JOHNSON SCHEMES AND CERTAIN MATRICES WITH INTEGRAL EIGENVALUES

AMANDA BURCROFF

The University of Michigan

Wednesday 6th September, 2017

Abstract. We are interested in the spectrum of matrices in the adjacency algebra of the Johnson scheme. In particular, we ask under what circumstances all eigenvalues are integral. Putting the question in a more general context, we introduce coherent configurations and metric schemes. An examination of the adjacency algebra will reveal that for commutative coherent configurations, including metric schemes, its elements are simultaneously diagonalizable. We construct the eigenspaces and the basis of minimal idempotents of the Johnson adjacency algebra. One tool for calculating the dimension of each eigenspace is a full-rank property of certain inclusion matrices (Gottlieb 1966); we prove a lattice-theoretic generalization of this result. We compute the eigenvalues of all matrices in this algebra, and provide several sufficient conditions of the integrality of the spectra.

1. Introduction 2
2. Preliminaries 3
   2.1. Linear algebra: Commuting normal matrices 3
   2.2. Theory of finite-dimensional algebras 5
   2.3. Relations and graphs 8
3. Configurations 10
   3.1. Coherent configurations 10
   3.2. The adjacency algebra 13
   3.3. Commutative coherent configurations 14
4. Association Schemes 16
   4.1. Association schemes and their adjacency algebras 16
   4.2. Metric schemes 17
   4.3. Hamming schemes 19
   4.4. Johnson schemes 19
5. Full-Rank Inclusion Matrices 20
   5.1. Gottlieb's theorem 20
   5.2. Lattices 21
   5.3. A property of modular complemented lattices 23
   5.4. Inclusion matrices of full rank 24
6. Common Eigenbasis Construction for the Johnson Adjacency Algebra 25
   6.1. Matrices in the Johnson adjacency algebra 25
   6.2. Construction of eigenspaces via a subset-weight system 26
7. Eigenvalues of Matrices in the Johnson Adjacency Algebra 28
   7.1. Computing eigenvalues 28
   7.2. Eigenvalues and Eberlein polynomials 30
   7.3. Conditions for the integrality of eigenvalues 31
Acknowledgments 32
References 32

Written for the 2017 University of Chicago REU under the direction of Prof. László Babai

1. Introduction

This investigation began with a recent question of Gábor Tusnády to László Babai. Tusnády, working in information theory, asked why the eigenvalues of the $\binom{n}{k} \times \binom{n}{k}$ matrix

$$M = (m_{AB}) = \left(\binom{|A \cap B|}{r} \right) \tag{1}$$

where A, B range over all k-subsets of a fixed n-set and r is an arbitrary nonnegative integer, always appeared to be integral. Babai suggested generalizing the question to matrices of the form $M = (m_{AB}) = (f(|A \cap B|))$ for a general function $f : \mathbb{Z}_{\geq 0} \to \mathbb{R}$. These matrices are precisely the matrices in the *adjacency algebra* of the *Johnson scheme* $\mathfrak{J}(n, k)$ (see Sec. 4.4).

The main spectral result of this paper is the following (see Cor. 7.5).

Theorem 1.1. *Let M be an $\binom{n}{k} \times \binom{n}{k}$ matrix in the adjacency algebra of the Johnson scheme $\mathfrak{J}(n, k)$; that is, a matrix of the form*

$$M = (m_{AB}) = (f(|A \cap B|)) \tag{2}$$

where A, B range over all k-subsets of a fixed n-set. The eigenvalues of M are given by $\lambda_0, \cdots, \lambda_k$, where

$$\lambda_t = \sum_{\ell=0}^{k} f(\ell) \sum_{m=0}^{t} (-1)^{t-m} \binom{k-m}{\ell-m} \binom{n-k+m-t}{k-\ell+m-t} \binom{t}{m}. \tag{3}$$

The eigenspace corresponding to the eigenvalue λ_t is independent of f and has dimension $\binom{n}{t} - \binom{n}{t-1}$.

In particular, if f is integer-valued, as in Tusnády's case, then the matrix will have an integral spectrum.

Remark 1.2. It is possible that not all λ_i above are distinct, in which case the statement of Theorem 1.1 is imprecise. For the precise statement and proof, see Cor. 7.5.

