

Fast Zeta Transforms for Lattices with Few Irreducibles*

Andreas Björklund[†]

Thore Husfeldt[‡]

Petteri Kaski[§]

Mikko Koivisto[¶]

Jesper Nederlof^{||}

Pekka Parviainen^{**}

Abstract

We investigate fast algorithms for changing between the standard basis and an orthogonal basis of idempotents for Möbius algebras of finite lattices. We show that every lattice with v elements, n of which are nonzero and join-irreducible (or, by a dual result, nonzero and meet-irreducible), has arithmetic circuits of size $O(vn)$ for computing the zeta transform and its inverse, thus enabling fast multiplication in the Möbius algebra. Furthermore, the circuit construction in fact gives optimal (up to constants) circuits for a number of lattices of combinatorial and algebraic relevance, such as the lattice of subsets of a finite set, the lattice of set partitions of a finite set, the lattice of vector subspaces of a finite vector space, and the lattice of positive divisors of a positive integer.

1 Introduction.

A significant number of computational applications have been found for algebras derived from a multiplicative base structure such as a group or a semigroup. For example, the group algebra of a finite Abelian group, together with a *fast algorithm* for transforming between the elementary basis and a basis of orthogonal idempotents (that is, a fast Fourier transform (FFT) [8, 22, 24, 32]), underlies modern signal processing and applications in theoretical computer science, including recent advances in parameterized algorithms [18, 31].

*This research was supported in part by the Swedish Research Council, project “Exact Algorithms” (A.B., T.H.) and by the Academy of Finland, Grants 252083 (P.K.), 256287 (P.K.), and 125637 (M.K.).

[†]Department of Computer Science, Lund University, Sweden, andreas.bjorklund@yahoo.se

[‡]IT University of Copenhagen, Denmark, thore@itu.dk

[§]Helsinki Institute for Information Technology HIIT, Department of Information and Computer Science, Aalto University, Finland, petteri.kaski@aalto.fi

[¶]Helsinki Institute for Information Technology HIIT, Department of Computer Science, University of Helsinki, Finland, mikko.koivisto@cs.helsinki.fi

^{||}Department of Informatics, University of Bergen, Norway, jesper.nederlof@ii.uib.no

^{**}Helsinki Institute for Information Technology HIIT, Department of Computer Science, University of Helsinki, Finland, pekka.parviainen@cs.helsinki.fi

Given the successes in the setting of group algebras, it is warranted to ask about algorithmic aspects of semigroup algebras. In this setting even the mathematical representation theory is still being developed (see [23, 29, 30]), and hence a potentially fruitful object of study from the perspective of algorithmics, in particular with an aim for specific applications. For example, currently the fastest known algorithm for graph coloring [4] is based on the semigroup algebra induced by the set union operation on the lattice of subsets of an n -element set. Again the key catalyst is a fast algorithm for transforming between bases, namely Yates’s algorithm [32], to enable fast algebra multiplication. Another important application domain arises in the study of Markov chains on finite semigroups, where the semigroup algebra can be used to obtain bounds on the rate of convergence towards the stationary distribution. A beautiful example in this setting is the hyperplane chamber walk [1, 6] and its generalization to left-regular bands [5], where the random walk on chambers can be analyzed through the semigroup algebra of an associated lattice of supports (cf. [5, §3]).

These applications suggest a study aimed specifically at a subfamily of semigroup algebras, namely the Möbius algebras of finite lattices. In more precise terms, for a field K and a finite lattice (L, \leq) , the *Möbius algebra* $K[L]$ is the vector space over K consisting of formal linear combinations of elements of L , and with multiplication of basis vectors $a, b \in L$ given by the lattice join $a \vee b$ and extended by linearity. Put otherwise, $K[L]$ is the semigroup algebra over K given by the join operation in L .

The algebra $K[L]$ is isomorphic to the direct product $K^{|L|}$, whose elements we can view as formal linear combinations of the basis vectors \hat{a} for $a \in L$ with pointwise multiplication induced by $\hat{a}\hat{a} = \hat{a}$ and $\hat{a}\hat{b} = 0$ for $a \neq b$. An algebra isomorphism from $K[L]$ to $K^{|L|}$ is the *zeta transform* $\zeta : K[L] \rightarrow K^{|L|}$ given by

$$(1.1) \quad \sum_{a \in L} \alpha_a a \mapsto \sum_{a \in L} \left(\sum_{b \leq a} \alpha_b \right) \hat{a}$$

and its inverse, the *Möbius transform* $\mu : K^{|L|} \rightarrow K[L]$,

given by

$$(1.2) \quad \sum_{a \in L} \gamma_a \hat{a} \mapsto \sum_{a \in L} \left(\sum_{b \leq a} \mu(b, a) \gamma_b \right) a$$

where $\mu(b, a)$ is the Möbius function of L . An immediate consequence is that two vectors $x, y \in K[L]$ may be multiplied in $K[L]$ by the formula

$$(1.3) \quad x \vee y = ((x\zeta)(y\zeta))\mu,$$

that is, by taking the zeta transforms of x and y , multiplying the transformed vectors pointwise, and taking the Möbius transform of the product. (See, for example, [28, §3.9] for a detailed derivation.)

From the perspective of fast algorithms, the multiplication formula (1.3) is analogous to, for example, the formula for multiplying polynomials via the fast Fourier transform. In our case, however, it is not immediate which lattices L admit a *fast zeta transform* and a *fast Möbius transform* in terms of the number of arithmetic operations in K required; that is, we are interested in finding small arithmetic circuits (see §1.1) that evaluate the transforms.

There are two natural ways to parameterize this quest for fast transforms. First, we observe that (1.1) and (1.2) essentially constitute multiplying a given v -element vector with a fixed $v \times v$ matrix determined by the lattice L , where $|L| = v$. Thus, we can measure the efficiency of evaluation for a family of lattices as a function of v , where a natural lower bound is $\Omega(v)$, the number of input and output gates required. For example, Yates’s algorithm [32] gives us an arithmetic circuit of size $\Theta(v \log v)$ for computing both (1.1) and (1.2) when L is the lattice of subsets of an n -element set, $v = 2^n$. A second, slightly more technical, objective is as follows. Consider the partial order relation \leq of L . To evaluate the value at $a \in L$, the zeta transform requires us to sum the values at each $b \leq a$. Of course, this summation need not be carried out explicitly at each a . In particular, one would rather use an intermediate value stored at some c with $b < c < a$, to account for b at a . This suggests that one should measure the size of the circuit as a function of the number $e(L)$ of *covering pairs* (a, c) in \leq , where $a \in L$ covers $c \in L$ if $c < a$ and there exists no $b \in L$ with $c < b < a$. For example, a v -element chain has $e = v - 1$ covering pairs, and the lattice of subsets of an n -element set has $e = \sum_i i \binom{n}{i} = 2^{n-1}n$ covering pairs. In particular, Yates’s algorithm establishes that there is an arithmetic circuit of size $\Theta(e)$ for computing both (1.1) and (1.2) for the subset lattice. It should also be noted that $v(L)$ is the number of vertices and $e(L)$ is the number of edges in a Hasse diagram of L .

