interested in bounding the number of variables of a minimally unsatisfiable k-DNF set in terms of the number of formulas in the set. For 1-DNF sets (i.e., CNF formulas), Tarsi's lemma says that the number of variables must be at most the number of formulas (i.e., clauses) minus one for minimal unsatisfiability to hold. This is easily seen to be tight by considering the example

$$\{x_1, x_2, \ldots, x_n,\ \bar{x}_1 \vee \bar{x}_2 \vee \ldots \vee \bar{x}_n\}\ . \tag{2}$$

No such bound holds for general k, however, since there is an easy construction shaving off a factor k^2. Namely, denoting by $\mathit{Vars}(\mathbb{D})$ the set of variables appearing somewhere in $\mathbb{D}$, we have the following lemma.

Lemma 2 ([10]). *There are arbitrarily large minimally unsatisfiable sets* $\mathbb{D}$ *of* k*-DNF formulas with* $|\mathit{Vars}(\mathbb{D})| \geq k^2(|\mathbb{D}| - 1)$.

Proof sketch. Consider any minimally unsatisfiable CNF formula consisting of $n+1$ clauses over n variables (for example, the one given in (2)). Substitute every variable x_i with

$$\left(x_i^1 \wedge \cdots \wedge x_i^k\right) \vee \left(x_i^{k+1} \wedge \cdots \wedge x_i^{2k}\right) \vee \cdots \vee \left(x_i^{k^2-k+1} \wedge \cdots \wedge x_i^{k^2}\right) \tag{3}$$

and expand every clause to a k-DNF formula. (Note that for this to work, we also need the easily verifiable fact that the negation of (3) can be expressed as a k-DNF formula.) It is straightforward to verify that the result is a minimally unsatisfiable k-DNF set, and this set has $n+1$ formulas over $k^2 n$ variables.

There is a big gap between this lower bound on the number of variables (in terms of the number of formulas) and the upper bound obtained in [10], stated next.

Theorem 3 ([10]). *Suppose that* $\mathbb{D}$ *is a minimally unsatisfiable* k*-DNF set containing* m *formulas. Then* $|\mathit{Vars}(\mathbb{D})| \leq (km)^{k+1}$.

A natural problem is to close, or at least narrow, this gap. In this work, we do so by substantially improving the bound in Lemma 2.

3 An Improved Lower Bound for Minimal Unsatisfiability

In this section, we present our construction establishing that the number of variables in a minimally unsatisfiable k-DNF set can be roughly at least the number of formulas raised to the kth power.

Theorem 4. *There exist arbitrarily large minimally unsatisfiable k-DNF sets $\mathbb{D}$ with m formulas over more than $\left(\frac{m}{4}\left(1-\frac{1}{k}\right)\right)^k$ variables.*

In particular, for any $k \geq 2$ there are minimally unsatisfiable k-DNF sets with m formulas over (more than) $(m/8)^k = (\Omega(m))^k$ variables.

Very informally, we will use the power afforded by the k-terms to construct a k-DNF set $\mathbb{D}$ consisting of roughly m formulas that encode roughly m^{k-1} "parallel" instances of the minimally unsatisfiable CNF formula in (2). These parallel instances will be indexed by coordinate vectors $\left(x^1_{i_1}, x^2_{i_2}, \ldots, x^{k-1}_{i_{k-1}}\right)$. We will add auxiliary formulas enforcing that only one coordinate vector $\left(x^1_{i_1}, x^2_{i_2}, \ldots, x^{k-1}_{i_{k-1}}\right)$ can have all coordinates true. This vector identifies which instance of the formula (2) we are focusing on, and all other parallel instances are falsified by their coordinate vectors not having all coordinates true.

Let us now formalize this intuition. We first present the auxiliary formulas constraining our coordinate vectors, which are the key to the whole construction.

3.1 A Weight Constraint *k*-DNF Formula Set

Let us write $\boldsymbol{x} = \left(x_1, \ldots, x_{m(k-1)}\right)$ to denote a vector of variables of dimension $m(k-1)$. Let $|\boldsymbol{x}| = \sum_{i=1}^{m(k-1)} x_i$ denote the *Hamming weight* of $\boldsymbol{x}$, i.e., the number of ones in the vector. We want to construct a k-DNF set $W_m(\boldsymbol{x})$ with $\mathrm{O}(m)$ formulas over $x_1, \ldots, x_{m(k-1)}$ and some auxiliary variables minimally expressing that $|\boldsymbol{x}| \leq 1$. That is, a vector $\boldsymbol{x}$ can be extended to a satisfying assignment for $W_m(\boldsymbol{x})$ if and only if $|\boldsymbol{x}| \leq 1$ but if we weaken any formula in the set, then there are satisfying assignments with $|\boldsymbol{x}| \geq 2$.

