Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 9 (2007)

Lower Bounds for OBDD-Based Proofs of Unsatisfiability and Symbolic Quantifier Elimination Algorithms*

Nathan Segerlind†

July 7, 2007

Abstract

We demonstrate a family of propositional formulas in conjunctive normal form so that a formula of size N requires size $2^{N^{\Omega(1)}}$ to refute using the tree-like OBDD refutation system of Atserias, Kolaitis and Vardi [3] with respect to all variable orderings. The lower bound generalizes earlier lower bounds on OBDD-based proofs of unsatisfiability in that it applies for all variable orderings, it applies when the clauses are processed according to an arbitrary schedule, and it applies when variables are eliminated via quantification. Current symbolic quantifier elimination algorithms for satisfiability generate tree-like proofs when run on unsatisfiable CNFs, so this lower bound applies to the run-times of these algorithms.

1 Introduction

Ordered binary decision diagrams (OBDDs) are data structures for representing Boolean functions [7, 8, 24] that are widely used when solving problems in circuit synthesis and model checking (cf. [7, 8, 23, 11]). A large number of OBDD-based algorithms have been implemented for solving the Boolean satisfiability problem [7, 32, 14, 9, 10, 1, 26, 25, 2, 12, 28, 16, 3, 18]. Several of these algorithms efficiently generate proofs of unsatisfiability for CNFs known to require exponential running times for resolution based methods (such as the $n+1$ to n pigeonhole principle). Moreover, OBDD proof systems can p-simulate several proof systems, such as resolution, unary cutting planes, and Gaussian refutations [3]. Given that they can do so much, what are the limitations of OBDD-based satisfiability algorithms?

In this paper, we present unsatisfiable CNFs and prove exponential size lower bounds for tree-like OBDD refutations of these CNFs. This implies run time lower bounds for satisfiability algorithms based on explicit OBDD construction and symbolic quantifier elimination.

An OBDD is a read-once branching program in which the variables appear according to a fixed order along every path (ie. the nodes are arranged in levels, all nodes at a level query the same variable, and each variable corresponds to at most one level) [7, 8, 24]. The ordering restriction enforces canonicity: For each fixed ordering, the OBDD computing a Boolean function is unique up to a linear-time computable normal form (cf. [24]). Because of this canonicity property, the equality test for two Boolean functions represented as OBDDs is simply a check that their OBDDs are identical. However, the choice of variable ordering can affect the size of the OBDD by an exponential factor and choosing a suitable variable ordering for a task is of utmost importance.

*Preliminary version available as ECCC-TR07-009

†Department of Computer Science, P. O. Box 751, Portland State University, Portland, Oregon, 97207, USA, nsegerli@cs.pdx.edu

ISSN 1433-8092

The results of this paper apply to two classes of OBDD-based satisfiability algorithms, explicit construction and symbolic quantifier elimination.

Explicit construction. In the literature, this is sometimes called the "OBDD apply" method. In this method, a variable ordering is selected, the OBDD for the CNF with respect to that ordering is constructed, and it is checked whether this OBDD is the constant false [7]. There are two opportunities for cleverness - the variable ordering used to construct the OBDDs, and the order in which the clauses are joined together, cf. [32, 1, 16]. Empirical studies [32, 12] and a mathematical analysis of the implementation in which the clauses are conjoined in the same order as the input presentation [15] have suggested that this method is incomparable with resolution.

Symbolic quantifier elimination. This method extends the explicit construction method by strategically eliminating variables via the application of existential quantifiers [14, 1, 28, 16, 31]. To determine if a CNF $\bigwedge_{i=1}^{m} C_i(\vec{x})$ is satisfiable, rather than build an OBDD for $\bigwedge_{i=1}^{m} C_i(\vec{x})$, it suffices to build one for $\exists \vec{x} \bigwedge_{i=1}^{m} C_i(\vec{x})$. This is can be more efficient because it is often the case that the OBDD for $\exists \vec{x} F(\vec{x}, \vec{y})$ are significantly smaller than the OBDD for $F(\vec{x}, \vec{y})$. One example of this approach is to first heuristically partition the variables into sets $X_1, \ldots X_k$ and the clauses into sets $A_1, \ldots A_k$ so that for each $i = 1, \ldots k$, the variables of X_i do not appear in the clauses belonging to sets $A_{i+1}, \ldots A_k$, then construct the OBDD for the quantified Boolean formula:

$$\exists X_k \left(\ldots \left(\exists X_2 \left(\exists X_1 \bigwedge_{C \in A_1} C(X_1, \ldots X_k) \right) \wedge \bigwedge_{C \in A_2} C(X_2, \ldots X_k) \right) \ldots \right) \wedge \bigwedge_{C \in A_k} C(X_k)$$

It has been observed that symbolic quantifier elimination leads to significant speed-ups over explicit OBDD construction on random 3-CNFs [14, 1], and that, on a certain mix of structured benchmarks, symbolic quantifier elimination solves more instances before time-out than solvers based on resolution or compressed resolution [16, 28].

When formalized as proof systems, these algorithms can be viewed as treelike versions of the OBDD propositional proof system described by Atserias, Kolaitis and Vardi [3]. This proof system is highly non-trivial: OBDDs are circuits not formulas, so this proof system is a kind of weak extended-Frege system[1]. Because it is not believed possible to convert OBDDs into formulas without an exponential blow-up, the OBDD proof system is not expected to be p-simulatable by Frege systems. The tree-like OBDD system possesses polynomial-size refutations of the $n+1$ to n pigeonhole principle, and it can p-simulate several interesting proof systems, such as tree-like resolution, Gaussian refutations over a finite field, and tree-like cutting planes refutations with unary coefficients [3].

The result and comparisons with earlier work. The main result of this paper is that for infinitely many values of N, there is an unsatisfiable CNF Φ of size N so that every tree-like OBDD refutation of Φ has size at least $2^{\Omega(\sqrt[7]{N/\log N})}$ (Theorem 12). This lower bound generalizes earlier work on proving size lower bounds for OBDD-based proofs of unsatisfiability in three ways: The proofs can use variable elimination via existential quantifiers, the clauses of the input CNF can be processed in any order (so long as they are recombined according to a tree-structure), and the variable ordering of the OBDDs can be arbitrary. The two previously published results regarding size lower bounds for OBDD-proofs of unsatisfiability either make use of a restriction on the order in which the clauses are processed, or hold only for a fixed ordering on the variables.

[1]Informally, Frege systems are the standard axiom-and-inference-rule style systems of propositional logic manipulating Boolean formulas whereas extended Frege systems manipulate Boolean circuits. From a computational complexity perspective, Frege systems can be thought of as working with concepts definable in NC^1 and extended Frege systems can be thought of as working with concepts definable in P. Cf. [13, 20].

In [15], Groote and Zantema prove a size lower bound for refutations in the OBDD-apply system that conjoins the clauses of the CNF in the order of the input listing (ie. to process $C_1 \wedge (C_2 \wedge C_3)$, an OBDD for $C_2 \wedge C_3$ is built and then one for $C_1 \wedge (C_2 \wedge C_3)$ is built). In fact, in that paper they give a size lower bound for refutations of a formula of the form $\neg x \wedge (x \wedge \psi)$, which is trivial to refute if the formula is processed as $(\neg x \wedge x) \wedge \psi$. Qualitatively, Theorem 12 generalizes their bound by allowing the clauses to be processed in an arbitrary order, and also by applying to systems that eliminate variables by quantification. However, their bound is quantitatively stronger: Where N is the size of the difficult CNF, their bound on refutation size is $2^{\Omega(\sqrt{N})}$ whereas ours is $2^{\Omega(\sqrt[7]{N/\log N})}$.

In [3], Atserias, Kolaitis, and Vardi formalized the OBDD-based propositional proof system incorporating symbolic quantifier elimination, and proved that for each fixed variable ordering, there is a CNF of size N that requires size $2^{N^{\Omega(1)}}$ to refute in the OBDD proof system using that particular variable ordering. The bounds of [3] and Theorem 12 are incomparable: The bound of [3] applies to the DAG like system as well the tree-like system whereas Theorem 12 only applies to the tree-like system, on the other hand, the lower bound of Theorem 12 holds for all variable orderings. The problem of proving a lower bound that holds for all variable orderings was stated as an open problem in [3], and Theorem 12 is a solution to this problem for the tree-like case.

All implementations of OBDD-based satisfiability algorithms known to the author [14, 1, 28, 16, 31] generate proofs of unsatisfiability in the tree-like OBDD system. Moreover, the results of [15] do not apply to these algorithms as typically there is a preprocessing analysis that chooses the order in which clauses are combined, and many of the algorithms incorporate symbolic quantifier elimination. The results of [3] do not apply to these algorithms because the variable ordering is typically selected by some static analysis of the input CNF.

The technique and its comparison with earlier work. The proof is a reduction: We produce a CNF so that if there is a small refutation of the CNF in the tree-like OBDD proof system, then there is a low-communication randomized two-player protocol for the set-disjointness function. The set-disjointness function has linear communication complexity [19, 30], so all refutations of this CNF must be large. The reduction is obtained by the interpolation by a communication game technique that has been well-used in the propositional proof complexity community for some time now [17, 5, 3]. However, accounting for all possible variable orderings for the OBDDs corresponds to proving communication lower bounds that hold for the best-case partition model.

The reductions of [29, 17, 3] construct a search problem in variables $\vec{U}$ and $\vec{V}$, $Search(\vec{U}, \vec{V})$, and a randomized one-sided-error reduction from set-disjointness (in variables $\vec{X}$ and $\vec{Y}$) to $Search(\vec{U}, \vec{V})$ in which player I creates an assignment to $\vec{U}$ using $\vec{X}$ and player II creates an assignment to $\vec{V}$ using $\vec{Y}$. These reductions make heavy use of the structure in the fixed partition of the variables into $\vec{U}$ and $\vec{V}$. In the best-case partition scenario that our reduction handles, we provide a search problem $Search(\vec{W})$ and show that no matter how the variables of $\vec{W}$ are partitioned into two equal-sized sets $\vec{U}$ and $\vec{V}$, there is a reduction from set-disjointness to the search problem in which player I to creates an assignment to $\vec{U}$ using $\vec{X}$ and player II to creates an assignment to $\vec{V}$ using $\vec{Y}$.

The technical heart of the analysis is a problem of the following form: Let n and m with $m = cn$ for some constant c be given, and let $E_1, \ldots E_m$ be subsets of sets of edges over vertex set $[n]$ and let $V_1, \ldots V_m$ be subsets of $[n]$ so that $\sum_{i=1}^{m} \sum_{j=1}^{m} |E_i[V_j]| = \alpha m^2 \binom{n}{2}$ for some constant $\alpha > 0$. Let T be the set of all $3t$-tuples $(i_1, \ldots i_t, j_1, \ldots j_t, X_1, \ldots X_t)$ where each X_k is a copy of $K_{1,2}$ in $E_{i_k}[V_{j_k}]$, the i_k's are distinct, the j_k's are distinct, and distinct X_k's share no vertices. How can we construct a distribution μ on T so that:

1. For all $(\vec{i}, \vec{j}, \vec{X})$ and $(\vec{k}, \vec{l}, \vec{Y})$ in the support of μ that differ in $O(1)$ many positions, $\mu(\vec{i}, \vec{j}, \vec{X}) = (1 \pm O(1))\mu(\vec{k}, \vec{l}, \vec{Y})$.

2. For every $k, l \in [t]$, the probability over μ that the vertices of $V(X_k) \cup V(X_l)$ induce a copy of $K_{2,4}$ in $E_{i_k}[V_{j_k}] \cap E_{i_l}[V_{i_l}]$ is at least $\Theta(1)$.

The desired range for the parameter t is $t = \gamma n$, where γ is constant we can solve for based on c,α and large enough n.

A natural first try is to take μ to be the uniform distribution on T and thereby get Property 1 for free. If the marginal distribution on (i_k, i_l, j_k, j_l) were close to uniform, so that $|E_{i_k}[V_{j_k}] \cap E_{i_l}[V_{j_l}]|$ has constant density with constant probability, and if conditioned on that event, the marginal distribution on X_k and X_l were close to uniform, we could appeal to convexity. However, the dependencies are legion, and it seems quite difficult to show that Property 2 holds for the uniform distribution on T (if it holds at all). Moreover, the gadgets used in the reduction are more complicated than this example and encounter even more dependencies. So we resort to an alternative distribution with enough local independence to guarantee Property 2, but not so much as to lose Property 1. In Section 10 we set up some simple and general sufficient conditions for distributions to satisfy properties like Properties 1 and 2. We then show in Section 11 that the randomized reduction (defined in Section 9) satisfies the sufficient conditions.

Future work. There are some natural "next step" questions to ask: Establishing lower bounds for random 3-CNFs, and separating the DAG-like system from the tree-like system. As to whether or not the unrestricted (DAG-like) OBDD system is polynomially bounded, shortly after this paper was released on the proof complexity mailing list, Jan Krajíček released an independently produced proof of a $2^{N^{\Omega(1)}}$ size lower bound for DAG-like OBDD refutations of a different family of unsatisfiable CNFs [21]. The techniques of Theorem 12 do not apply to the CNFs studied in his paper, nor do his techniques apply to the CNFs of Theorem 12.

Empirically, symbolic quantifier algorithms seem to be incomparable with resolution based sat solvers such as zChaff [28, 16]. Theoretically, however OBDD refutations can p-simulate resolution [3]. It seems that a significant factor in this gap may be that the symbolic quantifier elimination algorithms are building tree-like proofs whereas clause learning algorithms like zChaff build DAG-like resolution proofs (cf. [4]). It would be interesting both to implement an effective SAT solver that constructs DAG-like OBDD refutations, and also to prove that tree-like OBDD refutations cannot p-simulate DAG-like resolution.

Other possible extensions would be to extend the analysis to cover OBDD-based algorithms that incorporate a dynamic variable reordering package[2], and to provide an analysis for the so-called compressed methods [9, 10, 25, 26, 27] that perform a basic DLL or Davis-Putnam search and represent the clause database as an OBDD. These systems build OBDDs in different variables than those of the input CNF, and therefore Theorem 12 cannot be directly applied to these systems.

Thanks. To Albert Atserias and Moshe Vardi for interesting conversations at the at the Workshop on New Directions in Proof Complexity held at the Isaac Newton Institute for Mathematics. To Jan Krajíček, for securing the author's attendance to said workshop. To Jan Friso Groote for answering some questions about [15]. To Paul Beame for useful comments on an early draft of this paper. To Cindy Brown and Barton Massey of Portland State University for generous hospitality.

[2]In principle, dynamic reordering of OBDD variables should improve running times. However, current work with symbolic quantifier elimination algorithms for satisfiability has suggested that static variable orderings lead to better performance than dynamic variable orderings [1, 16]. Regardless, Theorem 12 does not apply to systems using dynamic variable reordering.

2 Notation and background

Definition 2.1 *The real numbers are denoted by* $\mathbb{R}$ *and* $[0,1]$ *denotes the closed unit interval. Let* n *be an integer. The set of integers* $\{1,\dots n\}$ *is denoted by* $[n]$*. For a set* S *and a non-negative integer* k*, the set of all* k*-tuples over* S *is denoted by* S^k *and the of all size* k *subsets of* S *is denoted by* $\binom{S}{k}$*. For a set* S *we let* χ_S *denote the indicator function for* S *with* $\chi_S(a) = 1$ *if* $a \in S$*,* $\chi_S(a) = 0$ *is* $a \notin S$*. The domain of* χ_S *will always clear from context. For a Cartesian product* $\prod_{i\in I} X_i$ *where* I *is a finite set, we say that the product is "*$|I|$ *dimensional" even though is no ector space structure defined on* $\prod_{i\in I} X_i$*. We write* X_I *as an abbreviation for the product* $\prod_{i\in I} X_i$*. Let* $\prod_{i\in I} X_i$ *and* $\prod_{j\in J} X_j$ *be a Cartesian product with* $I \cap J = \emptyset$*. For* $\vec{x} \in \prod_{i\in I} X_i$ *and* $\vec{y} \in \prod_{i\in J} X_i$ *we write* $\vec{x}\vec{y}$ *to denote the concatenation of* $\vec{x}$ *and* $\vec{y}$ *(an element of* $\prod_{i\in I\cup J} X_i$*). We use the same indices for elements in tuples as we do for the factors of the product, ie. for* $\vec{u} \in \prod_{i=j}^{t} X_i$*, we write* $\vec{u} = (u_j, \dots u_t)$*, we* do not *write* $\vec{u} = (u_1, \dots u_{t-j+1})$*. Let* f *be a function whose domain is a Cartesian product* $\prod_{i=1}^{t} X_i$*. For each* $j \in [t]$*, for each* $\vec{x} \in \prod_{i=1}^{j} X_i$*, we write* $f^{\vec{x}}$ *to denote the Curried function with domain* $\prod_{i=j+1}^{t} X_i$ *and* $f^{\vec{x}}(\vec{y}) = f(\vec{x}\vec{y})$*. Similarly, for* $A \subseteq \prod_{i=1}^{t} X_i$*,* $A^{\vec{x}} = \{\vec{y} \mid \vec{x}\vec{y} \in A\}$*. Let* $f : \prod_{i\in I} X_i \to R$*. We say that* f depends on a coordinate i*, with* $i \in I$*, if there exists* $\vec{x}, \vec{y} \in \prod_{i\in I} X_i$ *with* $x_j = y_j$ *for all* $j \in I \setminus \{i\}$*,* $x_i \neq y_i$*, and* $f(\vec{x}) \neq f(\vec{y})$*. If* f *depends on the coordinate* i*, we say that* i affects f*.*

Definition 2.2 *We use the word "graph" to mean a simple, loopless undirected graph. We use* $\subseteq$ *to denote the (not necessarily induced) subgraph relation, ie.* $G \subseteq H$ *if* $G = (V, E)$ *and* $H = (W, F)$ *with* $V \subseteq W$ *and* $E \subseteq F$ *(as sets). For any two disjoint nonempty sets* A *and* B*, we write* $K(A, B)$ *to denote the complete bipartite graph with partition* $\{A, B\}$*. Let* $G = (V, E)$ *be a graph. Let* $V_0 \subseteq V$ *and let* $E_0 \subseteq E$*. The set of edges* E_0 restricted to V_0*, written* $E_0[V_0]$*, is defined as* $E_0[V_0] = \{e \in E_0 \mid e \subseteq V_0\}$*.*

Definition 2.3 *Let* E *be a set of unordered pairs over* X*, and define* $\mathcal{K}_{1,2}(E) := \{(u, v, w) \in X^3 \mid v \neq w,\ \{u, v\} \in E,\ \{u, w\} \in E\}$*. Let* X *be a set. For* $U \subseteq X$ *define* $pm_X(U) : \{(u, v) \in X^2 \mid \{u, v\} \cap U \neq \emptyset\}$ *and* $tm_X(U) := \{(u, v, w) \in X^3 \mid \{u, v, w\} \cap U \neq \emptyset\}$*. (The mnemonic for this notation is "pairs over* X *that meet* U*" and "triples over* X *that meet* U*".)*

2.1 Probability notation

Definition 2.4 *Let* η *be a probability distribution over a set* X *and let* $f : X \to \mathbb{R}$*. We write* $\mathbb{E}_\eta[f]$ *to denote the expectation of* f *with respect to* η*. At times, the uniform distribution over a set will be written as* U*. Other times, we will write with* $E \subseteq S$*, we will write* $Pr_{x\in S}[E]$ *to denote the probability that* $x \in E$ *holds when* x *is selected uniformly from* S*.*

Definition 2.5 *Let* η *be a probability distribution on a Cartesian product* $\prod_{i=1}^{t} X_i$*. For each* $I \subseteq [t]$*, let* η_I *be the marginal distribution of* η *on* $\prod_{i\in I} X_i$*. For each* $j \in [t]$ *and each* $\vec{x} \in \prod_{i=1}^{j} X_i$*, let* $\eta^{\vec{x}}$ *be the probability distribution on* $\prod_{i=j}^{t} X_i$ *given by the formula* $\eta^{\vec{x}}(\vec{y}) = \frac{\eta(\vec{x}\vec{y})}{\eta_{[j]}(\vec{x})}$ *if* $\eta_{[j]}(\vec{x}) \neq 0$ *and* 0 *otherwise.*

Notice that $\eta^{\vec{x}}$ is the marginal distribution of η to the coordinates $[t] \setminus [j]$ conditioned on the event that the first j coordinates take the value $\vec{y}$. An immediate consequence of the definitions:

Lemma 1 *Let* $f : \prod_{i=1}^{t} X_i \to \mathbb{R}$*, let* $I = \{1, \dots i_0\}$*:* $\mathbb{E}_\eta[f] = \sum_{\vec{u}\in X_I} \eta_I(\vec{u}) \mathbb{E}_{\eta^{\vec{u}}}[f^{\vec{u}}]$

Unsurprisingly for a technique based on finding structure in a dense family of sets, we beat the stuffing out Jensen's Inequality and any averaging arguments that we find in the neighborhood.