In terms of the parameter v , ideally we would like to show that all lattices L of size v have circuits of size, say, $O(v \text{ polylog } v)$, for their zeta and Möbius transforms. However, this is not the case, because one can recover a lattice (up to isomorphism) from its zeta or Möbius circuit, and there are more lattices than there are small circuits. Indeed, there are $2^{\Theta(v^{3/2})}$ distinct lattices of size v [15, 16] but only $2^{O(N \log N)}$ bounded fan-in circuits with at most N gates, implying that most lattices of size v have circuits of size $\Omega(v^{3/2}/\log v)$. In terms of the parameter e , Kennes [14, §V] has shown a lower bound $\Omega(e)$ for the size of zeta circuits for all lattices L with e covering pairs. Thus, a circuit of size $O(e)$ is optimal up to constants and low-order terms. For example, the circuit given by Yates’s algorithm for the subset lattice is thus optimal. Consequently, it would appear natural to set as our objective to obtain circuits of size $O(e)$ for zeta transforms.

1.1 Main result. In this paper we give a novel circuit construction for the zeta transform and the Möbius transform on an arbitrary finite lattice (L, \leq) . The size of the circuit is bounded by two parameters, $v(L)$, the number of elements in the lattice, and $n(L)$, the number of nonzero elements that cannot be reduced to a join of two strictly lesser elements. Formally, an element $a \in L$ is *join-irreducible* if for all $b, c \in L$ it holds that $a = b \vee c$ implies $b = a$ or $c = a$. The *zero* element of a finite lattice is the unique minimum element.

To state our main result we require a precise definition for arithmetic circuits. An *arithmetic circuit* is a directed acyclic graph where the vertices of indegree 0 are called *input gates*. Each vertex that is not an input gate is called an *arithmetic gate* and is labeled with exactly one of $+$ or $-$. The gates labeled with $+$ have indegree 2, the gates labeled with $-$ have indegree 1. The output of the circuit obtained from one or more designated *output gates*, each of which may be either an input gate or an arithmetic gate. The *size* $|C|$ of C is the number of vertices in C .

THEOREM 1.1. *For every lattice L with v elements, n of which are nonzero and join-irreducible, there exist arithmetic circuits of size $O(vn)$ for both the zeta transform on L and the Möbius transform on L .*

This result holds also for the dual zeta transform, where $b \leq a$ is replaced with $b \geq a$ in (1.1), and the corresponding dual Möbius transform. Here it should be emphasized that the dual case is nontrivial because the bound still considers join-irreducible elements. Equivalently, we can replace “join-irreducible” with “meet-irreducible” in Theorem 1.1 and still consider (1.1).

Our strategy for constructing the circuits is to embed the lattice L with n nonzero join-irreducibles into the lattice $(2^{[n]}, \subseteq)$ of all subsets of $[n] = \{1, 2, \dots, n\}$. (This embedding is standard and will be reviewed in §2.) The embedding reduces the study of lattices to the study of set families $\mathcal{L} \subseteq 2^{[n]}$ that are intersection-closed (or, dually, union-closed). We say that \mathcal{L} is *intersection-closed* if $[n] \in \mathcal{L}$ and for all $A, B \in \mathcal{L}$ it holds that $A \cap B \in \mathcal{L}$. Similarly, \mathcal{L} is *union-closed* if $\emptyset \in \mathcal{L}$ and for all $A, B \in \mathcal{L}$ it holds that $A \cup B \in \mathcal{L}$.

With the embedding, our main result is a corollary of the following technical result.

THEOREM 1.2. *Let $\mathcal{L} \subseteq 2^{[n]}$ be a intersection-closed or union-closed family of size v . Then, there exist arithmetic circuits of size $O(vn)$ for both the zeta transform and the Möbius transform on (\mathcal{L}, \subseteq) .*

Given the set family \mathcal{L} as input, such circuits can be constructed in time $O(2^n n)$; by time we refer to the number of basic operations in the usual RAM model. But we have not found a general way to do the construction in time $O(vn)$. Indeed, such a general construction algorithm requires a fast algorithm for computing the closure operator associated with an arbitrary intersection-closed \mathcal{L} (cf. §2). For specific \mathcal{L} , faster algorithms can be obtained; in particular, if \mathcal{L} is the embedding of a lattice L , then one can compute closure via the join of L and then map back to \mathcal{L} .

It turns out that the bound $O(vn)$ is somewhat conservative in many cases. Indeed, our construction in fact gives optimal circuits – in the sense of meeting the $\Omega(e)$ lower bound of Kennes [14, §V] – for many lattices of practical relevance.

THEOREM 1.3. *Let L be a finite lattice such that $a \vee i$ covers a for all $a \in L$ and all join-irreducible $i \in L$ such that $i \not\leq a$. Then, there exist arithmetic circuits of size $O(e)$ for both the zeta transform and the Möbius transform on L .*

This result holds also in the dual case. Examples of lattices meeting the requirement in Theorem 1.3 are, for example, the lattice of subsets of a finite set, the lattice of set partitions of a finite set, and the lattice of vector subspaces of a finite vector space.

It should be noted, however, that the circuits from our construction are not always optimal and do depend on the details of the embedding of L to \mathcal{L} . Indeed, an extremal case occurs with the v -element chain embedded as $\mathcal{L} = \{[v-1] \setminus [i] : 0 \leq i \leq v-1\}$, with $n = e = v-1$, for which the construction underlying Theorem 1.2 gives a circuit of size $\Theta(n^2) = \Theta(v^2) = \Theta(e^2)$. On the other hand, the same chain embedded

as $\mathcal{L} = \{[i] : 0 \leq i \leq v-1\}$ does yield a circuit of size $O(e)$. The latter embedding generalizes to direct products of chains; in particular, we obtain circuits of size $O(e)$ for the lattice of positive divisors of a positive integer. (However, we omit a proof of this fact because such circuits can also be obtained by a less technical generalization of Yates’s algorithm. See, for example, Knuth [17, §4.6.4].)

We are currently not aware of a family of lattices that would have an $\omega(e)$ lower bound for the size of circuits required by the zeta or Möbius transforms.

1.2 Background and related work. We refer to Birkhoff [2] and Grätzer [11] for lattice theory, and Stanley [28] for associated enumerative aspects. The modern study of Möbius functions and Möbius inversion on partially ordered sets originates with Rota’s seminal work [25]. The Möbius algebra of a poset was introduced by Solomon [27] (but see also Davis [10] and Rota [26]) and systematized by Greene [12]. Greene’s survey on Möbius functions [13] and the proceedings edited by Crapo and Roulet [9] give further background.

The study of algorithmic aspects of Möbius inversion and Möbius algebras has evolved along at least two lines of study.

The first line of study concentrates on the subset lattice and applications to specific computational problems, starting with Kennes [14], who used Yates’ algorithm and the meet (intersection) product in the subset lattice to speed up an implementation of the Dempster–Shafer theory of evidence. Subsequently, Björklund *et al.* discovered the applicability of the fast join (union) product in the subset lattice to expedite algorithms for partitioning problems such as graph coloring [4] and other hard combinatorial problems with convolution-like recurrences over the subset lattice [3]. Motivated by applications in bounded-degree graphs, Björklund *et al.* showed that any down-closed (subset-closed) family $\mathcal{L} \subseteq 2^{[n]}$ admits circuits of size $O(|\mathcal{L}|n)$ for the zeta transform on (\mathcal{L}, \subseteq) by trimming Yates’s algorithm. Theorem 1.2 generalizes this result from down-closed \mathcal{L} to intersection-closed or union-closed \mathcal{L} (indeed, any down-closed \mathcal{L} is trivially intersection-closed, whereas intersection-closed families are a considerably more general class of set families; cf. §2).