We define $W_m(\boldsymbol{x})$ to be the set of k-DNF formulas listed in Figure 1. The intuition for the auxiliary variables is that z_j can be set to true only if the first $j(k-1)$ variables $x_1, \ldots, x_{j(k-1)}$ are all false, and w_j can be set to true only if at most one of the first $j(k-1)$ variables $x_1, \ldots, x_{j(k-1)}$ is true. The set W_m contains $2m-1$ formulas. Let us see that W_m minimally expresses that $\boldsymbol{x}$ has weight at most 1. For ease of notation, we will call the group of variables $\{x_{(j-1)(k-1)+1}, \ldots, x_{j(k-1)}\}$ the *jth block* and denote it by X_j.

Every $\boldsymbol{x}$ with $|\boldsymbol{x}| \leq 1$ can be extended to a satisfying assignment for $W_m(\boldsymbol{x})$. Since all x-variables appear only negatively, we can assume without loss of generality that $|\boldsymbol{x}| = 1$, so that all x_i are false except for a single variable in, say, the j_0th block X_{j_0}. We simply set z_j to true for $j < j_0$ and false for $j \geq j_0$, and we set all w_j to true.

Every satisfying assignment for $W_m(\boldsymbol{x})$ satisfies $|\boldsymbol{x}| \leq 1$. Assume on the contrary that $x_{i_1} = x_{i_2} = 1$; $i_1 \in X_{j_1}$, $i_2 \in X_{j_2}$; $j_1 \leq j_2$. We have that the truth of x_{i_1} forces z_j to false for all $j \geq j_1$, and then $x_{i_2} = 1$ forces w_j to false for all $j \geq j_2$. But this means that there is no way to satisfy the final formula (4g). So for all satisfying assignments it must hold that $|\boldsymbol{x}| \leq 1$.

After weakening any term in $W_m(\boldsymbol{x})$, the resulting set can be satisfied by an assignment giving weight at least 2 to $\boldsymbol{x}$. First, notice that weakening any of the unit terms (i.e., terms of size one) results in removing the

$$\overline{z}_1 \vee \left(\overline{x}_1 \wedge \cdots \wedge \overline{x}_{k-1}\right) \tag{4a}$$

$$\overline{z}_2 \vee \left(z_1 \wedge \overline{x}_k \wedge \cdots \wedge \overline{x}_{2(k-1)}\right) \tag{4b}$$

$$\vdots$$

$$\overline{z}_{m-1} \vee \left(z_{m-2} \wedge \overline{x}_{(m-2)(k-1)+1} \wedge \cdots \wedge \overline{x}_{(m-1)(k-1)}\right) \tag{4c}$$

$$\overline{w}_1 \vee z_1 \vee \bigvee_{i=1}^{k-1} \bigwedge_{\substack{i'=1\\ i' \neq i}}^{k-1} \overline{x}_{i'} \tag{4d}$$

$$\overline{w}_2 \vee z_2 \vee \left(w_1 \wedge \overline{x}_k \wedge \cdots \overline{x}_{2(k-1)}\right) \vee \bigvee_{i=k}^{2(k-1)} \left(z_1 \wedge \bigwedge_{\substack{i'=k\\ i' \neq i}}^{2(k-1)} \overline{x}_{i'}\right) \tag{4e}$$

$$\vdots$$

$$\begin{aligned} &\overline{w}_{m-1} \vee z_{m-1} \vee \left(w_{m-2} \wedge \overline{x}_{(m-2)(k-1)+1} \wedge \cdots \wedge \overline{x}_{(m-1)(k-1)}\right) \\ &\qquad\qquad \vee \bigvee_{i=(m-2)(k-1)+1}^{(m-1)(k-1)} \left(z_{m-2} \wedge \bigwedge_{\substack{i'=(m-2)(k-1)+1\\ i' \neq i}}^{(m-1)(k-1)} \overline{x}_{i'}\right) \end{aligned} \tag{4f}$$

$$\begin{aligned} &\left(w_{m-1} \wedge \overline{x}_{(m-1)(k-1)+1} \wedge \cdots \wedge \overline{x}_{m(k-1)}\right) \\ &\qquad\qquad \vee \bigvee_{i=(m-1)(k-1)+1}^{m(k-1)} \left(z_{m-1} \wedge \bigwedge_{\substack{i'=(m-1)(k-1)+1\\ i' \neq i}}^{m(k-1)} \overline{x}_{i'}\right). \end{aligned} \tag{4g}$$

Fig. 1. Weight constraint k-DNF formulas $W_m(\boldsymbol{x})$.

formula in question altogether. This can only make it easier to satisfy the whole set than if we just shrink a k-term. Hence, without loss of generality we can focus on shrinking k-terms. Let us consider the formulas in $W_m(\boldsymbol{x})$ one by one.

