Discrete Mathematics and Theoretical Computer Science . . . . . .
. . . . . **vol. 25:2 #22 (2023)**

Representing polynomial of ST-CONNECTIVITY

Jānis Iraids Juris Smotrovs

Faculty of Computing, University of Latvia, Riga, Latvia

revisions 18th Aug. 2022, 18th July 2023; accepted 19th Oct. 2023.

We show that the coefficients of the representing polynomial of any monotone Boolean function are the values of the Möbius function of an atomistic lattice related to this function. Using this we determine the representing polynomial of any Boolean function corresponding to a ST-CONNECTIVITY problem in acyclic quivers (directed acyclic multigraphs). Only monomials corresponding to unions of paths have non-zero coefficients which are $(-1)^D$ where D is an easily computable function of the quiver corresponding to the monomial (it is the number of plane regions in the case of planar graphs). We determine that the number of monomials with non-zero coefficients for the two-dimensional $n \times n$ grid connectivity problem is $2^{\Omega(n^2)}$.

Keywords: monotone Boolean function, representing polynomial, connectivity, atomistic lattice

1 Introduction

In this paper we study the representing polynomials of Boolean functions. Representations of Boolean functions by polynomials of various forms have a number of applications to computer science, from circuit lower bounds (Håstad, 1986) to machine learning (Linial et al., 1993; Bshouty and Tamon, 1996) and quantum query algorithms (Beals et al., 2001; Buhrman and de Wolf, 2002). A detailed overview of mathematical properties of such polynomials and their applications can be found in the textbook by O'Donnell (2014).

In the current paper we focus on exact representations of monotone Boolean functions, in particular, for Boolean functions that correspond to ST-CONNECTIVITY. The motivation of our work comes from quantum computing where subgraph connectivity problems emerge in the context of producing quantum speedups for various problems, such as Travelling Salesman Problem (Ambainis et al., 2019) and Edit Distance (Ambainis et al., 2020). It is well known that quantum algorithms can be described by polynomials (Beals et al., 2001) and this connection has been used to prove a number of lower bounds on quantum algorithms. In particular, the degree of the representing polynomial is used to give lower bounds in the exact quantum query model (where the algorithm has to output the correct answer with certainty) and the minimum degree of an approximating polynomial is used for the much more natural bounded error quantum algorithms. In many cases, the polynomials lower bound is asymptotically tight and characterizes quantum query complexity up to a constant factor. Because of that, we think that it may be interesting to understand polynomials that represent the corresponding subgraph connectivity problems.

ISSN 1365–8050

Even though we focus on the representing polynomials, they can be used to obtain optimal approximating polynomials in some cases (Beniamini, 2022).

We now give a more technical overview of problems that we study and our results. Every Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be expressed as a real multilinear polynomial in a unique way. We will refer to it as the representing polynomial of the Boolean function. Such a polynomial is often used to estimate various complexity measures of a Boolean function, or to construct an algorithm related to it.

The representing polynomials are often studied in the Fourier basis in which the bits 0 and 1 are replaced by values 1 and -1, respectively. In particular, the cited textbook mostly deals with these polynomials in the Fourier basis. However, we will concentrate on these polynomials in the standard, $\{0,1\}$ basis, using approach similar to the one employed by Beniamini and Nisan in the recent papers (Beniamini and Nisan, 2021; Beniamini, 2022) involving lattices, their Möbius functions and convex polytopes.

In this paper we deal with Boolean functions corresponding to the problem of ST-CONNECTIVITY in acyclic quivers (AQ-CONNECTIVITY). In such a problem, the input bits correspond to the arcs of a given acyclic quiver, denoting presence (1) or absence (0) of an arc, and the Boolean function is equal to 1 iff there is a path (consisting of present arcs) from a starting vertex s (source) to a final vertex t (sink). Instances of such problems are found in the Travelling Salesman Problem, where the graph is the Boolean hypercube (see, e.g., Ambainis et al. (2019)), and in the Edit Distance problem where the graph is a two-dimensional grid and the task is to determine the shortest distance (see, e.g., Ambainis et al. (2020)).

Boolean functions corresponding to AQ-CONNECTIVITY are monotone. In Section 3 we show that the coefficients of the representing polynomial of any monotone Boolean function are the values of the Möbius function (with minus sign) of the poset of unions of its prime implicants (Theorem 3). This generalizes the corresponding result by Beniamini and Nisan (2021, Proposition 3.4). We also characterize the posets obtainable as unions of prime implicants: they are exactly the finite atomistic lattices (Proposition 1 and Theorem 2).

Then, relating an acyclic quiver G to a flow polytope and using results from Hille (2003), we compute the corresponding Möbius function obtaining formula for the representing polynomial (Section 4):

$$p_G(x) = \sum_{H \in U(P_G) \setminus \{\varnothing\}} (-1)^{D(H)} \prod_{i \in H} x_i$$

where the summation variable H ranges over non-empty unions of paths from the source to the sink, and $D(H)$ is an easily computable function of H (in the case of a planar graph it is essentially the number of regions in which H divides the plane).