The second line of study is motivated by considerations in algebraic algorithms, in particular by the quest for generalizing FFTs from the setting of group algebras [22, 24] to non-group semigroup algebras. In this direction, the first breakthrough is due to Malandro and Rockmore [19], who gave a semigroup-FFT for the rook monoid R_n (the set of all partial permutations of $[n]$ under function composition), which is the semigroup

analog of the symmetric group. Subsequently, Malandro [20] developed a general framework for semigroup-FFTs for finite inverse semigroups (a semigroup S is an *inverse semigroup* if for each $x \in S$ there exists a *unique* $y \in S$ such that $xyx = x$ and $xyx = y$) and applied the framework to R_n and its wreath products by arbitrary finite groups. A key technical requirement of Malandro's framework is a fast (upward) zeta transform on the poset structure of S , which requires in the worst case one to deal with an arbitrary meet-semilattice [20, p. 296]. Malandro [20] develops specific fast zeta transforms on the poset structure of R_n and its wreath products by finite groups. In particular, Malandro gives an $O(|R_n| \log^3 |R_n|)$ FFT algorithm for R_n , which relies on a fast zeta transform on the poset structure of R_n that runs in $O(|R_n|n^3)$ time, followed by FFTs on symmetric groups in time $O(|R_n|n^2)$, where $n = O(\log |R_n|)$. The poset structure of R_n is obtained by representing a partial bijection of $[n]$ as a subset (partial matching) of $[n] \times [n]$ and ordering by subset inclusion. In particular, R_n is a meet-semilattice with respect to set intersection and hence a lattice after a formal maximum element is introduced. Viewed as a lattice, the nonzero join-irreducibles of R_n are the n^2 singleton subsets of $[n] \times [n]$. Thus, the dual of our Theorem 1.1 gives a circuit of size $O(|R_n|n^2)$ for the upward zeta transform on R_n , which speeds up Malandro's semigroup-FFT on R_n to $O(|R_n| \log^2 |R_n|)$ time. Since R_n is the inverse semigroup analogue of the symmetric group S_n , it is perhaps interesting to remark that currently the fastest known FFT on S_n is due to Maslen [21] and runs in time $O(|S_n| \log^2 |S_n|)$, which improves upon an $O(|S_n| \log^3 |S_n|)$ algorithm of Baum and Clausen [7]. Ideally, for a family of finite groups G one would like to obtain an $O(|G| \log |G|)$ FFT algorithm; we refer to Rockmore [24] for a discussion.

2 Preliminaries.

All observations in this section are well known and presented here for convenience of exposition only. We refer to Grätzer [11] for a recent comprehensive treatment of lattice theory.

2.1 Embedding into the subset lattice. This section reviews a well-known embedding of an arbitrary finite lattice (L, \leq) to an intersection-closed family $\mathcal{L} \subseteq 2^{[n]}$ via the spectrum map; cf. [11, §II.1.2]. Recall that \mathcal{L} is *intersection-closed* if $[n] \in \mathcal{L}$ and for all $A, B \in \mathcal{L}$ it holds that $A \cap B \in \mathcal{L}$. We write \emptyset for the empty set and $0 \in L$ for the minimum (or *zero*) element of L .

Suppose that the lattice L has exactly n elements that are nonzero and join-irreducible. Let us identify these elements arbitrarily with the elements in $[n] =$

$\{1, 2, \dots, n\}$. For an element $a \in L$, define the *spectrum* of a by

$$\varphi(a) = \{i \in [n] : i \leq a\}.$$

That is, $\varphi(a)$ is the set of nonzero join-irreducible elements that are below a in L . For the zero element $0 \in L$ we thus have $\varphi(0) = \emptyset$. Let us set $\vee\varphi(a) = \vee_{i \in \varphi(a)} i$ for every nonzero $a \in L$ and $\vee\varphi(0) = 0$.

When a is join-irreducible, clearly $a = \vee\varphi(a)$. We thus conclude by induction over rank that $a = \vee\varphi(a)$ holds for all $a \in L$. Consequently, for all $a, b \in L$ we have $a \leq b$ if and only if $\varphi(a) \subseteq \varphi(b)$. Since $[n]$ is the image of the maximum element of L under φ , and we have that $\varphi(a \wedge b) = \varphi(a) \cap \varphi(b)$ for all $a, b \in L$, we conclude that the image $\mathcal{L} = \varphi(L) \subseteq 2^{[n]}$ is intersection-closed. We thus have:

LEMMA 2.1. *The spectrum map $\varphi : L \rightarrow \mathcal{L}$ is an order isomorphism of (L, \leq) onto (\mathcal{L}, \subseteq) . Moreover, \mathcal{L} is intersection-closed.*

From Lemma 2.1 we have that Theorem 1.2 implies Theorem 1.1.

2.2 Closure operators and intersection-closed families.

This section reviews a well-known equivalence between closure operators and meet-closed subsets of finite lattices. For our purposes it suffices to restrict to the subset lattice $(2^{[n]}, \subseteq)$, although the equivalence holds more generally; cf. [11, §I.3.12].

A mapping $\perp : 2^{[n]} \rightarrow 2^{[n]}$ is a *closure operator* if (i) for all $A \subseteq [n]$ it holds that $A \subseteq A^\perp$; (ii) for all $A, B \subseteq [n]$ it holds that $A \subseteq B$ implies $A^\perp \subseteq B^\perp$; and (iii) for all $A \subseteq [n]$ it holds that $A^\perp = (A^\perp)^\perp$.

LEMMA 2.2. *The image of a closure operator is an intersection-closed set family. Conversely, if $\mathcal{L} \subseteq 2^{[n]}$ is intersection-closed, then there exists a unique closure operator with image \mathcal{L} .*

Proof. Let $\perp : 2^{[n]} \rightarrow 2^{[n]}$ be a closure operator and let $\mathcal{L} = \{S^\perp : S \subseteq [n]\}$ be its image. For all $A \in \mathcal{L}$ we thus have $A = S^\perp$ for at least one $S \subseteq [n]$, and hence by (iii) we conclude that $A^\perp = (S^\perp)^\perp = S = A$ holds for all $A \in \mathcal{L}$. By (i) we have $[n] \subseteq [n]^\perp$ and hence $[n] = [n]^\perp$. Thus, $[n] \in \mathcal{L}$. Let $A, B \in \mathcal{L}$. By (i) we have $A \cap B \subseteq (A \cap B)^\perp$. From $A \cap B \subseteq A$ we have $(A \cap B)^\perp \subseteq A^\perp = A$ by (ii). Similarly we conclude that $(A \cap B)^\perp \subseteq B$. Thus, $(A \cap B)^\perp \subseteq A \cap B$ and hence $A \cap B = (A \cap B)^\perp$. In particular, $A \cap B \in \mathcal{L}$. We conclude that \mathcal{L} is intersection-closed.