If we remove some literal $\overline{x}_i$ in (4a)–(4c), then we can set $x_i = 1$ but still have $z_1 = \cdots = z_{m-1} = 1$. This will allows us to set also $x_{m(k-1)} = 1$ in (4g) and still satisfy the whole set of formulas although $|\boldsymbol{x}| \geq 2$.

If we instead remove some z_j ($j \leq m-2$) in these formulas, then we can set all $x_i = 1$ for $x_i \in X_1 \cup \ldots \cup X_j$ (that already gives us weight ≥ 2) and $z_1 = \ldots = z_j = 0$, and then we set $z_{j+1} = \ldots = z_{m-1} = 1$ and $x_i = 0$ for $x_i \in X_{j+1} \ldots \cup \ldots X_m$. Note that $j \leq m-2$ implies that $z_{m-1} = 1$ which takes care of (4g), and then (4d)–(4f) are satisfied simply be setting all w_j to 0. This completes the analysis of the formulas (4a)–(4c).

In formula (4d), if we remove some $\overline{x}_{i'}$, then we can set $x_i = x_{i'} = w_1 = 1$ and extend this to a satisfying assignment for the rest of the formulas.

For the corresponding terms $z_{j-1} \wedge \bigwedge_{i'=(j-1)(k-1)+1,\ i' \neq i}^{j(k-1)} \overline{x}_j$ in (4e)–(4g), if we remove some $\overline{x}_{i'}$, we can again set $x_i = x_{i'} = 1$ and $z_1 = \ldots = z_{j-1} = 1$

$$W_m^j(\boldsymbol{x}^j) \qquad 1 \le j < k \tag{5a}$$

$$\bigvee_{\substack{(i_1,\ldots,i_{k-1}) \\ \in [m(k-1)]^{k-1}}} \left(x_{i_1}^1 \wedge \cdots \wedge x_{i_{k-1}}^{k-1} \wedge y_{i_1,\ldots,i_{k-1}}^{\nu} \right) \qquad 1 \le \nu \le m(k-1) \tag{5b}$$

$$\bar{u}_\nu \vee \bigvee_{\substack{(i_1,\ldots,i_{k-1}) \\ \in [m(k-1)]^{k-1}}} \left(x_{i_1}^1 \wedge \cdots \wedge x_{i_{k-1}}^{k-1} \wedge \overline{y}_{i_1,\ldots,i_{k-1}}^{\nu} \right) \qquad 1 \le \nu \le m(k-1) \tag{5c}$$

$$u_1 \vee \cdots \vee u_{m(k-1)} \tag{5d}$$

Fig. 2. Minimally unsatisfiable set of k-DNF formulas $\mathbb{D}_m^k$.

and then $w_j = \ldots = w_{m-1} = 1$ to satisfy the rest of the set, whereas removing z_{j-1} would allow us to assign to 1 all $x_i \in X_1 \cup \ldots \cup X_{j-1}$ and then still assign $w_j = \ldots = w_{m-1} = 1$.

For the other kind of terms $w_{j-1} \wedge \overline{x}_{(j-1)(k-1)+1} \wedge \cdots \wedge \overline{x}_{j(k-1)}$ in (4e)–(4g), if some $\overline{x}_i$ with $x_i \in X_j$ is removed, we can set this x_i to true as well as an arbitrary $x_{i'} \in X_1 \cup \ldots \cup X_{j-1}$, whereas removing w_{j-1} would allow as again to set to 1 all variables in $X_1 \cup \ldots X_{j-1}$. This proves the minimality of $W_m(\boldsymbol{x})$.

3.2 The Minimally Unsatisfiable k-DNF Set

Let us write $\boldsymbol{x}^j = \left(x_1^j, x_2^j, \ldots, x_{m(k-1)}^j\right)$, and let $W_m^j(\boldsymbol{x}^j)$ be the k-DNF set with $\mathrm{O}(m)$ formulas constructed above (over disjoint sets of variables for distinct j) minimally expressing that $|\boldsymbol{x}^j| \le 1$. With this notation, let $\mathbb{D}_m^k$ be the k-DNF set consisting of the formulas in Figure 2. It is worth noting that the range of the index ν does not have any impact on the following proof of minimal unsatisfiability, and it was set to $m(k-1)$ only to get the best numerical results.

It is easy to verify that $\mathbb{D}_m^k$ consists of less than $4mk$ k-DNF formulas over more than $(m(k-1))^k = \left(\frac{1}{4}(4mk)\left(1 - \frac{1}{k}\right)\right)^k$ variables. We claim that $\mathbb{D}_m^k$ is minimally unsatisfiable, from which Theorem 4 follows.