Proposition:(Jensen's Inequality) Let $f : D \to \mathbb{R}$, let $g : \mathbb{R} \to \mathbb{R}$ be a convex function, and let η be a probability distribution on D. $\mathbb{E}_\eta[g \circ f] \geq g(\mathbb{E}_\eta[f])$.

Lemma 2 *(Proof in Appendix Section A.) Let X be a finite set, and let $Y_1, \ldots Y_n$ be a family of subsets of X. Set $\alpha = \frac{1}{n}\sum_{i=1}^{n} |Y_i|/|X|$, and let k be a non-negative integer: $\frac{1}{n^k}\sum_{\vec{i}\in[n]^k} |\bigcap_{l=1}^{k} Y_{i_l}| \geq \alpha^k |X|$.*

Lemma 3 *(Proof in Appendix Section A.) There exists a constant $c > 0$ so that for every undirected graph $G = (V, E)$ with $|V| = N$ and $|E| \geq \alpha\binom{N}{2}$. We have that:*

$$\begin{array}{lcl} Pr_{\vec{u}\in V^3}[K(\{u_1\},\{u_2,u_3\}) \subseteq G] & \geq & \alpha^2 - (5/N) \\ Pr_{\vec{u}\in V^6}[K(\{u_1,u_2\},\{u_3,u_4,u_5,u_6\}) \subseteq G] & \geq & \alpha^8 - (23/N) \end{array}$$

Proposition: Let η be a probability measure on a space X, and let $f : X \to [0, 1]$ be measurable. For all $\epsilon \in [0, 1]$ and all $c > 0$ $\eta(\{x \mid f(x) \geq \frac{1}{c}\mathbb{E}_\eta[f]\}) \geq (1 - 1/c)\mathbb{E}_\eta[f]$.

Lemma 4 *Let X be a probability space with probability μ and let $f : X \to [0, 1]$. Let $\epsilon, \gamma \in [0, 1]$ be given. If $\mu(f^{-1}((\gamma, 1])) < \epsilon$ then $\mathbb{E}_\mu[f] < \epsilon + \gamma$.*

3 OBDDs, proofs and communication protocols

Definition 3.1 *(cf. [8, 24]) A* binary decision diagram *(also known as a* branching program*) is a rooted, directed acyclic graph in which every nonterminal node u labeled by a variable x_u and has two out-arcs, one two a node t_u and the other to a node f_u. Sinks are labeled by Boolean values. The function represented by a branching program is calculated by starting at the root and following a path to the sink as follows: If the current node u is labeled by the variable x_u, and x_u is assigned the value true, then follow the arc t_u, otherwise follow the arc labeled f_u. The value that the function takes is the value labeled on the sink. The* size *of a binary decision diagram is its number of nodes as a DAG. An* ordered binary decision diagram (OBDD) *is a binary decision diagram in which: Along every path from the source to a sink, every variable is queried at most once, and, there is fixed ordering so that along all paths from the source to a sink, the variables are queried consistently with that order.*

Definition 3.2 *Let $\mathcal{C}$ be a set of clauses in variables from a set V. A* OBDD derivation from $\mathcal{C}$ with respect to a variable ordering $\preceq$ on V *is a sequence of OBDDs $F_1, \ldots, F_m$ so that each OBDD is built from the variables of V with respect to the order $\preceq$, and each F_i either is a clause in $\mathcal{C}$, or follows from the preceding $F_1, \ldots F_{i-1}$ by an application of one of the following inference rules: (A, A_0, and B are OBDDs in the variables V with ordering $\preceq$, where $A \Rightarrow A_0$ as Boolean functions, and $\vec{x}$, $\vec{y}$, $\vec{z}$ are tuples of variables from V):*

$$\textit{Subsumption: } \frac{A}{A_0} \qquad \textit{Conjunction: } \frac{A(\vec{x},\vec{y}) \quad B(\vec{y},\vec{z})}{A(\vec{x},\vec{y}) \wedge B(\vec{y},\vec{z})} \qquad \textit{Projection: } \frac{A(x,\vec{y})}{\exists x A(x,\vec{y})}$$

For a set of clauses $\mathcal{C}$, an OBDD refutation of $\mathcal{C}$ *is a derivation from $\mathcal{C}$ whose final line is the OBDD "false". The size of an OBDD refutation is the sum of the sizes of its OBDDs. An OBDD derivation $F_1, \ldots F_m$ is said to be* treelike *if each F_i is used at most once as an antecedent to an inference.*

The projection rule is a special case of the subsumption rule, however, the projection rule is the one most used in satisfiability algorithms.

We make use of a well-known bound on the randomized two-party communication complexity of the set-disjointness function. For more on communication complexity see [22].

Definition 3.3 *Let $f(\vec{X},\vec{Y})$ be a function. A* randomized two-player protocol for *f is a two-party communication protocol in which Player I has private access to $\vec{X}$, Player II has private access to $\vec{Y}$, and the players share access to a source of random bits, so that for all inputs $\vec{X}$ and $\vec{Y}$, with probability at least $2/3$, the players agree upon the correct value of $f(\vec{X},\vec{Y})$. A* deterministic protocol *is one in which the answer arrived at by the players is independent of any randomness and is uniquely determined by the input $\vec{X},\vec{Y}$. The* cost of a protocol *is the maximum number of bits communicated between the two players taken over settings of the input and the random bits. The* randomized communication complexity of *f is the minimum cost of a randomized two-player protocol that computes f. The* set-disjointness function on *n* bits *is a Boolean function $setdisj_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with*

$$setdisj(\vec{X},\vec{Y}) = \begin{cases} 1 & \text{if } \exists i \in [n],\ X_i = Y_i = 1 \\ 0 & \text{otherwise} \end{cases}$$

Theorem 5 *([19, 30], cf. [22]) The two-party randomized communication complexity of $setdisj_n$ is $\Omega(n)$.*

All that is actually used about OBDDs is a simple connection between OBDDs and communication complexity that is the starting point for the reduction. We do not use it explicitly in this article, however, it is an ingredient for the proof of Lemma 8 which appears in [3].

Proposition: If there is size S OBDD for a function $f(x_1,\ldots x_n)$ with respect to the variable order $x_{i_1},\ldots x_{i_n}$, then for each $k \in [n]$, there is a two-party communication protocol computing f with respect to the variable partition $\{x_{i_1},\ldots x_{i_k}\},\{x_{i_k+1},\ldots x_{i_n}\}$ that uses $\lceil \log S \rceil$ many bits of communication.

4 The difficult CNFs: Indirect matching principles

The CNF $IndMatch_m$ is a propositional encoding of the fact that in a graph on $3m$ vertices, it is impossible to simultaneously have a perfect matching on $2m$ vertices and an independent set of size $2m+1$. It is similar to CNF $Match_m$ used by Impagliazzo, Pitassi, and Urquhart to prove size lower bounds for the tree-like cutting planes system [17]. However, in order to prove the CNFs difficult for tree-like OBDD refutations with respect to any variable ordering, we introduce a level of indirection via permutations. There are two kinds of variables used in the CNF $Match_m$:

1. *The edge variables.* There are $m \cdot \binom{3m}{2}$ many variables used to specify the matching: One variable x_e^i for each $i = 1,\ldots m$ and each $e \in \binom{[3m]}{2}$. The intended semantics is that the variable x_e^i is equal to one if and only if the edge e is the i'th edge of the matching.

2. *The vertex variables.* There are $(2m+1)3m = 6m^2+3m$ many variables used to specify the independent set: One variable y_u^j for each $j = 1,\ldots 2m+1$ and each $u \in [3m]$. The intended semantics is that the variable y_k^j is equal to one if and only if the vertex u is the j'th element of the independent set.

The set of all these variables is $MVars_m$. The following clauses form the CNF $Match_m$:

1. (At least m edges in the matching.) For each $i \in [m]$: $\bigvee_{e \in \binom{[3m]}{2}} x_e^i$
2. (Edges form a matching.) For each $i, j \in [2m]$ with $i \neq j$ and each $e, f \in \binom{[3m]}{2}$ with $e \cap f \neq \emptyset$: $\neg x_e^i \vee \neg x_f^j$
3. (At least $2m+1$ vertices in the independent set.) For each $j \in [2m+1]$: $\bigvee_{u \in [3m]} y_u^j$
4. (Vertices in the independent set are distinct.) For each $i, j \in [2m+1]$ with $i \neq j$ and each $u \in [3m]$: $\neg y_u^i \vee \neg y_u^j$
5. (The vertices are independent.) For each $e \in \binom{[3m]}{2}$ with $e = \{u, v\}$, each $k \in [m]$ and each $i, j \in [2m+1]$: $\neg y_u^i \vee \neg y_v^j \vee \neg x_e^k$

Notice that the CNF $Match_m$ has size $O(m^5)$.

The difference between the CNF $IndMatch_m$ and the CNF $Match_m$ is that we add variables specifying a permutation π, and for an assignment A to $MVars_m$, we interpret the independent set not as $\{u \mid \exists j \in [2m+1],\ A(y_u^j) = 1\}$ but instead as $\{\pi(u) \mid \exists j \in [2m+1],\ A(y_u^j) = 1\}$.

Definition 4.1 *Let N be given. A set Π of permutations of N is said to be* pairwise *independent if for all $a, b, c, d \in [N]$ with $a \neq b$ and $c \neq d$: $Pr_{\pi \in \Pi}[\pi(a) = c \ \wedge \ \pi(b) = d] = \frac{1}{N(N-1)}$.*

It is well-known that for any finite field, the set of mappings $\{x \mapsto ax + b \mid a \in \mathbb{F}^*,\ b \in \mathbb{F}\}$ is a pairwise independent family of permutations of size $|\mathbb{F}|(|\mathbb{F}| - 1)$.

Proposition: Whenever m is a power of 3, there is a pairwise-independent family of permutations for $[3m]$, Π_m, with $|\Pi_m| = 9m^2 - 3m$.

The variables used in the CNF $IndMatch_m$ are the variables used in $Match_m$, along with new variables for encoding a permutation: There are $l = \lceil \log(|\Pi|) \rceil$ many variables that encode a permutation from Π: $z_1, \ldots z_l$. The the variables $z_1, \ldots z_l$ encode the permutations of Π in some surjective fashion. This set of permutation variables is denoted $PVars_m$. The set of variables $IMVars_m$ is $MVars_m \cup PVars_m$. The CNF $IndMatch_m$ has the same clauses of type 1, type 2, type 3 and type 4 that $Match_m$ has, whereas the clauses enforcing independence are as follows:

(Independence between vertices after application of the permutation.) For each $\alpha_1, \ldots \alpha_l \in \{0, 1\}$, each $e \in \binom{[3m]}{2}$ with $e = \{u, v\}$, each $k \in [m]$ and each $i, j \in [2m+1]$, with π denoting the element of Π encoded by $\vec{\alpha}$: $\bigvee_{i=1}^{L} z_i^{1-\alpha_i} \vee \neg y_{\pi(u)}^i \vee \neg y_{\pi(v)}^j \vee \neg x_e^k$

Notice that the CNF $IndMatch_m$ has $O(m^7)$ many clauses, and size $O(m^7 \log m)$.

Definition 4.2 *Let π be a permutation of $[3m]$. For each variable $v \in MVars_m$ we define*

$$\pi(v) = \begin{cases} y_{\pi(u)}^j & \text{if } v = y_u^j \text{ for some } j \in [2m+1],\ u \in [3m] \\ x_e^i & \text{if } v = x_e^i \text{ for some } i \in [m],\ e \in \binom{[3m]}{2} \end{cases}$$

Lemma 6 *Let Γ be a refutation of $IndMatch_m$, with variable ordering $v_1, \ldots v_N$. For every $\pi \in \Pi$, there is a size at most $|\Gamma|$ refutation of $Match_m$ that uses the variable ordering $\pi(v_1), \ldots \pi(v_N)$.*

Proof: Let α be the assignment to $\vec{z}$ that selects the permutation π^{-1}. We apply the restriction α to Γ, and we see that the clauses of $IndMatch_m$ that that are not satisfied are the non-independence

clauses that do not use any $\vec{z}$ variables (ie. all clauses of type 1, type 2, type 3, and type 4), and the independence clauses of the form $\neg y^i_{\pi^{-1}(u)} \vee \neg y^j_{\pi^{-1}(v)} \vee \neg x^k_e$, for $i, j \in [2m+1]$, $u, v \in [3m]$, $k \in [m]$, and $e \in \binom{[3m]}{2}$. Within each OBDD of the refutation, each query to y^i_u is replaced by a query to $y^i_{\pi(u)}$. This means that y^i_u takes the place of $y^i_{\pi(u)}$ in the ordering.

Every OBDD is now constructed according to the query order $\pi(v_1), \ldots \pi(v_N)$. It is easily checked that the proof structure is preserved under this substitution so that the new derivation is a derivation with respect to the order $\pi(v_1), \ldots \pi(v_N)$ in the sense of Definition 3.2. Moreover, each clause $\neg y^i_{\pi^{-1}(u)} \vee \neg y^j_{\pi^{-1}(v)} \vee \neg x^k_e$, becomes $\neg y^i_u \vee \neg y^j_v \vee \neg x^k_e$, so that the new refutation is a refutation of $Match_m$. ∎

5 Variable partitions and their densities

The proof of Theorem 12 has two steps. A small refutation of $IndMatch_m$ with an arbitrary ordering of the variables $IMVars_m$ is used to construct a low-communication protocol for the false clause search associated with $Match_m$ - with respect to a "dense" partition of the variables $MVars_m$ between the two players. Set-disjointness is then shown to reduce to the false clause search for $Match_m$- whenever $MVars_m$ are partitioned in a dense enough fashion.

We view the partition of $MVars_m$ as splitting the players into an *edge player*, with access to variables in $\mathcal{V}_I$, and a *vertex player*, with access to variables in $\mathcal{V}_{II}$. In the reduction, the edge player will place his set disjointness variables X_l on edge variables x^i_e and the vertex player will place his set-disjointness variables Y_l on vertex variables y^j_u.

Definition 5.1 *Let m be a positive integer, and let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$. For each $i = 1, \ldots m$, define $E_i(\mathcal{V}_I)$ to be $\{e \in \binom{[3m]}{2} \mid x^i_e \in \mathcal{V}_I\}$. For each $j = 1, \ldots 2m+1$, define $V_j(\mathcal{V}_{II})$ to be $\{u \in [3m] \mid y^j_u \in \mathcal{V}_{II}\}$. Except for Lemma 9, we will not discuss more than one variable partition at a time, so we usually write E_i instead of $E_i(\mathcal{V}_I)$ and V_j instead of $V_j(\mathcal{V}_{II})$.*

An important complication is that for distinct $i_1, i_2 \in [m]$, it is possible that $E_{i_1} \neq E_{i_2}$. This means that not only does the edge used in assignment matter, but the identity of the variable specifying the edge matters as well. Similarly, it is possible that $V_{j_1} \neq V_{j_2}$, so that identity of the variable used to specify a vertex matters. Because the identity of the variables matters, in contrast with the reduction of [29], we treat the objects seen by the players as assignments to the variables, not merely sets of vertices and edges.

Definition 5.2 *Let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$. The* density of $(\mathcal{V}_I, \mathcal{V}_{II})$, $\delta(\mathcal{V}_I, \mathcal{V}_{II})$, *is defined as follows:*

$$\delta(\mathcal{V}_I, \mathcal{V}_{II}) := \frac{1}{m^2(2m+1)^5} \sum_{\vec{i} \in [m]^2} \sum_{\vec{j} \in [2m+1]^5} \frac{\left| \bigcap_{k=1}^5 E_{i_1}[V_{j_k}] \cap E_{i_2}[V_{j_k}] \right|}{\binom{3m}{2}}$$

6 From Refutation to Search

We transform small refutations of the $IndMatch_m$ principles into a low-communication protocol for a search problem in the variables $Mvars_m$.

Definition 6.1 *Let A be an assignment to $MVars_m$. We say that A is* non-degenerate *if it satisfies all of the clauses from $Match_m$ of type 1, type 2, type 3, and type 4. (Informally, this means that*

the assignment selects m distinct edges and $2m+1$ distinct vertices.) An edge $e \in \binom{[3m]}{2}$ is said to be bad for A *if $e = \{u, v\}$ and there exist $i, j \in [2m+1], k \in [m]$ with $A(y_u^i) = 1$, $A(y_v^j) = 1$, and $A(x_e^k) = 1$.*

Proposition: If A is non-degenerate then there exists an edge that is bad for A.