Let \mathcal{L} be intersection-closed and define $\perp : 2^{[n]} \rightarrow 2^{[n]}$ for all $A \subseteq [n]$ by $A^\perp = \bigcap \{B \in \mathcal{L} : A \subseteq B\}$. In particular, $A^\perp \in \mathcal{L}$ because \mathcal{L} is intersection-closed. Properties (i), (ii), and (iii) are immediate. To establish

uniqueness, let \perp_1 and \perp_2 be closure operators with image \mathcal{L} . We show that $S^{\perp_1} = S^{\perp_2}$ holds for all $S \subseteq [n]$ by induction over $|S| = n, n-1, \dots, 1$. The base case is established by $[n] = [n]^{\perp_1} = [n]^{\perp_2}$ from (i). To establish the inductive step, let $S \subseteq [n]$. If $S^{\perp_1} = S$, we have $S \in \mathcal{L}$ and hence there exists a $T \subseteq [n]$ with $T^{\perp_2} = S$. Thus, by (iii) we have $S = T^{\perp_2} = (T^{\perp_2})^{\perp_2} = S^{\perp_2}$. It follows that $S^{\perp_1} = S = S^{\perp_2}$. By symmetry thus $S^{\perp_1} = S$ if and only if $S^{\perp_2} = S$. By (i) it remains to consider the case when $S \subsetneq S^{\perp_1}$ and $S \subsetneq S^{\perp_2}$. From $S \subsetneq S^{\perp_1}$ and (ii) we have $S^{\perp_2} \subseteq (S^{\perp_1})^{\perp_2}$. Note that $|S| < |S^{\perp_1}|$. Thus, the induction hypothesis applies to S^{\perp_1} and we conclude $(S^{\perp_1})^{\perp_2} = (S^{\perp_1})^{\perp_1} = S^{\perp_1}$ by (iii). Thus, $S^{\perp_2} \subseteq S^{\perp_1}$ and hence $S^{\perp_1} = S^{\perp_2}$ by symmetry.

For an intersection-closed $\mathcal{L} \subseteq 2^{[n]}$ and $A \subseteq [n]$, let us call A^\perp the *bottom* of the elements above A in \mathcal{L} . (Indeed, A^\perp is the minimum of the elements in \mathcal{L} that contain A as a subset.)

LEMMA 2.3. *For all $A, B \subseteq [n]$, we have $(A \cup B)^\perp = (A^\perp \cup B^\perp)^\perp$.*

Proof. By (i) we have $A \subseteq A^\perp$ and hence $A \cup B \subseteq A^\perp \cup B$, which by (ii) implies $(A \cup B)^\perp \subseteq (A^\perp \cup B)^\perp$. From $A \subseteq A \cup B$ and (ii) we have $A^\perp \subseteq (A \cup B)^\perp$. By (i) we have $B \subseteq A \cup B \subseteq (A \cup B)^\perp$. Thus, $(A \cup B)^\perp$ is an upper bound of A^\perp and B , and hence $A^\perp \cup B \subseteq (A \cup B)^\perp$. By (ii) and (iii) we thus have $(A^\perp \cup B)^\perp \subseteq ((A \cup B)^\perp)^\perp = (A \cup B)^\perp$.

2.3 Complementary duality. Let us denote the complement of $A \subseteq [n]$ by $\bar{A} = [n] \setminus A$. From elementary set theory we recall that

$$(2.4) \quad \overline{A \cup B} = \bar{A} \cap \bar{B}$$

and that

$$(2.5) \quad A \subseteq B \quad \text{if and only if} \quad \bar{B} \subseteq \bar{A}.$$

For $\mathcal{L} \subseteq 2^{[n]}$, define the *complementary dual* of \mathcal{L} by $\bar{\mathcal{L}} = \{\bar{A} : A \in \mathcal{L}\}$. Observe that $|\mathcal{L}| = |\bar{\mathcal{L}}|$ and $\bar{\bar{\mathcal{L}}} = \mathcal{L}$.

Recall that \mathcal{L} is *union-closed* if $\emptyset \in \mathcal{L}$ and for all $A, B \in \mathcal{L}$ it holds that $A \cup B \in \mathcal{L}$. We observe that \mathcal{L} is union-closed if and only if $\bar{\mathcal{L}}$ is intersection-closed.

3 Proof of Theorem 1.2.

Let $\mathcal{L} \subseteq 2^{[n]}$ be intersection-closed or union-closed. Furthermore, suppose that \mathcal{L} has size $v = v(\mathcal{L})$ and suppose that the number of covering pairs in (\mathcal{L}, \subseteq) is $e = e(\mathcal{L})$.

It suffices to study arithmetic circuits for the following two computational problems. Let K be a field and

let $f : \mathcal{L} \rightarrow K$. First, suppose that we are given \mathcal{L} and f as input. Our task is to output the zeta transform of f on (\mathcal{L}, \subseteq) ; that is, the function $f\zeta : \mathcal{L} \rightarrow K$ defined for all $T \in \mathcal{L}$ by $f\zeta(T) = \sum_{S \in \mathcal{L}: S \subseteq T} f(S)$. Second, suppose we are given \mathcal{L} and $f\zeta$ as input. Our task is to output the Möbius transform of $f\zeta$ on (\mathcal{L}, \subseteq) , that is, to output f .

The proof will proceed in two steps. First, we present two algorithms, one in the intersection-closed case and one in the union-closed case, that construct in time $O(2^n n)$ an arithmetic circuit of size $O(vn)$ for the zeta transform on (\mathcal{L}, \subseteq) . In §3.1 we review preliminaries on ordered walks in $(2^{[n]}, \subseteq)$. In §3.2 and §3.3 we derive the recurrences for the zeta transforms on (\mathcal{L}, \subseteq) , which we then develop into circuit construction algorithms in §3.4 and §3.5. Second, we conclude the proof in §3.6 by indicating the modifications required to obtain the Möbius transforms. In §3.7 we indicate the modifications required to obtain the dual zeta transform and the dual Möbius transform.

3.1 Ordered walks and prefix equality. For subsets $A, B \subseteq [n]$, let us write $A\Delta B = (A \cap \bar{B}) \cup (B \cap \bar{A})$ for the symmetric difference of A and B .

For $S, T \subseteq [n]$, the (*ordered*) *walk* from S to T in $2^{[n]}$ is the sequence $W_0, W_1, \dots, W_n \subseteq [n]$ with $S = W_0$, $T = W_n$, and $W_{i-1}\Delta W_i \subseteq \{i\}$ for all $i \in [n]$. Intuitively, the walk transforms S to T in n steps, where step i either inserts i , deletes i , or does nothing as appropriate. In particular, the walk from S to T in $2^{[n]}$ is unique. (Note also that we may view the walk from S to T in graph-theoretic terms as a walk in the n -dimensional Boolean hypercube, with a loop attached to each vertex to account for the steps i with $W_{i-1} = W_i$.)