The main structural result is the description of the basis of symmetric orthogonal idempotents of the adjacency algebra of the Johnson scheme (see Cor. 7.3)

Outline of the paper. We begin with some preliminaries concerning linear algebra, finite-dimensional algebras, graphs, and digraphs (directed graphs) (Sec. 2). Central to our study is a review of the structure of *-*closed* matrix algebras (semisimplicity and direct decomposition to simple algebras) (Sec. 2.2.2). In particular, a *-closed commutative matrix algebra over $\mathbb{C}$ has a common orthonormal eigenbasis. While this fact follows from the general theory, we give a self-contained proof (based on the standard facts of linear algebra) (Thm. 2.13). We also give the real version (Thm. 2.14) where the matrices in the commutative algebra are assumed to be symmetric (and therefore their eigenvalues are real). This latter result will be the foundation of our subsequent study of the structure of the adjacency algebras of association schemes.

To put our combinatorial problem in a more general context, we provide an overview of *coherent configurations*, a class of highly regular combinatorial objects, following

Babai [2] (Sec. 3). Coherent configurations arose in a variety of contexts, including the theory of permutation groups (Schur [21] 1933, Higman [17] 1970), statistics (*association schemes* 1950s, see below), algorithms ([24] and [2]), and recently in the complexity of matrix multiplication [10]. We explore an algebraic structure associated with coherent configurations, known as the adjacency algebra (Sec. 3.2). In particular, we observe that the adjacency algebra of any coherent configuration is *-closed and therefore semisimple (Prop. 3.20 and Cor. 3.21). Restricting the adjacency algebra to *commutative coherent configurations* (Sec. 3.3) results in a commutative algebra, implying that the adjacency algebra over $\mathbb{C}$ has a common orthonormal eigenbasis (Cor. 3.26). We then further restrict to *classical association schemes*. For these structures, the adjacency algebra consists of symmetric matrices and therefore has a common orthonormal eigenbasis over the reals by Thm. 2.14 mentioned above. Association schemes originally arose in statistical design theory (Sec. 4). Much of our exploration draws on the work of Delsarte and Levenshtein [12] and Brouwer's exposition [9]. We then further restrict to *metric schemes*, which arise from the distance metric of *distance-regular graphs*. We give a self-contained proof of the central structure theorem (Thm. 4.14) that the adjacency algebra of a metric scheme has a unique basis of symmetric orthogonal idempotents.

Johnson schemes, generated by the distance-regular *Johnson graphs*, are a class of metric schemes arising in a variety of contexts, including combinatorics, information theory [18], and recently computational complexity theory [19]. They also play a key role in the study of the Graph Isomorphism problem [2]. In Sec. 6 and Sec. 7, we apply the general theory to the Johnson graphs. We carry out the construction of the eigenspaces for the Johnson graphs following the construction of the same eigenspaces for the *Kneser graphs* in [18] (Sec. 6). The construction requires finding the dimension of the eigenspaces, which is in turn based on a theorem of Gottlieb concerning full-rank *inclusion matrices* (Sec. 5). We include a proof of a lattice-theoretic generalization of Gottlieb's theorem found by my advisor's former student Barry Guiduli (Thm. 5.25). The main results concerning the spectrum and structure of the Johnson adjacency algebra are located in Sec. 7. These results follow quickly from the general theory of abstract algebras of association schemes; however, our exposition provides self-contained elementary proofs.

2. Preliminaries

This section consists of elementary background material so that the main results of this paper will be accessible to readers with a basic background in linear algebra. We will comment on more advanced topics without providing background, but these remarks are not fundamental to the main results.

2.1. **Linear algebra: Commuting normal matrices**

We begin by introducing symmetric and normal linear transformations. We then prove a sufficient condition for a set of linear transformations to be simultaneously diagonalizable. The space W below will always be either a finite-dimensional real euclidean space or a finite-dimensional complex Hermitian inner product space. $M_{m,n}(\mathbb{F})$ denotes the space of $m \times n$ matrices over the field $\mathbb{F}$. We write $M_n(\mathbb{F}) = M_{n,n}(\mathbb{F})$ for the algebra of $n \times n$ matrices over $\mathbb{F}$.

Definition 2.1. A linear transformation $\Phi : W \to W$ on a finite-dimensional real euclidean space W is said to be *symmetric* if

$$(\forall x, y \in W)(\langle \Phi x, y\rangle = \langle x, \Phi y\rangle)\,. \tag{4}$$

Fact 2.2. If Φ is symmetric and U is a Φ-invariant subspace of W, then $\Phi|_U$ is also symmetric.

Definition 2.3. Let $\Phi : V \to W$ be a linear map between finite-dimensional Hermitian inner product spaces. The adjoint of Φ, denoted by Φ^*, is the unique linear transformation $\Phi^* : W \to V$ such that $\langle \Phi v, w\rangle_W = \langle v, \Phi^* w\rangle_V$ for all $v \in V, w \in W$.