Since the number of monomials with non-zero coefficients is related to the communication complexity of the Boolean function (see, e.g., Section 4.4.1 in Beniamini and Nisan (2021)) and can be used to obtain a good approximating polynomial (Beniamini, 2022, Lemma 31), we estimate it in the case when G is a two-dimensional grid (Section 5). In Section 2 we provide some preliminaries, and Section 6 contains the conclusion.

2 Posets, their Möbius functions, and convex polytopes

Let $O = \langle S, \leqslant_O \rangle$ be a poset over S with order relation $\leqslant_O$. An antichain is any subset of S consisting of mutually incomparable elements (under the order relation $\leqslant_O$). A join of $s \in S$ and $t \in S$ is an element $u \in S$ such that $\forall v : (s \leqslant_O v \text{ and } t \leqslant_O v) \to (u \leqslant_O v)$ if it exists. In a slight abuse of the notation we will denote the join of s and t by $s \cup t$. A poset for which every pair of elements have a join is called

a join-semilattice. In a poset with least element $\varnothing$ an element a is called an atom if $\varnothing <_O a$ and there is no v such that $\varnothing <_O v <_O a$. A poset with least element $\varnothing$ is called atomistic if every element is a join of some set of atoms (join can be generalized to multiple elements by associativity). Consider the set inclusion poset $O = \langle 2^S, \subset \rangle$, and let A be some antichain of this poset. Then let $U(A)$ be the induced poset of unions: $U(A) = \langle \{\bigcup_{b\in B} b | B \subseteq A\}, \subset \rangle$.

For every poset O there exists a unique function called the Möbius function $\mu : S \times S \to \mathbb{R}$, with the following two properties:

1) For all $s \in S$: $\mu(s, s) = 1$, and

2) For all $u, v \in S$ such that $u <_O v$:

$$\sum_{s:u\leqslant_O s\leqslant_O v} \mu(u, s) = 0.$$

Let $H = \{x \in \mathbb{R}^n | ax = b\}$ denote a hyperplane and let $H^+ = \{x \in \mathbb{R}^n | ax \geq b\}$ denote one of the half-spaces whose boundary is H. An intersection of half-spaces $B = H_1^+ \cap H_2^+ \cap \cdots \cap H_m^+$ that is bounded is called a convex polytope. If $H^+ \cap B = B$, then the intersection $H \cap B$ is called a face of B; and each face itself is a polytope. Using the duality of linear programming one can show that

Lemma 1 (Schrijver (1986, Chapter 8, Eqn. (11)))**.** *A non-empty $F \subseteq \mathbb{R}^n$ is a face of $H_1^+ \cap H_2^+ \cap \cdots \cap H_m^+$ if and only if $F = \bigcap_{i\in M} H_i \cap \bigcap_{i\notin M} H_i^+$ for some $M \subseteq [m]$.*

In other words, a face corresponds to a system where some inequalities are replaced by equalities. This representation may be non-unique. Denote by $\mathcal{F}(B)$ the set of faces of polytope B. Then $\langle \mathcal{F}(B), \subset \rangle$ is a poset that is a lattice called the face lattice of polytope B. For a polytope B let its dimension be the largest n such that there exist $v_1, v_2, \ldots, v_{n+1} \in B$ such that $v_1 - v_{n+1}, v_2 - v_{n+1}, \ldots, v_n - v_{n+1}$ are linearly independent. Let us denote the dimension of a polytope B by $\dim B$. Let $\dim \varnothing = -1$. Then

Theorem 1 (Euler's relation, Grünbaum (2003); Brøndsted (1983))**.** *For any two faces $F_1, F_2 \in \mathcal{F}(B)$, such that $F_1 \subset F_2$:*

$$\sum_{F:F_1\subseteq F\subseteq F_2} (-1)^{\dim F} = 0. \tag{1}$$

Let μ_B denote the Möbius function of the face lattice of the polytope B.

Corollary 1.

$$\mu_B(F_1, F_2) = (-1)^{\dim F_2 - \dim F_1}. \tag{2}$$

Proof: Since the Möbius function is unique, it is sufficient to verify that μ_B as defined here satisfies the properties 1) and 2). Clearly, $\mu_B(F, F) = 1$. For $F_1 \subset F_2$:

$$\sum_{F:F_1\subseteq F\subseteq F_2} \mu_B(F_1, F) = \sum_{F:F_1\subseteq F\subseteq F_2} (-1)^{\dim F - \dim F_1} = (-1)^{\dim F_1} \sum_{F:F_1\subseteq F\subseteq F_2} (-1)^{\dim F} = 0. \tag{3}$$

□

3 Representing monotone functions

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function on n variables. For two n-bit strings x and y we will denote by x_i the i-th bit of the string, and say that $x \leq y$ if for all i: $x_i \leq y_i$. We say that a Boolean function is monotone if for all $x, y \in \{0,1\}^n$: $x \leq y$ implies $f(x) \leq f(y)$. We say that a set $I \subseteq [n]$ is a prime implicant of f if the property $(\forall i \in I : x_i = 1) \implies f(x) = 1$ holds for I, but fails for every subset $I' \subset I$. Every monotone Boolean function has a unique representation in terms of the set of its prime implicants denoted by P_f. Since P_f is an antichain in the inclusion poset of the subsets of $[n]$, we can consider its subposet $U(P_f)$.

