DIMACS Technical Report 2002-26
June 2002

An Algorithm for Dualization in Products of Lattices[1]

by

Khaled M. Elbassioni ,[2]

[1]This research was supported in part by the National Science Foundation Grant IIS-0118635, and by DIMACS, the National Science Foundation's Center for Discrete Mathematics and Theoretical Computer Science.
[2]Department of Computer Science, Rutgers University, 110 Frelinghuysen Road, Piscataway NJ 08854-8003; (elbassio@paul.rutgers.edu)

ABSTRACT

Let $\mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_n$ be the product of n lattices, each of which has a bounded width. Given a subset $\mathcal{A} \subseteq \mathcal{L}$, we show that the problem of extending a given partial list of maximal independent elements of $\mathcal{A}$ in $\mathcal{L}$ can be solved in quasi-polynomial time.

1 Introduction

Let $\mathcal{L} \stackrel{\text{def}}{=} \mathcal{L}_1 \times \cdots \times \mathcal{L}_n$ be the product of n partially ordered sets (posets). We assume that each poset $\mathcal{L}_i$ is a lattice, i.e., for every pair of elements $x, y \in \mathcal{L}_i$, there exists a unique minimum element called the *meet* and a unique maximum element called the *join*. Throughout we shall denote by $\preceq$ the precedence relation in $\mathcal{L}$ (and also in $\mathcal{L}_1, \ldots, \mathcal{L}_n$, i.e. if $p = (p_1, \ldots, p_n) \in \mathcal{L}$ and $q = (q_1, \ldots, q_n) \in \mathcal{L}$, then $p \preceq q$ in $\mathcal{L}$ if and only if $p_1 \preceq q_1$ in $\mathcal{L}_1$, $\ldots$, $p_n \preceq q_n$ in $\mathcal{L}_n$) and use, as customary, $\vee$ and $\wedge$ to denote the join and meet operators over $\mathcal{L}$. For $\mathcal{A} \subseteq \mathcal{L}$, denote by $\mathcal{A}^+ = \{x \in \mathcal{L} \mid x \succeq a, \text{ for some } a \in \mathcal{A}\}$ and $\mathcal{A}^- = \{x \in \mathcal{L} \mid x \preceq a, \text{ for some } a \in \mathcal{A}\}$, the ideal and filter generated by $\mathcal{A}$. Any element in $\mathcal{L} \setminus \mathcal{A}^+$ is called *independent of* $\mathcal{A}$. Let $\mathcal{I}(\mathcal{A})$ be the set of all maximal independent elements for $\mathcal{A}$ (also referred to as the *dual* of $\mathcal{A}$):

$$\mathcal{I}(\mathcal{A}) \stackrel{\text{def}}{=} \{p \in \mathcal{L} \mid p \notin \mathcal{A}^+ \text{ and } (q \in \mathcal{L}, q \succeq p, q \neq p \;\Rightarrow\; q \in \mathcal{A}^+)\}.$$

Then for any $\mathcal{A} \subseteq \mathcal{L}$, we have the following decomposition of $\mathcal{L}$:

$$\mathcal{A}^+ \cap \mathcal{I}(\mathcal{A})^- = \emptyset, \qquad \mathcal{A}^+ \cup \mathcal{I}(\mathcal{A})^- = \mathcal{L}. \tag{1}$$

Call a subset $\mathcal{A} \subseteq \mathcal{L}$ an antichain if no two elements are comparable in $\mathcal{A}$. Given $\mathcal{A} \subseteq \mathcal{L}$, we consider the problem of incrementally generating all elements of $\mathcal{I}(\mathcal{A})$:

DUAL$(\mathcal{L}, \mathcal{A}, \mathcal{B})$: *Given an antichain $\mathcal{A} \subseteq \mathcal{L}$ in a lattice $\mathcal{L}$ and a partial list of maximal independent elements $\mathcal{B} \subseteq \mathcal{I}(\mathcal{A})$, either find a new maximal independent element $x \in \mathcal{I}(\mathcal{A}) \setminus \mathcal{B}$, or prove that $\mathcal{A}$ and $\mathcal{B}$ form a dual pair: $\mathcal{B} = \mathcal{I}(\mathcal{A})$.*

Clearly, the entire set $\mathcal{I}(\mathcal{A})$ can be generated by initializing $\mathcal{B} = \emptyset$ and iteratively solving the above problem $|\mathcal{I}(\mathcal{A})| + 1$ times. If $\mathcal{L}$ is the Boolean cube, i.e., $\mathcal{L}_i = \{0, 1\}$ for all $i = 1, \ldots, n$, the above dualization problem reduces to the well known *hypergraph transversal* problem, which calls for enumerating all minimal subsets that intersect all edges of a given hypergraph. The complexity of the hypergraph transversal problem is still an important open question. The best known algorithm runs in quasi-polynomial time $poly(n, m) + m^{o(\log m)}$, where $m = |\mathcal{A}| + |\mathcal{B}|$ (see [9]), providing partial evidence that the problem is not NP-hard. In this note, we will extend this result by showing that the problem is still unlikely to be NP-hard when each $\mathcal{L}_i$ is a lattice with bounded width. Specifically, for $x \in \mathcal{L}_i$, denote by $x^\perp$ the set of immediate predecessors of x, i.e., $x^\perp = \{y \in \mathcal{L}_i \mid y \prec x, \; \nexists z \in \mathcal{L}_i : y \prec z \prec x\}$, and let in-deg$(\mathcal{L}_i) = \max\{|x^\perp| \; : \; x \in \mathcal{L}_i\}$. Similarly, denote by $x^\top$ the set of immediate successors of x, and let out-deg$(\mathcal{L}_i) = \max\{|x^\top| \; : \; x \in \mathcal{L}_i\}$. Let $d = \max_{i \in [n]} \max\{\text{in-deg}(\mathcal{L}_i), \text{out-deg}(\mathcal{L}_i)\}$, and $\mu = \mu(\mathcal{L}) \stackrel{\text{def}}{=} \max\{|\mathcal{L}_i| \; : \; i \in [n]\}$. Finally, denote by $W(\mathcal{L}_i)$ the *width* of $\mathcal{L}_i$, i.e. the maximum size of an antichain in $\mathcal{L}_i$ and let $W \stackrel{\text{def}}{=} \max_{i \in [n]}\{W(\mathcal{L}_i)\}$ be the maximum width of the n lattices. The main result of this paper is the following.

Theorem 1 *Problem DUAL$(\mathcal{L}, \mathcal{A}, \mathcal{B})$ can be solved in $poly(n, m, \mu(\mathcal{L})) + m^{d \cdot \rho(W) \cdot o(\log m)}$ time, if $\mathcal{L}$ is a product of lattices, where $m = |\mathcal{A}| + |\mathcal{B}|$ and $\rho(W) \stackrel{\text{def}}{=} 2W \ln(W + 1)$.*

Let us remark that the special case of Theorem 1 (with a slightly stronger bound) for integer lattices $\mathcal{L}_i = \{0, 1, 2, \dots\}$ (where $W = 1$) appears in [3], and implies that the set of minimal integer solutions for a monotone system of linear inequalities can be incrementally generated in quasi-polynomial time.

Let us also note that the result of Theorem 1 can be immediately extended to products of *join semi*-lattices, i.e. under the relaxed requirement that each two elements of $\mathcal{L}_i$ have only a unique maximum element. Indeed, for each join semi-lattice $\mathcal{L}_i$, let us add a minimum element l_i that precedes every element in $\mathcal{L}_i$. Then it is easy to see that the resulting poset $\mathcal{L}'_i \stackrel{\text{def}}{=} \mathcal{L}_i \cup \{l_i\}$ is a lattice with minimum element $l = (l_1, \dots, l_n)$ and maximum element $u = (u_1, \dots, u_n)$. Given subsets $\mathcal{A} \subseteq \mathcal{L}$ and $\mathcal{B} \subseteq \mathcal{I}(\mathcal{A})$, let us obtain a new set $\mathcal{B}' \subseteq \mathcal{L}' \stackrel{\text{def}}{=} \mathcal{L}'_1 \times \cdots \times \mathcal{L}'_n$ by extending $\mathcal{B}$ as follows. For each added minimum element l_i, we define a new element $b \in \mathcal{B}'$ by setting $b_i = l_i$, and $b_j = u_j$ for $j \neq i$. It is easy to check that $\mathcal{B}' \subseteq \mathcal{I}(\mathcal{A})$ (or otherwise $\mathcal{B}'$ can be easily extended by a new element of $\mathcal{I}(\mathcal{A})$), and that $\mathcal{A}, \mathcal{B}'$ are dual in $\mathcal{L}'$ if and only if $\mathcal{A}, \mathcal{B}$ are dual in $\mathcal{L}$.