Observation 2.4. An $m \times n$ matrix $A \in M_{m,n}(\mathbb{C})$ can be associated with a linear map $\Phi_A : \mathbb{C}^n \to \mathbb{C}^m$ by setting $\Phi_A x = Ax$ for all $x \in \mathbb{C}^n$.

Fact 2.5. Every linear map $\Phi : \mathbb{C}^n \to \mathbb{C}^m$ is associated with a unique matrix $A \in M_{m,n}(\mathbb{C})$.

Fact 2.6. Let $\Phi : \mathbb{C}^n \to \mathbb{C}^m$ be a linear map. If A is the matrix associated with Φ, then Φ^* is associated with the matrix A^*, the conjugate-transpose of A.

Definition 2.7. A linear transformation $\Phi : W \to W$ is called *normal* if $\Phi\Phi^* = \Phi^*\Phi$.

Fact 2.8 (Complex Spectral Theorem)**.** Let W be a finite-dimensional Hermitian inner product space. A linear transformation $\Phi : W \to W$ is normal if and only if Φ admits an orthonormal eigenbasis.

Fact 2.9 (Real Spectral Theorem)**.** Let W be a finite-dimensional real euclidean space. A linear transformation $\Phi : W \to W$ is symmetric if and only if Φ admits a real orthonormal eigenbasis.

Corollary 2.10. *If $P : \mathbb{R}^n \to \mathbb{R}^n$ is an orthogonal projection onto a subspace of $\mathbb{R}^n$ then P is symmetric.*

Fact 2.11. Let $\Phi : W \to W$ be a linear transformation and let $U \subseteq W$ be a Φ-invariant subspace. If Φ is normal, then $\Phi|_U$ is normal.

Lemma 2.12. *Let W be a finite-dimensional vector space (over any field). Let $\Phi_1, \Phi_2 : W \to W$ be commuting linear transformations. Then each eigenspace of Φ_1 is Φ_2-invariant.*

Proof. Let U be the eigenspace of Φ_1 corresponding to eigenvalue λ, so $U = \{x \in W : \Phi_1 x = \lambda x\}$. Fix a nonzero vector $x \in U$. Then $\Phi_1 x = \lambda x$, so

$$\Phi_1\Phi_2 x = \Phi_2\Phi_1 x = \Phi_2(\lambda x) = \lambda\Phi_2 x\,. \tag{5}$$

Therefore $\Phi_2 x \in U$. □

Theorem 2.13. *Let W be a finite-dimensional complex Hermitian inner product space. Let $\Phi_1, \ldots, \Phi_n$ be normal, commuting linear transformations on W. Then $\Phi_1, \ldots, \Phi_n$ have a common orthonormal eigenbasis.*

Proof. Let $d = \dim W$. We will proceed by induction on d. If all the Φ_i are scalar transformations then any basis is a common eigenbasis. This in particular settles the base case $d = 1$. Assume now that Φ_1 is not a scalar transformation, and let

$U_1, \ldots, U_t$ be the eigenspaces of Φ_1. By Fact 2.8, $V = U_1 \oplus \cdots \oplus U_t$ and the U_i are pairwise orthogonal. By Lemma 2.12, each U_i is Φ_j-invariant for all $1 \leq j \leq n$, and Fact 2.11 guarantees that each $\Phi_j|_{U_i}$ is normal. Therefore we can apply our inductive hypothesis to $\Phi_1|_{U_i}, \ldots, \Phi_n|_{U_i}$ for all $1 \leq i \leq t$ to produce a common orthonormal eigenbasis B_i for each eigenspace U_i of Φ_1. Let $B = \bigcup_{i=1}^{t} B_i$. By the orthogonal direct sum decomposition, B forms an orthonormal basis for W, and each vector in B is an eigenvector for each Φ_j $(1 \leq j \leq n)$. □

Thm. 2.13 will be used later in the proof of Cor. 2.37.

Theorem 2.14. *Let W be a finite-dimensional real euclidean space. Let $\Phi_1, \ldots, \Phi_n$ be symmetric, commuting linear transformations on W. Then $\Phi_1, \ldots, \Phi_n$ have a common real orthonormal eigenbasis.*

Proof. Following the proof of Thm. 2.13 in the real case, Fact 2.9 guarantees that we can find a common real orthonormal eigenbasis. □

2.2. **Theory of finite-dimensional algebras**

2.2.1. *Semisimple algebras.* We begin by reviewing the elements of the theory of finite-dimensional algebras. Let $\mathbb{F}$ be a field.