Definition 6.2 *Let m be a positive integer, and let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$. The search problem $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ is defined as follows:*

1. *Player I has private access to the variables of $\mathcal{V}_I$.*
2. *Player II has private access to the variables of $\mathcal{V}_{II}$.*
3. *Given a non-degenerate assignment A to $MVars_m$, the players must find a bad edge of A.*

Lemma 7 *There a exists a constant $c > 0$ so that for all $m \geq 84651$, if there is a size S tree-like OBDD refutation of $IndMatch_m$ then there is a partition $(\mathcal{V}_I, \mathcal{V}_{II})$ of $MVars_m$ so that $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq 2^{-13}$ and there exists a deterministic two-player protocol for the search problem $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ that uses at most $c \log S$ many bits of communication.*

The proof of Lemma 7 follows from combining the following to lemmas. To prove Lemma 7, simply take the partition of $MVars_m$ and the size S refutation of $Match_m$ guaranteed by Lemma 9 and feed them into Lemma 8.

Lemma 8 *(cf. [17, 3]) There exists a constant $c > 0$ so that for all m, and every partition $(\mathcal{V}_I, \mathcal{V}_{II})$ of $MVars_m$, if there is treelike OBDD refutation of $Match_m$ of size S that uses a variable order in which either every variable of $\mathcal{V}_I$ precedes every variable of $\mathcal{V}_{II}$, or vice-versa, then for each $i \in [n]$, then there is a deterministic two-player protocol for $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ that uses at most $c \log S$ many bit of communication.*

Lemma 9 *For $m \geq 84651$, if there exists size S refutation of $IndMatch_m$, then there exists a partition of $MVars_m$, $(\mathcal{V}_I, \mathcal{V}_{II})$, with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq 2^{-13}$, and a size S refutation of $Match_m$ in which every variable of $\mathcal{V}_I$ precedes every variable of $\mathcal{V}_{II}$, or vice-versa.*

Proof: Let $v_1, \ldots v_N$ be the variable ordering of $IMVars_m$ used by the refutation of $IndMatch_m$. Let i_0 be the first position to split either the set of vertex variables or the set of edge variables in half. More formally, for each $i = 1, \ldots N$, let $vvars(i)$ be the number of vertex variables in $\{v_1, \ldots v_i\}$, let $evars(i)$ be the number of edge variables in $\{v_1, \ldots v_i\}$, and let i_0 least integer with either $evars(i_0) \geq \frac{m}{2} \cdot \binom{3m}{2}$ or $vvars(i_0) \geq \frac{2m+1}{2} \cdot 3m$. Notice that there are two possible cases: The first is that $evars(i_0) \geq \frac{m}{2} \cdot \binom{3m}{2}$ so that $\{v_1, \ldots v_{i_0}\}$ contains exactly $\frac{m}{2} \cdot \binom{3m}{2}$ many edge variables and $\{v_{i_0+1}, \ldots v_N\}$ contains at least $\frac{1}{2} \cdot (6m^2 + 3m)$ many vertex variables. The second is that $vvars(i_0) \geq \frac{2m+1}{2} \cdot 3m$ so that $\{v_1, \ldots v_{i_0}\}$ contains exactly $\frac{1}{2} \cdot (6m^2 + 3m)$ many vertex variables and $\{v_{i_0+1}, \ldots v_N\}$ contains at least $\frac{m}{2} \cdot \binom{3m}{2}$ many edge variables. In the first case, we set $\mathcal{V}_I = \{v_1, \ldots v_{i_0}\}$ and $\mathcal{V}_{II} = \{v_{i_0+1}, \ldots v_N\}$. In the second case, we set $\mathcal{V}_{II} = \{v_1, \ldots v_{i_0}\}$ and $\mathcal{V}_I = \{v_{i_0+1}, \ldots v_N\}$. In either case, $\frac{1}{m} \sum_{i=1}^{m} |E_i| \geq \frac{1}{2}\binom{3m}{2}$ and $\frac{1}{2m+1} \sum_{i=1}^{2m+1} |V_j| \geq \frac{3m}{2}$. Therefore, by Lemma 2:

$$\frac{1}{(2m+1)^5} \sum_{\vec{j} \in [2m+1]^5} |V_{j_1} \cap V_{j_2} \cap V_{j_3} \cap V_{j_4} \cap V_{j_5}| \geq \frac{3m}{32} \tag{1}$$

$$\frac{1}{m^2}\sum_{\vec{i}\in[m]^2}|E_{i_1}\cap E_{i_2}| \geq \frac{1}{4}\binom{3m}{2} \tag{2}$$

We now calculate the expected value of $\delta(\pi(\mathcal{V}_I),\pi(\mathcal{V}_{II}))$ over $\pi\in\Pi$. We begin by noting that for all $i\in[m]$, $E_i(\pi(\mathcal{V}_I)) = E_i(\mathcal{V}_I) = E_i$ and for all $j\in[2m+1]$, $V_j(\pi(\mathcal{V}_{II})) = \pi(V_j(\mathcal{V}_{II})) = \pi(V_j)$. For each $\vec{\imath}\in[3m]^2$, let $E_{\vec{\imath}} = E_{i_1}\cap E_{i_2}$ and for each $\vec{\jmath}\in[2m+1]^5$, let $V_{\vec{\jmath}} = V_{j_1}\cap V_{j_2}\cap V_{j_3}\cap V_{j_4}\cap V_{j_5}$. For each $\{u,v\}\in\binom{[3m]}{2}$, by the pairwise independence of the permutations, we have that:

$$\begin{aligned}\Pr_{\pi\in\Pi}\left[\{\pi(u),\pi(v)\}\in E_{\vec{\imath}}\right] &= \sum_{\{a,b\}\in E_{\vec{\imath}}}\left(\Pr_{\pi\in\Pi}\left[\pi(u)=a,\ \pi(v)=b\right]+\Pr_{\pi\in\Pi}\left[\pi(u)=b,\ \pi(v)=a\right]\right)\\ &= \frac{2|E_{\vec{\imath}}|}{3m(3m-1)} = \frac{|E_{\vec{\imath}}|}{\binom{3m}{2}}\end{aligned}$$

Therefore, by linearity of expectation, we have that:

$$\mathbb{E}_{\pi\in\Pi}\left[\left|E_{\vec{\imath}}\left[\pi\left(V_{\vec{\jmath}}\right)\right]\right|\right] = \sum_{\{u,v\}\in\binom{V_{\vec{\jmath}}}{2}}\Pr_{\pi}\left[\{\pi(u),\pi(v)\}\in E_{\vec{\imath}}\right] = \frac{|E_{\vec{\imath}}|}{\binom{3m}{2}}\binom{|V_{\vec{\jmath}}|}{2}$$

And thus we bound $\mathbb{E}_{\pi\in\Pi}\left[\delta(\pi(\mathcal{V}_I,\mathcal{V}_{II}))|\right]$ from below as follows:

$$\begin{aligned}&\mathbb{E}_{\pi\in\Pi}\left[\frac{1}{m^2(2m+1)^5}\sum_{\vec{\imath}\in[m]^2}\sum_{\vec{\jmath}\in[2m+1]^5}\frac{\left|\bigcap_{k=1}^5 E_{i_1}(\pi(\mathcal{V}_I))\left[V_{j_k}(\pi(\mathcal{V}_{II}))\right]\cap E_{i_2}(\pi(\mathcal{V}_I))\left[V_{j_k}(\pi(\mathcal{V}_{II}))\right]\right|}{\binom{3m}{2}}\right]\\ =\ &\mathbb{E}_{\pi\in\Pi}\left[\frac{1}{m^2(2m+1)^5}\sum_{\vec{\imath}\in[m]^2}\sum_{\vec{\jmath}\in[2m+1]^5}\frac{\left|\bigcap_{k=1}^5 E_{i_1}\left[\pi(V_{j_k})\right]\cap E_{i_2}\left[\pi(V_{j_k})\right]\right|}{\binom{3m}{2}}\right]\\ =\ &\mathbb{E}_{\pi\in\Pi}\left[\sum_{\vec{\imath}\in[m]^2}\sum_{\vec{\jmath}\in[2m+1]^5}\frac{|E_{\vec{\imath}}\left[\pi\left(V_{\vec{\jmath}}\right)\right]|}{m^2(2m+1)^5\binom{3m}{2}}\right] = \sum_{\vec{\imath}\in[m]^2}\sum_{\vec{\jmath}\in[2m+1]^5}\frac{\mathbb{E}_{\pi\in\Pi}\left[\left|E_{\vec{\imath}}\left[\pi\left(V_{\vec{\jmath}}\right)\right]\right|\right]}{m^2(2m+1)^5\binom{3m}{2}}\\ =\ &\sum_{\vec{\imath}\in[m]^2}\frac{|E_{\vec{\imath}}|}{m^2\binom{3m}{2}}\sum_{\vec{\jmath}\in[2m+1]^5}\frac{\binom{|V_{\vec{\jmath}}|}{2}}{(2m+1)^5} \geq \sum_{\vec{\imath}\in[m]^2}\frac{|E_{\vec{\imath}}|}{m^2\binom{3m}{2}}\binom{3m/32}{2} \text{ (by Equation 1)}\\ =\ &\binom{3m/32}{2}\sum_{\vec{\imath}\in[m]^2}\frac{|E_{\vec{\imath}}|}{m^2\binom{3m}{2}} \geq \binom{3m/32}{2}\left(\frac{1}{4}\right) \text{ (by Equation 2)}\\ =\ &\frac{1}{4}\frac{(3m/32)(3m/32-1)}{2} = \frac{1}{4\cdot(32)^2}\frac{(3m)(3m-32)}{2}\\ =\ &\frac{1}{4\cdot(32)^2}\left(\binom{3m}{2}-\frac{(3m)(31)}{2}\right) = \frac{1}{2^{12}}\binom{3m}{2}\left(1-\frac{31}{3m-1}\right)\\ =\ &\left(2^{-12}-\frac{31}{3m-1}\right)\binom{3m}{2}\end{aligned}$$

Choose a permutation π with $\frac{1}{m^2(2m+1)^5}\sum_{\vec{\imath}\in[m]^2}\sum_{\vec{\jmath}\in[2m+1]^5}|E_{\vec{\imath}}\left[\pi\left(V_{\vec{\jmath}}\right)\right]| \geq \left(2^{-12}-\frac{31}{3m-1}\right)\binom{3m}{2}$. By Lemma 6, there is a size S refutation of $Match_m$ that uses the variable ordering $\pi(v_1),\ldots\pi(v_N)$. Notice that in this order, either every variable of $\pi(\mathcal{V}_I)$ precedes every variable of $\pi(\mathcal{V}_{II})$, or every variable of $\pi(\mathcal{V}_{II})$ precedes every variable of $\pi(\mathcal{V}_I)$. By the above calculation, $\delta(\pi(\mathcal{V}_I),\pi(\mathcal{V}_{II})) \geq 2^{-12}-\frac{31}{3m-1}$. Because $m\geq 84651$, we have $\frac{31}{3m-1}\leq 2^{-13}$, so $\delta(\pi(\mathcal{V}_I),\pi(\mathcal{V}_{II}))\geq 2^{-12}-2^{-13}=2^{-13}$. ∎

7 Reduction and lower bound

The reduction from $setdisj_n(\vec{X}, \vec{Y})$ to $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ uses public random coins to produce a "layout" that assigns certain variables from $\vec{X}$ variables of $\mathcal{V}_I$, and certain variables of $\vec{Y}$ to variables of $\mathcal{V}_{II}$, and hardwiring values for the rest of the variables in $MVars_m$. We define these layouts in Definition 8.2 in Section 8. We denote the set of all layouts by $\mathcal{L}$, and denote the assignment constructed using layout L with set-disjointness instance $(\vec{X}, \vec{Y})$ by $A_{L,\vec{X},\vec{Y}}$. The correctness of the reduction comes down to the following lemma:

Lemma 10 *(Proof in Section 8) For every $\delta_0 > 0$, there exist $c_0, c_1 > 0$ so that for all $m \geq 31(2/\delta_0)^8$, and all partitions of $MVars_m$, $(\mathcal{V}_I, \mathcal{V}_{II})$ with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$, for all n with $n \leq c_0 m$, there exists a set $\mathcal{L}$, a distribution $\mathcal{D}$ on $\mathcal{L}$ with probability function μ, a function $A : \mathcal{L} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{MVars_m}$, and a function $pe : \mathcal{L} \times \{0,1\}^n \times \{0,1\}^n \to \binom{[3m]}{2}$ so that:*

1. *For all $L \in \mathcal{L}$, $(\vec{X}, \vec{Y}) \in \{0,1\}^n \times \{0,1\}^n$, all $v \in \mathcal{V}_I$, $A_{L,\vec{X},\vec{Y}}(v)$ is determined by L and $\vec{X}$, and for all $v \in \mathcal{V}_{II}$, $A_{L,\vec{X},\vec{Y}}(v)$ is determined by L and $\vec{Y}$.*
2. *For all $L \in \mathcal{L}$, all $(\vec{X}, \vec{Y}) \in \{0,1\}^n \times \{0,1\}^n$, the assignment $A_{L,\vec{X},\vec{Y}}$ is non-degenerate.*
3. *For all $(\vec{X}, \vec{Y}) \in \{0,1\}^n \times \{0,1\}^n$, and all $e \in \binom{[3m]}{2}$, if e is bad for $A_{L,\vec{X},\vec{Y}}$, then $e = pe(L)$ or $setdisj_n(\vec{X}, \vec{Y}) = 1$.*
4. *For all $(\vec{X}, \vec{Y}) \in \{0,1\}^n \times \{0,1\}^n$ with $setdisj_n(\vec{X}, \vec{Y}) = 1$, there exists $\mathcal{S} \subseteq \mathcal{L}$ with $\mu(\mathcal{S}) \geq \delta_0^8/2^9$ so that for all $A \in \{A_{L,\vec{X},\vec{Y}} \mid L \in \mathcal{S}\}$:*

$$\max_{e \in \binom{[3m]}{2}} \mu(pe(L) = e \mid A_{L,\vec{X},\vec{Y}} = A,\ L \in \mathcal{S}) \leq 1 - c_1$$

Condition 1 is the requirement that the Player I can compute the value of $A_{L,\vec{X},\vec{Y}}(v)$ for $v \in \mathcal{V}_I$ without communicating with Player II, and that player II can compute $A_{L,\vec{X},\vec{Y}}(v)$ for $v \in \mathcal{V}_{II}$ without communication. Condition 2 guarantees that the assignment created is a valid instance of the $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ problem. The function pe can be thought of as specifying a "planted bad edge": The reduction is based on the idea of having positions with $X_k = Y_k = 1$ create bad edges. However, because the assignment is non-degenerate, there must always be some bad edge, even when $setdisj_n(\vec{X}, \vec{Y}) = 0$. The players knowingly create one such edge and we call this edge the planted edge for the layout, $pe(L)$. Condition 3 states that when $setdisj_n(\vec{X}, \vec{Y}) = 0$, the only bad edge is the planted edge. Condition 4 states that when $setdisj_n(\vec{X}, \vec{Y}) = 1$, conditioned on the layout coming from the set $\mathcal{S}$, no assignment is overly-correlated with a particular planted edge.

Lemma 11 *For all $\delta > 0$, there exist $C_0, C_1 > 0$ so that for all $m \geq 31(2/\delta)^8$, for all partitions of $MVars_m$, $(\mathcal{V}_I, \mathcal{V}_{II})$, with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta$, for all $n \leq C_0 m$, if there is a two-player deterministic protocol $SEARCH$ that solves $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ using r bits of communication, then the randomized communication complexity of $setdisj_n$ is $\leq C_1 r$.*

Proof: Let C_0 be the c_0 as in the statement of Lemma 10 with $\delta_0 = \delta$. We give a one-sided reduction that never gives a wrong answer when $setdisj_n(\vec{X}, \vec{Y}) = 0$, and when $setdisj_n(\vec{X}, \vec{Y}) = 1$, it gives the correct answer with probability $\geq c_1 \delta^8/2^9$, where c_1 is the second constant guaranteed by Lemma 10. Repeating the protocol a constant number of times and returning a 0 only if all runs produce a 0 gives a protocol with correctness $\geq 2/3$.

1. Using public randomness, the players select a reduction layout L according to the distribution $\mathcal{D}$ guaranteed by Lemma 10.

2. The players run $SEARCH$ using the assignment $A_{L,\vec{X},\vec{Y}}$ and let e be the edge returned by $SEARCH$. If $pe(L) = e$ then return 0, and if $pe(L) \neq e$ then return 1.

By Lemma 10, Condition 1, the players can compute the needed values of $A_{L,\vec{X},\vec{Y}}$ with no communication. By Lemma 10, Condition 2, the assignment $A_{L,\vec{X},\vec{Y}}$ is non-degenerate, and is therefore a legal input for the problem $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$. Consider the case when $\vec{X}$ and $\vec{Y}$ are disjoint. By Lemma 10, Condition 3, the only bad edge in $A_{L,\vec{X},\vec{Y}}$ is $pe(L)$, so the protocol returns 0. Consider the case when $\vec{X}$ and $\vec{Y}$ are intersecting. Apply Lemma 10, Condition 4, and let $\mathcal{S}$ be the set guaranteed for the pair $\vec{X}, \vec{Y}$. Define the event $\mathcal{B}$ as $\mathcal{B} = \{L \in \mathcal{S} \mid SEARCH(A_{L,\vec{X},\vec{Y}}) = pe(L)\}$. This is the event that the layout belongs to $\mathcal{S}$ and the protocol gives an erroneous answer. Let $A_{\mathcal{S}} = \{A_{L,\vec{X},\vec{Y}} \mid L \in \mathcal{S}\}$. For each $A \in A_{\mathcal{S}}$, let $\mathcal{S}_A = \{L \in \mathcal{S} \mid A_{L,\vec{X},\vec{Y}} = A\}$ and let $\mathcal{B}_A = \{L \in \mathcal{B} \mid A_{L,\vec{X},\vec{Y}} = A\}$. Because the protocol $SEARCH$ is deterministic, for every A, the function $L \mapsto pe(L)$ is constant on the set $\mathcal{B}_A$ (taking the value returned by $SEARCH(A)$). Therefore, by Lemma 10, Condition 4, for each $A \in A_{\mathcal{S}}$, $\mu(\mathcal{B}_A) \leq (1 - c_1)\mu(\mathcal{S}_A)$, and so:

$$\mu(\mathcal{B}) = \sum_{A \in A_{\mathcal{S}}} \mu(\mathcal{B}_A) \leq \sum_{A \in A_{\mathcal{S}}} \mu(\mathcal{S}_A)(1 - c_1) = (1 - c_1)\mu(\mathcal{S})$$

Therefore $\mu(\mathcal{S} \setminus \mathcal{B}) \geq c_1\mu(\mathcal{S}) \geq c_1\delta^8/2^9$. Of course, $\mathcal{S} \setminus \mathcal{B}$ is the event that $L \in \mathcal{S}$ and the protocol gives the answer 1.