2 Preliminaries

Let $\mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_n$ where each $\mathcal{L}_i$ is a lattice with minimum element l_i and maximum element u_i. Given two antichains $\mathcal{A} \subseteq \mathcal{L}$, and $\mathcal{B} \subseteq \mathcal{I}(\mathcal{A})$, we say that $\mathcal{B}$ is *dual to* $\mathcal{A}$ if $\mathcal{B} = \mathcal{I}(\mathcal{A})$, i.e., if $\mathcal{B}$ contains all the maximal elements of $\mathcal{L} \setminus \mathcal{A}^+$. Let us remark that, by (1), the latter condition is equivalent to $\mathcal{A}^+ \cup \mathcal{B}^- = \mathcal{L}$.

Given any $\mathcal{Q} \subseteq \mathcal{L}$, let us denote by

$$\mathcal{A}(\mathcal{Q}) = \{a \in \mathcal{A} \mid a^+ \cap \mathcal{Q} \neq \emptyset\}, \qquad \mathcal{B}(\mathcal{Q}) = \{b \in \mathcal{B} \mid b^- \cap \mathcal{Q} \neq \emptyset\},$$

the subsets of $\mathcal{A}, \mathcal{B}$ whose ideal and filter respectively intersect $\mathcal{Q}$. A simple but important observation, which will be used frequently in the algorithms below, is that

$$\mathcal{Q} \subseteq \mathcal{A}^+ \cup \mathcal{B}^- \iff \mathcal{Q} \subseteq \mathcal{A}(\mathcal{Q})^+ \cup \mathcal{B}(\mathcal{Q})^-. \tag{2}$$

Note that, for $a \in \mathcal{A}$ and $\mathcal{Q} = \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_n$, $a^+ \cap \mathcal{Q} \neq \emptyset$ if and only if $a_i^+ \cap \mathcal{Q}_i \neq \emptyset$, for all $i \in [n]$. Thus, the sets $\mathcal{A}(\mathcal{Q})$ and $\mathcal{B}(\mathcal{Q})$ can be found in $O(nm\mu)$ time.

To solve problem DUAL$(\mathcal{L}, \mathcal{A}, \mathcal{B})$, we shall use the same general approach used in [9] to solve the hypergraph transversal problem, by decomposing it into a number of smaller subproblems which are solved recursively. In each such subproblem, we start with a sublattice $\mathcal{Q} = \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_n \subseteq \mathcal{L}$ (initially $\mathcal{Q} = \mathcal{L}$), and two subsets $\mathcal{A}(\mathcal{Q}) \subseteq \mathcal{A}$ and $\mathcal{B}(\mathcal{Q}) \subseteq \mathcal{B}$, and we want to check whether $\mathcal{A}(\mathcal{Q})$ and $\mathcal{B}(\mathcal{Q})$ are dual in $\mathcal{Q}$. As mentioned before, the latter condition is equivalent to checking whether $\mathcal{Q} \subseteq \mathcal{A}(\mathcal{Q})^+ \cup \mathcal{B}(\mathcal{Q})^-$. To estimate the reduction in problem size from one level of the recursion to the next, we measure the change in the "volume" of the problem defined as $v = v(\mathcal{A}, \mathcal{B}) \stackrel{\text{def}}{=} |\mathcal{A}||\mathcal{B}|$. Since $\mathcal{B} \subseteq \mathcal{I}(\mathcal{A})$ is assumed, the following condition holds, by (1) for the original problem and all subsequent subproblems:

$$a \not\preceq b, \quad \text{for all } a \in \mathcal{A}, b \in \mathcal{B}. \tag{3}$$

In Section 4.1, we develop several rules for decomposing a given dualization problem into smaller subproblems. The algorithm will select between these rules in such a way that the total volume is reduced from one iteration to the next. The base case for recursion is when one of the sets $\mathcal{A}$ or $\mathcal{B}$ becomes sufficiently small, in which case the problem is easily seen to be polynomially solvable.

Proposition 1 *Suppose* $\min\{|\mathcal{A}|, |\mathcal{B}|\} \leq const$*, then problem DUAL*$(\mathcal{L}, \mathcal{A}, \mathcal{B})$ *can be solved in poly*$(n, m, \mu(\mathcal{L}))$ *time for any lattice product* $\mathcal{L}$*.*

Proof. Let us assume without loss of generality that $\mathcal{B} = \{b^1, \ldots, b^k\}$ for some constant k. For every $t \in [n]^k$ and $i \in [n]$, let $I_i^t = \{j \in [k] \mid t_j = i\}$ and define

$$\mathcal{Q}^x = \bigotimes_{i=1}^{n} \Big[\mathcal{Q}_i \setminus \bigcup_{j \in I_i^x} (b_i^j)^- \Big], \qquad \text{for } x \in [n]^k.$$

Then it follows that

$$\mathcal{Q} \subseteq \mathcal{A}^+ \cup \mathcal{B}^- \iff \forall x \in [n]^k : \mathcal{Q}^x \subseteq \mathcal{A}^+. \tag{4}$$

To see this, assume first that $\mathcal{Q} \subseteq \mathcal{A}^+ \cup \mathcal{B}^-$. If $q \in \mathcal{Q}^x, x \in [n]^k$, then $q \notin \mathcal{B}^-$ because, for every $j \in [k]$, we know that $q_{x_j} \in Q_{x_j} \setminus (b_{x_j}^j)^-$ and hence $q \notin (b^j)^-$. This shows that q must be in $\mathcal{A}^+$. On the other hand, if we assume that $\mathcal{Q}^x \subseteq \mathcal{A}^+$ for all $x \in [n]^k$ and consider any $q \in \mathcal{Q} \setminus \mathcal{B}^-$, then there must exist, for every $j \in [k]$, an $x_j \in [n]$, such that $q_{x_j} \notin (b_{x_j}^j)^-$. Now if we let $x = (x_1, \ldots, x_k)$ then $q_i \notin \bigcup_{j \in I_i^x} (b_i^j)^-$ for $i \in [n]$, implying that q is in Q^x and therefore, in $\mathcal{A}^+$. This proves (4).

Next we consider the problem DUAL$(\mathcal{Q}^x, \mathcal{A}, \emptyset)$ for $x \in [n]^k$. Observe that $\mathcal{Q}^x \subseteq \mathcal{A}^+$ if and only if $\mathrm{Min}(\mathcal{Q}^x) \subseteq \mathcal{A}^+$ where $\mathrm{Min}(\mathcal{Q}^x) = \mathrm{Min}(\mathcal{Q}_1^x) \times \cdots \times \mathrm{Min}(\mathcal{Q}_n^x)$ and $\mathrm{Min}(\mathcal{Q}_i^x)$ is the set of minimal elements of $\mathcal{Q}_i^x$. Now the latter problem is easily seen to be polynomially solvable as follows. Let $\mathrm{Min}(\mathcal{Q}_i^x) = \{q_i^1, \ldots, q_i^{k_i}\}$, for $i \in [n]$ where $k_i = |\mathcal{Q}_i|$. Assume without loss of generality that $\{x_i |\ i \in [k]\} = \{1, \ldots, l\}$, for some $l \leq k$, then our problem reduces to finding whether $\{q_1^{i_1}\} \times \cdots \times \{q_l^{i_l}\} \times \mathrm{Min}(\mathcal{Q}_{l+1}) \times \ldots \times \mathrm{Min}(\mathcal{Q}_n) \subseteq \mathcal{A}^+$ for all $(i_1, \ldots, i_l) \in [k_1] \times \cdots \times [k_l]$. Each such problem is equivalent to determining whether $\mathrm{Min}(\mathcal{Q}_{l+1}) \times \ldots \times \mathrm{Min}(\mathcal{Q}_n) \subseteq (\mathcal{A}^{i_1,\cdots,i_l})^+$, where $\mathcal{A}^{i_1,\cdots,i_l} = \{(a_{l+1}, \ldots, a_n) \mid a \in \mathcal{A},\ \ a_j \preceq q_j^{i_j}$ for $j = 1, \ldots, l,$ and $a_j^+ \cap \mathrm{Min}(\mathcal{Q}_j) \neq \emptyset$ for $j = l+1, \ldots, n\}$. Let $Q^y = \{(q_{l+1}^{y_{l+1}}, \ldots, q_n^{y_n})\}$, for $y \in [k_{l+1}] \times \cdots \times [k_n]$ and observe that $\mathcal{A}^{i_1,\cdots,i_l} \subseteq \mathrm{Min}(\mathcal{Q}_{l+1}) \times \ldots \times \mathrm{Min}(\mathcal{Q}_n)$ since $\mathcal{A} \subseteq \mathcal{Q}$ was assumed. Since each subproblem of the form $\mathcal{Q}^y \subseteq [(\mathcal{A}^{i_1,\cdots,i_l})^y]^+$ is trivially solvable in polynomial time, the required result follows. $\square$