To prove the claim, let us first verify unsatisfiability. If the k-DNF formulas $W_m^j(\boldsymbol{x})$ in (5a) are to be satisfied for all $j < k$, then there exists at most one $(k-1)$-tuple $(i_1^*, i_2^*, \ldots, i_{k-1}^*) \in [m(k-1)]^{k-1}$ such that $x_{i_1^*}^1, x_{i_2^*}^2, \ldots, x_{i_{k-1}^*}^{k-1}$ are all true. This forces $y_{(i_1^*, i_2^*, \ldots, i_{k-1}^*)}^{\nu}$ to true for all ν to satisfy the formulas in (5b), and then (5c) forces all u_ν to 0, so that (5d) is falsified. Hence, $\mathbb{D}_m^k$ is unsatisfiable.

Let us now argue that $\mathbb{D}_m^k$ is not only unsatisfiable, but *minimally* unsatisfiable in the sense of Definition 1. The proof is by case analysis over the different types of formulas in $\mathbb{D}_m^k$.

1. If we shrink any term in (5a)—say, in $W_m^1(\boldsymbol{x}^1)$—then by the minimality property in Section 3.1 we can set some $x_{i_1'}^1 = x_{i_1''}^1 = 1$ for $i_1' \neq i_1''$ and fix some $x_{i_2^*}^2 = \ldots = x_{i_{k-1}^*}^{k-1} = 1$ without violating the remaining clauses in

$W_m^1(\boldsymbol{x}^1), \ldots, W_m^{k-1}(\boldsymbol{x}^{k-1})$. This allows us to satisfy the formulas in (5b) and (5c) by setting $y^{\nu}_{(i'_1, i^*_2 \ldots, i^*_{k-1})} = 1$ and $y^{\nu}_{(i''_1, i^*_2 \ldots, i^*_{k-1})} = 0$ for all ν. Finally, set any u_ν to true to satisfy (5d). This satisfies the whole k-DNF set.

2. Next, suppose that we shrink some term $x^1_{i^*_1} \wedge x^2_{i^*_2} \wedge \cdots \wedge x^{k-1}_{i^*_{k-1}} \wedge y^{\nu}_{(i^*_1, \ldots, i^*_{k-1})}$ in the νth k-DNF formula in (5b). There are two subcases:
   (a) Some x-variable is removed, say, the variable $x^1_{i^*_1}$. Set $x^1_{i^*_1} = 0$ and $x^2_{i^*_2} = \ldots = x^{k-1}_{i^*_{k-1}} = y^{\nu}_{(i^*_1, i^*_2, \ldots, i^*_{k-1})} = 1$. This satisfies the νth formula in (5b). Then pick some $i'_1 \neq i^*_1$ and set $x^1_{i'_1} = 1$. All this can be done in a way that satisfies all clauses in (5a) since the weight of every $\boldsymbol{x}^j$ is one. Set $u_\nu = 1$ and $u_{\nu'} = 0$ for all $\nu' \neq \nu$ to satisfy (5d) and then $y^{\nu}_{(i'_1, i^*_2, \ldots, i^*_{k-1})} = 0$ to satisfy the νth formula in (5c) (all others are satisfied by literals $\bar{u}_{\nu'}$, $\nu' \neq \nu$). The νth formula in (5b) was satisfied above, and for all other $\nu' \neq \nu$ we set $y^{\nu'}_{(i'_1, i^*_2, \ldots, i^*_{k-1})} = 1$ to satisfy the rest of the formulas in (5b). This satisfies the whole k-DNF set.
   (b) The variable $y^{\nu}_{(i^*_1, \ldots, i^*_{k-1})}$ is eliminated. If so, set $x^1_{i^*_1} = \ldots = x^{k-1}_{i^*_{k-1}} = 1$ to satisfy the νth formula in (5b), $u_\nu = 1$ and $y^{\nu}_{(i^*_1, \ldots, i^*_{k-1})} = 0$ to satisfy (5d) and the νth formula in (5c), and $u_{\nu'} = 0$ and $y^{\nu'}_{(i^*_1, \ldots, i^*_{k-1})} = 1$ for all $\nu' \neq \nu$ to satisfy the rest of the formulas in (5b) and (5c). This is easily extended to an assignment satisfying (5a) as well.
3. For the νth formula in (5c), we may assume, for the same reasons as in Section 3.1, that we shrink a non-trivial k-term. Then we again have two subcases, treated similarly.
   (a) Some x-variable is removed, say $x^1_{i^*_1}$. Set $u_\nu = 1$, $x^1_{i^*_1} = 0$, $x^2_{i^*_2} = \ldots = x^{k-1}_{i^*_{k-1}} = 1$, and $y^{\nu}_{(i^*_1, i^*_2, \ldots, i^*_{k-1})} = 0$. This satisfies (5d) and the νth formula in (5c). Setting $u_{\nu'} = 0$ for $\nu' \neq \nu$ takes care of the rest of (5c). To satisfy (5b), pick some $i'_1 \neq i^*_1$ and set $x^1_{i'_1} = 1$, and $y^{\nu'}_{(i'_1, i^*_2, \ldots, i^*_{k-1})} = 1$ for all ν'. These assignments are all consistent with the weight constraints in (5a).
   (b) The literal $\overline{y}^{\nu}_{(i^*_1, \ldots, i^*_{k-1})}$ is eliminated. If so, set $x^1_{i^*_1} = \ldots = x^{k-1}_{i^*_{k-1}} = 1$ to satisfy the νth formula in (5c) and $u_\nu = 1$ to satisfy (5d). Setting $u_{\nu'} = 0$ for $\nu' \neq \nu$ takes care of the rest of (5c). Now we can satisfy all of (5b) by setting $y^{\nu'}_{(i^*_1, \ldots, i^*_{k-1})} = 1$ for all ν', and it is once again easy to see that the weight constraints in (5a) are also satisfied.
4. The disjunctive clause (5d) is removed. Set all u_ν to 0, and then set all $y^{\nu}_{i_1, \ldots, i_k}$ to 1, then (5a)–(5b) become easy to satisfy.