■

7.1 The lower bound

Theorem 12 *There exists a constant $C > 0$ so that for sufficiently large m, every tree-like OBDD refutation of $IndMatch_m$ has size at least 2^{Cm}.*

Proof: Apply Theorem 5 and choose $N \geq 0$ and $c^* > 0$ so that for every $n \geq N$, randomized two-player protocols for solving $setdisj_n$ require $\geq c^*n$ bits of communication. Let C_0 and C_1 be the constants of Lemma 11, and let m be so large that $m \geq 31(2/(2^{-13}))^8 = 31 \cdot 2^{112}$ (so that we can apply Lemma 11 with $\delta \geq 2^{-13}$), and $N \leq \lfloor C_0 m \rfloor$ (so that we can apply Theorem 5). Set $n = \lfloor C_0 m \rfloor$. Let $c > 0$ be the constant from Lemma 7. Let Γ be a tree-like OBDD refutation of $IndMatch_m$ of size S. Because $m > 84651$, we may apply Lemma 7 and choose a partition $(\mathcal{V}_I, \mathcal{V}_{II})$ so that $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq 2^{-13}$ and a two-player deterministic communication protocol $FindBadEdge_m(\mathcal{V}_I, \mathcal{V}_{II})$ that uses at most $c \log S$ bits of communication. By Lemma 11, there is a two-party randomized communication protocol for $setdisj_n$ on inputs from $\mathcal{P}_n$ that exchanges at most $C_1 \log S$ bits of communication. Therefore, applying the communication bound for set-disjointness, $C_1 \log S \leq c^*n = c^*\lfloor C_0 m \rfloor$, and thus $S \leq 2^{\frac{c^*\lfloor C_0 m \rfloor}{C_1}}$ ■

8 Reduction layouts

We now take a moment to discuss the gadgets underlying the reduction from set-disjointness to the problem of finding a bad edge. The basic idea is to create a bad edge for each k with $X_k = Y_k = 1$.

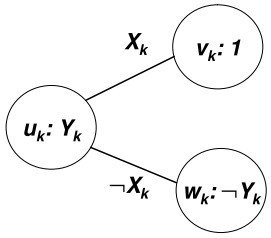

Figure 1: The basic set-disjointness gadget. A bad edge corresponds to the situation when an edge and both of its endpoints receive the label 1. The assignment uses: $x^{i_k}_{\{u_k,v_k\}} = X_k$, $x^{i_k}_{\{u_k,w_k\}} = \neg X_k$, $y^{j_{k,1}}_{v} = 1$, $y^{j_{k,2}}_{u_k} = Y_k$, and $y^{j_{k,2}}_{w_k} = \neg Y_k$. Notice that $\{u_k, w_k\}$ is never a bad edge, and that $\{u_k, v_k\}$ is a bad edge if and only if $X_k = Y_k = 1$.

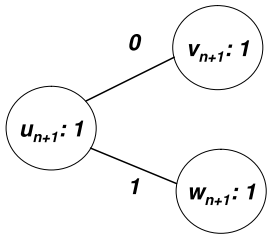

Figure 2: The set-disjointness gadget at the position with a planted bad edge. A bad edge corresponds to the situation when an edge and both of its endpoints receive the label 1. The assignment uses: $x^{i_{n+1}}_{\{u_{n+1},v_{n+1}\}} = 0$, $x^{i_{n+1}}_{\{u_{n+1},w_{n+1}\}} = 1$, $y^{j_{n+1,1}}_{u_{n+1}} = 1$, $y^{j_{n+1,2}}_{v_{n+1}} = 1$, $y^{j_{n+1,3}}_{w_{n+1}} = 1$.

To do this without communicating, the players use the public randomness to choose $u_k, v_k, w_k \in [3m]$ with the intent to place $\{u_k, v_k\}$ in the matching if $X_k = 1$ and $\{u_k, w_k\}$ in the matching if $X_k = 0$, and to place v_k in the independent no matter what, but to include u_k if $Y_k = 1$ and to include w_k if $Y_k = 0$. Of course, we must specify which variables are used to place the gadget, and those variables must be available to the players under the partition. The players use the public randomness to choose $i_k \in [m]$ with $x^{i_k}_{\{u_k,v_k\}}$, $x^{i_k}_{\{u_k,w_k\}} \in \mathcal{V}_I$ (equivalently, $\{u_k, v_k\}, \{u_k, w_k\} \in E_{i_k}$) and $j_{k,1}, j_{k,2} \in [m]$ with $y^{j_{k,1}}_{v_k}, y^{j_{k,2}}_{u_k}, y^{j_{k,2}}_{w_k} \in \mathcal{V}_{II}$, (equivalently, $v_k \in V_{j_{k,1}}$ and $u_k, w_k \in V_{j_{k,2}}$). The situation resembles that in Figure 1, with a bad edge occurring only if $X_k = Y_k = 1$ and only then only at $\{u_k, v_k\}$. The reduction plants one of these gadgets for each $k = 1, \ldots n$.

Because there are m edges in the matching and $2m + 1$ vertices in the set, one more vertex must be placed in addition to the two associated with each set-disjointness gadget. A final gadget (thought of as being at position $n+1$) will contain the "planted bad edge", in which three vertices u_{n+1}, v_{n+1}, and w_{n+1} are all placed in the set, and the edge $\{u_{n+1}, w_{n+1}\}$ is included. Because all three vertices are placed in the set, three variables $y^{j_{n+1,1}}_{u_{n+1}}$, $y^{j_{n+1,2}}_{v_{n+1}}$ and $y^{j_{n+1,3}}_{w_{n+1}}$ are needed with $u_{n+1} \in V_{j_{n+1,1}}$, $v_{n+1} \in V_{j_{n+1,2}}$, and $w_{n+1} \in V_{j_{n+1,3}}$.

The basic idea of the reduction is to randomly plant these $n + 1$ gadgets on disjoint variables. However, to ensure that the probabilities work out as claimed in Lemma 10, we make use of the density of the partition.

Definition 8.1 *Fix a partition of $MVars_m$, $(\mathcal{V}_I, \mathcal{V}_{II})$. Set $\delta = \delta(\mathcal{V}_I, \mathcal{V}_{II})$. For each $i \in [m]$ let $E_i = E_i(\mathcal{V}_I)$ and for each $j \in [2m+1]$ let $V_j = V_j(\mathcal{V}_{II})$. For each $i \in [m]$, let $N_3(i) = \{(j_1, j_2, j_3) \in$*

$[2m+1]^3 \mid j_1 \neq j_2,\ j_2 \neq j_3,\ j_3 \neq j_1,\ |E_i[V_{j_1} \cap V_{j_2} \cap V_{j_3}]| \geq (\delta/3)\binom{3m}{2}\}$, *and let* $N_2(i) = \{(j_1, j_2) \in [2m+1]^2 \mid \exists j_3 \in [2m+1],\ (j_1, j_2, j_3) \in N_3(i)\}$. *Set* $G = \{i \in [m] \mid |N_3(i)| \geq (\delta/12)(2m+1)^3\}$. *Of course, each of* G, $N_3(\cdot)$, *and* $N_2(\cdot)$ *depend upon the partition* $(\mathcal{V}_I, \mathcal{V}_{II})$, *but we drop that from notation as we will never discuss more than one partition at a time.*

Lemma 13 *Let* $\delta \in [0,1]$ *and let* m *be an integer* $\geq 3/\delta$, *and let* $(\mathcal{V}_I, \mathcal{V}_{II})$ *be a partition of* $MVars_m$ *with* $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta$. *The size of* G *is bounded from below as* $|G| \geq (\delta/12)\, m$

Proof: Let $\delta = \delta(\mathcal{V}_I, \mathcal{V}_{II})$. Because $m \geq 3/\delta \geq ((6/\delta) - 1)/2$, we have that $3/(2m+1) \leq \delta/2$. By Definition 5.2 , we have that:

$$\frac{1}{m^2(2m+1)^5} \sum_{\vec{i} \in [m]^2} \sum_{\vec{j} \in [2m+1]^5} |\bigcap_{k=1}^{5} (E_{i_1}[V_{j_k}] \cap E_{i_2}[V_{j_k}])| = \delta \binom{3m}{2}$$

And therefore $\frac{1}{m(2m+1)^3} \sum_{i \in [m]} \sum_{\vec{j} \in [2m+1]^3} |E_i[V_{j_1} \cap V_{j_2} \cap V_{j_3}]| \geq \delta\binom{3m}{2}$. Because the number of terms with $j_1 = j_2$, $j_2 = j_3$ or $j_1 = j_3$ is at most $3m(2m+1)^2$, such terms can contribute at most $\frac{1}{m(2m+1)^3} 3m(2m+1)^2\binom{3m}{2} = \frac{3}{2m+1}\binom{3m}{2}$ to this sum, so we have:

$$\frac{1}{m(2m+1)^3} \sum_{i \in [m]} \sum_{\substack{\vec{j} \in [2m+1]^3 \\ \vec{j} \text{ distinct}}} |E_i[V_{j_1} \cap V_{j_2} \cap V_{j_3}]| \geq (\delta - 3/(2m+1))\binom{3m}{2} \geq (\delta/2)\binom{3m}{2}$$

Combining this with the fact that for each $i \in [m]$, $|E_i| \leq \binom{3m}{2}$, by averaging, we have that with probability at least $\delta/6$ over the choice of i,j_1,j_2,j_3, with j_1, j_2, j_3 all distinct, that $|E_i[V_{j_1} \cap V_{j_2} \cap V_{j_3}]| \geq (\delta/3)\binom{3m}{2}$. Therefore, with probability at least $\delta/12$ over choices of i, there are at least $(\delta/12)[2m+1]^3$ many triples j_1, j_2, j_3 that are distinct and have $|E_i[V_{j_1} \cap V_{j_2} \cap V_{j_3}]| \geq (\delta/3)\binom{3m}{2}$. Therefore, $|G| \geq (\delta/12)m$.

■

Definition 8.2 *Fix an integer* m, *a partition* $(\mathcal{V}_I, \mathcal{V}_{II})$ *of* $MVars_m$.. *A* reduction layout (with respect to $(\mathcal{V}_I, \mathcal{V}_{II})$, of length n) *is a tuple* $(i_1, \ldots i_{n+1}, (j_{1,1}, j_{1,2}), \ldots (j_{n,1}, j_{n,2}), (j_{n+1,1}, j_{n+1,2}, j_{n+1,3}), (u_1, v_1, w_1), \ldots (u_{n+1}, v_{n+1}, w_{n+1}))$ *from the set* $[m]^{n+1} \times ([2m+1]^2)^n \times ([2m+1]^3) \times \left([3m]^3\right)^n$ *with the following properties:*

1. *The indices* $i_1, \ldots i_{n+1}$ *are distinct.*
2. *The indices* $j_{1,1}, j_{1,2}, \ldots j_{n,1}, j_{n,2}, j_{n+1,1}, j_{n+1,2}, j_{n+1,3}$ *are distinct.*
3. *The integers* $u_1, \ldots u_{n+1}, v_1, \ldots v_{n+1}, w_1, \ldots w_{n+1}$ *are distinct.*
4. *For each* $k = 1, \ldots n+1$, $\{u_k, v_k\} \in E_{i_k}$ *and* $\{u_k, w_k\} \in E_{i_k}$.
5. *For each* $k = 1, \ldots n+1$, $u_k, v_k, w_k \in V_{j_{k,1}} \cap V_{j_{k,2}}$.
6. $u_{n+1}, v_{n+1}, w_{n+1} \in V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}$.
7. *For all* $k \in [n+1]$, $i_k \in G$.
8. $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_{n+1})$
9. *For* $k \in [n]$, *each* $(j_{k,1}, j_{k,2}) \in N_2(i_k)$.

The set of all reduction layouts of length n with respect to $(\mathcal{V}_I, \mathcal{V}_{II})$ is denoted $\mathcal{L}_{m,n}(\mathcal{V}_I, \mathcal{V}_{II})$. When m, n, and $(\mathcal{V}_I, \mathcal{V}_{II})$ are clear from context, we simply write $\mathcal{L}$ and call $L \in \mathcal{L}$ a reduction layout*.*

When listing the elements of a reduction layout, we will abuse notation write $(\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ despite the fact that a reduction layout is emphatically *not* a member of the product set $[m]^{n+1} \times [2m+1]^{2n+3} \times [3m]^{n+1} \times [3m]^{n+1} \times [3m]^{n+1}$. This matters for the purpose of computing Hamming distances. The Hamming distance between two reduction layouts in $\mathcal{L}$ is their Hamming distance as elements of the $3n+3$ dimensional Cartesian product $[m]^{n+1} \times ([2m+1]^2)^n \times ([2m+1]^3) \times \left([3m]^3\right)^{n+1}$. In particular, if two reduction layouts $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ and $L^* = (\vec{\imath}^*, \vec{\jmath}^*, \vec{u}^*, \vec{v}^*, \vec{w}^*)$ differ in only that $(u_k, v_k, w_k) \neq (u_k^*, v_k^*, w_k^*)$ then they are at Hamming distance 1.

Definition 8.3 *Fix m, n, a partition $(\mathcal{V}_I, \mathcal{V}_{II})$ of $MVars_m$. Let $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ be a reduction layout from $\mathcal{L}$, and let $X_1, \ldots X_n, Y_1, \ldots Y_n$ be a set-disjointness instance. We define an assignment $A_{L,\vec{X},\vec{Y}}$ to the variables of $MVars_m$ as follows: Set $I = \{i_1, \ldots i_{n+1}\}$. Set $J = \{j_{1,1}, j_{1,2}, \ldots j_{n,1}, j_{n,2}, j_{n+1,1}, j_{n+1,2}, j_{n+1,3}\}$. Set $V = \{u_1, \ldots u_{n+1}, v_1, \ldots v_{n+1}, w_1, \ldots w_{n+1}\}$. Let β, $\beta(L)$, be the lexicographically first assignment to the variables $\{x_e^i \mid i \in [m] - I,\ e \in [3m - V]^2\}$ $\cup \{y_u^j \mid j \in [2m+1] - J,\ u \in [3m] - V\}$ so that β defines a matching of size $m - n - 1$ and an independent set of size $2(m - n - 1)$ on $[3m] \setminus V$. Define $A_{L,\vec{X},\vec{Y}}$ as follows:*

$$A_{L,\vec{X},\vec{Y}}(x_e^i) = \begin{cases} \beta(x_e^i) & \text{if } i \in [m] - I \text{ and } e \in ([3m] - V)^2 \\ X_k & \text{if } i = i_k \text{ and } e = \{u_k, v_k\} \text{ for some } k \in [n] \\ \neg X_k & \text{if } i = i_k \text{ and } e = \{u_k, w_k\} \text{ for some } k \in [n] \\ 1 & \text{if } i = i_{n+1} \text{ and } e = \{u_{n+1}, w_{n+1}\} \\ 0 & \text{otherwise} \end{cases}$$

$$A_{L,\vec{X},\vec{Y}}(y_x^j) = \begin{cases} \beta(y_x^j) & \text{if } j \in [2m+1] - J \text{ and } u \in [3m] - V \\ 1 & \text{if } j = j_{k,1} \text{ and } x = v_k \text{ for some } k \in [n] \\ Y_k & \text{if } j = j_{k,2} \text{ and } x = u_k \text{ for some } k \in [n] \\ \neg Y_k & \text{if } j = j_{k,2} \text{ and } x = w_k \text{ for some } k \in [n] \\ 1 & \text{if } j = j_{n+1,1} \text{ and } x = u_{n+1} \\ 1 & \text{if } j = j_{n+1,2} \text{ and } x = v_{n+1} \\ 1 & \text{if } j = j_{n+1,3} \text{ and } x = w_{n+1} \\ 0 & \text{otherwise} \end{cases}$$

Notice that when both players have access to the layout L, condition 4 of Definition 8.2 ensures that Player I can compute the assignment to all variables in $\mathcal{V}_I$ by only consulting his private set-disjointness variables, and conditions 5 and 6 similarly guarantee that Player can compute the assignment to all variables in $\mathcal{V}_{II}$ by only consulting his private set-disjointness variables. This guarantees Condition 1 in Lemma 10. The conditions 1, 2 and 3 of Definition 8.2 ensure that $A_{L,\vec{X},\vec{Y}}$ is well-defined and non-degenerate. This guarantees Condition 2 in Lemma 10.

Definition 8.4 *Let m and n be given. Let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a variable partition for $MVars_m$. Let $\vec{X}$, $\vec{Y}$ be a set-disjointness instance, and let $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ be a reduction layout from $\mathcal{L}_{m,n}$. The* planted edge for $\vec{X}, \vec{Y}, L$, *$pe(L)$, is defined to be $\{u_{n+1}, w_{n+1}\}$.*

Condition 3 of Lemma 10 is the content of the following lemma.

Lemma 14 *Let $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ be a reduction layout. If e is a bad edge of $A_{L,\vec{X},\vec{Y}}$ then $e = pe(L)$, or, $e = \{u_l, v_l\}$ with $X_l = Y_l = 1$.*

Proof: Let $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ be a reduction layout, and let $X_1, \ldots X_n, Y_1, \ldots Y_n$ be a set intersection instance. Let e be a bad edge for the assignment $A_{L,\vec{X},\vec{Y}}$. First of all, because β sets no bad edges, $e \cap V \neq \emptyset$. Furthermore, for all e with $|e \cap V| = 1$ have $A_{L,\vec{X},\vec{Y}}(x_e^i) = 0$ for all i, so $e \subseteq V$. Finally, for $e \subseteq V$, with some $A_{L,\vec{X},\vec{Y}}(x_e^i) = 1$, we have that for some $k \in [n]$, $e = \{u_k, v_k\}$ or $e = \{u_k, w_k\}$. Choose k so that $e = \{u_k, v_k\}$ or $e = \{u_k, w_k\}$. If $k = n+1$ then we must have that $e = \{u_{n+1}, w_{n+1}\}$, and e the bad edge, so consider the case when $k \leq n$. Notice that for all $i' \neq i_k$, $A_{L,\vec{X},\vec{Y}}(x_e^{i'}) = 0$. On the other hand, e is a bad edge, so there is some x_e^i that gets set to 1, therefore $A_{L,\vec{X},\vec{Y}}(x_e^{i_k}) = 1$. We now rule out the case that $e = \{u_k, w_k\}$. Because $A_{L,\vec{X},\vec{Y}}(x_e^{i_k}) = 1$, we have by construction that $X_k = 0$. Because e is bad, for some j, j', $A_{L,\vec{X},\vec{Y}}(y_{u_k}^j) = 1$ and $A_{L,\vec{X},\vec{Y}}(y_{w_k}^{j'}) = 1$. However, $y_{u_k}^j$ and $y_{w_k}^{j'}$ cannot both be set to 1. Suppose that $e = \{u_k, v_k\}$. Because $A_{L,\vec{X},\vec{Y}}(x_e^{i_l}) = 1$, we have by construction that $X_l = 1$. If $(X_l, Y_l) = (1,1)$, then the lemma holds. Otherwise, $Y_l = 0$. But in this case, we have that for all j, $A_{L,\vec{X},\vec{Y}}(y_{u_l}^j) = 0$, contradiction to e being a bad edge. ∎

9 The distribution on reduction layouts

There is a technical point that we defer until after we describe the distribution: Why the experiment does not get stuck and find itself in a position of attempting to choose an item from an empty set. For n a sufficiently small constant fraction of m, this is ruled out by some calculations that follow the description of the experiment.

