

The Approximate Degree of Bipartite Perfect Matching

Gal Beniamini ✉

The Hebrew University of Jerusalem, Israel

Abstract

The approximate degree of a Boolean function is the least degree of a real multilinear polynomial approximating it in the ℓ_∞ -norm over the Boolean hypercube. We show that the approximate degree of the Bipartite Perfect Matching function, which is the indicator over all bipartite graphs having a perfect matching of order n , is $\Theta(n^{3/2})$.

The upper bound is obtained by fully characterizing the unique multilinear polynomial representing the Boolean dual of the perfect matching function, over the reals. Crucially, we show that this polynomial has very small ℓ_1 -norm – only exponential in $\Theta(n \log n)$. The lower bound follows by bounding the spectral sensitivity of the perfect matching function, which is the spectral radius of its cut-graph on the hypercube [1, 15]. We show that the spectral sensitivity of perfect matching is exactly $\Theta(n^{3/2})$.

2012 ACM Subject Classification Mathematics of computing → Matchings and factors; Theory of computation → Algebraic complexity theory; Theory of computation → Oracles and decision trees

Keywords and phrases Bipartite Perfect Matching, Boolean Functions, Approximate Degree

Digital Object Identifier 10.4230/LIPIcs.CCC.2022.1

Related Version *Full Version:* <https://arxiv.org/abs/2004.14318>

Acknowledgements I would like to thank Noam Nisan and Nati Linial for helpful discussions. I would also like to thank Bruno Loff for pointing out typographical errors in an earlier version.

1 Introduction

The approximate degree of a Boolean function is the least degree of a real polynomial approximating the function in the ℓ_∞ -norm over the Boolean cube, to within constant error. Approximate degree is an important complexity measure with applications throughout theoretical computer science. Lower bounds on the approximate degree of a Boolean function imply such bounds on the communication complexity (of a related composed problem) [28, 30], and for its quantum query complexity [2]. For families of Boolean functions, upper bounds on the approximate degree have algorithmic merit, for instance in learning theory [17, 16] and differential privacy [31, 11], and conversely lower bounds imply separations in circuit complexity [20, 27]. For a recent survey, we refer the reader to [10].

In this paper we study the approximate degree of the bipartite perfect matching function. This is the Boolean function representing the *decision problem* of perfect matching – determining whether a given balanced bipartite graph contains a subset of edges in which every vertex is incident to exactly one edge.

► **Definition.** *The bipartite perfect matching function $\text{BPM}_n : \{0, 1\}^{n^2} \rightarrow \{0, 1\}$ is defined*

$$\text{BPM}_n(x_{1,1}, \dots, x_{n,n}) = \begin{cases} 1 & \{(i, j) : x_{i,j} = 1\} \text{ has a bipartite perfect matching} \\ 0 & \text{otherwise.} \end{cases}$$

The input bits of BPM_n select a subset of edges from the complete bipartite graph, and the output bit is set to 1 if and only if the chosen subgraph contains a bipartite perfect matching of order n .



© Gal Beniamini;
licensed under Creative Commons License CC-BY 4.0
37th Computational Complexity Conference (CCC 2022).

Editor: Shachar Lovett; Article No. 1; pp. 1:1–1:26



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



1:2 The Approximate Degree of Bipartite Perfect Matching

It is well known that any Boolean function can be uniquely and *exactly* represented by a multilinear polynomial over the reals (see [25]). In [3], the unique polynomial representing BPM_n was characterized, and in particular was shown to have full degree, n^2 . Conversely, it is not hard to construct low-degree polynomials *approximating* the perfect matching function, if one allows pointwise errors arbitrarily close to one half. Indeed, the $n \times n$ Permanent implies (by translation and scaling) such a polynomial of total degree n , and approximation error exponentially close to half. Approximate degree is an interpolation between these two settings, wherein we require the errors be bounded by an arbitrary constant *less than half*, say one third. The previous best-known upper bound on the approximate degree of perfect matching was $\mathcal{O}(n^{7/4})$, due to Lin and Lin [18], and no non-trivial lower bound was known.

Our main result is the following bound¹, which is tight up to low order terms.

► **Theorem 1** (The Approximate Degree Bipartite Perfect Matching). *For every $n \in \mathbb{N}$, the approximate degree of the bipartite perfect matching function is:*

$$\widetilde{\deg}(\text{BPM}_n) = \widetilde{\Theta}\left(n^{3/2}\right).$$

Most known techniques for bounding approximate degree are applicable only to functions which are either *symmetric* or *block-composed* (with some recent notable exceptions, e.g. [8, 9]). The perfect matching function falls into neither category, and is thus not amenable to standard techniques.

Our upper bound follows by investigating the “Boolean Dual” function of bipartite perfect matching: $\text{BPM}_n^*(x_{1,1}, \dots, x_{n,n}) = 1 - \text{BPM}_n(1 - x_{1,1}, \dots, 1 - x_{n,n})$. In this representation, we reverse the roles of the symbols 0 and 1. Concretely, for any input graph, the dual function BPM_n^* outputs 1 if and only if the *complement* of the graph *does not* contain a bipartite perfect matching. Equivalently, by Hall’s Marriage Theorem, the output is 1 if and only if the input graph *contains* a biclique over $n + 1$ vertices.

To present our characterization of the dual, let us introduce some notation. A balanced bipartite graph is said to be *totally ordered*, if there exists an ordering of its left vertices such that their neighbour sets form a chain with respect to inclusion, i.e. $N(a_1) \subseteq N(a_2) \subseteq \dots \subseteq N(a_n)$. We associate with every totally ordered graph a “representing sequence”, which encodes its biadjacency matrix up to permutations over both bipartitions. To construct this sequence, consider the automorphism which sorts the left and right vertices in descending order of degree. This yields a graph whose biadjacency matrix consists of a monotonically increasing sequence of *blocks*, which we succinctly describe using a list of pairs of integers, describing the width and height of each such block. By way of example, the biclique $K_{s,t} \subseteq K_{n,n}$ is an ordered graph whose biadjacency matrix consists of two blocks; the first s left vertices are all adjacent to the first t vertices on the right, and the remainder are all isolated.

Our result is the following *complete characterization* of the unique polynomial representing BPM_n^* over the reals, thereby resolving an open question of [3].

► **Theorem 2** (The Dual Polynomial of Bipartite Perfect Matching).

$$\text{BPM}_n^*(x_{1,1}, \dots, x_{n,n}) = \sum_{G \subseteq K_{n,n}} a_G^* \prod_{(i,j) \in E(G)} x_{i,j}$$

¹ The same bound also holds even for approximations with *exponentially small* error, see Section 4.

- If G is not totally ordered, then $a_G^* = 0$.
- Otherwise:

$$a_G^* = \binom{n - k_{t-1} - 1}{n - d_t} \cdot \prod_{i=1}^{t-1} f(d_{i+1} - k_{i-1}, d_i - k_{i-1}, k_i - k_{i-1})$$

where $0 \leq d_1 < d_2 < \dots < d_t \leq n$ and $0 = k_0 < k_1 < k_2 < \dots < k_t = n$ form the representing sequence of G , and $f : \mathbb{Z}^3 \rightarrow \mathbb{Z}$ is defined:

$$f(n, d, k) = \begin{cases} \binom{n-1}{k}, & d \leq 0 \\ -\binom{n-d-1}{k-d} \binom{k-1}{d-1}, & d > 0. \end{cases}$$

This characterization allows us to deduce that the ℓ_1 -norm of BPM_n^* (i.e., the sum of the magnitudes of its coefficients) is very small – only exponential in $\Theta(n \log n)$. The approximate degree upper bound then follows via two observations. Firstly, we relate the approximate degree of any Boolean function and its dual. Secondly, we show that any Boolean function whose representation over the $\{0, 1\}$ -basis has low ℓ_1 -norm, can be efficiently approximated in the ℓ_∞ -norm. The latter approach had also previously been employed by Sherstov in [29].

To obtain the lower bound on the approximate degree of matching, we consider a new complexity measure recently introduced by Aaronson, Ben-David, Kothari, Rao and Tal [1]. For any total Boolean function f , they define the *Spectral Sensitivity* to be the spectral radius of the bipartite graph defined by the f -bichromatic edges of the Hypercube (i.e., the f -cut of the cube). The notion of spectral sensitivity had notably (implicitly) also appeared at the heart of Huang’s breakthrough proof of the Sensitivity Conjecture [15]. The main technical Theorem of [1] states that the spectral sensitivity of any total Boolean function lower bounds its approximate polynomial degree – and it is this relation that we leverage.

We prove the following tight bound on the spectral sensitivity of BPM_n .

► **Theorem 3** (The Spectral Sensitivity of Bipartite Perfect Matching). *The Spectral Sensitivity of the bipartite perfect matching function is $\lambda(\text{BPM}_n) = \Theta(n^{3/2})$.*

One of our main motivations in studying the algebraic properties of BPM_n and its dual, is the following longstanding question: what is the least complexity of a *deterministic* algorithm for bipartite matching? Hopcroft and Karp’s algorithm [14] from half a century ago attains a running time of $\mathcal{O}(n^{5/2})^2$, and as of yet no known deterministic algorithm has been shown to break the “ $n^{5/2}$ -barrier”. In the last section of this paper we explore the above barrier through the lens of the Demand Query Model [22], which is a concrete complexity model for matching due to Nisan. The demand model was shown in [22] to “capture” the complexity of a wide class of algorithms (i.e., *combinatorial* algorithms), therefore any non-trivial lower bound on algorithms within the model would have far reaching implications. To this end, we draw connections between the *algebraic quantities* explored throughout this work, including approximate degree and the ℓ_1 -norm of the dual, and the *demand query complexity* of matching – see Figure 7. Furthermore, we exhibit an efficient quantum simulation for the demand model, showing that lower bounds in the quantum query model yield corresponding combinatorial bounds. The quantum query complexity of matching was shown by Zhang [32] to be at least $\Omega(n^{3/2})$, and by Lin and Lin [18] to be at most $\mathcal{O}(n^{7/4})$. Closing this gap is

² On *dense* graphs, wherein the number of edges is proportional to n^2 .

left as an open question, and we remark that any polynomial improvement on the lower bound would yield a non-trivial bound in the demand model³. Finally, we note that all the bounds obtained in this paper are compatible with the existence of quasi-linear demand query algorithms for bipartite matching, and this might be seen as weak evidence pointing in this direction. Obtaining non-trivial bounds on the demand query complexity of matching is left as our main open problem.

2 Preliminaries and Notation

2.1 Boolean Functions and Polynomial Representation

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. A polynomial $p \in \mathbb{R}[x_1, \dots, x_n]$ is said to *represent* f , if for every $x \in \{0, 1\}^n$, we have $p(x) = f(x)$. We recall that any Boolean function can be *uniquely* represented by a multilinear polynomial over the reals. Given the unique multilinear polynomial $p(x_1, \dots, x_n) = \sum_{S \subseteq [n]} a_S (\prod_{i \in S} x_i)$ representing f , we denote by $\text{mon}(f) = \{S \subseteq [n] : a_S \neq 0\}$ the set of all monomials appearing in its polynomial representation. Furthermore, we define the following two “norms”, which are defined using the unique representations of Boolean functions, over the Boolean and Fourier bases.