This completes the proof that $\mathbb{D}^k_m$ is minimally unsatisfiable as claimed, and Theorem 4 hence follows.

4 Implications for *k*-DNF Resolution Trade-offs

Let us start this section by a quick review of the relevant proof complexity context. The *k-DNF resolution* proof systems were introduced by Krajíček [14] as an intermediate step between resolution and depth-2 Frege. Roughly speaking, the kth member of this family, denoted henceforth by $\mathfrak{R}(k)$, is a system for reasoning in terms of k-DNF formulas. For $k = 1$, the lines in the proof are hence disjunctions of literals, and the system $\mathfrak{R}(1)$ is standard resolution. At the other extreme, $\mathfrak{R}(\infty)$ is equivalent to depth-2 Frege.

Informally, we can think of an $\mathfrak{R}(k)$-proof as being presented on a blackboard. The allowed derivation steps are to write on the board a clause of the CNF formula being refuted, to deduce a new k-DNF formula from the formulas currently on the board, or to erase formulas from the board. The *length* of an $\mathfrak{R}(k)$-proof is the total number of formulas appearing on the board (counted with repetitions) and the *(formula) space* is the maximal number of formulas simultaneously on the board at any time during the proof.

A number of works, for example, [2, 4, 5, 19, 20, 21], have proven superpolynomial lower bounds on the length of k-DNF refutations. It was also shown in [20, 21] that the $\mathfrak{R}(k)$-family forms a strict hierarchy with respect to proof length. Just as in the case for standard resolution, however, our understanding of space complexity in k-DNF resolution has remained more limited. Esteban et al. [13] established essentially optimal space lower bounds for $\mathfrak{R}(k)$ and also proved that the family of *tree-like* $\mathfrak{R}(k)$ systems form a strict hierarchy with respect to space. They showed that there are formulas F_n of size n that can be refuted in tree-like $(k + 1)$-DNF resolution in constant space but require space $\Omega(n/\log^2 n)$ in tree-like k-DNF resolution. It should be pointed out, however, that tree-like $\mathfrak{R}(k)$ for any $k \geq 1$ is strictly weaker than standard resolution, so the results in [13] left open the question of whether there is a strict space hierarchy for (non-tree-like) k-DNF resolution or not.

Recently, the first author in joint work with Ben-Sasson [10] proved that Krajíček's family of $\mathfrak{R}(k)$ systems do indeed form a strict hierarchy with respect to space. However, the parameters of the separation were much worse than for the tree-like systems in [13]; namely, the $\mathfrak{R}(k + 1)$-proofs have constant space but any $\mathfrak{R}(k)$-proof requires space $\Omega\bigl(\sqrt[k+1]{n/\log n}\bigr)$. It is not clear that there has to be a $(k+1)$st root in this bound. No matching upper bounds are known, and indeed for the special case of $\mathfrak{R}(2)$ versus $\mathfrak{R}(1)$ the lower bound proven in [10] is $\Omega\bigl(n/\log n\bigr)$, i.e., without a square root. Also, [10] established strong length-space trade-offs for k-DNF resolution, but again a $(k + 1)$st root is lost in the analysis compared to the corresponding results for standard resolution $\mathfrak{R}(1)$.

Returning now to the minimally unsatisfiable k-DNF sets, the reason [10] studied this concept was that it appeared related to a problem arising in their proof analysis, and they hoped that better *upper* bounds for minimal unsatisfiability would translate into improvements in the analysis. Instead, using ideas from the improved *lower* bound construction for minimal unsatisfiability in the previous section, we can show that the analysis of the particular proof technique employed in [10] is almost tight. Thus, any further substantial improvements of the bounds in that paper would have to be obtained by other methods.