Definition 9.1 *Let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a variable partition for $MVars_m$. Let G, $N_3(\cdot)$, and $N_2(\cdot)$ be as in Definition 8.1. The distribution $\mathcal{D}$ on $\mathcal{L}$ is given by the following experiment:*

1. *For each $k = 1, \ldots n+1$: Choose i_k from $G \setminus \{i_1, \ldots i_{k-1}\}$.*
2. *Set $J = \emptyset$.*
3. *For each $k = 1, \ldots n$:*
   (a) *Uniformly choose $(j_{k,1}, j_{k,2})$ from $N_2(i_k) \setminus pm_{[2m+1]}(J)$*
   (b) *Set $J := J \cup \{j_{k,1}, j_{k,2}\}$*
4. *Uniformly choose $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3})$ from $N_3(i_{n+1}) \setminus tm_{[2m+1]}(J)$*
5. *Set $J := J \cup \{j_{n+1,1}, j_{n+1,2}, j_{n+1,3}\}$*
6. *Set $V^* = \emptyset$.*
7. *For each $k = 1, \ldots n$:*
   (a) *Uniformly choose (u_k, v_k, w_k) from $\mathcal{K}_{1,2}(E_{i_k}\left[\left(V_{j_{k,1}} \cap V_{j_{k,2}}\right)\right]) \setminus tm_{[3m]}(V^*)$.*
   (b) *Set $V^* = V^* \cup \{u_k, v_k, w_k\}$.*
8. *Uniformly choose $(u_{n+1}, v_{n+1}, w_{n+1})$ from $\mathcal{K}_{1,2}(E_{i_{n+1}}\left[\left(V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}\right)\right]) \setminus tm_{[3m]}(V^*)$.*

9. *Return the layout* $(\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$.

Proposition: For all $L \in \mathcal{L}$, $\mu(L) > 0$.

The above proposition can be checked by iteratively noting that when we condition on the experiment producing a prefix of L, the probability that it selects the next coordinate of L is non-zero.

Lemma 15 *Let* $\delta_0 \in [0,1]$ *and let* m *be an integer* $\geq 450/\delta_0^2$. *Let* $(\mathcal{V}_I, \mathcal{V}_{II})$ *be a partition of* $MVars_m$ *with* $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$. *Let* n *given with* $\gamma = \frac{n+1}{m}$. *For all runs of the experiment in Definition 9.1, and for each* $k = 1, \ldots n$*:*

1. $|G \setminus \{i_1, \ldots i_{k-1}\}| > ((\delta_0/12) - \gamma)m$.
2. $|N_2(i_k) \setminus pm_{[2m+1]}(J) \geq ((\delta_0/3) - 2\gamma)(2m+1)^2$
3. $|N_3(i_{n+1}) \setminus tm_{[2m+1]}(J)| \geq ((\delta_0/3) - 3\gamma)(2m+1)^3$
4. $|\mathcal{K}_{1,2}\left(E_{i_k}\left[V_{j_{k,1}} \cap V_{j_{k,2}}\right]\right) \setminus tm_{[3m]}(V^*)| \geq (\delta_0^2/10 - 3\gamma)(3m)^3$
5. $|\mathcal{K}_{1,2}\left(E_{i_{n+1}}\left[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}\right]\right) \setminus tm_{[3m]}(V^*)| \geq (\delta_0^2/10 - 3\gamma)(3m)^3$

Proof: Set $\delta = \delta(\mathcal{V}_I, \mathcal{V}_{II})$. For each $k = 1, \ldots n$, as we choose $(j_{k,1}, j_{k,2})$ (and $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3})$), $|J| \leq 2n < 2(n+1) = 2\gamma m$ and as we choose each (u_k, v_k, w_k), $|V^*| \leq 3n < 3(n+1) = 3\gamma m$.

1. By Lemma 13, $|G| \geq (\delta/12)m \geq (\delta_0/12)m$. On the other hand, $|\{i_1, \ldots i_{k-1}\}| \leq n < \gamma m$. Therefore, $|G \setminus \{i_1, \ldots i_{k-1}\}| > ((\delta_0/12) - \gamma)m$.

2. Because $|J| \leq 2n$, we have that $pm_{[2m+1]}(J) \leq 2n(2m+1) + (2m+1)2n < 2(2\gamma m)(2m+1) = 2(2\gamma m)(2m+1) = 2\gamma(2m)(2m+1) < 2\gamma(2m+1)^2$. Combining this with the fact that $i_k \in G$ and therefore $|N_2(i_k)| \geq |N_3(i_k)| \geq (\delta/3)(2m+1)^2 \geq (\delta_0/3)(2m+1)^2$ we have that $|N_2(i_k) \setminus pm_{[2m+1]}(J)| \geq ((\delta_0/3) - 2\gamma)(2m+1)^2$.

3. Because $|J| \leq 2n$ we have that $tm_{[2m+1]}(J) \leq 3(2n)(2m+1)^2 < 3(2\gamma m)(2m+1)^2 = 3\gamma(2m)(2m+1)^2 < 3\gamma(2m+1)^3$. Because $i_p \in G$, $|N_3(i_p)| \geq (\delta/3)(2m+1)^3 \geq (\delta_0/3)(2m+1)^3$. Therefore: $|N_3(i_p) \setminus tm_{[2m+1]}(J)| \geq ((\delta_0/3) - 3\gamma)(2m+1)^3$.

4. Because $|V^*| \leq 3n$, $|tm(V^*)| \leq 3(3n)(3m)^2 < 3(3\gamma m)(3m)^2 = 3\gamma(3m)^3$. We now get a lower bound on the size of $\mathcal{K}_{1,2}\left(E_{i_k}[V_{j_{k,1}} \cap V_{j_{k,2}}]\right)$: First, because $(j_{k,1}, j_{k,2}) \in N_2(i_k)$, there exists some j' with $|E_i[V_{j'} \cap V_{j_{k,1}} \cap V_{j_{k,2}}]| \geq (\delta/3)\binom{3m}{2} \geq (\delta_0/3)\binom{3m}{2}$, so we have that $|E_{i_k}\left[V_{j_{k,1}} \cap V_{j_{k,2}}\right] \geq (\delta_0/3)\binom{3m}{2}$. Feeding this lower bound on the edge density into Lemma 3, we have that:

$$|\mathcal{K}_{1,2}(E_{i_k}\left[V_{j_{k,1}} \cap V_{j_{k,2}}\right])| \geq \left(\delta_0^2/9 - (5/m)\right) \cdot (3m)^3$$

Combining the upper bound on $|tm(V^*)|$ and with the preceding lower bound:

$$|\mathcal{K}_{1,2}(E_{i_k}\left[V_{j_{k,1}} \cap V_{j_{k,2}}\right]) \setminus tm(V^*)| \leq \left((\delta_0^2/9) - (5/m) - 3\gamma\right)(3m)^3$$

Because $m \geq 450/\delta_0^2$, we have that $5/m \leq \delta_0^2/90$ and therefore the above quantity is $\geq (\delta_0^2/9 - \delta_0^2/90 - 3\gamma)(3m)^3 = (\delta_0^2/10) - 3\gamma)(3m)^3$.

5. This derivation is identical to the previous, except that it uses the lower bound of $|E_i[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}]| \geq (\delta_0/3)\binom{3m}{2}$ that holds because $(j_{n+1,1}, j_{n+2,2}, j_{n+1,3}) \in N_3(i_{n+1})$.

■

The following two statements are used to prove Lemma 10.

Definition 9.2 *A reduction layout $L = (\vec{i}, \vec{j}, \vec{u}, \vec{v}, \vec{w})$ is said to be* l-switchable *if $(j_{n+1,2}, j_{l,1}, j_{l,2}) \in N_3(i_l)$ and $K(\{u_{n+1}, u_l\}, \{v_{n+1}, v_l, w_{n+1}, w_l\}) \subseteq E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}] \cap E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}]$. Let $\mathcal{S}^l$ denote the set of l-switchable reduction layouts from $\mathcal{L}$.*

Lemma 16 *(Proof in Section 11) For all $\delta_0 \in [0,1]$, for all $m \geq 31(2/\delta_0)^8$, all partitions $(\mathcal{V}_I, \mathcal{V}_{II})$ of $MVars_m$ with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$, for all $n \leq \frac{\delta_0^{10}}{2^{12} \cdot 3^{2} \cdot 5} m$, for all $l \in [n]$, $\mu(\mathcal{S}^l) \geq \delta_0^8/2^9$.*

Lemma 17 *(Proof in Section 11) For every $\delta_0 \in [0,1]$ for every integer $d \geq 1$ for all $m \geq 450/\delta_0^2$, for all partitions $(\mathcal{V}_I, \mathcal{V}_{II})$ of $MVars_m$ with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$, for all $n \leq (\delta_0^2/60)m$, for all reduction layouts $L, L^* \in \mathcal{L}$ with $HD(L, L^*) \leq k$, $\mu(L^*) \geq (\delta_0^2/20)^{2d} e^{-3d} \cdot \mu(L)$.*

9.1 The proof of Lemma 10

To prove Lemma 10 we use the following helper lemma.

Lemma 18 *(Proof immediately follows that of Lemma 10.) For all $\delta_0 \in [0,1]$, all $m \geq 450/\delta_0^2$, all partitions $(\mathcal{V}_I, \mathcal{V}_{II})$ of $MVars_m$ with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$, all $n \leq (\delta_0^2/20)m$, and all set-disjointness instances $(\vec{X},\vec{Y})$, there exists an involution $f : \mathcal{S}^l \to \mathcal{S}^l$ so that for all $L \in \mathcal{S}^l$, $A_{L,\vec{X},\vec{Y}} = A_{f(L),\vec{X},\vec{Y}}$, $pe(f(L)) \neq pe(L)$, and $\mu(f(L)) \geq \mu(L)(\delta_0^2/20)^{12} e^{-18}$.*

Proof:(of Lemma 10 from Lemma 18) Let $\delta_0 \in [0,1]$ be given. Set $c_0 = \frac{\delta_0^{10}}{2^{12} \cdot 3^{2} \cdot 5}$ Let $m \geq 31(2/\delta_0)^8$ and $n \leq c_0 m$ be given. Let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$ with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta$. We take $\mathcal{L} = \mathcal{L}_{m,n}(\mathcal{V}_I, \mathcal{V}_{II})$ per Definition 8.2, $\mathcal{D} = \mathcal{D}_{m,n}(\mathcal{V}_I, \mathcal{V}_{II})$ per Definition 9.1, $A : (L, \vec{X}, \vec{Y}) \to A_{L,\vec{X},\vec{Y}}$ per Definition 8.3, and pe per Definition 8.4.

Condition 1 and Condition 2 follow immediately from Definition 8.2, and Condition 3 follows from Lemma 14. What remains to be shown is Condition 4. Let $(\vec{X}, \vec{Y}) \in \{0,1\}^n \times \{0,1\}^n$ with $setdisj_n(\vec{X}, \vec{Y}) = 1$ be given. Choose $l \in [n]$ with $X_l = Y_l = 1$ and set $\mathcal{S} = \mathcal{S}^l$. By Lemma 16, $\mu(\mathcal{S}^l) \geq \delta^8/2^9$. Set $c = (\delta_0^2/20)^{12} e^{-18}$ (The constant of Lemma 18.) We now show that for all assignments A to $MVars_m$:

$$\max_e \mu(pe(L) = e \mid A_{L,\vec{X},\vec{Y}} = A,\ L \in \mathcal{S}^l) \leq 1/(1+c)$$

Let A be an assignment to $MVars_m$ and let $e \in \binom{[3m]}{2}$ be given. Let $\mathcal{B}_A^e = \{L \in \mathcal{S}^l \mid A_{L,\vec{X},\vec{Y}} = A,\ pe(L) = e\}$, let $\mathcal{S}_A^l = \{L \in \mathcal{S}^l \mid A_{L,\vec{X},\vec{Y}} = A\}$. Take take as f guaranteed by Lemma 18. Because f maps $\mathcal{S}^l$ to $\mathcal{S}^l$, we have that $f(\mathcal{B}_A^e) \subseteq \mathcal{S}^l$, because $A_{f(L),\vec{X},\vec{Y}} = A_{L,\vec{X},\vec{Y}} = A$, we have that $f(\mathcal{B}_A^e) \subseteq \mathcal{S}_A^l$, and because $pe(f(L)) \neq pe(L) = e$, we have that $f(\mathcal{B}_A^e) \subseteq \mathcal{S}_A^l \setminus \mathcal{B}_A^e$. Because f is an involution of $\mathcal{S}^l$, it is injective, and because $\mu(f(L)) \geq c\mu(L)$ for all L, we have that $\mu(\mathcal{S}_A^l \setminus \mathcal{B}_A^e) \geq \mu(f(\mathcal{B}_A^e)) \geq c_1 \mu(\mathcal{B}_A^e)$ and therefore $\mu(\mathcal{S}_A^l) = \mu(\mathcal{S}_A^l \setminus \mathcal{B}_A^e) + \mu(\mathcal{B}_A^e) \geq (1+c)\mu(\mathcal{B}_A^e)$. Therefore: $\mu(\{pe(L) = e\} \mid \{A_{L,\vec{X},\vec{Y}} = A,\ L \in \mathcal{S}^l\}) = \mu(\mathcal{B}_A^e \mid \mathcal{S}_A^l) = \frac{\mu(\mathcal{B}_A^e)}{\mu(\mathcal{S}_A^l)} \leq \frac{1}{1+c}$. Noting that $1/(1+c) = 1 - c/(1+c)$, we set $c_1 = c/(1+c)$ and we are done with this Lemma 10. ■

Proof:(of Lemma 18) Let $L = (\vec{i}, \vec{j}, \vec{u}, \vec{v}, \vec{w})$. We define $f(L) = (\vec{i}, \vec{j}^*, \vec{u}^*, \vec{v}^*, \vec{w}^*)$ below. The basic the idea is to modify the reduction layout L by swapping some vertices between the gadgets at positions $n+1$ and l so that the planted edge changes but the assignment remains the same.

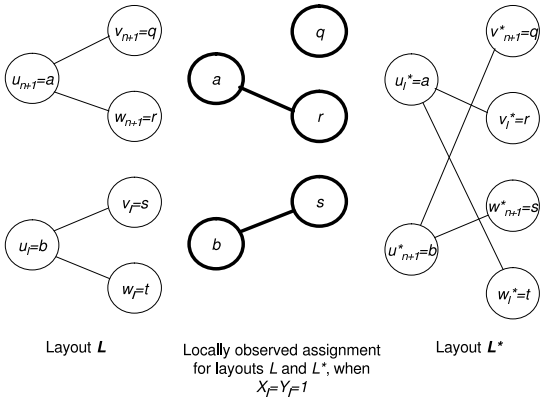

Figure 3: With layouts L and L^*, when $X_l = X_l = 1$, set of vertices and edges specified by the assignments $A_{L,\vec{X},\vec{Y}}$ and $A_{L^*,\vec{X},\vec{Y}}$ are equal. Notice however, that the planted edge under L is $\{a, r\}$ whereas the planted edge under L^* is $\{b, s\}$.

This is graphically illustrated in Figure 3. Because of the partitioning of the variables, it is not immediately clear that L^* will be a reduction layout. Among other things, we need to ensure that $\{u^*_l, w^*_l\} \in E_{i^*_l}$ and $\{j^*_{n+1,1}, j^*_{n+1,2}, j^*_{n+1,3}\} \in N_3(i^*_{n+1})$, which makes use of the hypothesis that L is l-switchable. We give the full definition of L^* below, along with the case analysis ensuring that the conclusions of the lemma hold.

$$i^*_k = \begin{cases} i_{n+1} & \text{if } k = l \\ i_l & \text{if } k = n+1 \\ i_k & \text{otherwise} \end{cases} \qquad u^*_i = \begin{cases} u_l & \text{if } i = n+1 \\ u_{n+1} & \text{if } i = l \\ u_i & \text{otherwise} \end{cases}$$

$$j^*_{k,1} = \begin{cases} j_{n+1,3} & \text{if } k = l \\ j_{l,2} & \text{if } k = n+1 \\ j_{k,1} & \text{otherwise} \end{cases} \qquad v^*_k = \begin{cases} w_{n+1} & \text{if } k = l \\ v_k & \text{otherwise} \end{cases}$$

$$j^*_{k,2} = \begin{cases} j_{n+1,1} & \text{if } k = l \\ j_{k,2} & \text{otherwise} \end{cases} \qquad w^*_k = \begin{cases} v_l & \text{if } k = n+1 \\ w_k & \text{otherwise} \end{cases}$$

$$j^*_{n+1,3} = j_{l,1}$$

We now check each of the properties required by Lemma 18. This is just case analysis and rewriting. However, in order to show that $f(L) \in \mathcal{S}^l$ we make use of the hypothesis that L is l-switchable.

The mapping f is an involution. This is verified by iterating the definition of f. Let $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ be a reduction layout, and let $(\vec{\imath}^*, \vec{\jmath}^*, \vec{u}^*, \vec{v}^*, \vec{w}^*) = f(L)$, and let $(\vec{\imath}^{**}, \vec{\jmath}^{**}, \vec{u}^{**}, \vec{v}^{**}, \vec{w}^{**}) = f(f(L))$. Applying the definitions shows that:

$$i^{**}_k = \begin{cases} i^*_{n+1} = i_l & \text{if } k = l \\ i^*_l = i_{n+1} & \text{if } k = n+1 \\ i^*_k = i_k & \text{otherwise} \end{cases} \qquad u^{**}_k = \begin{cases} u^*_l = u_{n+1} & \text{if } k = n+1 \\ u^*_{n+1} = u_l & \text{if } k = l \\ u^*_k = u_k & \text{otherwise} \end{cases}$$

$$j^{**}_{k,1} = \begin{cases} j^*_{n+1,3} = j_{l,1} & \text{if } k = l \\ j^*_{l,2} = j_{n+1} & \text{if } k = n+1 \\ j^*_{k,1} = j_{k,1} & \text{otherwise} \end{cases} \qquad v^{**}_k = \begin{cases} w^*_{n+1} = v_l & \text{if } k = l \\ v^*_k = v_k & \text{otherwise} \end{cases}$$

$$j^{**}_{k,2} = \begin{cases} j^*_{n+1,1} = j_{l,2} & \text{if } k = l \\ j^*_{k,2} = j_{k,2} & \text{otherwise} \end{cases} \qquad w^{**}_k = \begin{cases} v^*_l = w_{n+1} & \text{if } i = n+1 \\ w^*_k = w_k & \text{otherwise} \end{cases}$$

$$j^{**}_{n+1,3} = j^*_{l,1} = j_{n+1,3}$$

$A_{L,\vec{X},\vec{Y}} = A_{f(L),\vec{X},\vec{Y}}$. This is follows from expanding the definitions and doing a little bookkeeping, but it is kind of lengthy, so we defer it until the very end of this proof.