Note that, after performing decomposition, we may end up with a subproblem DUAL$(\mathcal{L}',$ $\mathcal{A}', \mathcal{B}')$, where $\mathcal{L}'$ is a sub-poset of $\mathcal{L}$, $\mathcal{A}' \subseteq \mathcal{A}$, $\mathcal{B}' \subseteq \mathcal{B}$, in which some elements of $\mathcal{A}'$, or $\mathcal{B}'$ do not belong to $\mathcal{L}'$. Clearly, if there is an $a \in \mathcal{A}'$ ($b \in \mathcal{B}'$) such that $a^+ \cap \mathcal{L}' = \emptyset$ (respectively, $b^- \cap \mathcal{L}' = \emptyset$) then this element a (respectively, b) can be *eliminated* from the subproblem by (2). On the other hand, if $a \notin \mathcal{L}'$ but $a^+ \cap \mathcal{L}' \neq \emptyset$, then a cannot be eliminated. In such a case, it is necessary to *project* the element a to the poset $\mathcal{L}'$, by replacing it with the set of minimal elements in $a^+ \cap \mathcal{L}'$. In general this minimal set may be large, causing the number of elements of $\mathcal{A}$ or $\mathcal{B}$ to increase exponentially after a succession of decompositions. However, if the sub-poset $\mathcal{L}'$ is a lattice, then each element in $\mathcal{A}'$ or $\mathcal{B}'$ projects only to *a single* element in $\mathcal{L}'$. Thus, as we will see below, we shall always maintain the property that each new subproblem is defined over lattices.

Before we prove Theorem 1, we show that the first algorithm of [9] can also be generalized for lattices to get a weaker bound than that of Theorem 1.

3 Algorithm A

Assume that $\mathcal{A}, \mathcal{B}$ satisfy (3), and let us denote, respectively, by l_i, u_i, the minimum and maximum elements of lattice $\mathcal{L}_i$. Define the *support* of $a \in \mathcal{A}$ ($b \in \mathcal{B}$) to be the set of all non-minimal coordinates of a (the set of all non-maximal coordinates of b):

$$\mathrm{Supp}(a) = \{i \in [n] \ : \ a_i \succ l_i\}, \qquad \mathrm{Supp}(b) = \{i \in [n] \ : \ b_i \prec u_i\}.$$

Elements of $\mathrm{Supp}(x)$ will be said to be *essential* for $x \in \mathcal{A} \cup \mathcal{B}$. The following lemma generalizes a known fact for dual Boolean functions (cf. [9]).

Lemma 1 *If $\mathcal{A}, \mathcal{B}$ are dual in $\mathcal{L}$, then there exists a point $x \in \mathcal{A} \cup \mathcal{B}$ with a logarithmically small support: $|\mathrm{Supp}(x)| \le \log m$, where $m = |\mathcal{A}| + |\mathcal{B}|$.*

Proof. Let $z \in \mathcal{L}$ be the vector obtained by picking each coordinate z_i randomly from $\{l_i, u_i\}$, $i = 1, \ldots, n$, and consider the random variable $N(z) \stackrel{\mathrm{def}}{=} |\{a \in \mathcal{A} \mid z \succeq a\}| + |\{b \in \mathcal{B} \mid z \preceq b\}|$. Then the expected value of $N(z)$ is given by

$$\begin{aligned} \mathbb{E}[N(z)] &= \textstyle\sum_{a\in\mathcal{A}} \Pr\{z \succeq a\} + \sum_{b\in\mathcal{B}} \Pr\{z \preceq b\} \\ &= \textstyle\sum_{a\in\mathcal{A}} \prod_{i\in\mathrm{Supp}(a)} \Pr\{z_i = u_i\} + \sum_{b\in\mathcal{B}} \prod_{i\in\mathrm{Supp}(b)} \Pr\{z_i = l_i\} \\ &= \textstyle\sum_{a\in\mathcal{A}} \left(\frac{1}{2}\right)^{|\mathrm{Supp}(a)|} + \sum_{b\in\mathcal{B}} \left(\frac{1}{2}\right)^{|\mathrm{Supp}(b)|}. \end{aligned} \tag{5}$$

Clearly if $\mathbb{E}[N(z)] < 1$, we can find an $x \in \mathcal{L} \setminus (\mathcal{A}^+ \cup \mathcal{B}^-)$ in polynomial time as follows: for $i = 1, \ldots, n$, use (5) to compute the expectations of $N(x_1, \ldots, x_{i-1}, l_i, z_{i+1}, \ldots, z_n)$ and $N(x_1, \ldots, x_{i-1}, u_i, z_{i+1}, \ldots, z_n)$ over $(z_{i+1}, \ldots, z_n) \in \{l_i, u_i\}^{n-i}$, and select the value of $x_i \in \{l_i, u_i\}$ so as to minimize the corresponding expectation.

Let us therefore assume that $\mathbb{E}[N(z)] \ge 1$, and let $r = \min\{|\mathrm{Supp}(z)| \ : \ z \in \mathcal{A} \cup \mathcal{B}\}$, then (5) implies that

$$1 \le \mathbb{E}[N(z)] \le (|\mathcal{A}| + |\mathcal{B}|) \left(\frac{1}{2}\right)^r = m \left(\frac{1}{2}\right)^r.$$

The lemma follows. $\square$

Next we show that, for any dual pair $(\mathcal{A}, \mathcal{B})$, an essential coordinate with high frequency exists for either $\mathcal{A}$ or $\mathcal{B}$.

Lemma 2 *Let $\mathcal{A}, \mathcal{B}$ be a pair of dual subsets of $\mathcal{L}$ with $|\mathcal{A}||\mathcal{B}| \geq 1$. Then there exists a coordinate $i \in [n]$ and a point $z \in \mathcal{L}_i$, such that either:*

(i) $|\{a \in \mathcal{A} \mid a_i \not\preceq z\}| \geq 1$ *and* $|\{b \in \mathcal{B} \mid b_i \preceq z\}| \geq \frac{|\mathcal{B}|}{W(\mathcal{L}_i)\log m}$, *or*

(ii) $|\{b \in \mathcal{B} \mid b_i \not\succeq z\}| \geq 1$ *and* $|\{a \in \mathcal{A} \mid a_i \succeq z\}| \geq \frac{|\mathcal{A}|}{W(\mathcal{L}_i)\log m}$.

Proof. By Lemma 1, $\mathcal{A} \cup \mathcal{B}$ contains an element x with a logarithmically small number of essential coordinates. Suppose without loss of generality that $x \in \mathcal{A}$. From condition (3), we know that for every $b \in \mathcal{B}$, there is an $i \in \mathrm{Supp}(b) \cap \mathrm{Supp}(x)$ such that $b_i \not\succeq x_i$. Letting $\mathcal{B}_i^x \stackrel{\mathrm{def}}{=} \{b \in \mathcal{B} \mid b_i \not\succeq x_i\}$ for $i \in \mathrm{Supp}(x)$, we conclude that

$$|\mathcal{B}| = |\bigcup_{i \in \mathrm{Supp}(x)} \mathcal{B}_i^x| \leq \sum_{i \in \mathrm{Supp}(x)} |\mathcal{B}_i^x|,$$

and therefore there is an $i \in [n]$ which is essential for at least $|\mathcal{B}|/|\mathrm{Supp}(x)| \geq |\mathcal{B}|/\log m$ elements of $\mathcal{B}$.

Let us now consider the set $\mathcal{Y} \stackrel{\mathrm{def}}{=} \mathcal{I}(\{x_i\})$ of maximal independent elements in $\mathcal{L}_i \setminus \{x_i\}^+$, and observe that

$$|\mathcal{B}_i^x| = |\bigcup_{z \in \mathcal{Y}} \{b \in \mathcal{B} \mid b_i \preceq z\}|, \tag{6}$$

where $i \in [n]$ is a frequent essential coordinate for $\mathcal{B}$. Noting that $|\mathcal{Y}| \leq W(\mathcal{L}_i)$, we conclude, by (6), that (i) holds. If x actually was a member of b, then by a similar argument we obtain (ii). □

We are now ready to state the first dualization algorithm for lattices.