Proposition 1. *The poset $\langle U(P_f), \subset\rangle$ is an atomistic lattice.*

Proof: Since $\langle U(P_f), \subset\rangle$ is a subposet of the lattice $\langle 2^{[n]}, \subset\rangle$ containing all the original joins (unions) of the elements of $U(P_f)$, it is an upper semilattice. Moreover, it is a lattice, since $U(P_f)$ contains $\varnothing$ as the least element, and any finite bounded upper semilattice is a lattice (see e.g. Proposition 3.3.1 in Stanley (2012)). Since the elements of P_f are incomparable, and $U(P_f)$ contains beside them only their unions (including the empty one), P_f is the set of atoms of $U(P_f)$, and every element of $U(P_f)$ is expressible as their join (union), i.e. the lattice $\langle U(P_f), \subset\rangle$ is atomistic. □

Theorem 2. *Every finite atomistic lattice is isomorphic to $\langle U(P_f), \subset\rangle$ for some monotone Boolean function f.*

Proof: Let $\langle L, \leqslant_L\rangle$ be a finite atomistic lattice, and let $A = \{a_1, a_2, \ldots, a_m\} \subset L$ be the set of its atoms.

We will prune a certain $(0,1)$-matrix M to construct the prime implicants $P_f = \{b_1, b_2, \ldots, b_m\}$ of the corresponding monotone Boolean function f.

Initially let the matrix M be of size $(2^m - 1) \times 2^m$, with columns indexed by subsets of $[m]$ and rows indexed by non-empty subsets of $[m]$. For $S, T \subseteq [m]$, $S \neq \varnothing$ we define

$$M_{S,T} = \begin{cases} 0 & \text{if } S \cap T = \varnothing, \\ 1 & \text{if } S \cap T \neq \varnothing. \end{cases} \tag{4}$$

We will delete some columns of this matrix to obtain its final form (and thus the correct set of prime implicants).

For each $i \in [m]$ the row $\{i\}$ will represent the prime implicant b_i as a bit string. More formally, to obtain b_i, let n be the current number of columns, then reindex the columns by numbers from 1 to n, and let $b_i = \{j \in [n] \mid M_{\{i\},j} = 1\}$. For convenience, let $u : [n] \to 2^{[m]}$ map the new column indices to the old ones. (Note that b_i, n, u all change when we delete a column of M.)

The remaining rows represent unions of prime implicants as bit strings in a similar way. In particular, row S represents $\bigcup_{i \in S} b_i$. Indeed: $M_{S,j} = 1 \Leftrightarrow \exists i\,(i \in S \cap u(j)) \Leftrightarrow \exists i \in S\,(M_{\{i\},j} = 1) \Leftrightarrow \exists i \in S\,(j \in b_i) \Leftrightarrow j \in \bigcup_{i \in S} b_i$. For the rest of the proof we revert to the original indexing of columns by subsets.

Initially $U(P_f)$ generated by M is isomorphic to Boolean algebra of rank m. (We don't need this fact explicitly, so we omit the proof.) We need to make it isomorphic to L. Since L is atomistic, every one of its elements is expressible as a union of its atoms. However, some unions of atoms may be equal between themselves. Suppose an equality $\bigcup_{j \in S} a_j = \bigcup_{j \in T} a_j$ holds for some distinct $S, T \subseteq [m]$. To achieve that

a corresponding equality holds for b_j, we remove from M all columns which make these unions distinct, that is, all columns W such that $M_{S,W} \neq M_{T,W}$.

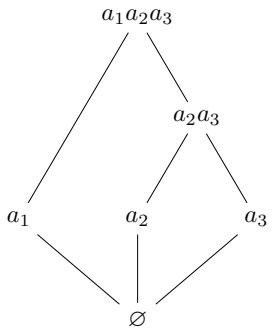

Fig. 1: Atomistic lattice with atoms a_1, a_2, a_3 and equalities $a_1a_2 = a_1a_3 = a_1a_2a_3$

		$\varnothing$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
$\{1\}$	b_1	0	1	0	0	1	1	0	1
$\{2\}$	b_2	0	0	1	0	1	0	1	1
$\{3\}$	b_3	0	0	0	1	0	1	1	1
$\{1,2\}$	b_1b_2	0	1	1	0	1	1	1	1
$\{1,3\}$	b_1b_3	0	1	0	1	1	1	1	1
$\{2,3\}$	b_2b_3	0	0	1	1	1	1	1	1
$\{1,2,3\}$	$b_1b_2b_3$	0	1	1	1	1	1	1	1

Fig. 2: Initial state of the matrix M. In addition to row indices the corresponding unions of prime implicants are specified. The rows b_1b_2, b_1b_3 and $b_1b_2b_3$ must be equal, therefore columns $\{2\}$ and $\{3\}$ making them different must be deleted.

	$\varnothing$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
b_1	0	1	1	1	0	1
b_2	0	0	1	0	1	1
b_3	0	0	0	1	1	1
b_1b_2	0	1	1	1	1	1
b_1b_3	0	1	1	1	1	1
b_2b_3	0	0	1	1	1	1
$b_1b_2b_3$	0	1	1	1	1	1

Fig. 3: State of the matrix M after the deletion of columns $\{2\}$ and $\{3\}$. Now the lattice generated by prime implicants b_1, b_2, b_3 is isomorphic to the lattice of Figure 1.