We do not go into details of the proof construction in [10] here, since it is rather elaborate. Suffice it to say that the final step of the proof boils down to studying k-DNF sets that imply Boolean functions with a particular structure, and proving lower bounds on the size of such DNF sets in terms of the number of variables in these Boolean functions. (Recall that a set $\mathbb{F}$ implies a function F, denoted $\mathbb{F} \vDash F$, if any satisfying truth value assignment to all of $\mathbb{F}$ must also satisfy F.) Having come that far in the construction, all that remains is a purely combinatorial problem, and no reference to space proof complexity or k-DNF resolution is needed.

For concreteness, below we restrict our attention to the case where the Boolean functions are exclusive or. More general functions can be considered, and have been studied in [10], and everything that will be said below applies to such Boolean functions with appropriate (and simple) modifications. Hence, from now on let us focus on DNF sets that "minimally imply" (in a sense made formal below) a particular kind of formulas that we will refer to as $\left(\wedge\vee\oplus^k\right)$*-block formulas*. A $\left(\wedge\vee\oplus^k\right)$-block formula is a CNF formula in which every variable x is replaced by $\bigoplus_{i=1}^{k} x_i$, where $x_1, \ldots, x_k$ are new variables. Thus, literals turn into unnegated or negated XORs, every XOR applies to exactly one "block" of k variables, and no XOR mixes variables from different blocks. Let us write this down as a formal definition.

Definition 5. *A* $\left(\wedge\vee\oplus^k\right)$-block formula *$G$ is a conjunction of disjunctions of negated or unnegated exclusive ors. The variables of G are divided into disjoint blocks $x_1, \ldots, x_k$, $y_1, \ldots, y_k$, $z_1, \ldots, z_k$ et cetera, of k variables each, and every XOR or negated XOR is over one full block of variables.*

The key behind the lower bounds on space in [10] is the result that if a k-DNF set $\mathbb{D}$ implies a $\left(\wedge\vee\oplus^{k+1}\right)$-block formula G with many variables, then $\mathbb{D}$ must also be large.

Theorem 6 ([10]). *Let k be some fixed but arbitrary positive integer. Suppose $\mathbb{D}$ is a k-DNF set and G is a $\left(\wedge\vee\oplus^{k+1}\right)$-block formula such that $\mathbb{D}$ implies G "precisely," in the sense that if we remove a single XOR or negated XOR from G (thus making the formula stronger, i.e., harder to satisfy), it no longer holds that $\mathbb{D}$ implies G. Then $|\mathit{Vars}(G)| = \mathrm{O}\left(|\mathbb{D}|^{k+1}\right)$.*

Using this theorem, one can get the $\sqrt[k+1]{n/\log n}$ space separation mentioned above between $\mathfrak{R}(k)$ and $\mathfrak{R}(k+1)$. Any improvement in the exponent in the bound in Theorem 6 would immediately translate into an improved space separation, and would also improve the k-DNF resolution trade-offs in [10].

Prior to the current paper, the best lower bound giving limits on what one could hope to achieve in Theorem 6 was linear, i.e., $|\mathit{Vars}(G)| = \Omega(|\mathbb{D}|)$. Namely, let G be a conjunction of XORs $(\bigoplus_{i=1}^{k+1} x_i) \wedge (\bigoplus_{i=1}^{k+1} y_i) \wedge (\bigoplus_{i=1}^{k+1} z_i) \wedge \cdots$ and $\mathbb{D}$ be the union of the expansions of every $\bigoplus_{i=1}^{k+1} x_i$ as a CNF formula. For this particular structure of G it is also easy to prove that $|\mathit{Vars}(G)| = \mathrm{O}(|\mathbb{D}|)$ for *any* choice of $\mathbb{D}$, but it was open what happens when we consider general formulas G.

For $k = 1$, [10] proved that a linear bound $\mathrm{O}(|\mathbb{D}|)$ in fact holds for any set of clauses $\mathbb{D}$ and any $\left(\wedge\vee\oplus^2\right)$-block formula G, but all attempts to extend the techniques used there to the case $k > 1$ have failed. And indeed, they have failed for a good reason, since building on the construction in Section 3 we can show that the best one can hope for in Theorem 6 is $|\mathit{Vars}(G)| = \mathrm{O}\big(|\mathbb{D}|^k\big)$.