For $S, T \subseteq [n]$ and $i \in \{0, 1, \dots, n\}$, let us write $S \equiv_i T$ as a shorthand for $S \cap [i] = T \cap [i]$. Intuitively, $S \equiv_i T$ indicates that S and T are identical in the first i elements of $[n]$.

Observe that the walk from S to T in $2^{[n]}$ satisfies $W_{i-1} \equiv_{i-1} W_i$ for all $i \in [n]$.

LEMMA 3.1. *A sequence $W_0, W_1, \dots, W_n \subseteq [n]$ satisfies $W_{i-1} \equiv_{i-1} W_i$ for all $i \in [n]$ if and only if it satisfies $W_i \equiv_i W_n$ for all $i \in [n]$.*

Proof. It is immediate that \equiv_i is an equivalence relation on $2^{[n]}$ and that \equiv_i implies \equiv_j for all $j \leq i$.

3.2 The bottom recurrence on an intersection-closed family. In this section we assume that the family $\mathcal{L} \subseteq 2^{[n]}$ is intersection-closed.

Let us now assume that $S, T \in \mathcal{L}$ with $S \subseteq T$. Consider the walk

$$W_0, W_1, \dots, W_n \subseteq [n]$$

from S to T in $2^{[n]}$. Projecting the walk to \mathcal{L} by taking \perp elementwise, we have

$$W_0^\perp, W_1^\perp, \dots, W_n^\perp \in \mathcal{L}.$$

Observe that since $S, T \in \mathcal{L}$, we have $S = W_0 = W_0^\perp$ and $T = W_n = W_n^\perp$. In particular, we can recover the original walk from the projection. Furthermore, the following lemma shows that the length- i prefixes of the original and projected walks agree.

LEMMA 3.2. *The walk from S to T in $2^{[n]}$ with $S \subseteq T$ satisfies $W_i \equiv_i W_i^\perp$ and $W_{i-1}^\perp \equiv_{i-1} W_i^\perp$ for all $i \in [n]$.*

Proof. By Lemma 3.1, the walk W_0, W_1, \dots, W_n from S to T satisfies $W_i \equiv_i W_n$ for all $i \in [n]$. From $S \subseteq T$ it follows that $W_i \subseteq W_n$ for all $i \in [n]$. By intersecting $W_i \subseteq W_i^\perp \subseteq W_n^\perp = W_n$ with $[i]$, we thus conclude that $W_i \equiv_i W_i^\perp$ and $W_i^\perp \equiv_i W_n^\perp$. By Lemma 3.1, the latter conclusion is equivalent to $W_{i-1}^\perp \equiv_{i-1} W_i^\perp$.

Let us now give a definition for a walk from $S \in \mathcal{L}$ to $T \in \mathcal{L}$ with $S \subseteq T$ that does not rely on projections and is intrinsic to \mathcal{L} . We will then show that there is a unique such walk, namely the one obtained by projecting the walk from S to T in $2^{[n]}$ to \mathcal{L} using \perp . This result will then immediately yield our “bottom recurrence” for computing the zeta transform on an intersection-closed \mathcal{L} .

For $S, T \in \mathcal{L}$ with $S \subseteq T$, a *bottom walk* from S to T in \mathcal{L} is a sequence $B_0, B_1, \dots, B_n \in \mathcal{L}$ with (i) $S = B_0$, (ii) $T = B_n$, (iii) for all $i \in [n]$ it holds that $B_{i-1} \equiv_{i-1} B_i$, and (iv) for all $i \in [n]$ it holds that either $B_{i-1} = B_i$ or both $i \notin B_{i-1}$ and $(B_{i-1} \cup \{i\})^\perp = B_i$.

LEMMA 3.3. *Let $S, T \in \mathcal{L}$ with $S \subseteq T$ and let*

$$B_0, B_1, \dots, B_n \in \mathcal{L}$$

be a bottom walk from S to T in \mathcal{L} . Then, we have

$$B_i = W_i^\perp$$

for all $i \in [n]$, where

$$W_0, W_1, \dots, W_n \subseteq [n]$$

is the walk from S to T in $2^{[n]}$. In particular, the bottom walk from S to T in \mathcal{L} is unique.

Proof. From Lemma 3.1 we conclude that $B_i \equiv_i B_n$ and $W_n \equiv_i W_i$ hold for all $i \in [n]$. Thus, because $B_i \equiv_i B_n = T = W_n \equiv_i W_i$, we have

$$(3.6) \quad i \in W_i \quad \text{if and only if} \quad i \in B_i.$$

Let now show by induction on i that $B_i = W_i^\perp$. The base case $i = 0$ is established by $S = B_0 = W_0 = W_0^\perp$,

where the last equality follows from $S \in \mathcal{L}$. For $i \geq 1$, suppose that $B_{i-1} = W_{i-1}^\perp$ holds. We must show that $B_i = W_i^\perp$. There are two cases to consider.

First, suppose that $B_i = B_{i-1}$. From $W_{i-1} \Delta W_i \subseteq \{i\}$ and $W_{i-1} \subseteq W_i$ we have that $W_i = W_{i-1}$ or $W_i = W_{i-1} \cup \{i\}$. If $W_i = W_{i-1}$, we have

$$B_i = B_{i-1} = W_{i-1}^\perp = W_i^\perp.$$

If $W_i = W_{i-1} \cup \{i\}$, we have $i \in W_i$ and hence $i \in B_i$ by (3.6). Thus, from $B_i = B_{i-1}$ it follows that $i \in B_{i-1}$. Using Lemma 2.3 to establish the second last equality, we thus conclude

$$\begin{aligned} B_i &= B_{i-1} = B_{i-1}^\perp = (B_{i-1} \cup \{i\})^\perp \\ &= (W_{i-1}^\perp \cup \{i\})^\perp = (W_{i-1} \cup \{i\})^\perp = W_i^\perp. \end{aligned}$$

Second, suppose that $i \notin B_{i-1}$ and $B_i = (B_{i-1} \cup \{i\})^\perp$. We have $i \in B_i$ and hence $i \in W_i$ by (3.6). Thus, by Lemma 2.3, we have

$$\begin{aligned} B_i &= (B_{i-1} \cup \{i\})^\perp = (W_{i-1}^\perp \cup \{i\})^\perp \\ &= (W_{i-1} \cup \{i\})^\perp = W_i^\perp. \end{aligned}$$

This completes the inductive step.

We remark that although a bottom walk is a chain $B_0 \subseteq B_1 \subseteq \dots \subseteq B_n$ in (\mathcal{L}, \subseteq) , it need not be a walk in the Hasse diagram of (\mathcal{L}, \subseteq) . In particular, B_i need not cover B_{i-1} in (\mathcal{L}, \subseteq) .

The following “bottom recurrence” computes the zeta transform on \mathcal{L} by accumulating along bottom walks in \mathcal{L} . For $S \in \mathcal{L}$, set $b_0(S) = f(S)$. For $Z \in \mathcal{L}$ and $i = 1, 2, \dots, n$, then, the value $b_i(Y)$ below is equal to the sum of the values of f over the elements $X \in \mathcal{L}$ for which both $X \subseteq Y$ and the bottom walk from X to Y arrives at Y in i or fewer steps. For all $Y \in \mathcal{L}$ and $i = 1, 2, \dots, n$, we set

$$(3.7) \quad b_i(Y) = \begin{cases} b_{i-1}(Y) & \text{if } i \notin Y, \\ b_{i-1}(Y) + \sum_{\substack{i \notin X \in \mathcal{L} \\ X \equiv_{i-1} Y \\ (X \cup \{i\})^\perp = Y}} b_{i-1}(X) & \text{if } i \in Y. \end{cases}$$

Because bottom walks are unique by Lemma 3.3, we have $b_n(T) = f\zeta(T)$ for all $T \in \mathcal{L}$.