► **Definition 4.** Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$, let $p(x_1, \dots, x_n) = \sum_{S \subseteq [n]} a_S \prod_{i \in S} x_i$ be the unique multilinear representation of f over the reals and let $\{\hat{f}_S : S \subseteq [n]\}$ be the Fourier spectrum of f . The ℓ_1 -norm and ℓ_1 -Fourier-norm of f are defined:

$$\|f\|_1 \stackrel{\text{def}}{=} \|p\|_1 \stackrel{\text{def}}{=} \sum_{S \subseteq [n]} |a_S|, \text{ and } \|\hat{f}\|_1 \stackrel{\text{def}}{=} \sum_{S \subseteq [n]} |\hat{f}_S|.$$

The ϵ -approximate degree of a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is the least degree of a real multilinear polynomial *approximating* f in the ℓ_∞ norm, with error at most ϵ . Hereafter, we use the standard notation and write $\widetilde{\text{deg}}_\epsilon(f)$ to denote the ϵ -approximate degree of f . In the case of $\epsilon = \frac{1}{3}$, we omit the ϵ and instead write $\widetilde{\text{deg}}(f)$.

► **Definition 5.** Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function, and let $0 < \epsilon < \frac{1}{2}$. The ϵ -approximate degree of f , $\widetilde{\text{deg}}_\epsilon(f)$, is the least degree of a real polynomial $p \in \mathbb{R}[x_1, \dots, x_n]$ satisfying $|f(x) - p(x)| \leq \epsilon$, for all $x \in \{0, 1\}^n$.

In the context of Boolean functions, it is sometimes useful to consider the transformation of a Boolean vector in which an arbitrary subset of bits have been flipped. Thus, if $x \in \{0, 1\}^n$, and $S \subseteq [n]$, we use the notation x^S to indicate the vector in which the coordinates S have been flipped. For any $i \in [n]$, the notation x^i is shorthand for $x^{\{i\}}$. Using this notation, we define the following two complexity measures for Boolean functions.

► **Definition 6.** Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$. The **sensitivity** of f at $x \in \{0, 1\}^n$ is:

$$\text{sens}_f(x) = |\{i \in [n] : f(x) \neq f(x^i)\}|$$

and similarly, the **block sensitivity** of f at x is:

$$\text{bs}_f(x) = \max\{s \in [n], \text{ such that } \exists B_1 \sqcup \dots \sqcup B_s \subseteq [n] : \forall i \in [s] : f(x) \neq f(x^{B_i})\}.$$

The sensitivity and block sensitivity of f are then defined by their corresponding measures on the worst case input, namely $\text{sens}(f) = \max_{x \in \{0, 1\}^n} \text{sens}_f(x)$ and $\text{bs}(f) = \max_{x \in \{0, 1\}^n} \text{bs}_f(x)$.

³ Theorem 1 implies that this lower bound *cannot be (polynomially) strengthened* by the “polynomial method”. In fact, neither can the (nonnegative-weight) Ambainis’ adversary technique, see [32].

2.2 Graph Theory

We use standard definitions and notation relating to graphs. If G is a graph, we denote its vertex set by $V(G)$, its edge set by $E(G)$, and its connected components by $C(G)$. The cardinalities of these sets are denoted $v(G)$, $e(G)$ and $c(G)$, respectively. For any vertex $v \in V(G)$, the neighbour set of v is denoted by $N(v)$, and its degree is denoted $\deg(v) = |N(v)|$. The set of all *perfect matchings* of G is denoted by $\text{PM}(G)$. We also use the following slightly less common quantity:

► **Definition 7.** The *cyclomatic number* of a graph is defined $\chi(G) \stackrel{\text{def}}{=} e(G) - v(G) + c(G)$.

The graph $G - v$, where $v \in V(G)$, is the graph over the vertices $V(G) \setminus \{v\}$ in which all the edges incident to v are omitted. If $U \subseteq V(G)$ is a set of vertices, the notation $G[U]$ refers to the *induced graph* on the vertices U , whose vertices are U and whose edges are the edges of G which are incident only to vertices in U . If $G \subseteq K_{n,n}$ and $S \subseteq E(K_{n,n})$ the notation $G \cup S$ refers to a graph over the vertices of $K_{n,n}$, whose edge set is $E(G) \cup S$.

For any graph G , the *adjacency matrix* A_G is a symmetric matrix whose rows and columns are labeled by $V(G)$, and whose entries are given by $(A_G)_{u,v} = \mathbb{1}\{\{u,v\} \in E(G)\}$. The *spectral radius* of G is defined $\rho(G) \stackrel{\text{def}}{=} \max\{|\lambda_i| : \lambda_i \in \text{Spec}(A_G)\}$, i.e., the maximum magnitude of any eigenvalue in the spectrum of A_G . Since the spectrum of bipartite graphs is *symmetric*, it holds that for any bipartite graph $\rho(G) = \lambda_1$.

Throughout this paper, we restrict our attention to *balanced bipartite graphs over the vertices of the complete bipartite graph, $K_{n,n}$* . By convention, we label the left vertices of $K_{n,n}$ by a_1, \dots, a_n , and the right vertices by b_1, \dots, b_n . The notation $G \subseteq K_{n,n}$ is used to indicate that G is a balanced bipartite graph over the vertices of $K_{n,n}$. Similarly, the notation $G \subseteq H$ indicates that $V(G) = V(H)$ and $E(G) \subseteq E(H)$.

2.3 Quantum Query Complexity

We consider the standard quantum query model (see, e.g., [7]). For a recent textbook on the framework of quantum computing, we refer the reader to [21]. In this paper, we refer to the bounded-error quantum query complexity $Q_2(f)$, which is the smallest number d , such that there exists a quantum query algorithm \mathcal{A} making at most d queries, and agreeing with the Boolean function f with probability at least two-thirds, on all Boolean inputs.

3 The Dual Polynomial of Bipartite Perfect Matching

This section centers around the proof of Theorem 2. To provide the proof, we must first familiarize ourselves with some useful definitions and notation. To this end, we begin by defining Boolean dual functions, and by recalling two relevant graph families: matching-covered graphs, and elementary graphs. Then, we introduce the notion of sorted and ordered graphs, which serve as the building blocks of our proof. Finally, we provide our proof of Theorem 2.

3.1 Boolean Dual Functions

► **Definition 8.** Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. The *Boolean Dual* function of f is denoted $f^* : \{0, 1\}^n \rightarrow \{0, 1\}$ and is defined $f^*(x_1, \dots, x_n) = 1 - f(1 - x_1, \dots, 1 - x_n)$.

Intuitively, in the Boolean dual, the symbols 0 and 1 switch roles. Geometrically, if we consider f to be a colouring of the vertices of the n -dimensional hypercube, the duality transformation simply mirrors all vertices and inverts their colours. Algebraically, when

representing the functions using multilinear polynomials over the reals, each monomial in the “primal” function corresponds to an AND function, whereas in the dual each monomial corresponds to an OR (over the original input bits). A Boolean function f and its dual f^* share many properties. For example, their Fourier spectra are identical (up to signs of Fourier coefficients, see [25]). Nevertheless, in the $\{0, 1\}$ basis, the unique multilinear polynomials representing f and f^* can differ greatly. By way of example, the polynomial representing AND_n consists of a single monomial, whereas its dual ($\text{AND}_n^* = \text{OR}_n$) has exactly $2^n - 1$ monomials.

3.2 Matching-Covered and Elementary Graphs

A graph $G \subseteq K_{n,n}$ is said to be *matching-covered* if every edge of G participates in some perfect matching, or equivalently if its edge set can be described as the union over a set of perfect matchings $S \subseteq PM(G)$.

► **Definition 9.** Let $G \subseteq K_{n,n}$ be a graph. G is *matching-covered* if and only if:

$$\forall e \in E(G) : \exists M \in PM(G) : e \in M.$$

Matching-covered graphs have many interesting combinatorial properties. The set of all such graphs, together with the subset relation over the edges, forms a lattice. A key result by Billera and Sarangarajan [5] showed that this lattice is, in fact, isomorphic to the face lattice of the Birkhoff polytope, B_n . This lattice was later shown by [3] to be intimately related to the multilinear polynomial representing the bipartite perfect matching function, BPM_n . Namely, the monomials of the polynomial are the elements of the lattice, and their coefficients are the Möbius numbers of this lattice.

A closely related family of graphs are the *Elementary Graphs*.

► **Definition 10.** Let $G \subseteq K_{n,n}$ be a graph. Then:

G is *elementary* $\iff G$ is a connected matching-covered graph.

Hereafter, we denote by $\text{MC}_n = \{G \subseteq K_{n,n} : G \text{ is matching-covered}\}$ the set of all matching-covered graphs, and similarly we denote $\text{EL}_n = \{G \subseteq K_{n,n} : G \text{ is elementary}\}$ for all elementary graphs. Elementary graphs were studied at length, both by Lovász and Plummer [26], and earlier by Heteyi [13]. Through their works they formulated robust characterizations of elementary graphs. In particular, we require the following theorem, due mostly to Heteyi:

► **Theorem 11** ([13]). Let $G = (A \sqcup B, E)$ be a bipartite graph. The following are equivalent:

- G is elementary.
- G has exactly two minimum vertex covers, A and B .
- $|A| = |B|$ and for every $\emptyset \neq X \subset A$, $|N(X)| > |X|$.
- $G = K_2$, or $v(G) \geq 4$ and for any $a \in A$, $b \in B$, $G - a - b$ has a perfect matching.
- G is connected and every edge is “allowed”, i.e., appears in a perfect matching of G .

3.3 Ordered Graphs

► **Definition 12.** Let $G \subseteq K_{n,n}$. G is a *totally ordered graph*, if there exists an ordering $\pi \in S_n$ of its left vertices, such that $N(a_{\pi(1)}) \subseteq N(a_{\pi(2)}) \subseteq \dots \subseteq N(a_{\pi(n)})$.

Given a totally ordered graph G , we may permute the vertices in its left and right bipartitions (separately) so that both bipartitions are sorted in decreasing order of degree. This automorphism produces a graph $H \cong G$, which we refer to as a “sorted ordered graph”. Our motivation in applying such a transformation is due to the fact that BPM_n^* is invariant to permutations over its bipartitions. Thus, the dual coefficient of any ordered graph and its corresponding sorted ordered graph are identical.

► **Definition 13.** Let $G \subseteq K_{n,n}$. G is a *sorted ordered graph* if:

$$\text{deg}(a_1) \leq \text{deg}(a_2) \leq \dots \leq \text{deg}(a_n), \text{ and } \forall i \in [n] : N(a_i) = \{b_1, \dots, b_{\text{deg}(a_i)}\}.$$

The adjacency relation of a sorted ordered graph can be succinctly and uniquely described by a short sequence of integers, which we dub the “representing sequence” of the graph.