	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$
b_1	1	1	1	0
b_2	0	1	0	1
b_3	0	0	1	1
b_1b_2	1	1	1	1
b_1b_3	1	1	1	1
b_2b_3	0	1	1	1
$b_1b_2b_3$	1	1	1	1

Fig. 4: The matrix M after removing columns which are unions of other columns: $\{1,2,3\} = \{1\} \cup \{2,3\}$ and $\varnothing$ (the empty union). Lattice generated by $\{b_1, b_2, b_3\}$ does not change. A monotone Boolean function with lattice isomorphic to that of Figure 1 must have at least 4 input bits, at least one per each of the remaining columns.

We perform this operation for every equality that holds between the unions of atoms a_j ensuring that the corresponding equality holds also for the unions of b_j. This process is illustrated in Figures 1–3 for an atomistic lattice with three atoms a_1, a_2, a_3 and identities $a_1 \cup a_2 = a_1 \cup a_3 = a_1 \cup a_2 \cup a_3$ (we omit

the operation signs in the Figures for the sake of brevity).

We claim that the matrix M remaining after these operations generates the lattice $U(P_f)$ which we need. To show that, it remains to prove that we haven't introduced any undesired equality among unions of b_j by removing too many columns.

Suppose the contrary: that for some $S, T \subseteq [m]$ we have $\bigcup_{j\in S} a_j \neq \bigcup_{j\in T} a_j$, but $\bigcup_{j\in S} b_j = \bigcup_{j\in T} b_j$. Here among different S that give the same union $\bigcup_{j\in S} a_j$, let us use the maximum S (i.e. such that no superset of S gives the same union), similarly let us use the maximum T. Since an equality among unions of a_j implies an equality among the corresponding unions of b_j, $\bigcup_{j\in S} b_j = \bigcup_{j\in T} b_j$ holds also for the new S and T, if we replaced any of them.

At least one of the sets $S \setminus T$ and $T \setminus S$ is nonempty; WLOG suppose that $S \setminus T \neq \varnothing$. The equality $\bigcup_{j\in S} b_j = \bigcup_{j\in T} b_j$ means that, among others, we have removed the column $[m]\setminus T$ from M because otherwise it would make these unions distinct: $S \cap ([m]\setminus T) = S \setminus T$, so $M_{S,[m]\setminus T} = 1$ while $M_{T,[m]\setminus T} = 0$. Let the equality which caused the removal of column $[m]\setminus T$ be $\bigcup_{j\in S'} a_j = \bigcup_{j\in T'} a_j$ where $M_{S',[m]\setminus T} = 1$ and $M_{T',[m]\setminus T} = 0$. Then $T' \subseteq T \subset S' \cup T$ and $\bigcup_{j\in T} a_j = \bigcup_{j\in (T\setminus T')\cup T'} a_j = \bigcup_{j\in (T\setminus T')\cup S'} a_j$. Note that in an atomistic lattice, if $\bigcup_{j\in X} a_j = \bigcup_{j\in Y} a_j$, then $\bigcup_{j\in X} a_j = \bigcup_{j\in Y} a_j = \bigcup_{j\in X\cup Y} a_j$, thus the last equality implies $\bigcup_{j\in T} a_j = \bigcup_{j\in T\cup S'} a_j$ which contradicts the maximality of T.

Thus no undesired equality was introduced, and L is isomorphic to $U(P_f)$ by mapping that for each $S \subseteq [m]$ maps $\bigcup_{j\in S} a_j$ to $\bigcup_{j\in S} b_j$. □

[Note. The matrix obtained at the end of the process described in this proof is not optimal in terms of size: any column with index expressible as a union of indices of some other remaining columns (including the empty union) can be removed, since that does not introduce any new equality (see Figure 4). Indeed, if columns $W_1, \ldots, W_k$ and $W = W_1 \cup \cdots \cup W_k$ remain, then any inequality of rows witnessed in the column W: $M_{S,W} = 0 \neq 1 = M_{T,W}$ is witnessed also in one of the columns W_i: $M_{S,W} = 0$ implies $M_{S,W_i} = 0$ for all i and $M_{T,W} = 1$ implies $M_{T,W_i} = 1$ for at least one i. After these redundant columns are removed, all other columns must remain. Indeed, if a column W is still present, then it is not a union of remaining columns, thus there exists an element $i \in W$ not belonging to any index V of a remaining column such that $V \subset W$. Then the inequality of rows $[m] \setminus W$ and $([m] \setminus W) \cup \{i\}$ is witnessed only in this column: $M_{[m]\setminus W,W} = 0 \neq 1 = M_{([m]\setminus W)\cup\{i\},W}$ while for any $V \subset W$: $M_{[m]\setminus W,V} = M_{([m]\setminus W)\cup\{i\},V} = 0$, and for any other V: $M_{[m]\setminus W,V} = M_{([m]\setminus W)\cup\{i\},V} = 1$. Removing this column would make these rows equal, but any rows that remained different after the process described in the proof of the theorem must remain different, since they correspond to different elements of the lattice. Since the columns of the matrix M correspond to input bits of the Boolean function f, the number of the remaining columns determines the minimum number of input bits of a monotone Boolean function corresponding to the given atomistic lattice.**]**