3.3 The dual recurrence on a union-closed family. In this section we assume that the family $\mathcal{L} \subseteq 2^{[n]}$ is union-closed. Accordingly, by complementary duality, $\bar{\mathcal{L}}$ is intersection-closed. In particular, we can use the existence of unique bottom walks in $\bar{\mathcal{L}}$ to derive a dual recurrence for \mathcal{L} .

Indeed, consider $S, T \in \mathcal{L}$ with $S \subseteq T$. Then, $\bar{S}, \bar{T} \in \bar{\mathcal{L}}$ with $\bar{T} \subseteq \bar{S}$. Since $\bar{\mathcal{L}}$ is intersection-closed, Lemma 3.3 implies that there is a unique bottom walk

$$\bar{T} = \bar{B}_0 \subseteq \bar{B}_1 \subseteq \dots \subseteq \bar{B}_n = \bar{S}$$

from \bar{T} to \bar{S} in $\bar{\mathcal{L}}$. We can thus traverse this walk *in the reverse direction* from \bar{S} to \bar{T} in $\bar{\mathcal{L}}$ to accumulate the zeta transform from S to T in \mathcal{L} . That is, in \mathcal{L} we start from S and walk to T along

$$S = B_n \subseteq B_{n-1} \subseteq \dots \subseteq B_0 = T.$$

Accordingly, the base case of the following dual recurrence is at $i = n$ and we work over decreasing $i = n, n-1, \dots, 1, 0$. Set $\bar{b}_n(S) = f(S)$ for all $S \in \mathcal{L}$.

For all $i = n, n-1, \dots, 1$ and $Y \in \mathcal{L}$, we set

$$(3.8) \quad \bar{b}_{i-1}(Y) = \begin{cases} \bar{b}_i(Y) & \text{if } i \notin Y, \\ \bar{b}_i(Y) + \sum_{\substack{i \notin X \in \mathcal{L} \\ Y \equiv_{i-1} X \\ (\bar{Y} \cup \{i\})^\perp = \bar{X}}} \bar{b}_i(X) & \text{if } i \in Y. \end{cases}$$

Here \perp refers to the closure operator that corresponds to $\bar{\mathcal{L}}$. Because bottom walks are unique by Lemma 3.3, we have $\bar{b}_0(T) = f\zeta(T)$ for all $T \in \mathcal{L}$.

We remark that the sum over X in (3.8) has at most one term; indeed, Y determines X by $(\bar{Y} \cup \{i\})^\perp = \bar{X}$. We remark also that this is not the case for the sum over X in (3.7), which may have more than one term.

3.4 From the bottom recurrence to a circuit.

In this section we assume that \mathcal{L} is intersection-closed. From the bottom recurrence (3.7), we can construct a circuit for the zeta transform on \mathcal{L} by proceeding levelwise with increasing $i = 1, 2, \dots, n$. It will be convenient to work with “pointers” $b_i(Y)$ that point to gates in the circuit being constructed.

To initialize the construction, start with an empty circuit. For each $Y \in \mathcal{L}$, introduce one input gate and set the pointer $b_0(Y)$ to point to this gate. Next, iterate over $i = 1, 2, \dots, n$. Assume that the pointers $b_{i-1}(Y)$ for $Y \in \mathcal{L}$ point to existing gates. First, set $b_i(Y)$ to point to the gate pointed by $b_{i-1}(Y)$ for each $Y \in \mathcal{L}$. (Note that more than one pointer may point to the same gate.) Iterate over the $X \in \mathcal{L}$ for which $i \notin X$ holds. Compute the set $Y = (X \cup \{i\})^\perp$. If $X \equiv_{i-1} Y$ holds, then introduce a new addition gate g whose inputs are the gates pointed by $b_{i-1}(X)$ and $b_i(Y)$, and finally set $b_i(Y)$ to point to g . When the iteration over X terminates, for each $Y \in \mathcal{L}$ it holds that the gate pointed by $b_i(Y)$ evaluates to (3.8). Proceed to consider the next value i .

Because each $X \in \mathcal{L}$ is considered at most once for each $i = 1, 2, \dots, n$, and \mathcal{L} has size v , the constructed circuit has $O(vn)$ gates.

The bottom A^\perp for every subset $A \subseteq [n]$ can be found using the recurrence

$$(3.9) \quad A^\perp = \begin{cases} A & \text{if } A \in \mathcal{L}, \\ \bigcap_{i \in [n] \setminus A} (A \cup \{i\})^\perp & \text{if } A \notin \mathcal{L}. \end{cases}$$

A direct implementation of (3.9) requires $O(2^n n)$ pairwise intersection operations of $O(n)$ -element sets. We observe that faster computation is possible by exploiting the fact that the intersection of the sets $(A \cup \{i\})^\perp$ is – because \mathcal{L} is intersection-closed – equal to the smallest one of these sets; this requires only $O(2^n n)$ pairwise comparisons of $O(\log n)$ -bit integers, which in the assumed model of computation takes time $O(2^n n)$.

If $X \equiv_{i-1} Y$ is tested naïvely in time $O(n)$, the overall running time becomes $O(2^n n^2)$. To reduce the running time to $O(2^n n)$, we observe that $X \cup \{i\} \equiv_{i-1} X$ and $Y = (X \cup \{i\})^\perp$ hold always. Thus, it suffices to precompute the tests $Y \equiv_{i-1} Y^\perp$ for every possible pair (Y, i) , as follows. Fix $Y \subseteq [n]$, and hence $D = Y^\perp$. Then compute the predicate $Y \equiv_{i-1} D$ iteratively for $i = 1, 2, \dots, n$ by relying on the fact that the predicate factors into the product of the predicates $Y \cap \{j\} = D \cap \{j\}$ for $j = 1, 2, \dots, i-1$.

We conclude that there is an algorithm that, given an intersection-closed family $\mathcal{L} \subseteq 2^{[n]}$ with $|\mathcal{L}| = v$ as input, in time $O(2^n n)$ constructs an arithmetic circuit of size $O(vn)$ for the zeta transform on \mathcal{L} .

3.5 From the dual recurrence to a circuit.

In this section we assume that \mathcal{L} is union-closed. Accordingly $\bar{\mathcal{L}}$ is intersection-closed, and \perp refers to the closure operator that corresponds to $\bar{\mathcal{L}}$.

From the dual recurrence (3.8), we can construct a circuit for the zeta transform on \mathcal{L} by proceeding levelwise with decreasing $i = n, n-1, \dots, 1$.