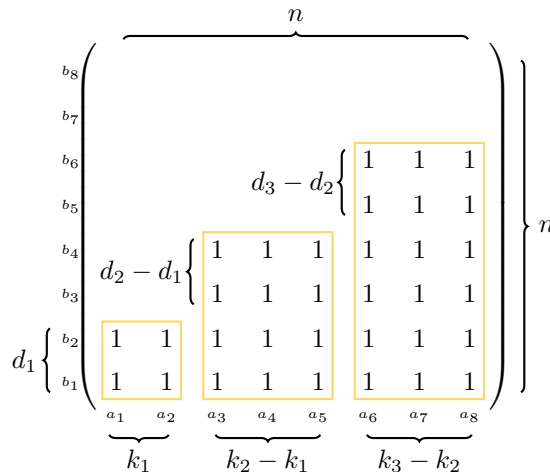
► **Definition 14.** Let $G \subseteq K_{n,n}$ be a sorted ordered graph. The *representing sequence* of G is defined by $\mathcal{S}_G = \{(d_1, k_1), \dots, (d_t, k_t)\}$, where:

$$0 \leq d_1 < d_2 < \dots < d_t \leq n, \text{ and } 0 < k_1 < k_2 < \dots < k_t = n$$

and furthermore:

$$\forall i \in [n] : N(a_i) = \begin{cases} \{b_1, \dots, b_{d_1}\}, & 0 < i \leq k_1 \\ \{b_1, \dots, b_{d_2}\}, & k_1 < i \leq k_2 \\ \vdots & \vdots \\ \{b_1, \dots, b_{d_t}\}, & k_{t-1} < i \leq k_t. \end{cases}$$

The *representing sequence* \mathcal{S}_G of a sorted ordered graph $G \subseteq K_{n,n}$ is essentially a “compressed” form of its degree sequence; each pair (d_i, k_i) in the sequence indicates a run of $(k_i - k_{i-1})$ left vertices, all of whose neighbour sets are exactly $\{b_1, \dots, b_{d_i}\}$. Thus, the biadjacency matrix of G is simply described in terms of \mathcal{S}_G , as shown in Figure 1.



■ **Figure 1** The biadjacency matrix of a sorted ordered graph G . The *representing sequence* of G is $\mathcal{S}_G = \{(d_1, k_1), (d_2, k_2), (d_3, k_3)\}$.

The building blocks in our proof of Theorem 2 consist of particular family of simple sorted ordered graphs – those whose representing sequence is of length exactly 2. In other words, these are the graphs whose left vertices can be partitioned into two sets, those having

full degree n , and those whose neighbour set is (the same) strict subset of the right vertices. This family also trivially includes all bicliques $K_{s,n}$. For this family of graphs, we introduce the following notation.

► **Notation 15.** Let $0 \leq d \leq n$ and $0 < k < n$. The notation $\langle n, d, k \rangle$ -block refers to the sorted ordered graph $G \subseteq K_{n,n}$, whose representing sequence is $\mathcal{S}_{\langle n, d, k \rangle} = \{(d, k), (n, n)\}$.

$$d \left\{ \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_k \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \right\} n$$

■ **Figure 2** The biadjacency matrix of an $\langle n, d, k \rangle$ -block.

3.4 Proof of Theorem 2

► **Definition 16.** Let $\text{BPM}_n^* : \{0, 1\}^{n^2} \rightarrow \{0, 1\}$ be the Boolean dual function of BPM_n :

$$\text{BPM}_n^*(x_{1,1}, \dots, x_{n,n}) = \begin{cases} 1 & \{(i, j) : x_{i,j} = 0\} \text{ does not have a bipartite perfect matching} \\ 0 & \text{otherwise.} \end{cases}$$

In [3], a complete characterization of the multilinear polynomial representing BPM_n over the reals was obtained, using a connection between the Möbius function of the Birkhoff polytope’s face lattice, and the cyclomatic numbers of matching-covered graphs. The polynomial representing BPM_n^* may be similarly expressed through the Möbius function of some lattice (that of graphs covered by “Hall Violators”, i.e., bicliques over $n + 1$ vertices). These representations allowed for a *partial* description of the *support* of BPM_n^* , which we require for our proof of Theorem 2 and will therefore now recall. The first two lemmas restrict the *support* of monomials in the dual polynomial to the set of *totally ordered graphs*, which are *not matching-covered*.

► **Lemma 17** ([3]). Let $G \subseteq K_{n,n}$. If G is not totally ordered, then $a_G^* = 0$.

► **Lemma 18** ([3]). Let $G \subseteq K_{n,n}$. If $G \in \text{MC}_n$, then $a_G^* = 0$.

The third lemma relates the Möbius numbers of the lattice of matching-covered graphs, with the dual coefficients of any graph $G \subseteq K_{n,n}$, thereby giving a closed-form expression for computing the dual coefficients (albeit by summing over possibly exponentially many summands).

► **Lemma 19** ([3]). Let $G \subseteq K_{n,n}$. The dual coefficient of G is:

$$a_G^* = (-1)^{e(G)+1} \sum_{\substack{H \supseteq G \\ H \in \text{MC}_n}} (-1)^{x(H)}.$$

► **Corollary 20.** *Let $G \subseteq K_{n,n}$ be a graph. If all the left vertices or all the right vertices of G are in the same connected component, then:*

$$a_G^* = \sum_{\substack{G \subseteq H \subseteq K_{n,n} \\ H \in \text{EL}_n}} (-1)^{|E(H) \setminus E(G)|}.$$

Proof. Recall that every connected component of a matching-covered graph is elementary. Furthermore, elementary graphs are balanced. Thus, $G \subseteq H \in \text{MC}_n \implies H$ is elementary, and we have:

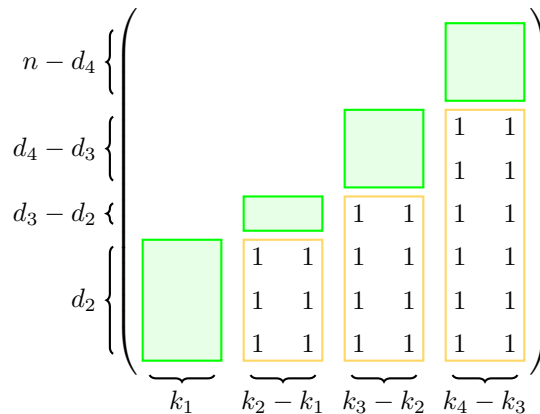
$$\begin{aligned} a_G^* &= (-1)^{e(G)+1} \sum_{\substack{H \supseteq G \\ H \in \text{MC}_n}} (-1)^{\chi(H)} \\ &= (-1)^{e(G)+1} \sum_{\substack{H \supseteq G \\ H \in \text{EL}_n}} (-1)^{e(H)-2n+1} = \sum_{\substack{H \supseteq G \\ H \in \text{EL}_n}} (-1)^{|E(H) \setminus E(G)|}. \end{aligned} \quad \blacktriangleleft$$

3.4.1 Reducing to Permitted Edges

We now make the following observation: if G is a totally ordered graph whose coefficient we wish to compute using Lemma 19, then we may *restrict* our attention to a particular subset of edges. Whereas Lemma 19 mandates that we consider every possible “completion” of G to a matching-covered graph, the following lemma shows that we can instead only consider completions which are confined to the set of “permitted edges” for G .

► **Definition 21.** *Let $G \subseteq K_{n,n}$ be a sorted ordered graph, and let $S_G = \{(d_1, k_1), \dots, (d_t, k_t)\}$ be its representing sequence. The **permitted edges** for G , denoted \mathcal{P}_G , are defined as follows:*

$$(a_i, b_j) \in \mathcal{P}_G \iff \begin{cases} d_1 < j \leq d_2, & 0 < i \leq k_1 \\ d_2 < j \leq d_3, & k_1 < i \leq k_2 \\ \vdots & \vdots \\ d_t < j \leq n, & k_{t-1} < i \leq k_t. \end{cases}$$



■ **Figure 3** A sorted ordered graph G , with $S_G = \{(d_1, k_1), (d_2, k_2), (d_3, k_3), (d_4, k_4)\}$. Orange blocks indicate the edges of G , and green blocks indicate the permitted edges, \mathcal{P}_G .

1:10 The Approximate Degree of Bipartite Perfect Matching

► **Lemma 22.** *Let $G \subseteq K_{n,n}$ be a sorted ordered graph. Then:*

$$a_G^* = \sum_{\substack{G \subseteq H \in \text{EL}_n \\ (E(H) \setminus E(G)) \subseteq \mathcal{P}_G}} (-1)^{|E(H) \setminus E(G)|}.$$

Proof. Let $S = E(K_{n,n}) \setminus (\mathcal{P}_G \sqcup E(G))$. By Lemma 19, Corollary 20, and using the inclusion-exclusion principle, we have:

$$\begin{aligned} a_G^* &= (-1)^{e(G)+1} \sum_{\substack{H \supseteq G \\ H \in \overline{\text{MC}}_n}} (-1)^{\chi(H)} \\ &= \sum_{\substack{G \subseteq H \in \text{EL}_n \\ (E(H) \setminus E(G)) \subseteq \mathcal{P}_G}} (-1)^{|E(H) \setminus E(G)|} + (-1)^{e(G)+1} \sum_{\substack{G \subseteq H \in \text{MC}_n \\ E(H) \cap S \neq \emptyset}} (-1)^{\chi(H)} \\ &= \sum_{\substack{G \subseteq H \in \text{EL}_n \\ (E(H) \setminus E(G)) \subseteq \mathcal{P}_G}} (-1)^{|E(H) \setminus E(G)|} + (-1)^{e(G)+1} \sum_{\emptyset \neq T \subseteq S} (-1)^{|T|} \sum_{(G \sqcup T) \subseteq H \in \text{MC}_n} (-1)^{\chi(H)}. \end{aligned}$$

Observe that for every $\emptyset \neq T \subseteq S$, the graph $G \sqcup T$ is *not* totally ordered. Therefore, by Lemma 17, every summand $\sum_{(G \sqcup T) \subseteq H \in \text{MC}_n} (-1)^{\chi(H)}$ in the above expression vanishes, thus concluding the proof. ◀

3.4.2 Factorizing into $\langle n, d, k \rangle$ -blocks

Having shown that only “permitted edges” need be considered, our next step is to reduce the computation of the dual coefficient a_G^* , to that of dual coefficients of *simpler* graphs. In order to do so, we must first handle the following “degenerate” case.

► **Lemma 23.** *Let $G \subseteq K_{n,n}$ be a sorted ordered graph and let $\mathcal{S}_G = \{(d_1, k_1), \dots, (d_t, k_t)\}$ be the representing sequence of G . If $\exists i \in [t-1]$ such that $d_{i+1} \leq k_i$, then $a_G^* = 0$.*

Proof. Let $i \in [t-1]$ such that $d_{i+1} \leq k_i$, and let $X = \{a_1, \dots, a_{k_i}\} \subsetneq \{a_1, \dots, a_n\}$. Then,

$$a_G^* = \sum_{\substack{G \subseteq H \in \text{EL}_n \\ (E(H) \setminus E(G)) \subseteq \mathcal{P}_G}} (-1)^{|E(H) \setminus E(G)|}$$

by Lemma 22, and therefore it suffices to show that any graph $H \supseteq G$ with $(E(H) \setminus E(G)) \subseteq \mathcal{P}_G$ is not elementary. Let H be such a graph. Then $|\mathcal{N}_H(X)| \leq d_{i+1} \leq k_i = |X|$, and by Theorem 11, H is indeed not elementary. ◀

Any sorted ordered graph G whose representing sequence is not degenerate in the above sense, can be neatly factorized into a set of $\langle n, d, k \rangle$ -blocks. In the following lemma we construct such a decomposition, and relate the dual coefficients of the each component with that of the original graph.