$pe(L) \neq pe(f(L))$. Because $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ is a reduction layout, $\{u_{n+1}, w_{n+1}\} \cap \{u_l, v_l\} = \emptyset$. Applying Definition 8.4, we see that $pe(L) = \{u_{n+1}, w_{n+1}\} \neq \{u_l, v_l\} = \{u^*_{n+1}, w^*_{n+1}\} = pe(f(L))$.

$\mu(f(L)) \geq \mu(L) \cdot (\delta_0^2/20e^3)^{12}$. In order to show this, we need that $\mu(L) > 0$ (which holds because $L \in \mathcal{L}$) and $\mu(f(L)) > 0$ (which depends on the fact that $f(L) \in \mathcal{L}$, which we show below). For now we take the non-zero mass of $f(L)$ as a given. The differences between L and $f(L)$ occur only at: $i_{n+1} \neq i^*_{n+1}$, $i_l \neq i^*_l$, $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \neq (j^*_{n+1,1}, j^*_{n+1,2}, j^*_{n+1,3})$, $(j_{l,1}, j_{l,2}) \neq (j^*_{l,1}, j^*_{l,2})$, $(u_l, v_l, w_l) \neq (u^*_l, v^*_l, w^*_l)$, and $(u_{n+1}, v_{n+1}, w_{n+1}) \neq (u^*_{n+1}, v^*_{n+1}, w^*_{n+1})$. Therefore $HD(L, f(L)) \leq 6$. We apply Lemma 17 to deduce that $\mu(f(L)) \geq \mu(L) \cdot (\delta_0^2/20)^{12} e^{-18}$.

For each $L \in \mathcal{S}^l$, $f(L) \in \mathcal{S}^l$. First we check that $f(L) = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ is indeed a reduction layout. We check each property from Definition 8.2:

1. The indices $i^*_1, \ldots i^*_{n+1}$ are distinct: This holds because $\vec{\imath}^*$ is a permutation of $\vec{\imath}$.
2. The indices $j^*_{1,1}, j^*_{1,2}, \ldots j^*_{n,1}, j^*_{n,2}, j^*_{n+1,1}, j^*_{n+1,2}, j^*_{n+1,3}$ are distinct: This holds because $\vec{\jmath}^*$ is a permutation of $\vec{\jmath}$.
3. The integers $u^*_1, \ldots u^*_{n+1}, v^*_1, \ldots v^*_{n+1}, w^*_1, \ldots w^*_{n+1}$ are distinct: This is true because $u^*_1, \ldots u^*_{n+1}$, $v^*_1, \ldots v^*_{n+1}$, $w^*_1, \ldots w^*_{n+1}$ is a permutation of $u_1, \ldots u_{n+1}, v_1, \ldots v_{n+1}, w_1, \ldots w_{n+1}$.
4. For each $k = 1, \ldots n+1$, $\{u^*_k, v^*_k\} \in E_{i^*_k}$ and $\{u^*_k, w^*_k\} \in E_{i^*_k}$: Because
$$K(\{u_l, u_{n+1}\}, \{v_l, v_{n+1}, w_l, w_{n+1}\}) \subseteq E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}] \cap E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}]$$
we have that $\{u^*_l, v^*_l\} = \{u_{n+1}, w_{n+1}\} \in E_{i_{n+1}} = E_{i^*_l}$, $\{u^*_l, w^*_l\} = \{u_{n+1}, w_l\} \in E_{i_{n+1}} = E_{i^*_l}$, $\{u^*_{n+1}, v^*_{n+1}\} = \{u_l, v_{n+1}\} \in E_{i_l} = E_{i^*_{n+1}}$, and $\{u^*_{n+1}, w^*_l\} = \{u_l, w_l\} \in E_{i_l} = E_{i^*_{n+1}}$. For $k \in [n] \backslash \{l\}$, we have that $\{u^*_k, v^*_k\} = \{u_k, v_k\} \in E_{i_k} = E_{i^*_k}$ and $\{u^*_k, w^*_k\} = \{u_k, w_k\} = E_{i_k} \in E_{i^*_k}$.
5. For each $k = 1, \ldots n+1$, $\{u^*_k, v^*_k, w^*_k\} \subseteq V_{j^*_{k,1}} \cap V_{j^*_{k,2}}$: Because
$$K(\{u_l, u_{n+1}\}, \{v_l, v_{n+1}, w_l, w_{n+1}\}) \subseteq E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}] \cap E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}]$$
we have that $\{u^*_l, v^*_l, w^*_l\} = \{u_{n+1}, w_{n+1}, w_l\} \subseteq V_{j_{n+1,3}} \cap V_{j_{n+1,1}} = V_{j^*_{l,1}} \cap V_{j^*_{l,2}}$. For the same reason, $\{u^*_{n+1}, v^*_{n+1}, w^*_{n+1}\} = \{u_l, v_{n+1}, v_l\} \subseteq V_{j_{l,2}} \cap V_{j_{n+1,2}} = V_{j^*_{n+1,1}} \cap V_{j^*_{n+1,2}}$. For $k \in [n] \setminus \{l\}$, we have that $\{u^*_k, v^*_k, w^*_k\} = \{u_k, v_k, w_k\} \subseteq V_{j_{k,1}} \cap V_{j_{k,2}} = V_{j^*_{k,1}} \cap V_{j^*_{k,2}}$.
6. We have that $\{u^*_{n+1}, v^*_{n+1}, w^*_{n+1}\} = \{u_l, v_{n+1}, v_l\} \subseteq V_{j_{l,1}} = V_{j^*_{n+1,3}}$, because
$$K(\{u_l, u_{n+1}\}, \{v_l, v_{n+1}, w_l, w_{n+1}\}) \subseteq E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}] \cap E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}]$$
7. For each $k \in [n+1]$, $i^*_k \in G$: This holds because $\vec{\imath}^*$ is a permutation of $\vec{\imath}$ and for each $k \in [n+1]$, $i_k \in G$.
8. $(j^*_{n+1,1}, j^*_{n+1,2}, j^*_{n+1,3}) \in N_3(i^*_{n+1})$: Because L is l-switchable, $(j_{n+1,1}, j_{l,1}, j_{l,2}) \in N_3(i_l)$, therefore, $(j^*_{n+1,1}, j^*_{n+1,2}, j^*_{n+1,3}) = (j_{l,2}, j_{n+1,2}, j_{l,1}) \in N_3(i_l) = N_3(i^*_{n+1})$.
9. For each $k = 1, \ldots n$: $(j^*_{k,1}, j^*_{k,2}) \in N_2(i^*_k)$. For $k \in [n] \setminus \{l\}$, we have that $(j^*_{k,1}, j^*_{k,2}) = (j_{k,1}, j_{k,2}) \in N_2(i_k) = N_2(i^*_k)$. When $k = l$, because L is a reduction layout, we have that $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_{n+1})$, and therefore $(j_{n+1,3}, j_{n+1,1}) \in N_2(i_{n+1})$. Thus: $(j^*_{l,1}, j^*_{l,2}) = (j_{n+1,3}, j_{n+1,1}) \in N_2(i_{n+1}) = N_2(i^*_l)$.

This establishes that $f(L) \in \mathcal{L}$. That $f(L) \in \mathcal{S}^l$ follows immediately from the hypothesis that $L \in \mathcal{S}^l$ and the definitions: $(j^*_{n+1,2}, j^*_{l,1}, j^*_{l,2}) = (j_{n+1,2}, j_{n+1,3}, j_{n+1,1}) \in N_3(i_{n+1}) = N_3(i^*_l)$ and

$$\begin{aligned} K(\{u^*_l, u^*_{n+1}\}, \{v^*_l, v^*_{n+1}, w^*_l, w^*_{n+1}\}) &= K(\{u_l, u_{n+1}\}, \{v_l, v_{n+1}, w_l, w_{n+1}\}) \\ &\subseteq E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}] \cap E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}] \\ &= E_{i_l}[V_{j_{l,2}} \cap V_{j_{n+1,2}} \cap V_{j_{l,1}}] \cap E_{i_{n+1}}[V_{j_{n+1,3}} \cap V_{j_{n+1,1}}] \\ &= E_{i^*_{n+1}}[V_{j^*_{n+1,1}} \cap V_{j^*_{n+1,2}} \cap V_{j^*_{n+1,3}}] \cap E_{i^*_l}[V_{j^*_{l,1}} \cap V_{j^*_{l,2}}] \end{aligned}$$

The proof that $A_{f(L),\vec{X},\vec{Y}} = A_{L,\vec{X},\vec{Y}}$: We expand the definitions of $A_{L,\vec{X},\vec{Y}}$ and $A_{f(L),\vec{X},\vec{Y}}$, per definition 8.3 Notice that $\{i_1, \ldots i_{n+1}\} = \{i^*_1, \ldots i^*_{n+1}\}$, $\{j_{1,1}, j_{1,2}, \ldots j_{n,1}, j_{n,2}, j_{n+1,1}, j_{n+1,2}, j_{n+1,3}, \} = \{j^*_{1,1}, j^*_{1,2}, \ldots j^*_{n,1}, j^*_{n,2}, j^*_{n+1,1}, j^*_{n+1,2}, j^*_{n+1,3}, \}$, and $\{u_1, \ldots u_{n+1}, v_1, \ldots v_{n+1}, w_1, \ldots w_{n+1}\} = \{u^*_1, \ldots u^*_{n+1}, v^*_1, \ldots v^*_{n+1}, w^*_1, \ldots w^*_{n+1}\}$. Let I, J, and V respectively denote these three sets. Because $\beta(L)$ and $\beta(L^*)$ are both the lexicographically first assignment to the variables

$$\{x^i_e \mid i \in [m] - I,\ e \in \binom{[3m - V]}{2}\} \cup \{y^j_u \mid j \in [2m+1] - J,\ u \in [3m] - V\}$$

so that β defines a matching of size $m - n - 1$ and an independent set of size $2(m - n - 1)$, we have that $\beta(L) = \beta(L^*)$. Write β for this assignment. We compare $A_{L,\vec{X},\vec{Y}}$ and $A_{f(L),\vec{X},\vec{Y}}$ directly:

$$A_{L,\vec{X},\vec{Y}}(x^i_e) = \begin{cases} \beta(x^i_e) & \text{if } i \in [m] - I \text{ and } e \in \binom{[3m]-V}{2} \\ X_k & \text{if } i = i_k \text{ and } e = \{u_k, v_k\} \text{ for some } k \in [n] \setminus \{l\} \\ \neg X_k & \text{if } i = i_k \text{ and } e = \{u_k, w_k\} \text{ for some } k \in [n] \setminus \{l\} \\ 1(= X_l) & \text{if } i = i_l \text{ and } e = \{u_l, v_l\} \\ 0(= \neg X_l) & \text{if } i = i_l \text{ and } e = \{u_l, w_l\} \\ 1 & \text{if } i = i_{n+1} \text{ and } e = \{u_{n+1}, w_{n+1}\} \\ 0 & \text{otherwise} \end{cases}$$

$$A_{f(L),\vec{X},\vec{Y}}(x^i_e) = \begin{cases} \beta(x^i_e) & \text{if } i \in [m] - I \text{ and } e \in \binom{[3m]-V}{2} \\ X_k & \text{if } i = i_k \text{ and } e = \{u_k, v_k\} \text{ for some } k \in [n] \setminus \{l\} \\ \neg X_k & \text{if } i = i_k \text{ and } e = \{u_k, w_k\} \text{ for some } k \in [n] \setminus \{l\} \\ 1 & \text{if } i = i_l (= i^*_{n+1}) \text{ and } e = \{u_l, v_l\} (= \{u^*_{n+1}, w^*_{n+1}\}) \\ 0 & \text{if } i = i_l (= i^*_{n+1}) \text{ and } e = \{u_l, w_l\} (= \{u^*_{n+1}, w^*_l\}) \\ 1(= X_l) & \text{if } i = i_{n+1} (= i^*_l) \text{ and } e = \{u_{n+1}, w_{n+1}\} (= \{u^*_l, v^*_l\}) \\ 0 & \text{otherwise} \end{cases}$$

$$A_{L,\vec{X},\vec{Y}}(y^j_x) = \begin{cases} \beta(y^j_x) & \text{if } j \in [2m+1] - J \text{ and } u \in [3m] - V \\ 1 & \text{if } j = j_{k,1} \text{ and } x = v_k \text{ for some } k \in [n] \\ Y_k & \text{if } j = j_{k,2} \text{ and } x = u_k \text{ for some } k \in [n] \setminus \{l\} \\ \neg Y_k & \text{if } j = j_{k,2} \text{ and } x = w_k \text{ for some } k \in [n] \setminus \{l\} \\ 1(= Y_l) & \text{if } j = j_{l,2} \text{ and } x = u_l \\ 0(= \neg Y_l) & \text{if } j = j_{l,2} \text{ and } x = w_l \\ 1 & \text{if } j = j_{n+1,1} \text{ and } x = u_{n+1} \\ 1 & \text{if } j = j_{n+1,2} \text{ and } x = v_{n+1} \\ 1 & \text{if } j = j_{n+1,3} \text{ and } x = w_{n+1} \\ 0 & \text{otherwise} \end{cases}$$

$$A_{f(L),\vec{X},\vec{Y}}(y_x^j) \quad = \quad \begin{cases} \beta(y_x^j) & \text{if } j \in [2m+1]-J \text{ and } u \in [3m]-V \\ 1 & \text{if } j = j_{k,1} \text{ and } x = v_k \text{ for some } k \in [n] \\ Y_k & \text{if } j = j_{k,2} \text{ and } x = u_k \text{ for some } k \in [n] \setminus \{l\} \\ \neg Y_k & \text{if } j = j_{k,2} \text{ and } x = w_k \text{ for some } k \in [n] \setminus \{l\} \\ 1 & \text{if } j = j_{l,2} (= j^*_{n+1,1}) \text{ and } x = u_l (= u^*_{n+1}) \\ 0 & \text{if } j = j_{l,2} (= j^*_{n+1,1} \text{ and } x = w_l (= w^*_l) \\ 1 (= X_l) & \text{if } j = j_{n+1,1} (= j^*_{l,2}) \text{ and } x = u_{n+1} = u^*_l \\ 1 & \text{if } j = j_{n+1,2} (= j^*_{n+1,2}) \text{ and } x = v_{n+1} = v^*_{n+1} \\ 1 & \text{if } j = j_{n+1,3} (= j^*_{l,1}) \text{ and } x = w_{n+1} = v^*_l \\ 0 & \text{otherwise} \end{cases}$$

■

10 Distributions from DDWB processes

To prove Lemmas 16 and 17, we make some detailed calculations about the distribution $\mathcal{D}$. It seems that by moving to slightly more general framework, some of the calculations and case analyses are simplified. In Lemma 22 in Section 11 we show that the distribution $\mathcal{D}$ falls into this framework and use the machinery of DDWB processes developed in this section to finish the proofs of Lemma 16 and Lemma 17.

Definition 10.1 *Let t be an integer, $X_1, \dots X_t$ be sets, and let $S_i : \prod_{k=1}^{i-1} X_k \to \mathfrak{P}(X_i)$, and $F_i : \prod_{k=1}^{i-1} X_k \to \mathfrak{P}(X_i)$ be families of maps with $i \in [t]$. We define the* dependent domains with blocking process for $S_1, \dots S_t$ and $F_1, \dots F_t$, $D(S_1, \dots S_t, F_1, \dots F_t)$, *recursively as follows:*

1. *If $S_1 \setminus F_1 \neq \emptyset$, then $D(S_1, F_1)$ is the distribution that uniformly selects an object from $S_1 \setminus F_1$*
2. *If for every $(u_1, \dots u_i)$ in the support of $D(S_1, \dots S_i, F_1, \dots F_i)$, we have that $S_{i+1}(u_1, \dots u_i) \setminus F_{i+1}(u_1, \dots u_i) \neq \emptyset$, then $D(S_1, \dots S_{i+1}, F_1, \dots F_{i+1})$ is the distribution that chooses $(u_1, \dots u_i)$ according to $D(S_1, \dots S_i, F_1, \dots F_i)$, and then uniformly selects u_{i+1} from $S_{i+1}(u_1, \dots u_i) \setminus F_{i+1}(u_1, \dots u_i)$.*

The blockage bound *of a DDWB process $\vec{S}$, $\vec{F}$ is the smallest $\beta \geq 0$ so that for all $i = 1, \dots t$ and all $\vec{u}$ in the support of $D(S_1, \dots S_{i-1}, F_1, \dots F_{i-1})$, $|F_i(\vec{u})| \leq \beta |S_i(\vec{u})|$. The* covering bound *for $\vec{S}$, $\vec{F}$ is the largest $\kappa \in [0,1]$ so that for all $i = 1, \dots t$ and all $\vec{u}$ the support of $D(S_1, \dots S_{i-1}, F_1, \dots F_{i-1})$, $|S_i(\vec{u}) \setminus F_i(\vec{u})| \geq \kappa |X_i|$.*

The following easy fact is the crux of some induction arguments.

Proposition: Let π be the distribution on $\prod_{i=1}^t X_i$ given by the DDWB process $\vec{S}$, $\vec{F}$. For each $a \in S_1 \setminus F_1$ (eg. every a in the support of $D(S_1, F_1)$), the distribution π^a is generated by the DDWB process on $\prod_{i=2}^t X_i$ given by $S_2^a, \dots S_t^a$, $F_2^a, \dots F_t^a$. If the process $\vec{S}$, $\vec{F}$ has a blockage bound $\leq \beta$, then the process $\vec{S}^a$, $\vec{F}^a$ has a blockage bound $\leq \beta$.

The following lemma is used to pass density results for the uniform distribution, such as Lemma 3, to certain DDWB distributions.