To initialize the construction, start with an empty circuit. For each $Y \in \mathcal{L}$, introduce one input gate and set the pointer $\bar{b}_n(Y)$ to point to this gate. Next, iterate over $i = n, n-1, \dots, 1$. Assume that the pointers $\bar{b}_i(Y)$ for $Y \in \mathcal{L}$ point to existing gates. First, set $\bar{b}_{i-1}(Y)$ to point to the gate pointed by $\bar{b}_i(Y)$ for each $Y \in \mathcal{L}$. Iterate over the $Y \in \mathcal{L}$ for which $i \in Y$ holds. Compute the set $\bar{X} = (\bar{Y} \cup \{i\})^\perp$ and take its complement to obtain the set X . If $X \equiv_{i-1} Y$ holds, then introduce a new addition gate g whose inputs are the gates pointed by $\bar{b}_i(X)$ and $\bar{b}_{i-1}(Y)$, and finally set $\bar{b}_{i-1}(Y)$ to point to g . When the iteration over Y terminates, for each $Y \in \mathcal{L}$ it holds that the gate pointed by $\bar{b}_{i-1}(Y)$ evaluates to (3.7). Proceed to consider the next value i .

Because each $Y \in \mathcal{L}$ is considered at most once for each $i = n, n-1, \dots, 1$, and \mathcal{L} has size v , the constructed circuit has $O(vn)$ gates.

We can compute \perp in time $O(2^{2n})$ using the techniques in §3.4 for the intersection-closed $\bar{\mathcal{L}}$. To test $Y \equiv_{i-1} X$, or equivalently, $\bar{Y} \equiv_{i-1} \bar{X}$ in time $O(2^{2n})$, we proceed as in §3.4 after observing that $\bar{Y} \cup \{i\} \equiv_{i-1} \bar{Y}$ and $\bar{X} = (\bar{Y} \cup \{i\})^\perp$ hold always. We conclude that there is an algorithm that, given an union-closed family \mathcal{L} of v subsets of $[n]$ as input, constructs an arithmetic circuit of size $O(vn)$ for the zeta transform on \mathcal{L} in time $O(2^{2n})$.

3.6 The Möbius transform. This section shows that the Möbius transform on \mathcal{L} admits fast evaluation over intersection-closed or union-closed \mathcal{L} .

For an intersection-closed \mathcal{L} , we reverse the bottom recurrence (3.7). Put otherwise, our input is $b_n = f\zeta$ and the task is to compute $b_0 = f$. We accomplish this by rearranging (3.7) so that

$$(3.10) \quad b_{i-1}(Y) = \begin{cases} b_i(Y) & \text{if } i \notin Y, \\ b_i(Y) - \sum_{\substack{i \notin X \in \mathcal{L} \\ Y \equiv_{i-1} X \\ (X \cup \{i\})^\perp = Y}} b_{i-1}(X) & \text{if } i \in Y, \end{cases}$$

which enables us to recover, for $i = n, n-1, \dots, 1$ and in order of increasing size $|Y|$ for each $Y \in \mathcal{L}$ in turn, the value $b_{i-1}(Y)$ from the values $b_i(Y)$ and the values $b_{i-1}(X)$ for $X \in \mathcal{L}$ with $|X| < |Y|$. Indeed, observe that $|X| < |X \cup \{i\}| \leq |(X \cup \{i\})^\perp| = |Y|$.

For a union-closed \mathcal{L} , we reverse the dual recurrence (3.8) analogously. Our input is $\bar{b}_0 = f\zeta$ and the task is to compute $\bar{b}_n = f$. Rearranging the recurrence, we obtain

$$(3.11) \quad \bar{b}_i(Y) = \begin{cases} \bar{b}_{i-1}(Y) & \text{if } i \notin Y, \\ \bar{b}_{i-1}(Y) - \sum_{\substack{i \notin X \in \mathcal{L} \\ X \equiv_{i-1} Y \\ (\bar{Y} \cup \{i\})^\perp = \bar{X}}} \bar{b}_i(X) & \text{if } i \in Y, \end{cases}$$

which enables us to recover, for $i = 1, 2, \dots, n$ and in order of increasing size $|Y|$ for each $Y \in \mathcal{L}$ in turn, the value $\bar{b}_{i-1}(Y)$ from the values $\bar{b}_i(Y)$ and the values $\bar{b}_i(X)$ for $X \in \mathcal{L}$ with $|X| < |Y|$. Indeed, observe that $|X| = n - |\bar{X}| = n - |(\bar{Y} \cup \{i\})^\perp| \leq n - |\bar{Y} \cup \{i\}| = |Y \setminus \{i\}| < |Y|$.

It is straightforward to translate the reverse recurrences (3.10) and (3.11) into circuits of size $O(vn)$ in time $O(2^{2n})$ by the techniques in §3.4 and §3.5.

3.7 The dual transforms. We proceed by complementary duality. Let $\mathcal{L} \subseteq 2^{[n]}$ and $f : \mathcal{L} \rightarrow K$ be given as input. For the dual zeta transform ζ' , we must compute $f\zeta'(T) = \sum_{S \in \mathcal{L}: T \subseteq S} f(S)$ for all $T \in \mathcal{L}$. Define $f' : \bar{\mathcal{L}} \rightarrow K$ for all $\bar{S} \in \bar{\mathcal{L}}$ by setting $f'(\bar{S}) = f(S)$.

For all $T \in \mathcal{L}$ we thus have $f\zeta'(T) = \sum_{S \in \mathcal{L}: T \subseteq S} f(S) = \sum_{S \in \mathcal{L}: \bar{S} \subseteq \bar{T}} f(S) = \sum_{\bar{S} \in \bar{\mathcal{L}}: \bar{S} \subseteq \bar{T}} f'(\bar{S}) = f'\zeta(\bar{T})$. In particular, given an intersection-closed (respectively, union-closed) \mathcal{L} and $f : \mathcal{L} \rightarrow K$ as input, we obtain the desired circuit for the dual transform by applying Theorem 1.2 to construct the zeta circuit for the union-closed (respectively, intersection-closed) $\bar{\mathcal{L}}$ and $f' : \bar{\mathcal{L}} \rightarrow K$. Because the Möbius transform is the inverse of the zeta transform, a similar construction applies.

4 Proof of Theorem 1.3.

Let $\mathcal{L} \subseteq 2^{[n]}$ be the embedding of L . In particular, \mathcal{L} is intersection-closed. We observe that the assumption in Theorem 1.3 is equivalent to the assumption that for all $X \in \mathcal{L}$ and all $i \in \bar{X}$ it holds that $(X \cup \{i\})^\perp$ covers X in (\mathcal{L}, \subseteq) .

Let us return to the circuit construction algorithm in §3.4. During the construction, each addition gate introduced to the circuit results from a specific pair $Y, X \in \mathcal{L}$ and a value $i \in Y \setminus X$ such that both $Y = (X \cup \{i\})^\perp$ and $Y \equiv_{i-1} X$. From $i \in Y \setminus X$ and $Y = (X \cup \{i\})^\perp$ it follows by assumption that the pair (Y, X) is a covering pair of (\mathcal{L}, \subseteq) , and hence the image of a covering pair of (L, \leq) . The following lemma shows that at most one addition gate gets introduced for each such pair (Y, X) . Thus, we conclude that the circuit has size $O(e)$.