Theorem 7. *For any $k > 1$ there are arbirarily large k-DNF sets $\mathbb{D}$ of size m and $\big(\wedge\vee\oplus^{k+1}\big)$-block formulas G such that $\mathbb{D}$ "precisely" implies G in the sense of Theorem 6 and $|\mathit{Vars}(G)| \geq (k+1)\big[\frac{m}{k+2}\big(1-\frac{1}{k}\big)\big]^k \geq k\big(\frac{m}{4k}\big)^k$.*

Proof. We utilize all the previous notation and start with the CNF formula

$$\bigwedge_{\nu\in[m(k-1)]} \; \bigvee_{(i_1,\ldots,i_{k-1})\in[m(k-1)]^{k-1}} y^{\nu}_{i_1,\ldots,i_{k-1}} \tag{6}$$

and substitute an exclusive or over variables $y^{\nu,r}_{i_1,\ldots,i_{k-1}}$, $r = 1,\ldots,k+1$, for every variable $y^{\nu}_{i_1,\ldots,i_{k-1}}$. This results in the formula

$$G = \bigwedge_{\nu\in[m(k-1)]} \; \bigvee_{(i_1,\ldots,i_{k-1})\in[m(k-1)]^{k-1}} \; \bigoplus_{r=1}^{k+1} y^{\nu,r}_{i_1,\ldots,i_{k-1}} \tag{7}$$

which will be our $\big(\wedge\vee\oplus^{k+1}\big)$-block formula. Clearly, G contains $(k+1)\cdot(m(k-1))^k$ variables. We claim that the following easy modification of the k-DNF set from Figure 2 "precisely" implies G in the sense of Theorem 6:

$$W^j_m(\boldsymbol{x}^j) \qquad 1 \leq j < k \tag{8a}$$

$$\bigvee_{(i_1,\ldots,i_{k-1})\in[m(k-1)]^{k-1}} \left(x^1_{i_1} \wedge \cdots \wedge x^{k-1}_{i_{k-1}} \wedge y^{\nu,1}_{i_1,\ldots,i_{k-1}}\right) \qquad 1 \leq \nu \leq m(k-1) \tag{8b}$$

$$\bigvee_{(i_1,\ldots,i_{k-1})\in[m(k-1)]^{k-1}} \left(x^1_{i_1} \wedge \cdots \wedge x^{k-1}_{i_{k-1}} \wedge \overline{y}^{\nu,r}_{i_1,\ldots,i_{k-1}}\right) \qquad \begin{array}{c} 1 \leq \nu \leq m(k-1), \\ 2 \leq r \leq k+1 \end{array} \tag{8c}$$

It is straightforward to verify that $\mathbb{D}$ consists of less than $m(k-1)(k+1) + 2mk \leq mk(k+2)$ k-DNF formulas. $\mathbb{D}$ implies G since once we have picked which variables $x^1_{i^*_1}, x^2_{i^*_2}, \ldots, x^{k-1}_{i^*_{k-1}}$ should be satisfied, $\mathbb{D}$ will force all XOR blocks $\bigoplus_{r=1}^{k+1} y^{\nu,r}_{i^*_1,\ldots,i^*_{k-1}}$, $j \in [m(k-1)]$ to true by requiring the variable $y^{\nu,1}_{i^*_1,\ldots,i^*_{k-1}}$ to be true and all other variables $y^{\nu,r}_{i^*_1,\ldots,i^*_{k-1}}$, $r \geq 2$, to be false. Finally, it is also easy to verify that if a single XOR block $\bigoplus_{r=1}^{k+1} y^{\nu,r}_{i^*_1,\ldots,i^*_{k-1}}$ is removed from G, then we can satisfy $\mathbb{D}$ but falsify the rest of the formula G (the proof is very similar to the one given in Section 3.2). Theorem 7 follows.

5 Concluding Remarks and Open Problems

We conclude this paper by discussing two remaining open problems. First, the most obvious problem still open is to close the gap between the lower bound

$(\Omega(m))^k$ and upper bound $(mk)^{k+1}$ on the number of variables that can appear in a minimally unsatisfiable k-DNF set with m formulas. A strong intuition expressed by [10] is that it should be possible to bring down the exponent from $k+1$ to k. Hence, we have the following conjecture, where for simplicity we fix k to remove it from the asymptotic notation.

Conjecture 8. Suppose that $\mathbb{D}$ is a minimally unsatisfiable k-DNF set for some arbitrary but fixed $k > 1$. Then the number of variables in $\mathbb{D}$ is at most $\mathrm{O}(|\mathbb{D}|)^k$.

Proving this conjecture would establish asymptotically tight bounds for minimally unsatisfiable k-DNF sets (ignoring factors involving the constant k).

Second, we again stress that the result in Theorem 7 does not per se imply any restrictions (that we are aware of) on what space separations or time-space trade-offs are possible for k-DNF resolution. The reason for this is that our improved lower bound only rules out *a particular approach* for proving better separations and trade-offs, but it does not say anything to the effect that the k-DNF resolution proof systems are strong enough to match this lower bound. It would be very interesting to understand better the strength of k-DNF resolution in this respect. Hence we have the following open problem (where due to space constraints we have to refer to [10] or [17] for the relevant formal definitions).

Problem 9. Let $Peb_G^{k+1}[\oplus]$ be the XOR-pebbling contradiction over some directed acyclic graph G. Is it possible that $\mathfrak{R}(k)$ can refute $Peb_G^{k+1}[\oplus]$ in space asymptotically better than the black-white pebbling price $\mathsf{BW\text{-}Peb}(G)$ of G?