Definition 2.15. An $\mathbb{F}$-*algebra* is a vector space $\mathscr{A}$ over $\mathbb{F}$ equipped with an additional multiplication operation $\times : \mathscr{A}^2 \to \mathscr{A}$ which satisfies both left and right distributivity as well as scalar compatibility.

Example 2.16. $M_n(\mathbb{F})$ forms an algebra.

Definition 2.17. Let $v_1, \ldots, v_n$ be elements of an algebra $\mathscr{A}$. The algebra *generated* by $v_1, \ldots, v_n$, denoted by $\mathrm{alg}(v_1, \ldots, v_n)$, is the smallest subalgebra of $\mathscr{A}$ containing $v_1, \ldots, v_n$.

Definition 2.18. The *space of polynomials over a field* $\mathbb{F}$, denoted by $\mathbb{F}[t]$, is the set of all finite linear combinations of nonnegative powers of the variable t with coefficients in $\mathbb{F}$.

Fact 2.19. Let A be an element of an algebra $\mathscr{A}$. Then

$$\mathrm{alg}(A) = \{f(A) : f \in \mathbb{F}[t]\} \tag{6}$$

Definition 2.20. Let $\mathscr{A}$ be an algebra, and let $e_1, \ldots, e_n$ be a basis of $\mathscr{A}$, i.e., a basis of the underlying vector space. The *structure constants* $c_{i,j}^k$ of $\mathscr{A}$ with respect to this basis are the unique coefficients satisfying

$$e_i e_j = \sum_{k=1}^{n} c_{i,j}^k e_k \,. \tag{7}$$

Remark 2.21. Given a basis $e_1, \ldots, e_k$, the structure constants determine the algebra.

Definition 2.22. The *radical* of a finite-dimensional algebra is the unique largest nilpotent ideal.

We denote the radical of $\mathscr{A}$ by rad $\mathscr{A}$.

Definition 2.23. An algebra $\mathscr{A}$ is called *semisimple* if rad $\mathscr{A} = \{0\}$.

Definition 2.24. An algebra $\mathscr{A}$ is called *simple* if $\mathscr{A} \neq \{0\}$ and $\mathscr{A}$ has no nontrivial ideal.

Theorem 2.25 (Wedderburn)**.** *If $\mathscr{A}$ is a finite-dimensional semisimple algebra then $\mathscr{A}$ is the direct sum of simple algebras with identity.*

Theorem 2.26 (Wedderburn)**.** *If $\mathscr{A}$ is a simple finite-dimensional algebra with identity over $\mathbb{C}$ then $\mathscr{A}$ is isomorphic to $M_k(\mathbb{C})$ for some natural number k.*

The proof appears in Wedderburn's classic paper [23], see [22, Sec. 13.11] or [14, Sec. 4.3].

Definition 2.27. An element A of an algebra $\mathscr{A}$ is called *idempotent* if $A^2 = A$.

Definition 2.28. Two elements A_1, A_2 of an algebra $\mathscr{A}$ are called *orthogonal* if $A_1A_2 = A_2A_1 = 0$.

Fact 2.29. If $\mathscr{A}$ is a semisimple commutative finite-dimensional algebra over $\mathbb{C}$, then $\mathscr{A}$ has a unique basis of orthogonal idempotents.

2.2.2. **-closed matrix algebras.*

Definition 2.30. Let $A \in M_n(\mathbb{C})$. The *adjoint* A^* of A is its conjugate-transpose.

Definition 2.31. Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, and let $\mathscr{A}$ be a subalgebra of $M_n(\mathbb{F})$. If $\mathscr{A}$ is closed under adjoints, then we call $\mathscr{A}$ **-closed* .

Remark 2.32. The concept of *-closed algebras is a special case of the concepts of operator algebras, von Neumann algebras, and C^*-algebras.

Proposition 2.33. *Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. If a subalgebra $\mathscr{A}$ of $M_n(\mathbb{F})$ is *-closed, then $\mathscr{A}$ is semisimple.*

Proof. Let $\mathscr{A}$ be a *-closed subalgebra of $M_n(\mathbb{F})$. Suppose $M \in$ rad $\mathscr{A}$. By hypothesis $M^* \in \mathscr{A}$, so we have $M^*M \in$ rad $\mathscr{A}$, as rad $\mathscr{A}$ is an ideal. M^*M is nilpotent by its inclusion in rad $\mathscr{A}$, thus all its eigenvalues are 0. But M^*M is self-adjoint. By the Spectral Theorem, M^*M is diagonalizable with the entries along the diagonal being precisely the eigenvalues. Thus M^*M is similar to the zero matrix, so $M^*M = 0$. For all $v \in \mathbb{F}^n$, we have

$$0 = \langle 0, v\rangle = \langle M^*Mv, v\rangle = \langle Mv, Mv\rangle = \|Mv\|^2 \ . \tag{8}$$

Hence M maps every vector to 0, so we conclude that M is the zero matrix. Therefore rad $\mathscr{A} = \{0\}$. □

Thm. 2.25 now holds with coordinates in the decomposition being *-closed. We now state the analogues of Wedderburn's theorems for *-closed algebras.