Step 1. If $\min\{|\mathcal{A}|, |\mathcal{B}|\} < \delta(W) \stackrel{\mathrm{def}}{=} \sqrt{(W+3)\log(W+2)}$, then the dualization problem can be solved in $O(n^{\delta(W)}W^{\delta(W)}m\mu)$ time using Proposition 1.
Step 2. For each $k \in [n]$: if $a_k \notin \mathcal{L}_k$ for some $a \in \mathcal{A}$ ($b_k \notin \mathcal{L}_k$ for some $b \in \mathcal{B}$), set $a_k \leftarrow \bigwedge\{x \mid x \in a_k^+ \cap \mathcal{L}_k\}$ (respectively, set $b_k \leftarrow \bigvee\{x \mid x \in b_k^- \cap \mathcal{L}_k\}$). Thus we may assume that $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L}$.
Step 3. Check if there is an $x \in \mathcal{A} \cup \mathcal{B}$ with $|\mathrm{Supp}(x)| \leq \log m$ essential coordinates. If no such x can be found, a new point in $\mathcal{L} \setminus (\mathcal{A}^+ \cup \mathcal{B}^-)$ can be obtained as described in the proof of Lemma 1. Otherwise, assume without loss of generality, that $x = a^o \in \mathcal{A}$ and find an $i \in \mathrm{Supp}(a^o)$, and a $z \in \mathcal{L}_i$, for which condition (i) of Lemma 2 is satisfied. Let us suppose, again without any loss of generality, that $i = 1$ and set $\mathcal{L}_1' \leftarrow \mathcal{L}_1 \setminus z^-$, $\mathcal{L}_1'' \leftarrow \mathcal{L}_1 \cap z^-$. Let $\mathcal{X}$ denote the set of minimal elements in $\mathcal{L}_1'$ and define $\mathcal{L}_1^x = \mathcal{L}_1' \cap x^+$ for $x \in \mathcal{X}$. Let further

$$\mathcal{A}_1'' = \{a \in \mathcal{A} \mid a_1 \preceq z\}, \qquad \mathcal{B}_1' = \{b \in \mathcal{B} \mid b_1 \not\preceq z\},$$

and observe that $|\mathcal{A}_1''| \leq |\mathcal{A}| - 1$ and $|\mathcal{B}_1'| \leq (1 - \frac{1}{W\log m})|\mathcal{B}|$ hold by Lemma 1(i).

Step 4. Denoting by $\mathcal{L}^x = \mathcal{L}_1^x \times \mathcal{L}_2 \times \ldots \times \mathcal{L}_n$, for $x \in \mathcal{X}$, and $\mathcal{L}'' = \mathcal{L}_1'' \times \mathcal{L}_2 \times \ldots \times \mathcal{L}_n$ the sub-lattices of $\mathcal{L}$ induced by the above decomposition, then $\mathcal{A}$ and $\mathcal{B}$ are dual in $\mathcal{L}$ if and only if

$$\mathcal{A}, \mathcal{B}_1' \text{ are dual in } \mathcal{L}^x, \quad \text{for all } x \in \mathcal{X}, \tag{7}$$

and

$$\mathcal{A}_1'', \mathcal{B} \text{ are dual in } \mathcal{L}'', \tag{8}$$

each of which is a dualization problem over lattices. Thus by applying the algorithm recursively to these subproblems, we reduce the computation on a problem of volume $v = |\mathcal{A}||\mathcal{B}|$ to computing the solutions for a set of $|\mathcal{X}| \le W$ subproblems (7) of volume

$$v(\mathcal{A}, \mathcal{B}_1') = |\mathcal{A}||\mathcal{B}_1'| \le |\mathcal{A}|(1-\epsilon)|\mathcal{B}| = (1-\epsilon)v,$$

each, and another subproblem (8) of volume

$$v(\mathcal{A}_1'', \mathcal{B}) = |\mathcal{A}_1''||\mathcal{B}| = (|\mathcal{A}|-1)|\mathcal{B}| \le v - \delta,$$

where $\epsilon = 1/(W \log m)$ and $\delta = \delta(W)$. This leads to the recurrence

$$C(v) \le 1 + W \cdot C((1-\epsilon)v) + C(v-\delta).$$

To evaluate this recurrence, we first iterate k times to get $C(v) \le k + kW \cdot C((1-\epsilon)v) + C(v - k\delta)$. Letting $k = \lceil \frac{v\epsilon}{\delta} \rceil$ yields $C(v) \le (1 + (W+1)(\frac{v\epsilon}{\delta}+1))C((1-\epsilon)v)$, and hence $C(v) \le (1 + (W+1)(\frac{v\epsilon}{\delta}+1))^{\log v/\epsilon} = (W + 2 + \frac{W+1}{\delta} v\epsilon)^{\log v/\epsilon}$. Since $\min\{|\mathcal{A}|, |\mathcal{B}|\} \ge \delta$, we have $v \ge \delta^2$ and thus

$$v\left(1 - \frac{W+1}{\delta}\epsilon\right) \ge \delta^2\left(1 - \frac{W+1}{\delta W(1+\log\delta)}\right) \ge W+2, \tag{9}$$

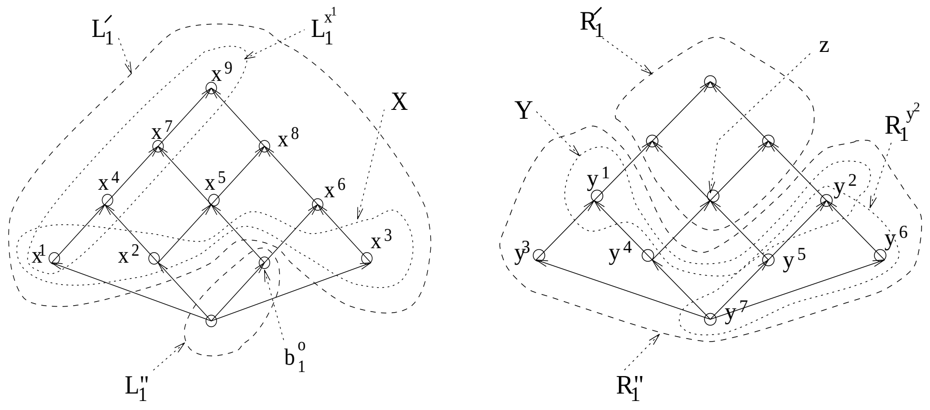
for all $W \ge 1$, by our selection of $\delta(W)$. Since $v \le m^2$, we get $C(v) \le v^{\log v/\epsilon}$ by (9), implying that the running time of the algorithm is $O(m^{4W\log^2 m+1}(nW)^{\sqrt{(W+3)\log(W+2)}}\mu)$.

4 Algorithm B

In this section we prove Theorem 1.

4.1 Decomposition rules

In general, the algorithm to be described below, will decompose a given problem by selecting an $i \in [n]$ and decomposing $\mathcal{L}_i$ into a number of sub-lattices, defining accordingly a number of lattice products. Specifically, let $a^o \in \mathcal{A}$, $b^o \in \mathcal{B}$ be arbitrary. By (3), there exists



a: Rules (i) and (ii).

b: Rules (i') and (ii').

Figure 1: Decomposing the lattice $\mathcal{L}_1$.

an $i \in [n]$, such that $a_i^o \not\preceq b_i^o$. Let us assume, without loss of generality, that $i = 1$ and set $\mathcal{L}_1' \leftarrow \mathcal{L}_1 \setminus (b_1^o)^-$, $\mathcal{L}_1'' \leftarrow \mathcal{L}_1 \cap (b_1^o)^-$. (Alternatively, we may set $\mathcal{L}_1' \leftarrow \mathcal{L}_1 \cap (a_1^o)^+$ and $\mathcal{L}_1'' \leftarrow \mathcal{L}_1 \setminus (a_1^o)^+$.) For brevity, we shall denote by $\overline{\mathcal{L}}$ the product $\mathcal{L}_2 \times \cdots \times \mathcal{L}_n$, and accordingly by $\overline{q}$ the vector $(q_2, \ldots, q_n)$, for an element $q = (q_1, q_2, \ldots, q_n) \in \mathcal{L}$.