Let $p : \mathbb{R}^n \to \mathbb{R}$ be a multilinear polynomial. We can write p as a linear combination of monomials:

$$p(x_1, x_2, \ldots, x_n) = \sum_{S\subseteq[n]} \alpha_S \prod_{i\in S} x_i. \tag{5}$$

We say that a real multilinear polynomial p represents a Boolean function f if $p(x) = f(x)$ for all $x \in \{0,1\}^n$. Every Boolean function has a unique polynomial p that represents it. The poset $U(P_f)$ and its associated Möbius function $\mu_{U(P_f)}$ have a crucial role in determining the coefficients α_S:

Theorem 3. *Let f be a monotone Boolean function not identical to* 1*. Then its representing polynomial is*

$$p_f(x_1, x_2, \ldots, x_n) = \sum_{S \in U(P_f) \setminus \{\varnothing\}} -\mu_{U(P_f)}(\varnothing, S) \prod_{i \in S} x_i. \tag{6}$$

Proof: We will show that the polynomial p_f equals f on all $x \in \{0,1\}^n$. Clearly, when $f(x) = 0$ then for each $S \in U(P_f) \setminus \{\varnothing\}$ there exists an i such that $x_i = 0$, and so $p_f(x) = 0$. If $f(x) = 1$, then let S be such that $x_i = 1 \iff i \in S$. Let $S' = \cup\{I | I \in P_f, I \subseteq S\}$. S' cannot be empty since $f(x) = 1$. Then

$$p_f(x) = \sum_{T \in U(P_f): T \subseteq S'} \alpha_T = \sum_{T \in U(P_f): T \subseteq S'} -\mu_{U(P_f)}(\varnothing, T) + \mu_{U(P_f)}(\varnothing, \varnothing) = 1.$$

□

4 Möbius function of AQ-CONNECTIVITY

Let $G = \langle V, E, s, t \rangle$ be a directed multigraph without cycles, namely, an acyclic quiver, where V is the set of vertices, E is the set of arcs with $s : E \to V$ and $t : E \to V$ defining the source and target of an arc. For our purposes we can fix V, s, t and associate G with the set of its arcs E. Thus we will write $H \subseteq G$ when H is a subquiver of G, etc. Let $S(G) \subseteq V$ be the set of vertices with no incoming arcs – sources, and let $T(G) \subseteq V$ be vertices with no outgoing arcs – sinks.

Definition 1. *In* AQ-CONNECTIVITY$_G$ *we are given a subquiver H of some fixed quiver G as a set of bits defining its arcs $x_e = \begin{cases} 1 \text{ if } e \in H \\ 0 \text{ if } e \notin H \end{cases}$, and our task is to determine if there is a non-empty path from a vertex in $S(G)$ to a vertex in $T(G)$ using only the arcs in H.*

Since we allow multigraphs, i.e., graphs which can have multiple arcs $e_1, \ldots, e_m$ with the same sources and targets $s(e_1) = \cdots = s(e_m)$, $t(e_1) = \cdots = t(e_m)$, for our purposes we can assume that there is exactly one source and one sink, because we can merge all sources into one (and similarly — all sinks) without affecting connectivity. Henceforth, we will denote the unique source as s and the unique sink as t.

Given an acyclic quiver G, let P_G be the finite set of paths connecting sources and sinks. Note that P_G has to be an antichain in the poset of subquivers of G. The following two theorems are a special case of Theorem 3.2 from Hille (2003). We give our proofs for completeness.

Theorem 4. *For all acyclic quivers G the poset $U(P_G)$ is isomorphic to a face lattice of a convex polytope.*

Proof: For an acyclic quiver G and its subquiver $H \subseteq G$, let $F(H)$ be the set of unit flows from s to t, i.e., $F(H)$ consists of all vectors in $\mathbb{R}^{|G|}$

$$F(H) = \{(f_e)_{e \in G}\}_{f \in \mathbb{R}^{|G|}},$$

such that the following additional constraints are satisfied:

(a) Flow is non-negative: $\forall e \in G : f_e \geq 0$;

(b) The total flow is 1: $\sum_{\substack{e:e\in G\\ s(e)=s}} f_e = 1$;

(c) Flow conservation: $\forall v \notin \{s,t\} : \sum_{\substack{e:e\in G\\ t(e)=v}} f_e = \sum_{\substack{e:e\in G\\ s(e)=v}} f_e$.

(d) Flow is restricted to the subquiver: $\forall e \notin H : f_e = 0$;

Next, we show that $F : U(P_G) \to 2^{\mathbb{R}^{|G|}}$ is indeed the bijection we sought. First, $F(H)$ shares almost all constraints with $F(G)$ except equalities (d). By Lemma 1 the faces of $F(G)$ correspond to the system of $F(G)$ where some inequalities are replaced by equalities, i.e., $f_e = 0$ for some $H' \subseteq G$. Thus, $F(H)$ is a face of $F(G)$ for any $H \in U(P_G)$ since the inequalities $f_e \geq 0$ are replaced by equalities $f_e = 0$ for $e \notin H$. On the other hand, for a subquiver H' there exists a $H \in U(P_G)$ such that $H = \bigcup \{p \in P_G | p \subseteq H'\}$. But subquivers H and H' correspond to the same face; since all $e \in H' \setminus H$ have no path in H' containing them, the flow on these arcs must be zero: $f_e = 0$ for $e \in H' \setminus H$. By construction the inclusion property is obviously preserved, since the flow is more constrained on a subquiver. □

Next we give a simple formula for computing the dimension of a face of the flow polytope. Let $D(H) = |H| - |\{s(e)|e \in H\} \cup \{t(e)|e \in H\} \setminus \{s,t\}| - 1$.