We remark that for standard resolution, i.e., 1-DNF resolution, the answer to this question is that XOR-pebbling contradictions over two or more variables *cannot* be refuted in space less than the black-white pebbling price, as proven in [10]. For k-DNF resolution with $k > 1$, however, the best known lower bound is $\Omega\left(\sqrt[k+1]{\mathsf{BW\text{-}Peb}(G)}\right)$, as also shown in [10]. There is a wide gap here between the upper and lower bounds since, as far as we are aware, there are no known k-DNF resolution proofs that can do better than space linear in the pebbling price (which is achievable by standard resolution).

Acknowledgements The authors would like to thank Eli Ben-Sasson for getting them to work together on this problem and for many stimulating discussions. We also gratefully acknowledge the *ICALP* anonymous reviewers, whose comments helped improve this manuscript considerably. The first author is grateful to Johan Håstad, Nati Linial, and Klas Markström for thoughtful comments and advice about the problem of minimally unsatisfiable k-DNF sets.

The first author did this work while at the Massachusetts Institute of Technology, supported by the Royal Swedish Academy of Sciences, the Ericsson Research Foundation, the Sweden-America Foundation, the Foundation Olle Engkvist Byggmästare, and the Foundation Blanceflor Boncompagni-Ludovisi, née Bildt. He is currently supported by Swedish Research Council grant 621-2010-4797.

The second author did part of this work while with Steklov Mathematical Institute, supported by the Russian Foundation for Basic Research, and with Toyota Technological Institute at Chicago.

References

[1] R. Aharoni and N. Linial. Minimal non-two-colorable hypergraphs and minimal unsatisfiable formulas. *J Comb. Theory*, 43:196–204, 1986.

[2] M. Alekhnovich. Lower bounds for k-DNF resolution on random 3-CNFs. In *Proc. 37th ACM Symposium on Theory of Computing*, pp. 251–256, 2005.

[3] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Space complexity in propositional calculus. *SICOMP*, 31(4):1184–1211, 2002.

[4] A. Atserias and M. L. Bonet. On the automatizability of resolution and related propositional proof systems. *Info. Comp*, 189(2):182–201, 2004.

[5] A. Atserias, M. L. Bonet, and J. L. Esteban. Lower bounds for the weak pigeonhole principle and random formulas beyond resolution. *Info. Comp*, 176(2):136–152, 2002.

[6] S. Baumer, J. L. Esteban, and J. Torán. Minimally unsatisfiable CNF formulas. *Bulletin of the EATCS*, 74:190–192, 2001.

[7] E. Ben-Sasson and N. Galesi. Space complexity of random formulae in resolution. *Rand. Struc. Alg.*, 23(1):92–109, 2003.

[8] E. Ben-Sasson and J. Nordström. Short proofs may be spacious: An optimal separation of space and length in resolution. In *Proc. 49th IEEE Symposium on Foundations of Computer Science*, pp. 709–718, 2008.

[9] E. Ben-Sasson and J. Nordström. A space hierarchy for k-DNF resolution. Technical Report TR09-047, Electronic Colloquium on Computational Complexity, 2009.

[10] E. Ben-Sasson and J. Nordström. Understanding space in proof complexity: Separations and trade-offs via substitutions. In *Proc. 2nd Symposium on Innovations in Computer Science*, pp. 401–416, 2011.

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

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

[13] J. L. Esteban, N. Galesi, and J. Messner. On the complexity of resolution with bounded conjunctions. *TCS*, 321(2-3):347–370, 2004.

[14] J. Krajíček. On the weak pigeonhole principle. *Fund. Math.*, 170(1-3):123–140, 2001.

[15] O. Kullmann. An application of matroid theory to the SAT problem. In *Proc. 15th IEEE Conference on Computational Complexity*, pp. 116–124, 2000.

[16] J. Nordström. Narrow proofs may be spacious: Separating space and width in resolution. *SICOMP*, 39(1):59–121, 2009.

[17] J. Nordström. Pebble games, proof complexity and time-space trade-offs. *Logical Methods in Computer Science*, 2011. To appear.

[18] J. Nordström and J. Håstad. Towards an optimal separation of space and length in resolution (Extended abstract). In *Proc. 40th ACM Symposium on Theory of Computing*, pp. 701–710, 2008.

[19] A. A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. Manuscript.

[20] N. Segerlind. Exponential separation between $\mathrm{Res}(k)$ and $\mathrm{Res}(k+1)$ for $k \leq \epsilon \log n$. *IPL*, 93(4):185–190, 2005.

[21] N. Segerlind, S. R. Buss, and R. Impagliazzo. A switching lemma for small restrictions and lower bounds for k-DNF resolution. *SICOMP*, 33(5):1171–1200, 2004.