Let $\mathcal{X}$ be the set of *minimal* elements in $\mathcal{L}_1'$ and define $\mathcal{L}_1^x = \mathcal{L}_1' \cap x^+$ for $x \in \mathcal{X}$ (see Figure 1-a). Let further

$$\begin{aligned} \mathcal{A}_1' &= \{a \in \mathcal{A} \mid a_1 \not\preceq b_1^o\}, & \mathcal{A}_1'' &= \mathcal{A} \setminus \mathcal{A}_1', \\ \mathcal{B}_1' &= \{b \in \mathcal{B} \mid b_1 \not\preceq b_1^o\}, & \mathcal{B}_1'' &= \mathcal{B} \setminus \mathcal{B}_1'. \end{aligned}$$

Denoting by $\mathcal{L}^x = \mathcal{L}_1^x \times \mathcal{L}_2 \times \cdots \times \mathcal{L}_n$, for $x \in \mathcal{X}$, and by $\mathcal{L}'' = \mathcal{L}_1'' \times \mathcal{L}_2 \times \cdots \times \mathcal{L}_n$ the sub-lattices of $\mathcal{L}$ induced by the above decomposition, we conclude by (2) that $\mathcal{A}$ and $\mathcal{B}$ are dual in $\mathcal{L}$ *if and only if*

$$\mathcal{A}, \mathcal{B}_1' \quad \text{are dual in } \mathcal{L}^x, \quad \text{for all } x \in \mathcal{X}, \tag{10}$$

$$\mathcal{A}_1'', \mathcal{B} \quad \text{are dual in } \mathcal{L}'', \tag{11}$$

each of which is a dualization problem on lattices. Thus we obtain our first decomposition rule:

Rule (i) Solve $|\mathcal{X}|$ subproblems (10) together with subproblem (11).

Clearly, subproblems (10) and (11) are not independent. Once we know that (11) is satisfied, we gain some information about the solution of subproblem (10). The following lemma shows how to utilize such dependence to further decompose (10).

Lemma 3 *Given $z \in \mathcal{L}_1$, let $\mathcal{L}_1' = \mathcal{L}_1 \cap z^+$, $\mathcal{L}_1'' \subseteq \mathcal{L}_1 \cap z^- \setminus \{z\}$ be two disjoint subsets of $\mathcal{L}_1$. Define*

$$\begin{aligned} \mathcal{A}'' &= \{a \in \mathcal{A} \mid a_1^+ \cap \mathcal{L}_1'' \neq \emptyset\}, & \mathcal{A}' &= \{a \in \mathcal{A} \setminus \mathcal{A}'' \mid a_1^+ \cap \mathcal{L}_1' \neq \emptyset\}, \\ \mathcal{B}' &= \{b \in \mathcal{B} \mid b_1^- \cap \mathcal{L}_1' \neq \emptyset\}, & \mathcal{B}'' &= \{b \in \mathcal{B} \setminus \mathcal{B}' \mid b_1^- \cap \mathcal{L}_1'' \neq \emptyset\}. \end{aligned}$$

Suppose further that we know that $\mathcal{L}_1' \times \overline{\mathcal{L}} \subseteq (\mathcal{A}' \cup \mathcal{A}'')^+ \cup (\mathcal{B}')^-$*, then*

$$\mathcal{L}_1'' \times \overline{\mathcal{L}} \subseteq (\mathcal{A}'')^+ \cup (\mathcal{B}' \cup \mathcal{B}'')^- \iff \forall a \in \widetilde{\mathcal{A}} : \mathcal{L}_1'' \times (\overline{\mathcal{L}} \cap \overline{a}^+) \subseteq (\mathcal{A}'')^+ \cup (\mathcal{B}'')^-,$$

where $\widetilde{\mathcal{A}} = \{a \in \mathcal{A}' \cup \mathcal{A}'' |\ a_1 \preceq z\}$.

Proof. Suppose first that $\mathcal{L}_1'' \times \overline{\mathcal{L}} \subseteq (\mathcal{A}'')^+ \cup (\mathcal{B}' \cup \mathcal{B}'')^-$. Let $(q_1, \overline{q}) \in \mathcal{L}_1'' \times (\overline{\mathcal{L}} \cap \overline{a}^+)$ for some $a \in \widetilde{\mathcal{A}}$, then $(q_1, \overline{q}) \in (\mathcal{A}'')^+ \cup (\mathcal{B}' \cup \mathcal{B}'')^-$. If $(q_1, \overline{q}) \preceq (b_1, \overline{b}) \in \mathcal{B}'$, then by the definition of $\mathcal{B}'$, there is a $y \in \mathcal{L}_1'$ such that $y \preceq b_1$. But then, $a \in \widetilde{\mathcal{A}}$, $\overline{q} \in \overline{\mathcal{L}} \cap \overline{a}^+$ and $y \in \mathcal{L}_1'$ imply that $(a_1, \overline{a}) \preceq (z, \overline{q}) \preceq (y, \overline{q}) \preceq (b_1, \overline{b})$, which contradicts the assumed duality condition (3). This shows that $(q_1, \overline{q}) \in (\mathcal{A}'')^+ \cup (\mathcal{B}'')^-$.

For the other direction, let $(q_1, \overline{q}) \in (\mathcal{L}_1'' \times \overline{\mathcal{L}}) \setminus (\mathcal{B}')^-$. Since $x \preceq y$ for all $x \in \mathcal{L}_1''$, $y \in \mathcal{L}_1'$, we must have $(y, \overline{q}) \notin (\mathcal{B}')^-$ for all $y \in \mathcal{L}_1'$, for otherwise we get the contradiction $(q_1, \overline{q}) \preceq (y, \overline{q}) \preceq (b_1, \overline{b})$ for some $b \in \mathcal{B}'$. Now we use our assumption that $\mathcal{L}_1' \times \overline{\mathcal{L}} \subseteq (\mathcal{A}' \cup \mathcal{A}'')^+ \cup (\mathcal{B}')^-$ to conclude that $(y, \overline{q}) \in (\mathcal{A}' \cup \mathcal{A}'')^+$ for all $y \in \mathcal{L}_1'$. In particular, we have $(z, \overline{q}) \succeq (a_1, \overline{a})$ for some $(a_1, \overline{a}) \in \mathcal{A}' \cup \mathcal{A}''$. But this implies that $a \in \widetilde{\mathcal{A}}$ and hence that $(q_1, \overline{q}) \in \mathcal{L}_1'' \times (\overline{\mathcal{L}} \cap \overline{a}^+)$ for some $a \in \widetilde{\mathcal{A}}$. This gives $(q_1, \overline{q}) \in (\mathcal{A}'')^+ \cup (\mathcal{B}'')^-$. □

By considering the dual lattice of $\mathcal{L}$ (that is, the lattice $\mathcal{L}^*$ with the same set of elements as $\mathcal{L}$, but such that $x \prec y$ in $\mathcal{L}^*$ whenever $x \succ y$ in $\mathcal{L}$), and exchanging the roles of $\mathcal{A}$ and $\mathcal{B}$, we get the following symmetric version of Lemma 3.

Lemma 4 *Let* $\mathcal{L}_1'' = \mathcal{L}_1 \cap z^-$, $\mathcal{L}_1' \subseteq \mathcal{L}_1 \cap z^+ \setminus \{z\}$ *be two disjoint subsets of* $\mathcal{L}_1$ *where* $z \in \mathcal{L}_1$*. Let* $\mathcal{A}'', \mathcal{A}', \mathcal{B}'', \mathcal{B}'$ *be defined as in Lemma 3, and let* $\widetilde{\mathcal{B}} = \{b \in \mathcal{B}' \cup \mathcal{B}'' |\ b_1 \succeq z\}$*. Suppose we know that* $\mathcal{L}_1'' \times \overline{\mathcal{L}} \subseteq (\mathcal{A}'')^+ \cup (\mathcal{B}' \cup \mathcal{B}'')^-$*, then*

$$\mathcal{L}_1' \times \overline{\mathcal{L}} \subseteq (\mathcal{A}' \cup \mathcal{A}'')^+ \cup (\mathcal{B}')^- \iff \forall b \in \widetilde{\mathcal{B}} : \mathcal{L}_1' \times (\overline{\mathcal{L}} \cap \overline{b}^-) \subseteq (\mathcal{A}')^+ \cup (\mathcal{B}')^-.$$