► **Lemma 24.** *Let $G \subseteq K_{n,n}$ be a sorted ordered graph. Let $\mathcal{S}_G = \{(d_1, k_1), \dots, (d_t, k_t)\}$ be the representing sequence of G , where $\forall i \in [t-1] : d_{i+1} > k_i$. Denote $k_0 = 0$, $d_{t+1} = n$, and:*

$$\forall i \in [t] : A_i = \{a_{k_{i-1}+1}, \dots, a_{d_{i+1}}\}, \quad B_i = \{b_{k_{i-1}+1}, \dots, b_{d_{i+1}}\}$$

Furthermore, $\forall i \in [t]$ let $G_i = G[A_i \sqcup B_i]$ be the induced graph on the vertices $A_i \sqcup B_i$. Then:

$$a_G^* = \prod_{i=1}^t a_{G_i}^*.$$

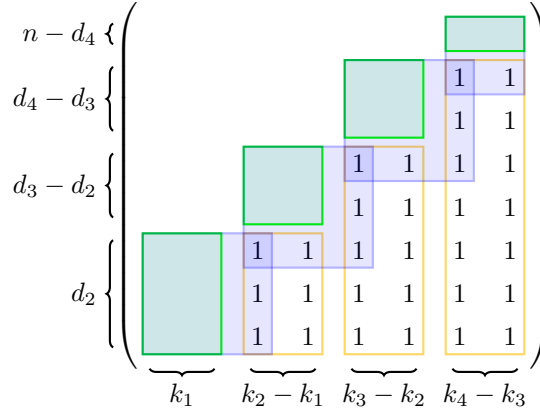
Proof. For all $i \in [t]$, let $S_i = \{a_{k_{i-1}+1}, \dots, a_{k_i}\}$ and $T_i = \{b_{d_i+1}, \dots, b_{d_{i+1}}\}$. Observe that the permitted edges for G are partitioned by the sets S_i, T_i as follows: $\mathcal{P}_G = \bigsqcup_{i=1}^t (S_i \times T_i)$. Furthermore, since $\forall i \in [t] : d_i > k_{i-1}$, we have:

$$\forall i \in [t] : (A_i \times B_i) \cap \mathcal{P}_G = (S_i \times T_i).$$

Thus, each induced graph G_i ‘‘covers’’ the set $(S_i \times T_i)$, and the set of all induced graphs covers all the permitted edges \mathcal{P}_G . Since $d_i > k_{i-1}$, then $\forall i \in [t-1] : G_i$ has at least one left vertex, $a_{d_{i+1}}$, whose neighbour set in G_i is the entire right bipartition B_i . Similarly, in G_t the neighbour set of the right vertex $b_{k_{t-1}+1}$ is the entire left bipartition A_t . Thus, by Corollary 20:

$$\forall i \in [t] : a_{G_i}^* = \sum_{\substack{G_i \subseteq H \\ H \text{ is elementary}}} (-1)^{|E(H) \setminus E(G)|}.$$

To complete the proof, it remains to show a bijection between elementary completions of G using the permitted edges \mathcal{P}_G , and elementary completions of each of the graphs G_i .



■ **Figure 4** A sorted ordered graph G , with $\mathcal{S}_G = \{(d_1, k_1), (d_2, k_2), (d_3, k_3), (d_4, k_4)\}$. The permitted edges are covered. Orange blocks indicate the edges of G , green blocks indicate the permitted edges, and blue blocks are the induced graphs G_i .

Let $G \subseteq H \in \text{EL}_n$ such that $(E(H) \setminus E(G)) \subseteq \mathcal{P}_G$. For all $i \in [t]$, let $H_i = H[A_i \sqcup B_i]$. Since $H \supseteq G$, clearly also $\forall i \in [t] : H_i \supseteq G_i$. It remains to show that every such H_i is elementary. To this end, we use Theorem 11: let $i \in [t]$ and let $\emptyset \neq X \subsetneq A_i$. If $X \cap A_{i+1} \neq \emptyset$ then H_i has a vertex of full degree, and so $|N_{H_i}(X)| = |B_i| = |A_i| > |X|$. Otherwise, if $X \cap A_{i+1} = \emptyset$ then let $X' = X \sqcup \{a_1, \dots, a_{k_{i-1}}\}$. Observe that $N_H(X') = N_H(X) = N_{H_i}(X) \sqcup \{b_1, \dots, b_{k_{i-1}}\}$. However, H is elementary, therefore $|N_H(X')| > |X'| = |X| + k_{i-1}$. In both cases we have $|N_{H_i}(X)| > |X|$ and H_i is elementary.

Conversely, let $H_1 \supseteq G_1, \dots, H_t \supseteq G_t$ be elementary graphs. Then it suffices to show that $H \supseteq G$ whose edges are $E(H) = E(G) \cup E(H_1) \cup E(H_2) \cup \dots \cup E(H_t)$ is also elementary. Let $X \subsetneq A$, let i be the largest index such that $a_i \in X$, and let j be the index for which $k_{j-1} < i \leq k_j$. Thus:

$$N_H(X) = N_{H_j}(X \cap A_j) \sqcup \{b_1, \dots, b_{k_{i-1}}\}.$$

If $X \cap A_j = A_j$, then $N_{H_j}(X \cap A_j) = B_j$ and thus $|N_H(X)| = k_{i-1} + |B_j| = d_{j+1} > k_j \geq |X|$, and indeed H is elementary. Otherwise, since H_j is elementary and $(X \cap A_j) \subsetneq A_j$, we have $|N_{H_j}(X \cap A_j)| > |X \cap A_j|$, and therefore:

$$|N_H(X)| = |N_{H_j}(X \cap A_j)| + k_{i-1} > |X \cap A_j| + k_{i-1} \geq |X|. \quad \blacktriangleleft$$

3.4.3 The Dual Coefficients of $\langle n, d, k \rangle$ -blocks

Finally, having reduced the computation of the dual coefficient of an arbitrary ordered graph G to that of simple “blocks”, we are left with the task of directly computing the dual coefficient for any such block.

► **Lemma 25.** *Let $0 \leq d \leq n$, $0 < k < n$. Then, the coefficient of the $\langle n, d, k \rangle$ -block is:*

$$a_{\langle n, d, k \rangle}^* = \begin{cases} \binom{n-1}{k}, & d = 0 \\ -\binom{n-d-1}{k-d} \binom{k-1}{d-1}, & d > 0. \end{cases} \quad (\star)$$

Proof. The proof is by induction on n , d and k . For the base case, let G be an $\langle 2, d, 1 \rangle$ -block, where $d \in \{0, 1, 2\}$. In all three cases, only $K_{2,2} \supseteq G$ is elementary, thus by Corollary 20 they all satisfy equation (\star) , as required. Next, we use complete induction. Let G be an $\langle n, d, k \rangle$ -block, where $n > 2$, and assume equation (\star) holds for all $\langle n', d', k' \rangle$ -blocks, such that:

$$(n' < n) \vee (n' = n \wedge k' = k \wedge d' > d).$$

If $d > k$, then $\forall X \subsetneq \{a_1, \dots, a_n\} : |N(X)| > |X|$, thus by Theorem 11, G is elementary and by Lemma 18, $a_G^* = 0$. Otherwise, $d \leq k$. In this case, denote $S = \{(a_1, b_n), \dots, (a_k, b_n)\}$, and partition the set of all elementary graphs containing G into two disjoint sets,

$$\mathcal{H}_1 = \{G \subseteq H \in \text{EL}_n : E(H) \cap S \neq \emptyset\}, \text{ and } \mathcal{H}_2 = \{G \subseteq H \in \text{EL}_n : E(H) \cap S = \emptyset\},$$

and by Corollary 20, the dual coefficient of G is given by the sum over these sets:

$$a_G^* = \sum_{H \in \mathcal{H}_1} (-1)^{|E(H) \setminus E(G)|} + \sum_{H \in \mathcal{H}_2} (-1)^{|E(H) \setminus E(G)|}.$$

The contributions of \mathcal{H}_1 . To sum the contributions of all graphs in \mathcal{H}_1 , we use the inclusion-exclusion principle. First, note that BPM_n^* is invariant to permutations over each bipartition (that is, if $H \cong G$ then $a_G^* = a_H^*$). Therefore, for every subset $T \subseteq S$ of selected edges, we may, without loss of generality, “sort” the graph to obtain an isomorphic sorted ordered graph. Consequently, denote $\forall t \in [k] : G_t = G \cup \{(a_{k-t+1}, b_{d+1}), \dots, (a_k, b_{d+1})\}$. By the inclusion-exclusion principle, we have

$$\sum_{H \in \mathcal{H}_1} (-1)^{|E(H) \setminus E(G)|} = \sum_{t=1}^k (-1)^{t+1} \binom{k}{t} \cdot (-1)^t \cdot a_{G_t}^* = - \sum_{t=1}^k \binom{k}{t} \cdot a_{G_t}^*.$$

If $t = k$, then G_t is an $\langle n, d+1, k \rangle$ -block, for which the induction hypothesis holds. Otherwise, for $t \in [k-1]$, the biadjacency matrix of each graph G_t can be partitioned into blocks, as follows:

The contributions of \mathcal{H}_2 . If $k = n - 1$, then $\mathcal{H}_2 = \emptyset$, thus there are no contributions from \mathcal{H}_2 . This assertion follows since for any $H \supseteq G$ with $E(H) \cap S = \emptyset$, we have $|N(\{a_1, \dots, a_{n-1}\})| \leq n - 1 = |\{a_1, \dots, a_{n-1}\}|$. Thus, by Theorem 11, H is not elementary. Otherwise, if $k < n - 1$, we claim that:

$$\sum_{H \in \mathcal{H}_2} (-1)^{|E(H) \setminus E(G)|} = a_{\langle n-1, d, k \rangle}^*.$$

Since the induction hypothesis holds for the $\langle n - 1, d, k \rangle$ -block, proving the above identity would yield an expression for the contributions of \mathcal{H}_2 . Denote the $\langle n - 1, d, k \rangle$ -block by G' . To prove the aforementioned identity, it remains to show a bijection between elementary graphs $G' \subseteq H' \in EL_{n-1}$, and elementary graphs $G \subseteq H \in EL_n$, where $E(H) \cap S = \emptyset$. Furthermore, we must also maintain $|E(H') \setminus E(G')| = |E(H) \setminus E(G)|$, for any two graphs H' and H which are mapped to one another by the bijection. The bijection is defined as follows:

$H \mapsto H'$: Let $H \supseteq G$ be an elementary graph such that $E(H) \cap S = \emptyset$. We claim that $H' = H - a_n - b_n$ is also elementary. By Theorem 11, it suffices to show that $\forall X \subsetneq \{a_1, \dots, a_{n-1}\} : |N_{H'}(X)| > |X|$. If $X \cap \{a_{k+1}, \dots, a_{n-1}\} \neq \emptyset$, then $N_{H'}(X) = \{b_1, \dots, b_{n-1}\}$. Thus $|N_{H'}(X)| = n - 1 > |X|$. Otherwise, if $X \cap \{a_{k+1}, \dots, a_{n-1}\} = \emptyset$, then $N_{H'}(X) = N_H(X)$ and therefore: $|N_{H'}(X)| = |N_H(X)| > |X|$, as required.

$H' \mapsto H$: Let $H' \supseteq G'$ be an elementary graph. We claim that the graph $H \subseteq K_{n,n}$ where $E(H) = E(H') \sqcup \{(a_{k+1}, b_n), \dots, (a_n, b_n)\}$, is also elementary. Once again, we use Theorem 11. Let $X \subsetneq \{a_1, \dots, a_n\}$. If $X \cap \{a_{k+1}, \dots, a_n\} \neq \emptyset$, then $N_H(X) = \{b_1, \dots, b_n\}$. Thus $|N_H(X)| = n > |X|$. Otherwise, if $X \cap \{a_{k+1}, \dots, a_n\} = \emptyset$, then $N_H(X) = N_{H'}(X)$ and therefore: $|N_H(X)| = |N_{H'}(X)| > |X|$, as required.