Theorem 5. *If $H \in U(P_G)$, then the dimension of the corresponding face is*

$$\dim F(H) = D(H). \tag{7}$$

Proof: First, the lemma is clearly true for empty quiver and a single path from P_G.

Denote by $A \overset{\bullet}{\subset} B$, if $A, B \in U(P_G)$, $A \subset B$ and $\neg\exists C \in U(P_G) : A \subset C \subset B$. Let us show that for all $H, H' \in U(P_G)$ such that $H \overset{\bullet}{\subset} H'$: $\Delta := H' \setminus H$ is an ear of H', i.e., a path $(v_0, v_1, \ldots, v_k)$ whose internal vertices $v_1, v_2, \ldots, v_{k-1}$ have no other adjacent arcs in H'. Hence $D(H') = D(H) + 1$. Let us prove by contradiction assuming that Δ is not an ear. Clearly, there exists some subset $\delta \subseteq \Delta$ that is an ear of $\delta \cup H$; one can start a path with any arc of Δ and extend the path by traveling backwards and forwards along arcs in Δ until a vertex with an adjacent arc in H is encountered. Consider the initial vertex v_{init} of δ. There must be a path $\alpha \subseteq H$ [potentially empty] from s to v_{init}. If v_{init} has no incoming arcs in H then $v_{init} = s$. If v_{init} has an incoming edge in H then α is a path from s to v_{init}. Symmetrically reasoning we obtain a path ω from the final vertex to t. Clearly, $\alpha \cup \delta \cup \omega \in P_G$ and so $\delta \cup H \in U(P_G)$. Thus $H \subset H \cup \delta \subset H \cup \Delta = H'$ — a contradiction.

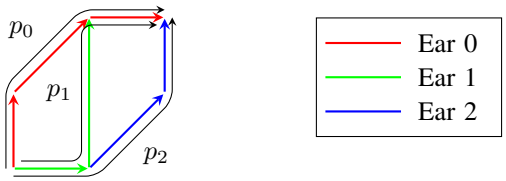

Fig. 5: Ear decomposition

Each $H \in U(P_G)$ has an "ear decomposition" described as $\varnothing = H_{-1} \overset{\bullet}{\subset} H_0 \overset{\bullet}{\subset} H_1 \overset{\bullet}{\subset} \cdots \overset{\bullet}{\subset} H_{D(H)-1} \overset{\bullet}{\subset} H_{D(H)} = H$. In particular, let the path $\alpha \cup \delta \cup \omega \in P_G$ added from H_{k-1} to H_k be denoted by p_k. Then $H_k = H_{k-1} \cup p_k$.

Let $\mathbb{1}(p) = (f_e)_{e \in G}$ denote the unit flow along path p: $f_e = \begin{cases} 1 \text{ if } e \in p \\ 0 \text{ if } e \notin p \end{cases}$. Any flow satisfying all but the non-negativity constraints (i.e., satisfying (b),(c),(d)) for H is an affine combination of $\{\mathbb{1}(p_i) | i \in \{0, 1, \ldots, D(H)\}\}$. We can establish this by induction on $D(H)$. This is obviously the case for $D(H) = -1$ and $D(H) = 0$. Assuming that it is true for $D(H) = k - 1$, $k > 0$, let f be the flow vector. Note that the flow f_e for arcs e in the ear $e \in H_{D(H)} \setminus H_{D(H)-1}$ must be equal. Consider the flow

$$f' = f - f_e(\mathbb{1}(p_k) - \mathbb{1}(p_{k-1})). \tag{8}$$

f' satisfies constraints (b),(c),(d) for $H_{D(H)-1}$ and so by inductive assumption f' is in the affine span of $\{\mathbb{1}(p_i) | i \in \{0, 1, \ldots, D(H) - 1\}\}$. We conclude that $\dim F(H) \leq |\{p_0, p_1, \ldots, p_{D(H)}\}| - 1 = D(H)$.

$\{\mathbb{1}(p_i) - \mathbb{1}(p_0) | i \in \{1, \ldots, D(H)\}\}$ are linearly independent because each $\mathbb{1}(p_i) - \mathbb{1}(p_0)$ is outside the linear span of $\{\mathbb{1}(p_i) - \mathbb{1}(p_0) | i \in \{1, \ldots, i - 1\}\}$. Obviously, $\{\mathbb{1}(p_i) | i \in \{0, 1, \ldots, D(H)\}\}$ belong to $F(H)$. Therefore $\dim F(H) \geq D(H)$. □

Corollary 2. *The unique multilinear polynomial representing* AQ-CONNECTIVITY$_G$ *is:*

$$p_G(x) = \sum_{H \in U(P_G) \setminus \{\varnothing\}} (-1)^{D(H)} \prod_{i \in H} x_i. \tag{9}$$