Lemma 19 *Let $\prod_{i=1}^{t} X_i$ be a Cartesian product, and let $f : \prod_{i=1}^{t} X^i \to [0,1]$ be a function that depends upon at most k coordinates, $i_1, \ldots i_k$. Let U be the uniform distribution on $\prod_{i=1}^{t} X_i$, and let π be a DDWB distribution on $\prod_{i=1}^{t} X_i$ given by some $\vec{S}$ and $\vec{F}$. If the following two conditions are satisfied:*

1. *For all $\vec{a} \in \prod_{i=1}^{t} X_i$, if $f(\vec{a}) > 0$ then for all $j = 1, \ldots k$, $a_{i_j} \in S_{i_j}(a_1, \ldots a_{i_j - 1})$.*
2. *The DDWB process $\vec{S}$, $\vec{F}$ has blockage bound $\leq \beta$.*

Then $\mathbb{E}_{\pi}[f] \geq \mathbb{E}_{U}[f] - k\beta$.

Proof: We prove the claim by induction on k. The lemma clearly holds for $k = 0$, as in that case f is constant over $\prod_{i=1}^{t} X_i$, and therefore $\mathbb{E}_{\pi}[f] = \mathbb{E}_{U}[f]$. We now assume that the lemma holds for functions that depend on only k coordinates, and demonstrate that it holds for functions that depend on only $k+1$ coordinates.

Let t, $\prod_{i=1}^{t} X_i$, π, $\vec{S}$, $\vec{F}$, and be given as in the statement of the lemma- with f dependent only upon $k+1$ coordinates, $i_1, \ldots i_{k+1}$. Let $i = i_1$ be the first coordinate upon which the function f depends. Set $I = [i-1]$ and $J = [t] \setminus [i]$. Let $X_I = \prod_{k \in I} X_k$ and $X_J = \prod_{k \in J} X_k$.

We reduce to the induction hypothesis by showing that for each $\vec{u} \in X_I$, $a \in X_i$, so that $(u_1, \ldots u_{i-1}, a)$ is in the support of $D(S_1, \ldots S_i, F_1, \ldots F_i)$, the conditions of the induction hypothesis are met for the function $f^{\vec{u}a}$, with process $D(S_{i+1}^{\vec{u}a}, \ldots S_t^{\vec{u}a}, F_{i+1}^{\vec{u}a}, \ldots F_t^{\vec{u}a})$, and distribution $\pi^{\vec{u}a}$. Observe that the distribution $\pi^{\vec{u}a}$ is given by the DDWB process $S_{i+1}^{\vec{u}a}, \ldots S_t^{\vec{u}a}$ and $F_{i+1}^{\vec{u}a}, \ldots F_t^{\vec{u}a}$, a process with blockage bound $\leq \beta$ because $\vec{S}$, $\vec{F}$ has blockage bound $\leq \beta$. Moreover, the function $f^{\vec{u}a} : \prod_{j=i+1}^{t} X_i \to [0,1]$ depends on at most k coordinates. By specializing the hypothesis "for all $\vec{a}$, if $f(\vec{a}) > 0$ then for all $j = 1, \ldots k$, $a_{i_j} \in S_{i_j}(a_1, \ldots a_{i_j - 1})$" to inputs with prefix $\vec{u}a$ and weakening its conclusion to cover only $j = 2, \ldots k$, we have that "for all $\vec{b} \in X_J$ so that $f(\vec{u}a\vec{b}) > 0$, for all $j = 2, \ldots k$, $b_{i_j} \in S_{i_j}(\vec{u}, a, b_{i+1}, \ldots b_{i_j - 1})$". This is equivalent to "for all $\vec{b} \in X_J$ so that $f^{\vec{u}a}(\vec{b}) > 0$, for all $j = 2, \ldots k$, $b_{i_j} \in S_{i_j}^{\vec{u}a}(b_{i+1}, \ldots b_{i_j - 1})$". Therefore by the induction hypothesis we have that:

$$\mathbb{E}_{\pi^{\vec{u}a}}[f^{\vec{u}a}] \geq \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] - k\beta \tag{3}$$

Furthermore, from the hypothesis "for all $\vec{u} \in \prod_{i=1}^{t} X_i$, if $f(\vec{u}) > 0$ then $\forall j \in [k+1]$, $u_{i_j} \in S_{i_j}(u_1, \ldots u_{i_j - 1})$" we conclude that for all $\vec{v} \in \prod_{j=1}^{i} X_j$ with $\mathbb{E}_{U^{\vec{v}}}[f^{\vec{v}}] > 0$, $v_i \in S_i(v_1, \ldots v_{i-1})$. Therefore, for all $\vec{u} = (u_1, \ldots u_{i-1}) \in X_I$

$$\mathbb{E}_{U^{\vec{u}}}[f^{\vec{u}}] = \sum_{a \in X_i} \frac{1}{|X_i|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] = \sum_{a \in S_i(\vec{u})} \frac{1}{|X_i|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] \leq \sum_{a \in S_i(\vec{u})} \frac{1}{|S_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] \tag{4}$$

We now bound the expectation of f with respect to π from below.

$$\begin{aligned}
\mathbb{E}_{\pi}[f] &= \sum_{\vec{u} \in X_I} \pi_I(\vec{u}) \sum_{a \in X_i} \sum_{\vec{b} \in X_J} \pi^{\vec{u}}(a\vec{b}) f(\vec{u}a\vec{b}) \\
&= \sum_{\vec{u} \in Supp(\pi_I)} \pi_I(\vec{u}) \sum_{a \in X_i} \sum_{\vec{b} \in X_J} \frac{\chi_{S_i(\vec{u}) \setminus F_i(\vec{u})}(a)}{|S_i(\vec{u}) \setminus F_i(\vec{u})|} \pi^{\vec{u}a}(\vec{b}) f(\vec{u}a\vec{b}) \\
&= \sum_{\vec{u} \in Supp(\pi_I)} \pi_I(\vec{u}) \sum_{a \in S_i(\vec{u})} \sum_{\vec{b} \in X_J} \frac{1 - \chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u}) \setminus F_i(\vec{u})|} \pi^{\vec{u}a}(\vec{b}) f(\vec{u}a\vec{b})
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\vec{u}\in Supp(\pi_I)} \pi_I(\vec{u}) \sum_{a\in S_i(\vec{u})} \frac{1-\chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u})\setminus F_i(\vec{u})|} \sum_{\vec{b}\in X_J} \pi^{\vec{u}a}(\vec{b}) f(\vec{u}a\vec{b}) \\
&= \sum_{\vec{u}\in Supp(\pi_I)} \pi_I(\vec{u}) \sum_{a\in S_i(\vec{u})} \frac{1-\chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u})\setminus F_i(\vec{u})|} \mathbb{E}_{\pi^{\vec{u}a}}[f^{\vec{u}a}] \\
&\geq \sum_{\vec{u}\in Supp(\pi_I)} \pi_I(\vec{u}) \sum_{a\in S_i(\vec{u})} \frac{1-\chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u})\setminus F_i(\vec{u})|} \left(\mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] - k\beta\right) \text{ by Equation 3} \\
&= -k\beta + \sum_{\vec{u}\in Supp(\pi_I)} \pi_I(\vec{u}) \sum_{a\in S_i(\vec{u})} \frac{1-\chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u})\setminus F_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] \\
&\geq -k\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \sum_{a\in S_i(\vec{u})} \frac{1-\chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] \\
&\geq -k\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \left(\sum_{a\in S_i(\vec{u})} \frac{1}{|S_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] - \sum_{a\in S_i(\vec{u})} \frac{\chi_{F_i(\vec{u})}(a)}{|S_i(\vec{u})|} \right) \\
&\geq -k\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \left(\sum_{a\in S_i(\vec{u})} \frac{1}{|S_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] - \frac{|F_i(\vec{u})|}{|S_i(\vec{u})|} \right) \\
&\geq -k\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \left(\sum_{a\in S_i(\vec{u})} \frac{1}{|S_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] - \beta \right) \\
&= -(k+1)\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \sum_{a\in S_i(\vec{u})} \frac{1}{|S_i(\vec{u})|} \mathbb{E}_{U^{\vec{u}a}}[f^{\vec{u}a}] \\
&\geq -(k+1)\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \mathbb{E}_{U^{\vec{u}}}[f^{\vec{u}}] \text{ by Equation 4} \\
&= -(k+1)\beta + \sum_{\vec{u}\in supp(\pi_I)} \pi_I(\vec{u}) \mathbb{E}_U[f] = -(k+1)\beta + \mathbb{E}_U[f]
\end{aligned}
$$

The penultimate equality holds because the function f is independent of the coordinates of I, and therefore, for all $\vec{u} \in X_I$, $\mathbb{E}_{U^{\vec{u}}}[f^{\vec{u}}] = \mathbb{E}_U[f]$.

■

Lemma 20 *Let π be a distribution on the Cartesian product $\prod_{i=1}^t X_i$ given by a DDWB process $\vec{S}$, $\vec{F}$ with covering bound κ. Let c and d be arbitrary. Let $\vec{u}, \vec{v} \in \prod_{i=1}^t X_i$ be arbitrary. Let $I_0 \subseteq [t]$ so that $|I_0| = d$. If for all $i = 1, \ldots t$,*

1. *$\pi(\vec{u}) > 0$ and $\pi(\vec{v}) > 0$*
2. *For all $i \in [t] \setminus I_0$, $S_i(u_1, \ldots u_{i-1}) = S_i(v_1, \ldots v_{i-1})$*
3. *For all $i \in [t] \setminus I_0$, $|F_i(u_1, \ldots u_{i-1}) \oplus F_i(v_1, \ldots v_{i-1})| \leq (c/t)|X_i|$*

then $\pi(\vec{v}) < \kappa^{-d} e^{c/\kappa} \pi(\vec{u})$.

Proof: Explicit calculation reveals that:

$$\begin{aligned}
\frac{\pi(\vec{u})}{\pi(\vec{v})} &= \frac{\prod_{i=1}^{t}\left(\frac{1}{|S_i(u_1,\ldots u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|}\right)}{\prod_{i=1}^{t}\left(\frac{1}{|S_i(v_1,\ldots v_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}\right)} = \prod_{i=1}^{t}\frac{|S_i(v_1,\ldots v_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|} \\
&= \prod_{i\in I_0}\frac{|S_i(v_1,\ldots v_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|}\prod_{i\in[t]\setminus I_0}\frac{|S_i(v_1,\ldots v_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|} \\
&\leq \prod_{i\in I_0}\frac{|X_i|}{\kappa|X_i|}\prod_{i\in[t]\setminus I_0}\frac{|S_i(v_1,\ldots v_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|} \\
&= \kappa^{-d}\prod_{i\in[t]\setminus I_0}\frac{|S_i(v_1,\ldots v_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|} = \kappa^{-d}\prod_{i\in[t]\setminus I_0}\frac{|S_i(u_1,\ldots u_{i-1})\setminus F_i(v_1,\ldots v_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|} \\
&\leq \kappa^{-d}\prod_{i\in[t]\setminus I_0}\frac{|S_i(u_1,\ldots u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|+|F_i(v_1,\ldots v_{i-1})\oplus F_i(u_1,\ldots u_{i-1})|}{|S_i(u_1,\ldots,u_{i-1})\setminus F_i(u_1,\ldots u_{i-1})|} \\
&\leq \kappa^{-d}\prod_{i\in[t]\setminus I_0}\left(1+\frac{(c/t)|X_i|}{\kappa|X_i|}\right) \leq \kappa^{-d}e^{(t-d)\frac{c}{t\kappa}} \leq \kappa^{-d}e^{\frac{c}{\kappa}}
\end{aligned}$$

■

Definition 10.2 *We say that a function* $F:\prod_{i=1}^{l}X_i\to\mathfrak{P}(S)$ *is* ϵ-Lipschitz *if whenever* $HD(\vec{u},\vec{v})\leq d$, *we have that* $|F(\vec{u})\oplus F(\vec{v})|\leq\epsilon d|S|$.

Corollary 21 *Let* π *be a distribution on the Cartesian product* $\prod_{i=1}^{t}X_i$ *given by a DDWB process* $\vec{S}$, $\vec{F}$ *with covering bound* κ *so that each coordinate* $i_0\in[t]$ *affects at most* a *functions* S_i *and each* F_i *is* c/t*-Lipschitz. Let* $\vec{u},\vec{v}\in\prod_{i=1}^{t}X_i$ *be given so that* $\pi(\vec{u})>0$ *and* $\pi(\vec{v})>0$. *Then:*

$$\pi(\vec{v})<\kappa^{-aHD(\vec{u},\vec{v})}e^{cHD(\vec{u},\vec{v})/\kappa}\pi(\vec{u})$$

Proof: Let $\Delta=\{i\in[t]\mid u_i\neq v_i\}$ and let $I_0=\{i\in[t]\mid S_i$ depends upon some $i\in\Delta\}$. We apply Lemma 20: Condition 1 holds by hypothesis. By hypothesis, $|I_0|\leq aHD(\vec{u},\vec{v})$. Condition 2 holds because for all $i\in[t]\setminus I_0$, S_i depends only upon indices where $\vec{u}$ and $\vec{v}$ agree. Condition 3 holds because the F_i's are c/t-Lipschitz: $|F_i(u_1,\ldots u_{i-1})\oplus F_j(v_1,\ldots v_{i-1})|\leq(c/t)HD(\vec{u},\vec{v})|X_i|=(cHD(\vec{u},\vec{v})/t)|X_i|$. ■

The blocking functions that we encounter in our distributions are easily seen to be Lipschitz:

Proposition:

1. The function $(u_1,\ldots u_{i-1})\mapsto\{u_1,\ldots u_{i-1}\}$ from $[n]^{i-1}$ to $\mathfrak{P}([n])$ is $1/n$-Lipschitz.
2. The function $((u_1,v_1),\ldots(u_{i-1},v_{i-1}))\mapsto pm_{[n]}(\{u_1,\ldots u_{i-1},v_1,\ldots v_{i-1}\})$ from $[n^2]^{i-1}$ to $\mathfrak{P}([n]^2)$ is $4/n$-Lipschitz.
3. The function $((u_1,v_1),\ldots(u_{i-1},v_{i-1}))\mapsto tm_{[n]}(\{u_1,v_1\ldots u_{i-1},v_{i-1}\})$ from $\left([n]^2\right)^{i-1}$ to $\mathfrak{P}([n]^3)$ is $6/n$-Lipschitz.
4. The function $((u_1,v_1,w_1),\ldots(u_{i-1},v_{i-1},w_{i-1}))\mapsto tm_{[n]}(\{u_1,v_1,w_1,\ldots u_{i-1},v_{i-1},w_{i-1}\})$ from $\left([n]^3\right)^{i-1}$ to $\mathfrak{P}([n]^3)$ is $9/n$-Lipschitz.

11 The distribution $\mathcal{D}$ is a DDWB distribution

We give a DDWB process $\vec{S}$, $\vec{F}$ and show that it produces the distribution $\mathcal{D}$ used to generate reduction layouts used in the reduction from set-disjointness to the *FindBadEdge* search lemma. This enables us to use the machinery of DDWB distributions to prove Lemma 16 and Lemma 17.

Definition 11.1 *Let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$. Let G, $N_3(\cdot)$, $N_2(\cdot)$ be as in Definition 8.1. We define a DDWB process $\vec{S}$, $\vec{F}$ over the Cartesian product $[m]^{n+1} \times \left([2m+1]^2\right)^n \times \left([2m+1]^3\right) \times \left([3m]^3\right)^{n+1}$ as follows:*

1. *When choosing i_k given $i_1, \ldots i_{k-1}$: $X_k = [m]$, $S_k = G$ and $F_k(i_1, \ldots i_{k-1}) = \{i_1, \ldots i_{k-1}\}$.*
2. *When choosing $(j_{k,1}, j_{k,2})$ given $\vec{\imath}, (j_{1,1}, j_{1,2}), \ldots (j_{k-1,1}, j_{k-1,2})$ (with $k \leq n$), we have $X_{n+1+k} = [2m+1]^2$, $S_{n+1+k}(\vec{\imath}, (j_{1,1}, j_{1,2}), \ldots (j_{k-1,1}, j_{k-1,2})) = N_2(i_k)$, and:*

$$F_{n+1+k}(\vec{\imath}, (j_{1,1}, j_{1,2}), \ldots (j_{k-1,1}, j_{k-1,2})) \quad = \quad pm_{[2m+1]}\left(\{j_{1,1}, j_{1,2}, \ldots j_{k-1,1}, j_{k-1,2}\}\right)$$

3. *When choosing $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3})$ given $\vec{\imath}, (j_{1,1}, j_{1,2}), \ldots (j_{n,1}, j_{n,2})$, we have $X_{2n+2} = [2m+1]^3$, $S_{2n+2}(\vec{\imath}, (j_{1,1}, j_{1,2}), \ldots (j_{n,1}, j_{n,2})) = N_3(i_{n+1})$, and:*

$$F_{2n+2}(\vec{\imath}, (j_{1,1}, j_{1,2}), \ldots (j_{n,1}, j_{n,2})) \quad = \quad tm_{[2m+1]}\{j_{1,1}, j_{1,2}, \ldots j_{n,1}, j_{n,2}\}$$

4. *For $k \leq n$, when choosing (u_k, v_k, w_k) given $\vec{\imath}, \vec{\jmath}, (u_1, v_1, w_1), \ldots (u_{k-1}, v_{k-1}, w_{k-1})$, $X_{2n+2+k} = [3m]^3$, $S_{2n+2+k}(\vec{\imath}, \vec{\jmath}, (u_1, v_1, w_1), \ldots (u_{k-1}, v_{k-1}, w_{k-1})) = \mathcal{K}_{1,2}\left(E_{i_k}[V_{j_{k,1}} \cap V_{j_{k,2}}]\right)$, and*

$$F_{2n+2+k}(\vec{\imath}, \vec{\jmath}, (u_1, v_1, w_1), \ldots (u_{k-1}, v_{k-1}, w_{k-1})) \quad = \quad tm_{[3m]}(\{u_1, v_1, w_1, \ldots u_{k-1}, v_{k-1}, w_{k-1}\})$$

5. *When choosing $(u_{n+1}, v_{n+1}, w_{n+1})$ given $\vec{\imath}, \vec{\jmath}, (u_1, v_1, w_1), \ldots (u_n, v_n, w_n)$, $X_{3n+3} = [3m]^3$, $S_{3n+3}(\vec{\imath}, \vec{\jmath}, (u_1, v_1, w_1), \ldots (u_{k-1}, v_{k-1}, w_{k-1})) = \mathcal{K}_{1,2}\left(E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}]\right)$, and*

$$F_{3n+3}(\vec{\imath}, \vec{\jmath}, (u_1, v_1, w_1), \ldots (u_n, v_n, w_n)) \quad = \quad tm_{[3m]}(\{u_1, v_1, w_1, \ldots u_n, v_n, w_n\})$$

Notice that each coordinate affects at most two of the domain functions S_k.