Summing up the contributions. Finally, we have reduced the computation of the coefficient $a_{\langle n, d, k \rangle}^*$ to a sum of coefficients $a_{\langle n', d', k' \rangle}^*$ for which the induction hypothesis holds. It now remains to sum up the contributions for each possible case. If $d > 0$ and $k = n - 1$, then:

$$a_G^* = \sum_{H \in \mathcal{H}_1} (-1)^{|E(H) \setminus E(G)|} = -\binom{n-d-2}{k-d-1} \binom{k-1}{d-1} = -\binom{n-d-1}{k-d} \binom{k-1}{d-1}.$$

If $d > 0$ and $k < n - 1$, then:

$$a_G^* = \sum_{H \in \mathcal{H}_1} (-1)^{|E(H) \setminus E(G)|} + \sum_{H \in \mathcal{H}_2} (-1)^{|E(H) \setminus E(G)|} = -\binom{n-d-1}{k-d} \binom{k-1}{d-1}.$$

If $d = 0$ and $k = n - 1$, then:

$$a_G^* = \sum_{H \in \mathcal{H}_1} (-1)^{|E(H) \setminus E(G)|} = \binom{n-2}{k-1} = \binom{n-1}{k}.$$

And lastly, if $d = 0$ and $k < n - 1$, then:

$$a_G^* = \sum_{H \in \mathcal{H}_1} (-1)^{|E(H) \setminus E(G)|} + \sum_{H \in \mathcal{H}_2} (-1)^{|E(H) \setminus E(G)|} = \binom{n-2}{k-1} + \binom{n-2}{k} = \binom{n-1}{k}. \blacktriangleleft$$

3.4.4 Putting It Together

We are now ready to prove Theorem 2.

Proof. Let $G \subseteq K_{n,n}$. If G is not totally ordered, then by Lemma 17, $a_G^* = 0$. Otherwise, if G is totally ordered and there exists some $i \in [t-1]$ such that $d_{i+1} \leq k_i$, then by Lemma 23, $a_G^* = 0$, and indeed:

$$f(d_{i+1} - k_{i-1}, d_i - k_{i-1}, k_i - k_{i-1}) = \binom{d_{i+1} - k_{i-1} - 1}{k_i - k_{i-1}} = 0.$$

Finally, if G is totally ordered, and $\forall i \in [t-1] : d_{i+1} > k_i$, then let $A_i = \{a_{k_{i-1}+1}, \dots, a_{d_{i+1}}\}$, $B_i = \{b_{k_{i-1}+1}, \dots, b_{d_{i+1}}\}$, $\forall i \in [t]$, where $k_0 = 0$ and $d_{t+1} = n$. Furthermore $\forall i \in [t]$, let $G_i = G[A_i \sqcup B_i]$ be the induced graph on the vertices $A_i \sqcup B_i$. By Lemma 24, we have $a_G^* = \prod_{i=1}^t a_{G_i}^*$. Observe that $\forall i \in [t-1]$, the graph G_i is an $\langle d_{i+1} - k_{i-1}, d_i - k_{i-1}, k_i - k_{i-1} \rangle$ -block. Thus, its coefficient is given by the expression in Lemma 25. However, the last graph G_t may *not* be a “block”. In fact, there are two possible cases: either $d_t = n$, in which case G_t is a complete bipartite graph, and thus $a_{G_t}^* = 1$. Otherwise, $d_t < n$, and G_t is a biclique joining $n - k_{t-1}$ left vertices to $n - d_t$ right vertices. In this case, since a_G^* is invariant to swapping the two bipartitions, then without loss of generality we may do so, thus obtaining an isomorphic $\langle n - k_{t-1}, 0, n - d_t \rangle$ -block. Thus, we have:

$$a_{G_t}^* = \begin{cases} 1, & d_t = n \\ \binom{n - k_{t-1} - 1}{n - d_t}, & d_t < n \end{cases} = \binom{n - k_{t-1} - 1}{n - d_t}.$$

Putting it all together, we obtain:

$$\begin{aligned} a_G^* &= \prod_{i=1}^t a_{G_i}^* = \binom{n - k_{t-1} - 1}{n - d_t} \cdot \prod_{i=1}^{t-1} a_{\langle d_{i+1} - k_{i-1}, d_i - k_{i-1}, k_i - k_{i-1} \rangle} \\ &= \binom{n - k_{t-1} - 1}{n - d_t} \cdot \prod_{i=1}^{t-1} f(d_{i+1} - k_{i-1}, d_i - k_{i-1}, k_i - k_{i-1}). \quad \blacktriangleleft \end{aligned}$$

3.5 Corollaries of Theorem 2: The ℓ_1 -norms of BPM_n

Theorem 2 allows us to compute the dual coefficient of any graph $G \subseteq K_{n,n}$. It is not hard to see that for some graphs $G \subseteq K_{n,n}$, the coefficient a_G^* may be *exponential* in n . For instance, the biclique $K_{n, n/2}$ is an ordered graph whose representing sequence is $(\frac{n}{2}, n)$. Therefore its dual coefficient is $\binom{n-1}{\frac{n}{2}} \sim \frac{2^n}{\text{poly}(n)}$. We claim that the aforementioned bound is qualitatively tight. Namely, for *every* graph $G \subseteq K_{n,n}$, the coefficient a_G^* is *at most* exponential in $2n$.

► **Lemma 26.** *Let $G \subseteq K_{n,n}$. The dual coefficient of G is bounded by $|a_G^*| \leq 2^{2n}$.*

Proof. If G is not totally ordered then by Lemma 17 $a_G^* = 0$. Otherwise, let $\{(d_1, k_1), \dots, (d_t, k_t)\}$ be the *representing sequence* of G , let $k_0 = 0$, and let:

$$f(n, d, k) = \begin{cases} \binom{n-1}{k}, & d \leq 0 \\ -\binom{n-d-1}{k-d} \binom{k-1}{d-1}, & d > 0. \end{cases}$$

Observe that both in the case $d \leq 0$ and in the case $d > 0$, we have $|f(n, d, k)| \leq 2^{n-d+k}$ (by bounding every binomial coefficient). Therefore, using Theorem 2 we obtain:

$$|a_G^*| = \binom{n - k_{t-1} - 1}{n - d_t} \cdot \prod_{i=1}^{t-1} |f(d_{i+1} - k_{i-1}, d_i - k_{i-1}, k_i - k_{i-1})| \leq 2^{n+d_t} \leq 2^{2n}. \quad \blacktriangleleft$$

1:16 The Approximate Degree of Bipartite Perfect Matching

Thus, the multilinear polynomial representing BPM_n^* is “simple” in the following sense: its ℓ_1 -norm (the sum of absolute values of its coefficients) is small, over both the $\{0, 1\}$ and Fourier basis.

► **Corollary 27.** *Let $n > 2$. Then:*

$$\|\text{BPM}_n^*\|_1 = 2^{\Theta(n \log n)}, \text{ and furthermore } \hat{\|\text{BPM}_n\|_1} = \hat{\|\text{BPM}_n^*\|_1} = 2^{\Theta(n \log n)}.$$

Proof. In [3], the number of monomials in BPM_n^* was bounded by:

$$(n!)^2 \leq |\text{mon}(\text{BPM}_n^*)| \leq (n+2)^{2n+2}$$

thus, using Lemma 26, we deduce:

$$(n!)^2 \leq \|\text{BPM}_n^*\|_1 \leq (n+2)^{2n+2} \cdot 2^{2n} \Rightarrow \|\text{BPM}_n^*\|_1 = 2^{\Theta(n \log n)}.$$

As for the Fourier ℓ_1 -norm, we note that the magnitudes of the Fourier coefficients of any Boolean function and its dual are identical (see e.g., [25]), therefore $\hat{\|\text{BPM}_n\|_1} = \hat{\|\text{BPM}_n^*\|_1}$. Furthermore, recall that $\forall S \subseteq [n]$, $\hat{\|\text{AND}_S\|} = \hat{\|\Pi_{i \in S} x_i\|} = 1$. Thus, by subadditivity and homogeneity:

$$\hat{\|\text{BPM}_n\|_1} = \hat{\|\text{BPM}_n^*\|_1} \leq \sum_{G \subseteq K_{n,n}} |a_G^*| \cdot \hat{\|\text{AND}_G\|} = \|\text{BPM}_n^*\|_1 = 2^{\Theta(n \log n)}. \quad \blacktriangleleft$$

4 The Upper Bound on $\widetilde{\text{deg}}_\epsilon(\text{BPM}_n)$

In this section we obtain an upper bound on the approximate degree of the bipartite perfect matching function, which holds even for exponentially small values of ϵ .

► **Theorem 28.** *Let $2^{-n \log n} \leq \epsilon \leq \frac{1}{3}$. The ϵ -approximate degree of BPM_n is bounded by:*

$$\widetilde{\text{deg}}_\epsilon(\text{BPM}_n) = \mathcal{O}(n^{3/2} \sqrt{\log n}).$$

This bound is essentially a corollary Theorem 2, alongside two further observations. First, we show that the approximate degree of any Boolean function and its dual are identical (for all $\epsilon > 0$). We then prove that Boolean functions whose representing polynomials have small ℓ_1 -norm over the $\{0, 1\}$ basis, can be efficiently approximated by low degree polynomials. The latter approach was also employed by Sherstov in [29]. Let us remark that, to obtain the upper bound on the approximate degree of BPM_n it would have sufficed to merely show that the magnitudes of all dual coefficients are, at most, exponential in $\Theta(n \log n)$. However, we do not know of a simpler proof of this fact, other than leveraging the complete characterization of BPM_n^* given by Theorem 2.

► **Lemma 29.** *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function, and let f^* be its dual. Then:*

$$\forall 0 < \epsilon < \frac{1}{2} : \widetilde{\text{deg}}_\epsilon(f) = \widetilde{\text{deg}}_\epsilon(f^*).$$

Proof. Let $\epsilon > 0$, and let $p \in \mathbb{R}[x_1, \dots, x_n]$ be a real polynomial that ϵ -approximates f pointwise. Let $p^* \in \mathbb{R}[x_1, \dots, x_n]$ be the real polynomial defined by: $p^*(x_1, \dots, x_n) = 1 - p(1 - x_1, \dots, 1 - x_n)$ (i.e., replace each variable x_i with $(1 - x_i)$, negate all coefficients, and add 1). Observe that $\text{deg}(p^*) \leq \text{deg}(p)$, since p^* is obtained by a linear transformation on p , thus the degree cannot increase. Furthermore, $\forall x_1, \dots, x_n \in \{0, 1\}$, we have:

$$\begin{aligned} |f^*(x_1, \dots, x_n) - p^*(x_1, \dots, x_n)| &= |1 - f(1 - x_1, \dots, 1 - x_n) - (1 - p(1 - x_1, \dots, 1 - x_n))| \\ &= |f(1 - x_1, \dots, 1 - x_n) - p(1 - x_1, \dots, 1 - x_n)| \leq \epsilon. \end{aligned}$$

The converse similarly follows, since $(f^*)^* = f$. ◀

For the second lemma, we require a well known Theorem regarding the approximate degree of the AND_n function. Nisan and Szegedy [23] first showed that for the regime of $\epsilon = \Theta(1)$, we have $\widetilde{\text{deg}}_{1/3}(\text{AND}_n) = \Theta(\sqrt{n})$. Their result was extended by Buhrman, Cleve, De Wolf and Zalka [6], who determined the approximate degree of AND for any $\epsilon > 0$.