To use Lemma 4, suppose that subproblem (11) has no solution (i.e. there is no $q \in \mathcal{L}'' \setminus [(\mathcal{A}_1'')^+ \cup (\mathcal{B}_1' \cup \mathcal{B}_1'')^-]$). We proceed in this case as follows. For $x \in \mathcal{L}_1$, let $\widetilde{\mathcal{A}}(x) = \{a \in \mathcal{A} \mid a_1 \preceq x\}$, $\widetilde{\mathcal{B}}(x) = \{b \in \mathcal{B} \mid b_1 \succeq x\}$, and $\mathcal{A}_1'(x) = \{a \in \mathcal{A}_1' \mid a_1 = x\}$. Let us use $x^1, \ldots, x^k$ to denote the elements of $\mathcal{L}_1'$ and assume, without loss of generality, that they are topologically sorted in this order, that is, $x^j \prec x^h$ implies $j < h$ (see Figure 1-a). Let us decompose (10) (which is equivalent to checking whether $\mathcal{L}_1' \times \overline{\mathcal{L}} \subseteq \mathcal{A}^+ \cup (\mathcal{B}_1')^-$) further into the k subproblems

$$\{x^j\} \times \overline{\mathcal{L}} \subseteq \left[\left(\bigcup_{y \in (x^j)^\perp} \widetilde{\mathcal{A}}(y)\right) \cup \mathcal{A}_1'(x^j)\right]^+ \cup (\mathcal{B}_1')^-, \quad j = 1, \ldots, k. \tag{12}$$

The following lemma will allow us to eliminate the contribution of the set $\mathcal{A}_1''$ in subproblems (12) at the expense of possibly introducing at most $|\mathcal{B}|^d$ additional subproblems.

Lemma 5 *Given $x^j \in \mathcal{L}_i'$, suppose we know that $(y^- \cap \mathcal{L}_1) \times \overline{\mathcal{L}} \subseteq \widetilde{\mathcal{A}}(y)^+ \cup \mathcal{B}^-$ for all $y \in (x^j)^\perp$. Then (12) is equivalent to*

$$\{x^j\} \times \left[\overline{\mathcal{L}} \cap \left(\bigwedge_{y \in (x^j)^\perp} \overline{b}(y)\right)^-\right] \subseteq \mathcal{A}_1'(x^j)^+ \cup (\mathcal{B}_1')^-, \tag{13}$$

for all collections $\{b(y) \in \widetilde{\mathcal{B}}(y) \mid y \in (x^j)^\perp\}$. (That is, if $(x^j)^\perp = \{y^1, \ldots, y^s\}$, then we consider all collections of the form $\{b(y^1), \ldots, b(y^s)\}$, where $b(y^1) \in \widetilde{\mathcal{B}}(y^1), \ldots,$ $b(y^s) \in \widetilde{\mathcal{B}}(y^s)$. Note that $\bigwedge_{y \in (x^j)^\perp} \overline{b}(y)^- = \left(\bigwedge_{y \in (x^j)^\perp} b_2(y)^-, \ldots, \bigwedge_{y \in (x^j)^\perp} b_n(y)^-\right)$.)

Proof. We prove by induction on $|Y|$, where $Y \subseteq (x^j)^\perp$, that

$$\begin{array}{c} \{x^j\} \times \overline{\mathcal{L}} \subseteq \left[\left(\bigcup_{y \in (x^j)^\perp} \widetilde{\mathcal{A}}(y)\right) \cup \mathcal{A}_1'(x^j)\right]^+ \cup (\mathcal{B}_1')^- \qquad \Longleftrightarrow \\ \{x^j\} \times \left[\overline{\mathcal{L}} \cap \left(\bigwedge_{y \in Y} \overline{b}(y)^-\right)\right] \subseteq \left[\left(\bigcup_{y \in (x^j)^\perp \setminus Y} \widetilde{\mathcal{A}}(y)\right) \cup \mathcal{A}_1'(x^j)\right]^+ \cup (\mathcal{B}_1')^-, \end{array} \tag{14}$$

for all collections $\{b(y) \in \widetilde{\mathcal{B}}(y) \mid y \in Y\}$. This trivially holds for $Y = \emptyset$ and will prove the lemma for $Y = (x^j)^\perp$. To show (14), assume that it holds for some $Y \subset (x^j)^\perp$ and let $x \in (x^j)^\perp \setminus Y$. Consider a subproblem of the form

$$\{x^j\} \times \left[\overline{\mathcal{L}} \cap \left(\bigwedge_{y \in Y} \overline{b}(y)^-\right)\right] \subseteq \left[\widetilde{\mathcal{A}}(x) \cup \left(\bigcup_{y \in (x^j)^\perp \setminus (Y \cup \{x\})} \widetilde{\mathcal{A}}(y)\right) \cup \mathcal{A}_1'(x^j)\right]^+ \cup (\mathcal{B}_1')^-,$$

for some collection $\{b(y) \in \widetilde{\mathcal{B}}(y) \mid y \in Y\}$. Now we apply Lemma 4 with $z \leftarrow x$, $\mathcal{L}_1'' \leftarrow z^- \cap \mathcal{L}_1$, $\mathcal{L}_1' \leftarrow \{x^j\}$, $\mathcal{A}'' \leftarrow \widetilde{\mathcal{A}}(x)$, $\mathcal{A}' \leftarrow \left(\bigcup_{y \in (x^j)^\perp \setminus (Y \cup \{x\})} \widetilde{\mathcal{A}}(y)\right) \cup \mathcal{A}_1'(x^j)$, $\mathcal{B}' \leftarrow \mathcal{B}_1'$, and $\widetilde{\mathcal{B}} \leftarrow \widetilde{\mathcal{B}}(x)$ to get the required result. □

Informally, Lemma 5 says that, given $x^j \in \mathcal{L}_1'$, if the dualization subproblems for all sub-lattices that lie below x^j have been already verified to have no solution, then we can replace the solution to subproblem (12) by solving at most $\prod_{y \in (x^j)^\perp} |\widetilde{\mathcal{B}}(y)|$ subproblems of the form (13). Observe that it is important to check subproblems (12) in the topological order $j = 1, \ldots, k$ in order to be able to use Lemma 5. Thus we get

Rule (ii) Solve subproblem (11). If it has a solution then we get a point $q \in \mathcal{L} \setminus (\mathcal{A}^+ \cup \mathcal{B}^-)$. Otherwise, we solve subproblems (13), for all collections $\{b(y) \in \widetilde{\mathcal{B}}(y) \mid y \in (x^j)^\perp\}$, for $j = 1, \ldots, k$ (in the topological order).

Suppose finally that we decompose $\mathcal{L}_1$ by selecting an element $z \in \mathcal{L}_1$, letting $\mathcal{R}_1' \leftarrow \mathcal{R}_1 \cap z^+$, $\mathcal{R}_1'' \leftarrow \mathcal{L}_1 \setminus z^+$, $\mathcal{R}' = \mathcal{R}_1' \times \overline{\mathcal{L}}$, and $\mathcal{R}'' = \mathcal{R}_1'' \times \overline{\mathcal{L}}$. Let $\mathcal{Y}$ denote the set of *maximal* elements in $\mathcal{R}_1''$ and define $\mathcal{R}_1^y = \mathcal{R}_1'' \cap y^-$ for $y \in \mathcal{Y}$ (see Figure 1-b). Let further

$$\begin{array}{rclcrcl} \mathcal{A}_2' &=& \{a \in \mathcal{A} \mid a_1 \succeq z\}, & \qquad & \mathcal{A}_2'' &=& \mathcal{A} \setminus \mathcal{A}_2', \\ \mathcal{B}_2' &=& \{b \in \mathcal{B} \mid b_1 \succeq z\}, & & \mathcal{B}_2'' &=& \mathcal{B} \setminus \mathcal{B}_2'. \end{array}$$

By exchanging the roles of $\mathcal{A}$ and $\mathcal{B}$ and replacing $\mathcal{L}$ by its dual lattice $\mathcal{L}^*$ in rules (i), (ii) above, we can also derive the following symmetric versions of these rules:

Rule (i′) Solve the subproblem

$$\mathcal{A}, \mathcal{B}_2' \text{ are dual in } \mathcal{R}', \tag{15}$$

and the $|\mathcal{Y}|$ subproblems

$$\mathcal{A}_2'', \mathcal{B} \text{ are dual in } \mathcal{R}_1^y \times \overline{\mathcal{L}}, \quad \text{for all } y \in \mathcal{Y}. \tag{16}$$

Rule (ii′) Solve subproblem (15), and if it does not have a solution, then solve the subproblems

$$\{y^j\} \times \left[\overline{\mathcal{L}} \cap \left(\bigvee_{x \in (y^j)^\top} \overline{a}(x)\right)^+\right] \subseteq (\mathcal{A}_2'')^+ \cup (\mathcal{B}_2''(y^j))^-, \tag{17}$$

for all collections $\{a(x) \in \widetilde{\mathcal{A}}(x) \mid x \in (y^j)^\top\}$, for $j = 1, \ldots, h$, where $y^1, \ldots, y^h$ denote the elements of $\mathcal{R}_1''$ in *reverse* topological order, and $\mathcal{B}_2''(x) = \{a \in \mathcal{B}_2'' \mid b_1 = x\}$.