Lemma 22 *Let $\delta_0 \in [0,1]$ be given, and let $m \geq 450/\delta_0^2$ be given. Let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$ so that $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$ and let $\gamma = \frac{n+1}{m}$. The distribution $\mathcal{D}(\mathcal{V}_I, \mathcal{V}_{II})$ is generated by the DDWB process $\vec{S}$, $\vec{F}$ over the Cartesian product $[m]^{n+1} \times \left([2m+1]^2\right)^n \times ([2m+1]^3) \times \left([3m]^3\right)^{n+1}$. Moreover, this process has blockage bound $\leq 30\gamma/\delta_0^2$ and it has covering bound $\geq \min\{\delta_0^2/10 - 3\gamma, \delta_0/3 - 3\gamma, \delta_0/12 - \gamma\}$.*

Proof: That the DDWB process $\vec{S}$, $\vec{F}$ generates the distribution $\mathcal{D}$ follows immediately by comparing the above functions with the experiment of Definition 8.2. The covering bounds follow immediately from Lemma 15, and the blockage bounds are implicit in those calculations. ∎

Corollary 23 *If $\gamma \leq \delta_0^2/60$, then the covering bound of the process is $\geq \delta_0^2/20$, ie. $\kappa \geq \delta_0^2/20$.*

Now we use Lemma 20 to prove Lemma 17:

Proof:(of Lemma 17) Let $L = (\vec{\imath}, \vec{\jmath}, \vec{u}, \vec{v}, \vec{w})$ and $L^* = (\vec{\imath}^*, \vec{\jmath}^*, \vec{u}^*, \vec{v}^*, \vec{w}^*)$ be two reduction layouts from $\mathcal{L}^p$ with $HD(L, L^*) \leq d$. Let $\vec{S}$ and $\vec{F}$ be the DDWB process for generating the distribution $\mathcal{D}^p$ as described in Definition 11.1.

We now check that the hypotheses of Corollary 21 are met with the process $\vec{S}$, $\vec{F}$ over $[m]^{n+1} \times \left([2m+1]^2\right)^n \times ([2m+1]^3) \times \left([3m]^3\right)^{n+1}$, with $t = 3n+3$, with $\pi = \mu$, and with $\vec{u} = L^*$, $\vec{v} = L$ By Lemma 22 and Corollary 23, the DDWB process generating μ has $\kappa \geq \delta_0^2/20$ and $\gamma = \frac{n+1}{m} \leq \delta_0^2/60$.

1. $\mu(L) > 0$ and $\mu(L^*) > 0$. This is satisfied because $L \in \mathcal{L}$, and $L^* \in \mathcal{L}$.

2. Each coordinate affects at most two of the domain functions S_i.

3. This simply applies Proposition 10 to the definitions of the blocking functions. The functions $F_1, \ldots F_{n+1}$ are $1/m$-Lipschitz. The functions $F_{n+2}, \ldots F_{2n+1}$ are $4/(2m+1)$-Lipschitz. The function F_{2n+2} is $6/(2m+1)$-Lipschitz. The functions $F_{2n+3}, \ldots F_{3n+3}$ are $9/(2m+1)$-Lipschitz. Because $m = \frac{n+1}{\gamma} = \frac{t}{3\gamma}$, all of the functions are c/t-Lipschitz for some $c = \Theta(\gamma)$.

Therefore, by Corollary 21:

$$\mu(L) \leq \kappa^{-2d} e^{\Theta(d\gamma)/\kappa} \mu(L^*)$$

■

Now we use Lemma 19 to prove Lemma 16.

Proof:(of Lemma 16) Fix $m > 31(2/\delta_0)^2$, and let $(\mathcal{V}_I, \mathcal{V}_{II})$ be a partition of $MVars_m$ with $\delta(\mathcal{V}_I, \mathcal{V}_{II}) \geq \delta_0$. Let n be given so that $n \leq \delta_0^{10}/(2^{12} \cdot 3^2 \cdot 5)m$. Let $l \in [n]$ be given. Let U be uniform distribution on $[m]^{n+1} \times \left([2m+1]^2\right)^n \times ([2m+1]^3) \times \left([3m]^3\right)^{n+1}$. Let μ be the mass function for the distribution $\mathcal{D}$; view μ as a distribution on $[m]^{n+1} \times \left([2m+1]^2\right)^n \times ([2m+1]^3) \times \left([3m]^3\right)^{n+1}$ whose support is on $\mathcal{L}$. Set β to be the blockage bound for the DDWB process generating $\mathcal{D}$. Let $\mathcal{A} \subseteq [m]^{n+1} \times \left([2m+1]^2\right)^n \times ([2m+1]^3) \times \left([3m]^3\right)^{n+1}$ be the event that: $i_l \in G$ and $i_{n+1} \in G$, $(j_{l,1}, j_{l,2}) \in N_2(i_l)$, $(j_{n+1,2}, j_{l,1}, j_{l,2}) \in N_3(i_l)$, $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_{n+1})$, and $K\left(\{u_{n+1}, u_l\}, \{v_{n+1}, v_l, w_{n+1}, w_l\}\right) \subseteq E_{i_l}\left[V_{j_{l,1}} \cap V_{j_{l,2}}\right] \cap E_{i_{n+1}}\left[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}\right]$. Checking against Definition 9.2 reveals that $\mathcal{S}^l = \mathcal{L} \cap \mathcal{A}$, and because $\mu(\mathcal{L}) = 1$, $\mu(\mathcal{S}^l) = \mu(\mathcal{L} \cap \mathcal{A}) = \mu(\mathcal{A})$.

Because the event $\mathcal{A}$ depends only upon the six coordinates i_l, i_{n+1}, $(j_{l,1}, j_{l,2})$, $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3})$, (u_l, v_l, w_l), and $(u_{n+1}, v_{n+1}, w_{n+1})$, and the event $\mathcal{A}$ implies that $(u_l, v_l, w_l) \in \mathcal{K}_{1,2}\left(E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}]\right)$ and $(u_{n+1}, v_{n+1}, w_{n+1}) \in \mathcal{K}_{1,2}\left(E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}]\right)$, we may apply Lemma 19 to conclude:

$$\mu(\mathcal{A}) \geq U(\mathcal{A}) - 6\beta \tag{5}$$

Let I denote the indices $1, \ldots 2n+2$ (so that, using our abused notation, the coordinates of I correspond to $\vec{\imath}, \vec{\jmath}$). Let $A = \mathcal{A}_I$, a note that is a subset of the event that $i_l, i_{n+1} \in G$, $(j_{l,1}, j_{l,2}) \in N_2(i_l)$, $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_{n+1})$, and $(j_{n+1,2}, j_{l,1}, j_{l,2}) \in N_3(i_l)$. For each $\vec{\imath}$ and $\vec{\jmath}$ set $D(\vec{\imath}, \vec{\jmath}) = |E_{i_l}\left[V_{j_{l,1}} \cap V_{j_{l,2}}\right] \cap E_{i_{n+1}}\left[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}\right]|/\binom{3m}{2}$. By Lemma 3: $U(\mathcal{A}^{\vec{\imath},\vec{\jmath}}) \geq (D(\vec{\imath}, \vec{\jmath}))^8 - 23/3m$. Therefore:

$$U(\mathcal{A}) \geq \mathbb{E}_U[(D^8 - 23/3m) \cdot \chi_A] = \mathbb{E}_U[(D \cdot \chi_A)^8] - 23/3m \geq \left(\mathbb{E}_U[D \cdot \chi_A]\right)^8 - 23/3m \tag{6}$$

Set $\delta = \delta(\mathcal{V}_I, \mathcal{V}_{II})$, and let C be the event that $|\{j_{l,1}, j_{l,2}, j_{n+1,1}, j_{n+1,2}, j_{n+1,3}\}| < 5$. Notice that for all $(\vec{\imath}, \vec{\jmath}) \in C^c$, if $|E_{i_l}[V_{j_{l,1}} \cap V_{j_{l,2}}] \cap E_{i_{n+1}}[V_{j_{n+1,1}} \cap V_{j_{n+1,2}} \cap V_{j_{n+1,3}}]|/\binom{3m}{2} = D(\vec{\imath}, \vec{\jmath}) > \delta/3$ then $(j_{l,1}, j_{l,2}) \in N_2(i_l)$, $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_{n+1})$, $(j_{n+1,2}, j_{l,1}, j_{l,2}) \in N_3(i_l)$, so by virtue of $(\vec{\imath}, \vec{\jmath}) \notin A$, $\{i_l, i_{n+1}\} \not\subseteq G$. Moreover, we have that $(j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_l)$. Therefore:

$$\{(\vec{\imath}, \vec{\jmath}) \in A^c \mid D(\vec{\imath}, \vec{\jmath}) \geq \delta/3\} \subseteq C \cup \{(\vec{\imath}, \vec{\jmath}) \mid (j_{n+1,1}, j_{n+1,2}, j_{n+1,3}) \in N_3(i_l) \cap N_3(i_{n+1}),\ \{i_l, i_{n+1}\} \not\subseteq G\}$$

For each $\vec{\imath}$ with $\{i_l, i_{n+1}\} \not\subseteq G$ we have that $|N_3(i_l) \cap N_3(i_{n+1})| < (\delta/12)(2m+1)^3$ and therefore $U\left(\{(\vec{\imath}, \vec{\jmath}) \in A^c \mid D(\vec{\imath}, \vec{\jmath}) \geq \delta/3\} \setminus C\right) < \delta/12$. By the union bound, $U(C) \leq 10/(2m+1)$ so $U\left(\{(\vec{\imath}, \vec{\jmath}) \in A^c \mid D(\vec{\imath}, \vec{\jmath}) \geq \delta/3\}\right) < \delta/12 + 10/(2m+1)$. By Lemma 4, $\mathbb{E}_U[D \cdot \chi_{A^c}] < \delta/3 + \delta/12 + 10/(2m+1)$. Therefore:

$$\begin{aligned}\mathbb{E}_U[D \cdot \chi_A] &\geq \mathbb{E}_U[D] - 10/(2m+1) - 5\delta/12 = 7\delta/12 - 10/(2m+1) \\ &\geq 7\delta/12 - 6/(2(36/\delta)) = 7\delta/12 - \delta/12 \geq \delta/2 \geq \delta_0/2 \end{aligned} \quad (7)$$

Combining equations 5, 6, and 7, we have:

$$\mu(\mathcal{A}) \geq U(\mathcal{A}) - 6\beta \geq (\mathbb{E}_U[D \cdot \chi_A])^8 - 23/3m - 6\beta \geq (\delta_0/2)^8 - 23/3m - 6\beta$$

Because $m > 31(2/\delta_0)^8$, we have that $23/3m < (1/4)(2/\delta_0)^8$. By Lemma 22, $\beta \leq 30\gamma/\delta_0^2 \leq \delta_0^{10}/(2^8 \cdot 3^2 \cdot 5)/\delta_0^2 = (1/24)(\delta_0/2)^8$. Therefore:

$$\mu(\mathcal{A}) > (\delta_0/2)^8 - (1/4)(\delta_0/2)^8 - 6(1/24)(\delta_0/2)^8 = (1/2)(\delta_0/2)^8$$

■

References

[1] A. Aguirre and M. Vardi. Random 3-SAT and BDDs: The plot thickens further. In *Principles and Practice of Constraint Programming*, pages 121–136, 2001.

[2] F. Aloul, M. Mneimneh, and K. Sakallah. ZBDD-based backtrack search SAT solver. In *Eleventh IEEE/ACM Workshop on Logic & Synthesis*, pages 131–136, 2002.

[3] A. Atserias, P. Kolaitis, and M. Vardi. Constraint propagation as a proof system. In *Tenth International Conference on Principles and Practice of Constraint Programming*, pages 77–91, 2004.

[4] P. Beame, H. Kautz, and A. Sabharwal. Towards understanding and harnessing the potential of clause learning. *Journal of Artificial Intelligence Research*, 22:319–351, 2004.

[5] P. Beame, T. Pitassi, and N. Segerlind. Lower bounds for lovász-schrijver systems and beyond follow from multiparty communication complexity. In *Proceedings of the Thirty-Second International Colloquium on Automata, Languages, and Programming*, pages 1176–1188, 2005.

[6] M. L. Bonet, J. L. Esteban, and N. Galesiand J. Johannsen. On the relative complexity of resolution refinements and cutting planes proof systems. *SIAM Journal on Computing*, 30(5):1462–1484, 2000.

[7] R. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, C-35(8):677–691, 1986.

[8] R. Bryant. Symbolic boolean manipulation with ordered binary decision diagrams. *ACM Computing Surveys*, 24(3):293–318, 1992.

[9] P. Chatalic and L. Simon. Multi-resolution on compressed sets of clauses. In *Proceedings of the Twelfth International Conference on Tools with Artificial Intelligence*, pages 2–10, 2000.

[10] P. Chatalic and L. Simon. Zres: The old Davis-Putnam procedures meets ZBDDs. In *Proceedings of the Seventeenth International Conference on Automated Deduction*, pages 449–454, 2000.

[11] E. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 1999.

[12] C. Coarfa, D. Demopoulos, A. S. M. Aguirre, D. Subramanian, and M. Vardi. Random 3-SAT: The plot thickens. *Constraints*, 8(3):243–261, 2003.

[13] S. Cook and A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.

[14] J. F. Groote. Hiding propositional constants in BDDs. *Formal Methods in System Design: an International Journal*, 8(1):91–96, 1996.

[15] J. F. Groote and H. Zantema. Resolution and binary decision diagrams cannot simulate each other polynomially. *Discrete Applied Mathematics*, 130(2), 2003.

[16] J. Huang and A. Darwiche. Toward good elimination ordering for symbolic SAT solving. In *Proceedings of the Sixteenth IEEE Conference on Tools with Artificial Intelligence*, pages 566–573, 2004.

[17] R. Impagliazzo, T. Pitassi, and A. Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Ninth Annual Symposium on Logic in Computer Science*, pages 220–228, 1994.

[18] T. Jussila, C. Sinz, and A. Biere. Extended resolution proofs for symbolic SAT solving with quantification. In *Proceedings of the Ninth International Conference on Theory and Applications of Satisfiability Testing*, pages 54–60, 2006.

[19] B. Kalyanasundaram and G. Schnitger. The probabilistic communication complexity of set intersection. *SIAM Journal of Discrete Mathematics*, 5(4):545–557, 1992.

[20] J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*. Cambridge University Press, 1995.

[21] J. Krajíček. An exponential lower bound for a constraint propagation proof system based on ordered binary decision diagrams. Technical Report 7, Electronic Colloquium on Computational Complexity, 2007.

[22] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[23] K. McMillan. *Symbolic Model Checking*. PhD thesis, Carnegie Mellon, 1992.

[24] C. Meinel and T. Theobald. *Algorithms and Data Structures in VLSI Design*. Springer-Verlag, 1998.

[25] D. Motter and I. Markov. A compressed breadth-first search for satisfiability. In *Fourth International Workshop on Algorithms Engineering and Experiments (ALENEX)*, pages 29–42, 2002.

[26] D. Motter and I. Markov. Overcoming resolution-based lower bounds for SAT solvers. In *Eleventh IEEE/ACM Workshop on Logic and Synthesis*, pages 373–378, 2002.

[27] D. Motter, J. Roy, and I. Markov. Resolution cannot polynomially simulate compressed-BFS. *Annals of Mathematics and Artificial Intelligence*, 44(1–2):121–156, 2005.

[28] G. Pan and M. Vardi. Search vs. symbolic techniques in satisfiability solving. In *The Seventh International Conference on Theory and Applications of Satisfiability Testing*, 2004.

[29] R. Raz and A. Wigderson. Monotone circuits for matching require linear depth. *Journal of the ACM*, 39(3):736–744, 1992.

[30] A. A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

[31] C. Sinz and A. Biere. Extended resolution proofs for conjoining BDDs. In *First International Computer Science Symposium in Russia*, pages 600–611, 2006.

[32] T. Uribe and M. Stickel. Ordered binary decision diagrams and the Davis-Putnam procedure. In *Proceedings of the First International Conference on Constraints in Computational Logics*, pages 34–49, 1994.

A Elementary calculations

Proof:(Of Lemma 2 A standard application of the convexity of the function $x \mapsto x^k$. For each $x \in X$, let $d_x = |\{i \in [n] \mid x \in Y_i\}|$. Set $\bar{d_x} = \frac{1}{|X|}\sum_{x\in X} d_x$. We have that $\bar{d_x} = \frac{1}{|X|}\sum_{x\in X} d_x = \frac{1}{|X|}\sum_{i=1}^{n} |Y_i| = \alpha n$, and therefore by Jensen's Inequality:

$$\frac{1}{n^k}\sum_{\vec{i}\in[n]^k} |\bigcap_{l=1}^{k} Y_{i_l}| = \frac{1}{n^k}\sum_{x\in X} d_x^k \geq \frac{1}{n^k}|X|\left(\bar{d_x}\right)^k \geq \frac{1}{n^k}|X|\left(\alpha n\right)^k = \alpha^k|X|$$

■

Proof:(of Lemma A.)

1. Conditioned on the choice of u_1, the probability that $\{u_1, u_2\} \in E$ and $\{u_1, u_3\} \in E$ is $\left(\frac{d_{u_1}}{N}\right)^2$. Because $\frac{1}{N}\sum_u d_u = \frac{1}{N}2\alpha\binom{N}{2} = \alpha(N-1)$, convexity shows that the probability that $\{u_1, u_2\} \in E$ and $\{u_1, u_3\} \in E$ is at least $N^{-3} \cdot N(\alpha(N-1))^2 = \alpha^2(1 - 2/N + 1/N^3)$. We now subtract out the probability that u_1, u_2, u_3 are not all distinct, which is clearly no more than $3/N$, and we obtain the stated bound.

2. For each u_1 and u_2, let $D(u_1, u_2)$ be the number of common neighbors of u_1 and u_2. Because the average degree of $u \in V$ is $\alpha(N-1)$, Lemma 2 shows that $\frac{1}{N^2}\sum_{\vec{u}\in V^2} D(u_1, u_2) \geq \alpha^2((N-1)/N)^2(N-1) \geq \alpha^2(1-2/N)$. Conditioned on the choice of u_1, u_2, the probability that all edges are present is clearly $(D(u_1, u_2)/N)^4$. Apply Jensen's Inequality and we have that the probability that all edges are present is at least $\left(\alpha^2(1-2/N)\right)^4 = \alpha^8(1-2/N)^4 \geq \alpha^8(1-8/N)$. We now subtract out the probability that $u_1, u_2, u_3, u_4, u_5, u_6$ are not all distinct, which is clearly no more than $\binom{6}{2}/N = 15/N$, and we obtain the stated bound.

■

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/