► **Theorem 30** ([6]). *Let $n \in \mathbb{N}$ and let $2^{-n} \leq \epsilon \leq \frac{1}{3}$. Then:*

$$\widetilde{\text{deg}}_\epsilon(\text{AND}_n) = \Theta\left(\sqrt{n \cdot \log(1/\epsilon)}\right).$$

Consider a Boolean function f . If the representing polynomial of f has small ℓ_1 -norm, then one may use the following straightforward approach for constructing a low-degree approximating polynomial for f : approximate (with sufficiently small ϵ) every *monomial* of the representing polynomial. Since each monomial is an AND function, we may appeal to Theorem 30 to obtain a low-degree approximation. Thus, the polynomial approximating f is given by summing the approximating polynomials for each of its monomials. This scheme is implemented in the following lemma, whose proof appears in the full version of this paper.

► **Lemma 31.** *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function and let $p \in \mathbb{R}[x_1, \dots, x_n]$ be the unique multilinear polynomial representing f . If $3 < \|p\|_1 < 2^n$, then:*

$$\forall \epsilon \in \left(\frac{1}{\|p\|_1}, \frac{1}{3}\right) : \widetilde{\text{deg}}_\epsilon(f) = \mathcal{O}\left(\sqrt{n \cdot \log \|p\|_1}\right).$$

The proof of Theorem 28 now follows.

Proof. Let $2^{-n \log n} \leq \epsilon \leq \frac{1}{3}$. Then, using Corollary 27 and Lemmas 29 and 31, we have:

$$\widetilde{\text{deg}}_\epsilon(\text{BPM}_n) = \widetilde{\text{deg}}_\epsilon(\text{BPM}_n^*) = \mathcal{O}(n^{3/2} \sqrt{\log n}). \quad \blacktriangleleft$$

5 The Lower Bound $\widetilde{\text{deg}}(\text{BPM}_n) = \Omega(n^{3/2})$

In this section we obtain a lower bound on the approximate degree of perfect matching, which matches the upper bound of Theorem 28, up to the low order term $\sqrt{\log n}$.

► **Theorem 32.** *The approximate degree of BPM_n is bounded by $\widetilde{\text{deg}}(\text{BPM}_n) = \Omega(n^{3/2})$.*

Aaronson, Ben-David, Kothari, Rao and Tal [1] recently proved that for any *total* Boolean function f , $\text{deg}(f) = \mathcal{O}\left(\widetilde{\text{deg}}(f)^2\right)$ (which is optimal, as exemplified by the OR_n function). Their proof is composed of two primary steps. First, they make the key observation that, at the heart of Huang's proof for the sensitivity conjecture [15], there (implicitly) lies a new complexity measure: **Spectral Sensitivity**. Their main technical Theorem is to then show that this aforementioned quantity lower-bounds approximate degree. It is this relation that we wish to leverage. ⁴

⁴ From the quadratic relation between degree and approximate degree [1] and using the fact that BPM_n has full degree [3], the *weaker* lower bound of $\widetilde{\text{deg}}(\text{BPM}_n) = \Omega(n)$ also immediately follows.

5.1 Spectral Sensitivity and the Sensitivity Graph

► **Definition 33** (Sensitivity Graph [1]). *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. The **Sensitivity Graph** of f is the graph G_f over the vertices $\{0, 1\}^n$ whose edges are:*

$$\forall x, y \in \{0, 1\}^n : \{x, y\} \in E(G_f) \iff |x \oplus y| = 1 \wedge f(x) \neq f(y).$$

Thus, G_f is the subgraph containing all the bi-chromatic edges of the n -dimensional Hypercube whose vertices are labeled by f (the “ f -cut” of the Hypercube).

► **Definition 34** (Spectral Sensitivity [1]). *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function and let G_f be its sensitivity graph. The **Spectral Sensitivity** of f is defined by $\lambda(f) \stackrel{\text{def}}{=} \rho(G_f)$.*

Observe that the sensitivity graph of *any* Boolean function f is a bipartite graph whose bipartitions are given by $f^{-1}(0)$ (hereafter, the “left” vertices) and $f^{-1}(1)$ (the “right” vertices). Clearly as all the edges of the sensitivity graph are bi-chromatic, these two sets form a valid bipartition. In the case of BPM_n , we note that (perhaps rather confusingly) the sensitivity graph is a bipartite graph in which each vertex $x \in \{0, 1\}^{n^2}$ is, itself, associated with a bipartite graph (corresponding to the input x).

Under this notation, the main Theorem of [1] states the following.

► **Theorem 35** ([1]). *For any total Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, we have:*

$$\lambda(f) = \Theta(\widetilde{\deg}(f)).$$

5.2 A Tight Bound on the Spectral Sensitivity of BPM_n

In what follows, we obtain tight bounds on the Spectral Sensitivity of BPM_n .

► **Theorem 36.** *The spectral sensitivity of matching is bounded by $\lambda(\text{BPM}_n) = \Theta(n^{3/2})$.*

This tight bound on $\lambda(\text{BPM}_n)$ yields our approximate degree lower bound, and also shows that this is the *best bound attainable* by the method of Spectral Sensitivity for the perfect matching function.

► **Corollary 37.** *The approximate degree of matching is bounded by $\widetilde{\deg}(\text{BPM}_n) = \Omega(n^{3/2})$.*

Proof. Follows from Theorem 36 and Theorem 35. ◀

5.2.1 The Upper Bound $\lambda(\text{BPM}_n) = \Theta(n^{3/2})$

The spectrum of bipartite graphs has several nice properties. Their eigenfunctions come in pairs with negated eigenvalues (thus their spectrum is symmetric). Another well-known result regarding the spectrum of bipartite graphs is Hölder’s inequality for matrix norms:

► **Proposition 38.** *Let G be a bipartite graph and let Δ_L and Δ_R be the maximal left and right degrees, correspondingly. Then, $\rho(G) \leq \sqrt{\Delta_L \Delta_R}$.*

Recall that the degree of any vertex in the sensitivity graph is equal, by definition, to the number of bi-chromatic edges incident to it – which is its sensitivity. Thus, by Proposition 38, for any Boolean function f we have $\lambda(f) \leq \sqrt{s_0(f) \cdot s_1(f)}$, where $s_b(f) \stackrel{\text{def}}{=} \max_{x \in f^{-1}(b)} \text{sens}_f(x)$, $\forall b \in \{0, 1\}$. This simple observation suffices to obtain the upper bound:

► **Proposition 39.** *For any $n \geq 1$, we have $\lambda(\text{BPM}_n) \leq n^{3/2}$.*

Proof. Recall that $\lambda(\text{BPM}_n) \leq \sqrt{s_0(\text{BPM}_n) \cdot s_1(\text{BPM}_n)}$. Since the sensitivity of *any* input is at most n^2 (the number of input bits), we immediately have $s_0(\text{BPM}_n) \leq n^2$ (and in fact, $s_0(\text{BPM}_n) = \Theta(n^2)$). As for the 1-sensitivity, clearly for every $G \in \text{BPM}_n^{-1}(1)$, the only sensitive edges are those present in some matching. The union of all matchings is matching-covered, and every edge in an elementary component is sensitive if and only if the component is K_2 (see Theorem 11), thus $s_1(\text{BPM}_n) \leq n$. ◀

5.2.2 The Lower Bound $\lambda(\text{BPM}_n) = \Omega(n^{3/2})$

Let us now consider the lower bound. By Cauchy's Interlace Theorem (and using the fact that for bipartite graphs, $\rho(G) = \lambda_1$), it holds that for any *bipartite* graph G , the spectral radius of G is no smaller than that of any *induced subgraph* of G . Thus, it suffices to exhibit an induced subgraph of the sensitivity graph of BPM_n , whose spectral radius is large. In the following Theorem, we construct such a connected bi-regular induced subgraph, and bound its spectral radius.

► **Theorem 40.** *For any $n > 2$ we have $\lambda(\text{BPM}_n) \geq \frac{n^{3/2}}{3\sqrt{3}} - \mathcal{O}(n) = \Omega(n^{3/2})$.*

Proof. Let $n > 2$ and let $\frac{n+1}{3} < k < n$ be a natural number. Let $A = A_1 \sqcup A_2$ and $B = B_1 \sqcup B_2$ be disjoint sets such that $|A_1| = |B_1| = k$ and $|A_2| = |B_2| = n - k$. For every $t \in \mathbb{N}^+$, denote the set of all matchings joining t vertices of A_2 with t vertices of B_2 , by $M_t(A_2, B_2)$. Consider the following two sets of graphs:

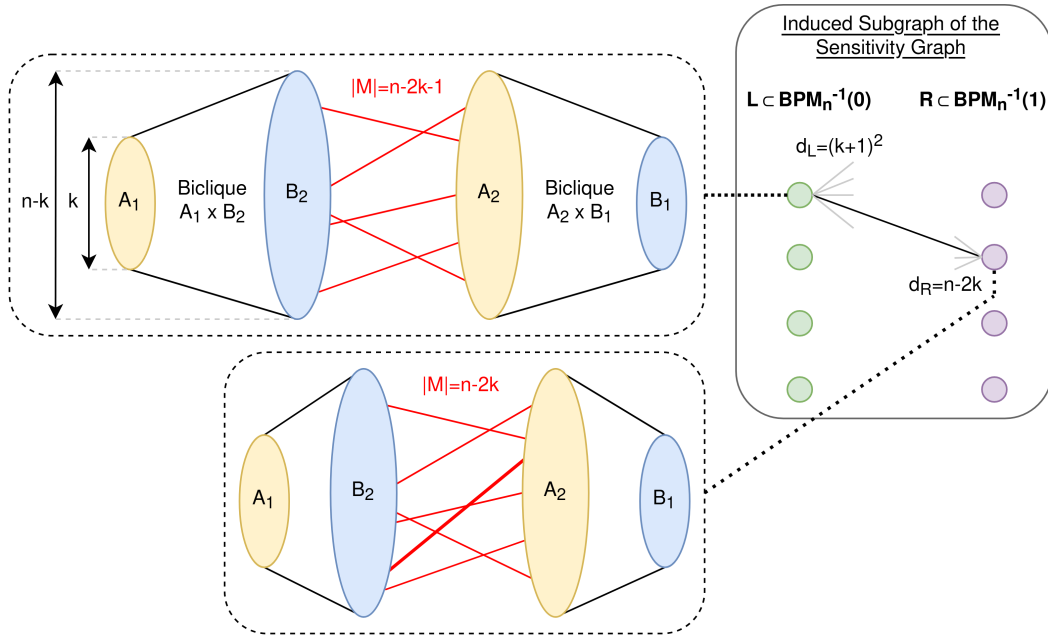
$$\begin{aligned} \mathcal{R} &= \{G = (A \sqcup B, (A_1 \times B_2) \sqcup (A_2 \times B_1) \sqcup E(M)) : M \in M_{n-2k}(A_2, B_2)\} \\ \mathcal{L} &= \{G = (A \sqcup B, (A_1 \times B_2) \sqcup (A_2 \times B_1) \sqcup E(M)) : M \in M_{n-2k-1}(A_2, B_2)\}. \end{aligned}$$

Let G_{BPM_n} be the sensitivity graph of BPM_n , and let $H = G_{\text{BPM}_n}[\mathcal{L} \sqcup \mathcal{R}]$ be its induced subgraph over the aforementioned set of graphs (vertices). By Cauchy's Interlace Theorem the spectral radius of H is at most that of G , therefore $\lambda(\text{BPM}_n) = \rho(G_{\text{BPM}_n}) \geq \rho(H)$.