Finally it remains to remark that all the decomposition rules described above result, indeed, in dualization subproblems over lattices.

4.2 The algorithm

Given antichains $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_n$ that satisfy the necessary duality condition (3), we proceed as follows:

Step 1. For each $k \in [n]$:

1. (*eliminate:*) if $a_k^+ \cap \mathcal{L}_k = \emptyset$ for some $a \in \mathcal{A}$ ($b_k^- \cap \mathcal{L}_k = \emptyset$ for some $b \in \mathcal{B}$), then a (respectively, b) can be discarded from further consideration;

2. (*project:*) if $a_k \notin \mathcal{L}_k$ for some $a \in \mathcal{A}$ ($b_k \notin \mathcal{L}_k$ for some $b \in \mathcal{B}$), set $a_k \leftarrow \bigwedge\{x \mid x \in a_k^+ \cap \mathcal{L}_k\}$ (respectively, set $b_k \leftarrow \bigvee\{x \mid x \in b_k^- \cap \mathcal{L}_k\}$), which is an element of $\mathcal{L}_k$ since $\mathcal{L}_k$ is a lattice. Note that the duality condition (3) continues to hold after such replacements.

Thus we may assume for next steps that $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L}$.

Step 2. If $\min\{|\mathcal{A}|, |\mathcal{B}|\} < \delta = 2$, then dualization can be solved in $poly(n, m, \mu)$ time.

Step 3. Let $a^o \in \mathcal{A}$, $b^o \in \mathcal{B}$. Find an $i \in [n]$ such that $a_i^o \not\preceq b_i^o$. Assume, without loss of generality, that $i = 1$ and set $\mathcal{L}_1' \leftarrow \mathcal{L}_1 \setminus (b_1^o)^-$, $\mathcal{L}_1'' \leftarrow \mathcal{L}_1 \cap (b_1^o)^-$. Let $\mathcal{X}, \mathcal{A}_1', \mathcal{A}_1'', \mathcal{B}_1', \mathcal{B}_1''$, and $\widetilde{\mathcal{B}}$ be as defined in the previous subsection, and let

$$\epsilon_1^{\mathcal{A}} = \frac{|\mathcal{A}_1'|}{|\mathcal{A}|}, \qquad \epsilon_1^{\mathcal{B}} = \frac{|\mathcal{B}_1''|}{|\mathcal{B}|}.$$

Observe that $\epsilon_1^{\mathcal{A}} > 0$ and $\epsilon_1^{\mathcal{B}} > 0$ since $a^o \in \mathcal{A}'_1$ and $b^o \in \mathcal{B}''_1$.

Step 4. Define $\epsilon(v) = \rho(W)/\chi(v)$, where $v = v(\mathcal{A}, \mathcal{B})$, $\rho(W) = 2W\ln(W+1)$, and $\chi(v)$ is defined to be the unique positive root of the equation

$$\left(\frac{\chi(v)}{\rho(W)}\right)^{\chi(v)} = \frac{v^d}{(1-e^{-\rho(W)})(\delta^d - 1)}$$

and observe that $\epsilon(v) < 1$ for $v \geq \delta^2$, $\delta \geq 2$.

If $\min\{\epsilon_1^{\mathcal{A}}, \epsilon_1^{\mathcal{B}}\} > \epsilon(v)$, we use decomposition rule (i), which amounts to solving recursively $|\mathcal{X}|$ subproblems (10), each of which has a volume of at most $v(\mathcal{A}, \mathcal{B}'_1) = |\mathcal{A}||\mathcal{B}'_1|$, and subproblem (11) of volume $v(\mathcal{A}''_1, \mathcal{B}) = |\mathcal{A}''_1||\mathcal{B}|$. This gives rise to the recurrence

$$\begin{aligned} C(v) &\leq 1 + |\mathcal{X}|C(|\mathcal{A}||\mathcal{B}'_1|) + C(|\mathcal{A}''_1||\mathcal{B}|) \\ &\leq 1 + W.C((1-\epsilon_1^{\mathcal{B}})v) + C((1-\epsilon_1^{\mathcal{A}})v) \\ &\leq 1 + (W+1)C((1-\epsilon(v))v). \end{aligned} \tag{18}$$

Step 5. If $\epsilon_1^{\mathcal{A}} \leq \epsilon(v)$, we apply rule (ii) and get the recurrence

$$\begin{aligned} C(v) &\leq 1 + C(|\mathcal{A}''_1||\mathcal{B}|) + \sum_{j=1}^{k}\left(\prod_{y \in (x^j)^\perp} |\widetilde{\mathcal{B}}(y)|\right) C(|\mathcal{A}'_1(x^j)||\mathcal{B}'_1|) \\ &\leq 1 + C(|\mathcal{A}''_1||\mathcal{B}|) + |\widetilde{\mathcal{B}}|^d \sum_{j=1}^{k} C(|\mathcal{A}'_1(x^j)||\mathcal{B}'_1|) \\ &\leq 1 + C((1-\epsilon_1^{\mathcal{A}})v) + |\mathcal{B}|^d C(\epsilon_1^{\mathcal{A}} v) \\ &\leq 1 + C((1-\epsilon_1^{\mathcal{A}})v) + \frac{v^d}{\delta^d} C(\epsilon_1^{\mathcal{A}} v) \\ &\leq C((1-\epsilon)v) + \frac{v^d}{\delta^d - 1} C(\epsilon v), \quad \text{for some } \epsilon \in (0, \epsilon(v)] \end{aligned} \tag{19}$$

where the second inequality follows from the fact that $|(x^j)^\perp| \leq d$, the third inequality follows from $\sum_{j=1}^{k} C(|\mathcal{A}'_1(x^j)||\mathcal{B}'_1|) \leq C(\sum_{j=1}^{k} |\mathcal{A}'_1(x^j)||\mathcal{B}'_1|) = C(|\mathcal{A}'_1||\mathcal{B}'_1|)$ since $\{\mathcal{A}'_1(x^j) \mid j = 1, \ldots, k\}$ is a partition of $\mathcal{A}'_1$ and the function $C(\cdot)$ is super-additive, the forth inequality follows from $|\mathcal{B}|^d \leq v(|\mathcal{A}|, |\mathcal{B}|)^d/\delta^d$, and the last inequality follows from the fact that $v \geq \delta^2$ and $\delta \geq 2$.

Step 6. We assume for next steps that $\epsilon_1^{\mathcal{A}} > \epsilon(v)$. Then there exists a point $z \in \mathcal{X}$, such that $|\{a \in \mathcal{A} \mid a_1 \succeq z\} \geq \epsilon_1^{\mathcal{A}}|\mathcal{A}|/|\mathcal{X}| > \epsilon(v)|\mathcal{A}|/W$. Let $\mathcal{R}'_1 \leftarrow \mathcal{R}_1 \cap z^+$, $\mathcal{R}''_1 \leftarrow \mathcal{L}_1 \setminus z^+$, and let $\mathcal{Y}, \mathcal{A}'_2, \mathcal{A}''_2, \mathcal{B}'_2, \mathcal{B}''_2, \widetilde{\mathcal{A}}$ be as defined in the previous subsection. Let also

$$\epsilon_2^{\mathcal{A}} = \frac{|\mathcal{A}'_2|}{|\mathcal{A}|}, \qquad \epsilon_2^{\mathcal{B}} = \frac{|\mathcal{B}''_2|}{|\mathcal{B}|},$$

and observe that $\epsilon_2^{\mathcal{A}} > \frac{\epsilon(v)}{W}$ by our selection of $z \in \mathcal{L}_1$, and that $\epsilon_2^{\mathcal{B}} > 0$ since $b^o \notin \mathcal{B}'_2$.