Proof: By Theorem 3 we have:

$$p_G(x) = \sum_{H \in U(P_G) \setminus \{\varnothing\}} -\mu_{U(P_G)}(\varnothing, H) \prod_{i \in H} x_i. \tag{10}$$

By Theorem 4 the poset $U(P_G)$ is isomorphic to the face lattice of a polytope, and by the Corollary 1 of Euler's relation:

$$p_G(x) = \sum_{H \in U(P_G) \setminus \{\varnothing\}} -(-1)^{\dim F(H) - \dim \varnothing} \prod_{i \in H} x_i = \sum_{H \in U(P_G) \setminus \{\varnothing\}} (-1)^{\dim F(H)} \prod_{i \in H} x_i. \tag{11}$$

Finally, by Theorem 5 we conclude that

$$p_G(x) = \sum_{H \in U(P_G) \setminus \{\varnothing\}} (-1)^{D(H)} \prod_{i \in H} x_i. \tag{12}$$

□

Corollary 3. *The degree of* $p_G(x)$ *is maximal:* $\deg p_G(x) = |G|$.

Proof: Since the whole quiver G is also a union of paths: $G \in U(P_G)$, the coefficient at its monomial is $(-1)^{D(G)}$, i.e. not zero. □

5 Size of $U(P_G)$ for 2D grids

Let G_n be a directed grid: the vertices of this quiver are labeled by $\{0, 1, \ldots, n\}^2$ and there is an arc from vertex (i_1, j_1) to (i_2, j_2) iff $(i_1 = i_2 \wedge j_2 = j_1 + 1)$ or $(j_1 = j_2 \wedge i_2 = i_1 + 1)$.

Theorem 6. $|U(P_{G_n})| \in 2^{\Omega(n^2)}$.

Proof: Consider the subgraph H of grid consisting of all the horizontal edges and vertical edges with $i_1 \in \{0, n\}$ (see Figure 6).

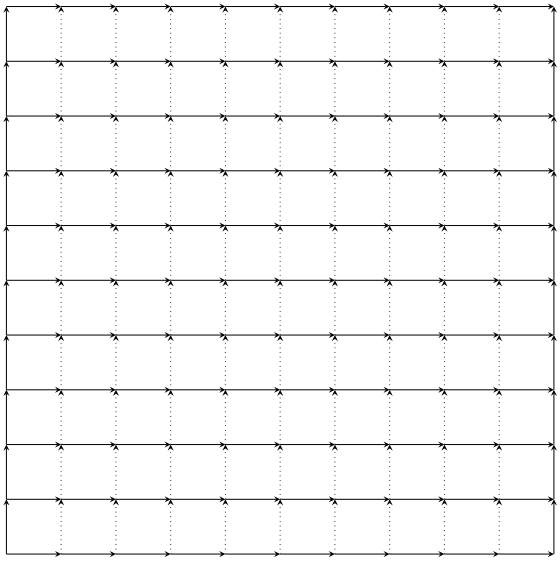

Fig. 6: The subgraph H of grid G_n for $n = 10$

Clearly, all the subgraphs containing H are unions of paths since $H \in U(P_{G_n})$ and for any edge $e \notin H$ there is a path consisting of e and only edges in H. The number of such subgraphs is $2^{(n+1)(n-1)}$. □

Unfortunately, this shows that the approximating polynomial produced by the construction scheme described in Beniamini (2022, Lemma 31) either has degree $\Omega(n^2)$ or the estimate of its degree is not optimal.

Let $D^{\mathrm{AND}}(f)$ denote the decision tree complexity of computing a function f using a decision tree whose nodes are allowed to compute an AND of an arbitrary subset of input bits. Then, in light of (Beniamini and Nisan, 2021, Lemma 3.15) stating that $D^{\mathrm{AND}}(f) \geq \log_3 |mon(f)|$ where $mon(f)$ is the set of monomials with non-zero coefficients, we conclude that

Corollary 4. $D^{\mathrm{AND}}(\text{AQ-CONNECTIVITY}_{G_n}) = \Omega(n^2)$.

6 Conclusion

Like Beniamini and Nisan (2021), we studied also the dual f^* of the function: $f^*(x_1, x_2, \ldots, x_n) = \neg f(\neg x_1, \neg x_2, \ldots, \neg x_n)$. Let AQ-CONNECTIVITY$^*(x_1, x_2, \ldots, x_n) = \sum_{S \subseteq [n]} \alpha^*_S \prod_{i \in S} x_i$. Prime im-

plicants of AQ-CONNECTIVITY* are the minimal cuts. Even though we did not manage to prove it for arbitrary quivers, we found that for the quivers we analyzed the following properties are true:

- $\alpha_S^* \in \{-1, 0, 1\}$;
- The sets S corresponding to the non-zero α_S^* together with the empty set constitute an Eulerian lattice with the usual subset inclusion relation. However, unlike for AQ-CONNECTIVITY the elements of this lattice are not all unions of minimal cuts, but a subset of them. In particular, a slight generalization of Lemma 4.6 from Beniamini and Nisan (2021) to any function with the union of prime implicants $U(P_f)$ being an Eulerian lattice holds. However, for AQ-CONNECTIVITY it is not a sufficient criterion to determine whether $\alpha_S^* = 0$.