Observe that every graph $G \in \mathcal{R}$ has a perfect matching, which can be constructed by taking the $(n - 2k)$ -size matching between A_2 and B_2 and matching the remaining k vertices of A_2 with B_1 , and similarly the remaining k vertices of B_2 with A_1 (this can always be done, since the bicliques K_{A_2, B_1} , K_{A_1, B_2} are subgraphs of G). Conversely, every graph $G \in \mathcal{L}$ does not have a perfect matching. For example, the set A_2 violates Hall's condition, since: $|N(A_2)| = n - 2k - 1 + k = n - k - 1 < n - k = |A_2|$. Thus, \mathcal{R} is the right bipartition of H , and \mathcal{L} is its left bipartition.

Let us characterize the edges of H . Let $G \in \mathcal{R}$ and let M be its corresponding $(n - 2k)$ -size matching between A_2 and B_2 . For every edge $e \in M$, we have by construction $(G \setminus \{e\}) \in \mathcal{L}$. Furthermore, for any edge $e \in (E(G) \setminus M)$, the graph $(G \setminus \{e\})$ does not contain one of the bicliques K_{A_2, B_1} , K_{A_1, B_2} , and is therefore not in \mathcal{R} . Consequently the degree of each right vertex of H is $d_R = \deg_H(G) = |M| = n - 2k$.

Similarly, let $G \in \mathcal{L}$ and let M be its $(n - 2k - 1)$ -size matching between A_2 and B_2 . Denote by S, T the left and right vertices of M , correspondingly. Then, for any $u \in (A_2 \setminus S)$, $v \in (B_2 \setminus T)$, the graph $G \sqcup \{(u, v)\}$ has a $(n - 2k)$ -size matching, and is thus in \mathcal{R} . Adding any other edge e to G would either join a vertex from A_1 to a vertex from B_1 , or e would be incident to a vertex in M . In both cases, $G \sqcup \{e\}$ is not in \mathcal{L} . Thus the degree of each left vertex of H is $d_L = \deg_H(G) = (|A_2| - |S|) \cdot (|B_2| - |T|) = (k + 1)^2$.



■ **Figure 6** The induced subgraph $H = G_{\text{BPM}_n}[\mathcal{L} \sqcup \mathcal{R}]$ of the sensitivity graph for BPM_n .

Finally, observe that any bi-regular bipartite graph, and in particular H , satisfies $\rho(H) \geq \sqrt{d_L \cdot d_R}$ (this follows, for example, by considering the eigenfunction which places weight $\sqrt{d_L}$ on each left vertex, and $\sqrt{d_R}$ on each right vertex)⁵. To conclude the proof, fix $k = \lfloor \frac{n}{3} \rfloor - 1$. Thus:

$$\lambda(\text{BPM}_n) = \rho(G) \geq \rho(H) \geq \sqrt{\left(\left\lfloor \frac{n}{3} \right\rfloor\right)^2 \cdot \left(n - 2\left(\left\lfloor \frac{n}{3} \right\rfloor - 1\right)\right)} = \frac{n^{3/2}}{3\sqrt{3}} - \mathcal{O}(n). \quad \blacktriangleleft$$

References

- 1 Scott Aaronson, Shalev Ben-David, Robin Kothari, Shramas Rao, and Avishay Tal. Degree vs. approximate degree and quantum implications of Huang’s sensitivity theorem. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, 2021.
- 2 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald De Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001.
- 3 Gal Beniamini and Noam Nisan. Bipartite perfect matching as a real polynomial. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, 2021.
- 4 Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.
- 5 Louis J Billera and Aravamuthan Sarangarajan. The combinatorics of permutation polytopes. In *Formal power series and algebraic combinatorics*, volume 24, pages 1–23, 1994.
- 6 Harry Buhrman, Richard Cleve, Ronald De Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. In *40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)*, pages 358–368. IEEE, 1999.
- 7 Harry Buhrman and Ronald De Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002.

⁵ We remark that it is not hard to see that H is connected for any $n > 2$. Thus the top eigenvalue of H is *simple*, and consequently our bound does not freely extend, by interlacing, to eigenvalues other than the spectral radius of G_{BPM_n} .

- 8 Mark Bun, Robin Kothari, and Justin 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.
- 9 Mark Bun and Justin Thaler. A nearly optimal lower bound on the approximate degree of AC^0 . *SIAM Journal on Computing*, 49(4):FOCS17–59, 2019.
- 10 Mark Bun and Justin Thaler. Guest column: Approximate degree in classical and quantum computing. *ACM SIGACT News*, 51(4):48–72, 2021.
- 11 Karthekeyan Chandrasekaran, Justin Thaler, Jonathan Ullman, and Andrew Wan. Faster private release of marginals on small databases. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 387–402, 2014.
- 12 Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
- 13 Gábor Hetyei. Rectangular configurations which can be covered by 2×1 rectangles. *Pécsi Tan. Foisk. Közl.*, 8:351–367, 1964.
- 14 John E Hopcroft and Richard M Karp. An $n^{5/2}$ algorithm for maximum matchings in bipartite graphs. *SIAM Journal on computing*, 2(4):225–231, 1973.
- 15 Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019.
- 16 Adam Tauman Kalai, Adam R Klivans, Yishay Mansour, and Rocco A Servedio. Agnostically learning halfspaces. *SIAM Journal on Computing*, 37(6):1777–1805, 2008.
- 17 Adam R Klivans and Rocco A Servedio. Learning DNF in time $2^{\delta(n^{1/3})}$. *Journal of Computer and System Sciences*, 68(2):303–318, 2004.
- 18 Cedric Yen-Yu Lin and Han-Hsuan Lin. Upper bounds on quantum query complexity inspired by the Elitzur-Vaidman bomb tester. In *Proceedings of the 30th Conference on Computational Complexity, CCC '15*, 2015.
- 19 Kurt Mehlhorn and Erik M Schmidt. Las vegas is better than determinism in VLSI and distributed computing. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 330–337, 1982.
- 20 Marvin L Minsky and Seymour A Papert. *Perceptrons: expanded edition*, 1988.
- 21 Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*, 2002.
- 22 Noam Nisan. The demand query model for bipartite matching. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 592–599. SIAM, 2021.
- 23 Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational complexity*, 4(4):301–313, 1994.
- 24 Noam Nisan and Avi Wigderson. On rank vs. communication complexity. *Combinatorica*, 15(4):557–565, 1995.
- 25 Ryan O’Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.
- 26 M.D. Plummer and L. Lovász. *Matching Theory*. North-Holland Mathematics Studies. Elsevier Science, 1986.
- 27 Alexander A Sherstov. Separating AC^0 from depth-2 majority circuits. *SIAM Journal on Computing*, 38(6):2113–2129, 2009.
- 28 Alexander A Sherstov. The pattern matrix method. *SIAM Journal on Computing*, 40(6):1969–2000, 2011.
- 29 Alexander A Sherstov. Algorithmic polynomials. *SIAM Journal on Computing*, 49(6):1173–1231, 2020.
- 30 Yaoyun Shi and Yufan Zhu. Quantum communication complexity of block-composed functions. *arXiv preprint*, 2007. [arXiv:0710.0095](https://arxiv.org/abs/0710.0095).
- 31 Justin Thaler, Jonathan Ullman, and Salil Vadhan. Faster algorithms for privately releasing marginals. In *International Colloquium on Automata, Languages, and Programming*, pages 810–821. Springer, 2012.
- 32 Shengyu Zhang. On the power of Ambainis’s lower bounds. In *International Colloquium on Automata, Languages, and Programming*, pages 1238–1250. Springer, 2004.

A Towards Fine Grained Bounds for Bipartite Perfect Matching

The main thrust of this section, and indeed one of the motivating factors for the work in this paper, revolves around the following longstanding open question:

► **Open Problem 41** (The $n^{5/2}$ -Barrier for Bipartite Matching⁶). *Is there a **deterministic** algorithm for bipartite perfect matching running in time $o(n^{5/2})$?*

Hopcroft and Karp’s [14] algorithm, designed half a century ago, attains a runtime of $\mathcal{O}(n^{5/2})$ when applied to *dense* graphs (i.e., when the number of edges is $\Theta(n^2)$). Since then, no known deterministic algorithm has been able to break this barrier, in the dense regime. To make matters concrete, in what follows let us consider the *decision variant* of the problem, as represented by BPM_n ; we are given a balanced bipartite graph with n vertices in each bipartition, and wish to determine whether a perfect matching exists. Secondly, let us fix the following computational model.

The Demand Query Model

In recent work, Nisan [22] introduced a new *concrete complexity model* for bipartite matching, known as the “Demand Query Model”. This model appears to be particularly well-suited for the matching problem, for two primary reasons. Firstly, Nisan showed that *combinatorial* matching algorithms can be efficiently simulated within the model (in fact, this holds even for parallel, online, approximate and other classes of algorithms, see [22]). For instance, Hopcroft and Karp’s algorithm, whose running time is $\mathcal{O}(n^{5/2})$, can be “translated” into demand query algorithm making $\mathcal{O}(n^{3/2})$ queries. Since each query can be trivially simulated in $\mathcal{O}(n)$ time, this appears to capture the complexity of the aforementioned algorithm in a fine-grained manner. Secondly, the queries in this model are *simple enough* that *we could hope to prove lower bounds against them*.

In this framework, algorithms are modeled by decision trees. Each internal node corresponds to a demand query, and each leaf is labeled by an output, either 0 or 1. A demand query consists of a left vertex u and an ordering $\pi \in S_n$, induced on the right vertices. The result of such a query is the first right vertex v , according to the ordering π , for which the edge (u, v) exists in the graph (or \perp if no such edge exists). A root-to-leaf path in the tree corresponds to a particular set of answers to the queries made along the path. Thus, the set of all such paths partitions the set of all graphs $G \subseteq K_{n,n}$, whereby each graph G is associated with a single leaf. Any graph $G \subseteq K_{n,n}$ which is “consistent” with the answers made along a root-to-leaf path, must also be consistent with the labeling of that leaf. The “cost” of an algorithm in this model is measured by the depth of the tree (i.e., the worst-case amount of queries made on any particular input). As this is an information-theoretic model, we disregard the amount of computation necessary to construct (or deduce the existence of) a perfect matching, and instead only measure the minimal amount of *information* required to do so.