Step 7. If $\epsilon_2^{\mathcal{B}} > \epsilon(v)$, then we use decomposition rule (i') which gives

$$
\begin{aligned}
C(v) &\leq 1 + C(|\mathcal{A}||\mathcal{B}_2'|) + |\mathcal{Y}|C(|\mathcal{A}_2''||\mathcal{B}|) \\
&\leq 1 + C((1-\epsilon_2^{\mathcal{B}})v) + W.C((1-\epsilon_2^{\mathcal{A}})v) \\
&\leq 1 + C((1-\epsilon(v))v) + W.C((1-\frac{\epsilon(v)}{W})v), \qquad (20)
\end{aligned}
$$

since $\epsilon_2^{\mathcal{A}} > \frac{\epsilon(v)}{W}$ and $\epsilon_2^{\mathcal{B}} > \epsilon(v)$.
Step 8. Finally if $\epsilon_2^{\mathcal{B}} \leq \epsilon(v)$, use decomposition rule (ii') and get thus the recurrence

$$
\begin{aligned}
C(v) &\leq 1 + C(|\mathcal{A}||\mathcal{B}_2'|) + \sum_{j=1}^{h}\left(\prod_{x\in(y^j)^\top} |\widetilde{\mathcal{A}}(x)|\right) C(|\mathcal{A}_2''||\mathcal{B}_2''(y^j)|) \\
&\leq C((1-\epsilon)v) + \frac{v^d}{\delta^d - 1}C(\epsilon v), \quad \text{for some } \epsilon \in (0, \epsilon(v)] \qquad (21)
\end{aligned}
$$

symmetric to (19).

4.3 Proof of Theorem 1

Since for $\min\{|\mathcal{A}|, |\mathcal{B}|\} \leq \delta$, Step 2 of the algorithm implies that $C(v) = 1$, we may assume that $\min\{|\mathcal{A}|, |\mathcal{B}|\} \geq \delta$, i.e. $v \geq \delta^2 = 4$. Following [9], we shall show by induction on $v = v(\mathcal{A}, \mathcal{B}) \geq 4$ that recurrences (18)-(21) imply that

$$C(v) \leq v^{\chi(v)}.$$

Let us consider first recurrence (20). Using the induction hypothesis and the monotonicity of $\mathcal{X}(v)$, we obtain

$$
\begin{aligned}
C(v) &\leq 1 + [(1-\epsilon(v))v]^{\chi(v)} + W[(1-\frac{\epsilon(v)}{W})v]^{\chi(v)} \\
&\leq 1 + \left(e^{-\rho(W)} + We^{-\rho(W)/W}\right) v^{\chi(v)} \leq v^{\chi(v)}, \qquad (22)
\end{aligned}
$$

since $1 - e^{-\rho(W)} - We^{-\rho(W)/W} \geq 1/2$ for all $W \geq 1$.

Let us consider next (18) and note that the monotonicity of $C(v)$ implies that $C((1-\epsilon(v))v) \leq C((1-\frac{\epsilon(v)}{W})v)$, concluding by (18) and (22) that $C(v) \leq v^{\chi(v)}$ for this case too.

Let us now consider (19) and apply induction to get

$$C(v) \leq [(1-\epsilon)v]^{\chi(v)} + \frac{v^W}{\delta^W - 1}[\epsilon v]^{\chi(v)} = \psi(\epsilon)v^{\chi(v)},$$

where $\psi(\epsilon) \stackrel{\text{def}}{=} (1-\epsilon)^{\chi(v)} + \frac{v^W}{\delta^W - 1}\epsilon^{\chi(v)}$. Since $\psi(\epsilon)$ is convex in ϵ, $\psi(0) = 1$, $\epsilon \leq \epsilon(v)$, and

$$\psi(\epsilon(v)) = \left(1 - \frac{\rho(W)}{\chi(v)}\right)^{\chi(v)} + \frac{v^W}{\delta^W - 1}\left(\frac{\rho(W)}{\chi(v)}\right)^{\chi(v)} \leq e^{-\rho(W)} + \frac{v^W}{\delta^W - 1}\left(\frac{\rho(W)}{\chi(v)}\right)^{\chi(v)} = 1,$$

by the definition of $\chi(v)$, it follows that $\psi(\epsilon) \leq 1$ and hence, $C(v) \leq v^{\chi(v)}$.

Finally, by symmetry, recurrence (21) also implies by induction that $C(v) \leq v^{\chi(v)}$.

Note that, for $\delta \geq 2$, $d \geq 1$ and $W \geq 1$, we have $(\chi/\rho(W))^{\chi} < 3\,(v/\delta)^{d}$, and thus,

$$\chi(v) < \frac{d\log(v/\delta) + \log 3}{\log(\chi/\rho(W))} \sim \frac{d\rho(W)\log v}{\log d + \log\log v}.$$

As $v(\mathcal{A}, \mathcal{B}) < m^2$, we get $\chi(v) = d\rho(W) \cdot o(\log m)$. This establishes the bound stated in Theorem 1. □

Acknowledgments

I am grateful to Endre Boros, Vladimir Gurvich and Leonid Khachiyan for helpful discussions.

References

[1] R. Agrawal, H. Mannila, R. Srikant, H. Toivonen and A. I. Verkamo, Fast discovery of association rules, in *Advances in Knowledge Discovery and Data Mining* (U. M. Fayyad, G. Piatetsky-Shapiro, P. Smyth and R. Uthurusamy, eds.), pp. 307-328, AAAI Press, Menlo Park, California, 1996.

[2] J. C. Bioch and T. Ibaraki, Complexity of identification and dualization of positive Boolean functions, *Information and Computation* 123 (1995) 50-63.

[3] E. Boros, K. Elbassioni, V. Gurvich, L. Khachiyan and K.Makino, On generating all minimal integer solutions for a monotone system of linear inequalities, in *Automata, Languages and Programming, 28th International Colloquium, ICALP 2001* (F. Orejas, P. G. Spirakis and Jan Van Leeuwen, eds.), pp. 92-103 (Springer Verlag, Berlin, Heidelberg, New York, July 2001). To appear in *SIAM Journal on Computing*, 2002.

[4] E. Boros, K. Elbassioni, V. Gurvich and L. Khachiyan, An inequality for polymatroid functions and its applications, to appear in *Discrete Applied Mathematics*, 2002. (DIMACS Technical Report 2001-14, Rutgers University, "http://dimacs.rutgers.edu/TechnicalReports/2001.html").

[5] E. Boros, V. Gurvich, L. Khachiyan and K. Makino, Dual bounded generation: partial and multiple transversals of a hypergraph, *SIAM Journal on Computing* **30** (6) (2001) 2036-2050.

[6] E. Boros, V. Gurvich, L. Khachiyan and K. Makino, An inequality limiting the number of maximal frequent sets, DIMACS Technical Report 2000-37, Rutgers University.

[7] E. Boros, P.L. Hammer and J.N. Hooker, Predicting cause-effect relationships from incomplete discrete observations, *SIAM Journal on Discrete Mathematics* **7** (1994), 481-491.

[8] Y. Crama, Dualization of regular Boolean functions, *Discrete Applied Mathematics* 16 (1987) 79-85.

[9] M. L. Fredman and L. Khachiyan, On the complexity of dualization of monotone disjunctive normal forms, *Journal of Algorithms*, 21 (1996) 618-628.

[10] V. Gurvich and L. Khachiyan, On generating the irredundant conjunctive and disjunctive normal forms of monotone Boolean functions, *Discrete Applied Mathematics*, 96-97 (1999) 363-373.

[11] D. Gunopulos, R. Khardon, H. Mannila, and H. Toivonen, Data mining, hypergraph transversals and machine learning, in *Proceedings of the 16th ACM-SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, (1997) pp. 12-15.

[12] E. Lawler, J. K. Lenstra and A. H. G. Rinnooy Kan, Generating all maximal independent sets: NP-hardness and polynomial-time algorithms, *SIAM Journal on Computing*, 9 (1980) 558-565.

[13] K. Makino and T. Ibaraki, Interior and exterior functions of Boolean functions, *Discrete Applied Mathematics*, 69 (1996) 209-231.

[14] R. C. Read and R. E. Tarjan, Bounds on backtrack algorithms for listing cycles, paths, and spanning trees, *Networks* 5 (1975) 237-252.

[15] R. Srikant and R. Agrawal, Mining generalized association rules. In *Proc. 21st International Conference on Very Large Data Bases*, pp. 407-419, 1995.

[16] R. Srikant and R. Agrawal, Mining quantitative association rules in large relational tables. In *Proc. of the ACM-SIGMOD 1996 Conference on Management of Data*, pp. 1-12, 1996.