LEMMA 4.1. *For all $Y, X \subseteq [n]$ there is at most one $i \in Y \setminus X$ such that $Y \equiv_{i-1} X$.*

Proof. If $Y \setminus X$ is nonempty, we must have $i = \min Y \setminus X$.

To establish the dual version of the theorem, let $\bar{\mathcal{L}}$ be the embedding of L . In particular, $\bar{\mathcal{L}}$ is union-closed. The assumption in Theorem 1.3 is equivalent to the assumption that for all $\bar{Y} \in \bar{\mathcal{L}}$ and all $i \in Y$ it holds that $(\bar{Y} \cup \{i\})^\perp$ covers \bar{Y} in $(\bar{\mathcal{L}}, \subseteq)$.

Let us return to the dual circuit construction algorithm in §3.5. Each addition gate introduced to the circuit results from a specific pair $Y, X \in \mathcal{L}$ and a value $i \in Y \setminus X$ such that both $\bar{X} = (\bar{Y} \cup \{i\})^\perp$ and $Y \equiv_{i-1} X$. From $i \in Y \setminus X$ and $\bar{X} = (\bar{Y} \cup \{i\})^\perp$ it follows by assumption that the pair (\bar{X}, \bar{Y}) is a covering pair of $(\bar{\mathcal{L}}, \subseteq)$, and hence the image of a covering pair of (L, \leq) . From Lemma 4.1 we conclude that at most one addition gate gets introduced for each such pair (\bar{X}, \bar{Y}) . Thus, also the dual circuit has size $O(e)$.

In both cases similar reasoning gives an $O(e)$ bound for the circuit that computes the Möbius transform.

Acknowledgment. The authors are grateful to the anonymous reviewers for their valuable comments that helped to considerably strengthen the paper.

References

- [1] P. Bidigare, P. Hanlon, and D. Rockmore. A combinatorial description of the spectrum for the Tsetlin library and its generalization to hyperplane arrangements. *Duke Math. J.*, 99(1):135–174, 1999.
- [2] G. Birkhoff. *Lattice Theory*, volume 25 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, R.I., third edition, 1979.
- [3] A. Björklund, T. Husfeldt, P. Kaski, and M. Koivisto. Fourier meets Möbius: fast subset convolution. In *STOC’07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pp. 67–74. ACM, New York, 2007.
- [4] A. Björklund, T. Husfeldt, and M. Koivisto. Set partitioning via inclusion-exclusion. *SIAM J. Comput.*, 39(2):546–563, 2009.
- [5] K. S. Brown. Semigroups, rings, and Markov chains. *J. Theoret. Probab.*, 13(3):871–938, 2000.
- [6] K. S. Brown and P. Diaconis. Random walks and hyperplane arrangements. *Ann. Probab.*, 26(4):1813–1854, 1998.
- [7] M. Clausen and U. Baum. Fast Fourier transforms for symmetric groups: theory and implementation. *Math. Comp.*, 61(204):833–847, 1993.
- [8] J. W. Cooley and J. W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Math. Comp.*, 19:297–301, 1965.
- [9] H. Crapo and G. Roulet, editors. *Möbius Algebras*. University of Waterloo, Waterloo, Ont., 1971.
- [10] R. L. Davis. Order algebras. *Bull. Amer. Math. Soc.*, 76:83–87, 1970.
- [11] G. Grätzer. *Lattice Theory: Foundation*. Birkhäuser / Springer Basel AG, Basel, 2011.
- [12] C. Greene. On the Möbius algebra of a partially ordered set. *Advances in Math.*, 10:177–187, 1973.
- [13] C. Greene. The Möbius function of a partially ordered set. In *Ordered Sets (Banff, Alta., 1981)*, volume 83 of *NATO Adv. Study Inst. Ser. C: Math. Phys. Sci.*, pp. 555–581. Reidel, Dordrecht, 1982.
- [14] R. Kennes. Computational aspects of the Möbius transformation of graphs. *IEEE Transactions on Systems, Man and Cybernetics*, 22(2):201–223, 1992.
- [15] D. J. Kleitman and K. J. Winston. The asymptotic number of lattices. *Ann. Discrete Math.*, 6:243–249, 1980. Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Colorado State Univ., Fort Collins, Colo., 1978).
- [16] W. Klotz and L. Lucht. Endliche Verbände. *J. Reine Angew. Math.*, 247:58–68, 1971.
- [17] D. E. Knuth. *The Art of Computer Programming*, volume 2, Seminumerical Algorithms. Addison–Wesley, Upper Saddle River, N.J., 3rd edition, 1998.
- [18] I. Koutis and R. Williams. Limits and applications of group algebras for parameterized problems. In S. Albers, A. Marchetti-Spaccamela, Y. Matias, S. Nikolettseas, and W. Thomas, editors, *Automata, Languages and Programming*, volume 5555 of *Lecture Notes in Computer Science*, pp. 653–664. Springer, Berlin, 2009.
- [19] M. Malandro and D. Rockmore. Fast Fourier transforms for the rook monoid. *Trans. Amer. Math. Soc.*, 362(2):1009–1045, 2010.
- [20] M. E. Malandro. Fast Fourier transforms for finite inverse semigroups. *J. Algebra*, 324(2):282–312, 2010.
- [21] D. K. Maslen. The efficient computation of Fourier transforms on the symmetric group. *Math. Comp.*, 67(223):1121–1147, 1998.
- [22] D. K. Maslen and D. N. Rockmore. Generalized FFTs—a survey of some recent results. In *Groups and Computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pp. 183–237. Amer. Math. Soc., Providence, RI, 1997.
- [23] J. Rhodes and Y. Zalcstein. Elementary representation and character theory of finite semigroups and its application. In *Monoids and Semigroups with Applications (Berkeley, CA, 1989)*, pp. 334–367. World Sci. Publ., River Edge, NJ, 1991.
- [24] D. N. Rockmore. Recent progress and applications in group FFTs. In *Computational Noncommutative Algebra and Applications*, volume 136 of *NATO Sci. Ser. II Math. Phys. Chem.*, pp. 227–254. Kluwer Acad. Publ., Dordrecht, 2004.
- [25] G.-C. Rota. On the foundations of combinatorial theory. I. Theory of Möbius functions. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 2:340–368 (1964), 1964.
- [26] G.-C. Rota. On the combinatorics of the Euler characteristic. In *Studies in Pure Mathematics (Presented to Richard Rado)*, pp. 221–233. Academic Press, London, 1971.
- [27] L. Solomon. The Burnside algebra of a finite group. *J. Combinatorial Theory*, 2:603–615, 1967.
- [28] R. P. Stanley. *Enumerative Combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.
- [29] B. Steinberg. Möbius functions and semigroup representation theory. *J. Combin. Theory Ser. A*, 113(5):866–881, 2006.
- [30] B. Steinberg. Möbius functions and semigroup representation theory. II. Character formulas and multiplicities. *Adv. Math.*, 217(4):1521–1557, 2008.
- [31] R. Williams. Finding paths of length k in $O^*(2^k)$ time. *Inform. Process. Lett.*, 109(6):315–318, 2009.
- [32] F. Yates. *The Design and Analysis of Factorial Experiments*. Imperial Bureau of Soil Science, Harpenden, England, 1937.