The following topics could be of interest for future research:

- What other useful classes of monotone Boolean functions, besides the Bipartite Perfect Matching (Beniamini and Nisan, 2021) and AQ-CONNECTIVITY, have simple Möbius functions?
- The lattices of Bipartite Perfect Matching and AQ-CONNECTIVITY are Eulerian implying simplicity coefficients of the representing polynomial. Is there a simple (good, useful) characterization of the monotone Boolean functions whose lattices are Eulerian?
- Can the representing polynomial of some AQ-CONNECTIVITY problem be used to improve its complexity estimations? For instance, the current quantum query complexity estimations for the $n \times n$ two-dimensional grid still have gap between $\Omega(n^{1.5})$ and $O(n^2)$ (Ambainis et al., 2020). Since the quantum query complexity is lower bounded by the minimum degree of an approximating polynomial (divided by 2), one of the questions is: can the representing polynomial be used to obtain lower bounds exceeding $\Omega(n^{1.5})$ for the degree of an approximating polynomial?

Acknowledgements

The authors wish to thank Andris Ambainis for useful suggestions on how to improve the paper. This research was supported by QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme (QuantAlgo project), ERDF project 1.1.1.5/18/A/020 "Quantum algorithms: from complexity theory to experiment" and the Latvian Quantum Initiative under European Union Recovery and Resilience Facility project no. 2.3.1.1.i.0/1/22/I/CFLA/001.

References

S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM (JACM)*, 51(4):595–605, 2004.

S. Aaronson, R. Kothari, W. Kretschmer, and J. Thaler. Quantum lower bounds for approximate counting via Laurent polynomials. *arXiv preprint arXiv:1904.08914*, 2019.

A. Ambainis, K. Balodis, J. Iraids, M. Kokainis, K. Prūsis, and J. Vihrovs. Quantum speedups for exponential-time dynamic programming algorithms. In *Proceedings of the 2019 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1783–1793, 2019. doi: 10.1137/1.9781611975482.107. arXiv:1807.05209.

A. Ambainis, K. Balodis, J. Iraids, K. Khadiev, V. Kļevickis, K. Prūsis, Y. Shen, J. Smotrovs, and J. Vihrovs. Quantum lower and upper bounds for 2D-grid and Dyck language. In J. Esparza and D. Král', editors, *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 8:1–8:14, 2020. doi: 10.4230/LIPIcs.MFCS.2020.8. arXiv:2007.03402.

W. Baldoni and M. Vergne. Kostant partitions functions and flow polytopes. *Transformation Groups*, 13 (3):447–469, 2008. ISSN 1531-586X. doi: 10.1007/s00031-008-9019-8. URL https://doi.org/10.1007/s00031-008-9019-8.

R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. doi: 10.1145/502090.502097. URL https://doi.org/10.1145/502090.502097.

G. Beniamini. The approximate degree of Bipartite Perfect Matching. In S. Lovett, editor, *37th Computational Complexity Conference (CCC 2022)*, volume 234 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 1:1–1:26, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-241-9. doi: 10.4230/LIPIcs.CCC.2022.1. URL https://drops.dagstuhl.de/opus/volltexte/2022/16563.

G. Beniamini and N. Nisan. Bipartite Perfect Matching as a Real polynomial. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1118–1131. Association for Computing Machinery, 2021. doi: 10.1145/3406325.3451002. arXiv:2001.07642.

A. Brøndsted. *An introduction to convex polytopes*. Springer New York, NY, 1983.

N. H. Bshouty and C. Tamon. On the Fourier spectrum of monotone functions. *J. ACM*, 43(4):747–770, 1996. doi: 10.1145/234533.234564. URL https://doi.org/10.1145/234533.234564.

H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey. *Theor. Comput. Sci.*, 288(1):21–43, 2002. doi: 10.1016/S0304-3975(01)00144-X. URL https://doi.org/10.1016/S0304-3975(01)00144-X.

M. Bun, R. Kothari, and J. Thaler. The polynomial method strikes back: Tight quantum query bounds via dual polynomials. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 297–310, 2018.

B. Grünbaum. *Convex polytopes*. Springer New York, NY, second edition, 2003.

J. Håstad. Almost optimal lower bounds for small depth circuits. In J. Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 6–20. ACM, 1986. doi: 10.1145/12130.12132. URL https://doi.org/10.1145/12130.12132.

L. Hille. Quivers, cones and polytopes. *Linear Algebra and its Applications*, 365:215–237, 2003. ISSN 0024-3795. doi: https://doi.org/10.1016/S0024-3795(02)00406-8. URL https://www.sciencedirect.com/science/article/pii/S0024379502004068. Special Issue on Linear Algebra Methods in Representation Theory.

R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, second edition, 2013. ISBN 0521386322.

N. Linial, Y. Mansour, and N. Nisan. Constant depth circuits, Fourier transform, and learnability. *J. ACM*, 40(3):607–620, 1993. doi: 10.1145/174130.174138. URL https://doi.org/10.1145/174130.174138.

R. O'Donnell. *Analysis of Boolean functions*. Cambridge University Press, 2014.

A. Schrijver. *Theory of linear and integer programming*. John Wiley and Sons, 1986.

R. P. Stanley. *Enumerative combinatorics, Volume I*. Cambridge University Press, second edition, 2012.