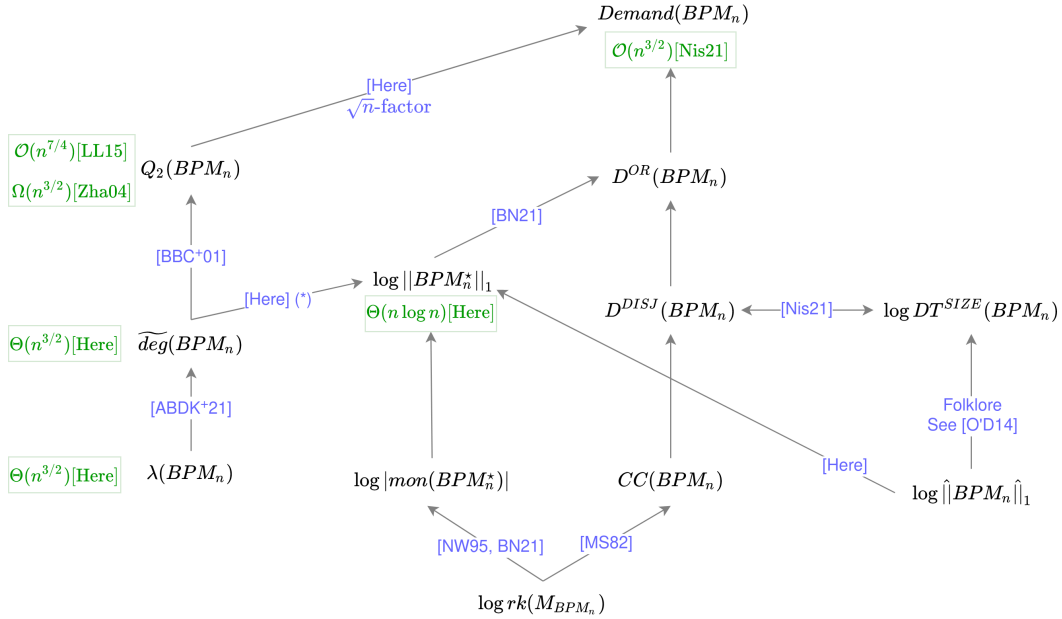
A.1 The Demand Query Complexity of Matching

Open Problem 41 remains as of yet unsettled. In light of the efficient simulation of combinatorial algorithms by the demand model, one could formulate the following closely related question: “can one construct quasi-linear demand-query algorithms for matching?”, or in the contrapositive:

⁶ In fact we are only interested in *polynomial* improvements to this running time, i.e., bounds of the form $n^{5/2-\varepsilon}$ for some constant $\varepsilon > 0$.

► **Open Problem 42** (The Demand Query Complexity of Matching). *Is there some constant $\varepsilon > 0$ such that $\text{Demand}(\text{BPM}_n) = \Omega(n^{1+\varepsilon})$?*

To better understand $\text{Demand}(\text{BPM}_n)$, we have drawn connections between the demand query complexity of BPM_n and other, mostly algebraic, complexity measures relating to BPM_n and its dual – a representative collection of which are detailed in Figure 7.



■ **Figure 7** Relations between complexity measures of BPM_n . An arrow $f(n) \rightarrow g(n)$ indicates that $f = \tilde{O}(g)$ (excluding logs) – with two exceptions. The arrow $Q_2(\text{BPM}_n) \rightarrow \text{Demand}(\text{BPM}_n)$ incurs a \sqrt{n} -factor loss, see Subsection A.3, and the arrow $\widetilde{\text{deg}}(\text{BPM}_n) \rightarrow \log \|\text{BPM}_n^*\|_1$ represents the bound provided by Lemma 31. Green blocks correspond to bounds on their adjacent quantity. Every arrow $f \rightarrow g$ is accompanied by the corresponding citation in blue, apart from trivial relations wherein they are omitted. Bounds and relations marked [Here] denote results shown in this paper.

The following table details the complexity measures appearing in Figure 7.

Query Complexity Measures	
Measure	Definition
$\text{Demand}(\text{BPM}_n)$	The least depth of a decision tree computing BPM_n , whose internal nodes are labeled by demand queries.
$D^{\text{OR}}(\text{BPM}_n)$	The least depth of a decision tree computing BPM_n , whose internal nodes are labeled by ORs over arbitrary subsets of the input bits.
$D^{\text{DISJ}}(\text{BPM}_n)$	The least depth of a decision tree computing BPM_n , whose internal nodes are labeled by <i>disjunctions</i> over <i>literals</i> , e.g. $(x_1 \vee \bar{x}_3 \vee x_7)$.
$\text{DT}^{\text{SIZE}}(\text{BPM}_n)$	The least amount of leaves in a <i>classical</i> decision tree computing BPM_n .
$Q_2(\text{BPM}_n)$	The bounded-error quantum query complexity of BPM_n .

Communication Complexity Measures	
Measure	Definition
$CC(\text{BPM}_n)$	The two-party deterministic communication complexity of BPM_n , where we fix an <i>arbitrary</i> partition over the input bits.
$rk(M_{\text{BPM}_n})$	The real rank of the communication matrix corresponding to the above communication problem.

Algebraic Complexity Measures	
Measure	Definition
$ mon(\text{BPM}_n^*) $	Number of non-zero coefficients in the unique representing polynomial.
$\ \text{BPM}_n^*\ _1$	Sum of magnitudes of coefficients in the unique representing polynomial.
$\lambda(\text{BPM}_n)$	The spectral sensitivity of BPM_n (see Definition 34).
$\widetilde{\deg}(\text{BPM}_n)$	The approximate degree of BPM_n .

A.2 Drawing the Connections

Decision Tree Measures

It is not hard to see that every demand query can be simulated by at most logarithmically many OR-queries, by performing binary search on the right vertices. Similarly trivially, every OR query can be seen as a disjunction wherein no literal is negated, thus we also have $D^{\text{DISJ}}(\text{BPM}_n) \leq D^{\text{OR}}(\text{BPM}_n)$. The latter quantity, $D^{\text{DISJ}}(\text{BPM}_n)$, is of particular interest – Nisan observed [22] that for any Boolean function the least *depth* of a *disjunction decision tree* computing the function is equivalent, up to a $\log n$ -factor, to the minimum *size* (i.e., number of leaves) of a *classical decision tree* computing it. The minimum decision tree size computing a Boolean function is known to be related to Fourier-analytic properties of the function. For example, a folklore result states that it is lower bounded by the Fourier ℓ_1 -norm of the function (see e.g. [25]).

Communication Complexity Measures

Given a disjunction decision tree computing a Boolean function, one naturally obtains a corresponding 2-party deterministic communication protocol. The protocol simply simulates the tree by “solving”, at every step, the current disjunction. This simulation can be done efficiently, since any disjunction requires only 2-bits of communication (Alice and Bob compute their parts of the disjunction separately, and communicate the answer bits to one another). In the argument above, the actual partition determining Alice and Bob’s shares of the input bits is inconsequential. For any such fixed partition, one can consider the *communication matrix*, which is the Boolean matrix whose rows are indexed by Alice’s inputs, and columns by Bob’s inputs. It is well known (by a result of [19]), that the log of the real rank of this matrix yields a lower bound on the deterministic communication complexity of its corresponding problem.

The ℓ_1 -norm of BPM_n^*

A surprisingly pivotal complexity measure arising in Figure 7 is the ℓ_1 -norm of the dual function of matching. Firstly, this measure trivially bounds the number of *monomials* appearing in its representing polynomial (since all coefficients are integers), which in turn

bounds the rank of the communication matrix, by a classical result of [24] (every monomial corresponds to a rank-1 matrix). The same quantity, $\|\text{BPM}_n^*\|_1$, also bounds the Fourier ℓ_1 -norm of BPM_n (equivalently BPM_n^*), as we observe in Corollary 27, as well as yielding bounds on the approximate degree, via the scheme detailed in Lemma 31. With regards to lower bounds, in [3] it was shown that for any Boolean function f it holds that $\log \|f^*\|_1$ lower bounds the least depth of an *OR* decision tree computing f .

Through our complete characterization of the dual polynomial given in Theorem 2, we were able to deduce the tight bound $\log \|\text{BPM}_n^*\|_1 = \Theta(n \log n)$ (see Corollary 27), thereby implying all of the aforementioned bounds. We conjecture that this low-norm representation of BPM_n^* has more far-reaching consequences – in particular, that it can be used to construct a quasi-linear deterministic communication protocol for the bipartite matching problem.⁷

Approximate Degree and Quantum Query Complexity

The “polynomial method” in quantum computation [2] states that the acceptance probability of any d query quantum algorithm can be written as a degree $2d$ polynomial. Thus, the approximate degree of any Boolean function serves as a lower bound on its Quantum query complexity. In this paper we have obtained tight upper and lower bounds on this quantity, showing that $\widetilde{\text{deg}}(\text{BPM}_n) = \widetilde{\Theta}(n^{3/2})$. To complete the connections specified in Figure 7, it remains to relate the quantum query complexity to our main object of study; $\text{Demand}(\text{BPM}_n)$.

A.3 Quantum Bounds Imply Combinatorial Bounds

In this section, we make one final simple observation regarding the demand query model: *demand query algorithms can be efficiently simulated by quantum queries*. Recall that every demand query can be simulated by logarithmically many *OR*-queries, each over at most n bits (corresponding to the right vertices). In his seminal paper, Grover [12] showed that the OR_n function can be computed, to constant error, using $\mathcal{O}(\sqrt{n})$ quantum queries (which is tight, see [4]). Thus, replacing each demand query by the majority over several invocations of Grover’s algorithm, and using Chernoff’s bound to suitably reduce the error, we obtain:⁸

► **Proposition 43.** *If there exists a demand query algorithm for BPM_n making at most d queries, then:*

$$Q_2(\text{BPM}_n) = \mathcal{O}(\sqrt{n} \cdot d \cdot \text{polylog}(d)).$$

Consequently, any lower bound of the form $Q_2(\text{BPM}_n) = \Omega(n^{3/2+\varepsilon})$, for some constant $\varepsilon > 0$, would imply a (polynomially) super-linear lower bound on the demand query complexity of BPM_n , thereby resolving Open Question 42. Such a result might suggest that quasi-linear *combinatorial algorithms* for bipartite perfect matching are improbable, which we consider a very interesting prospect. Nevertheless, at present the quantum query complexity of BPM_n remains undetermined. Lin and Lin [18] constructed an efficient quantum algorithm, yielding

⁷ Indeed, it is not hard to show that for any *monotone* Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and any partition over its inputs, we have $CC(f) \leq \min \{|\text{mon}(f)|, |\text{mon}(f^*)|\}^2$, which can be seen as a single step towards this direction.

⁸ In fact, by a similar approach we can also show that for any Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, the quantum query complexity is bounded by $Q_2(f) = \mathcal{O}(\sqrt{n} \cdot \log \text{DT}^{\text{SIZE}}(f) \cdot \log \log \text{DT}^{\text{SIZE}}(f))$, where $\text{DT}^{\text{SIZE}}(f)$ is the minimal *size* of a classical decision tree computing f . This observation might be useful in cases where there exist relatively “unbalanced” decision trees computing f .

1:26 The Approximate Degree of Bipartite Perfect Matching

an upper bound of $\mathcal{O}(n^{7/4})$. Conversely, through Ambainis' adversary technique, Zhang [32] has obtained an upper bound of $\Omega(n^{3/2})$. Our main theorem (Theorem 1) implies that this lower bound *cannot be (polynomially) strengthened by the "Polynomial Method"*. In fact, neither can Ambainis' adversary bounds be used to this end, since it is known (see e.g. [32]) that the best bound attainable by this method cannot exceed $\sqrt{C_0(f)C_1(f)}$. Closing this gap is left as an open problem.

► **Open Problem 44** (Quantum Query Complexity of Matching). *Close the gap on $Q_2(\text{BPM}_n)$.*