Fact 2.34. Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. If $\mathscr{A}$ is a *-closed subalgebra of $M_n(\mathbb{F})$, then $\mathcal{A}$ is the direct sum of *-closed simple algebras with identity.

Definition 2.35. We say that an isomorphism of *-closed complex algebras is a *-isomorphism if it preserves adjoints.

Fact 2.36. If $\mathscr{A}$ is a simple *-closed subalgebra of $M_n(\mathbb{C})$, then $\mathscr{A}$ is *-isomorphic to $M_k(\mathbb{C})$ for some natural number k.

For the proofs of Facts 2.34 and 2.36, see [14, Sec. 5.1].

Corollary 2.37. *If $\mathscr{A}$ is a commutative *-closed subalgebra of $M_n(\mathbb{C})$, then $\mathscr{A}$ has a unique basis of orthogonal self-adjoint idempotents.*

While this result follows from Fact 2.34, we shall give a direct elementary proof (see Thm. 2.13).

Proof. Since $\mathscr{A}$ is commutative and *-closed, each $A \in \mathscr{A}$ is normal. By Thm 2.13, there exists a common orthonormal eigenbasis $e_1, \ldots, e_m$ for the linear transformations corresponding to a basis $A_0, \ldots, A_n$ of $\mathscr{A}$. Define $\lambda(\ell, j)$ to be the unique value such that $A_\ell e_j = \lambda(\ell, j) e_j$. We say $e_i \sim e_j$ if $(\forall \ell \in \{0, \ldots, n\})(\lambda(\ell, i) = \lambda(\ell, j))$. Let $U_0, \ldots, U_k$ be the spans of the equivalence classes of $e_1, \ldots, e_m$. Let V be the underlying vector space of $\mathscr{A}$. Since the basis was chosen to be orthogonal, the U_i are pairwise orthogonal and $V = U_0 \oplus \cdots \oplus U_k$.

Let $E_t : V \to V$ be the orthogonal projection to U_t, for $t = 0, \ldots, k$. Fix s such that $e_s \in U_t$. We can assume every matrix in $\mathscr{A}$ is diagonal by changing the basis of V to be $e_1, \ldots, e_m$. Let g_ℓ be the Lagrange interpolation polynomial sending $\lambda(\ell, s)$ to 1 and all other diagonal entries of A_ℓ to 0. We conclude $E_t = \prod_{\ell=0}^{n} g_\ell(A_\ell) \in \mathscr{A}$. Since $\sum_{t=0}^{k} \mathrm{rk}(E_t) = \sum_{t=0}^{k} \dim(U_t) = m$, $E_0, \ldots, E_k$ forms the desired orthogonal self-adjoint idempotent basis, and in particular $k = n$. Uniqueness follows from Fact 2.29. □

Corollary 2.38. *If $\mathscr{A}$ is a commutative subalgebra of $M_n(\mathbb{R})$ consisting of symmetric matrices, then $\mathscr{A}$ has a unique basis of orthogonal symmetric idempotents.*

Proof. The proof is the same as the proof of Cor. 2.37, *mutatis mutandis.* □

2.2.3. *The algebra of polynomials of a matrix.* In this subsection we consider the algebra $\mathrm{alg}(A)$ generated by the matrix $A \in M_n(\mathbb{C})$.

Definition 2.39. Let A be an $n \times n$ matrix over a field $\mathbb{F}$. The *minimal polynomial* of A is the monic polynomial f of least degree such that $f(A) = 0$.

Next, we review a few properties concerning the degree of the minimal polynomial of a matrix and the dimension of the algebra generated by the matrix.

Definition 2.40. Two matrices $A, B \in M_n(\mathbb{F})$ are said to be *similar* if there exists an invertible $S \in M_n(\mathbb{F})$ such that $A = S^{-1}BS$.

Fact 2.41. Similar matrices in $M_n(\mathbb{C})$ have the same minimal polynomial.

Proposition 2.42. *Let $A \in M_n(\mathbb{C})$. The dimension of* $\mathrm{alg}(A)$ *is the degree of the minimal polynomial of A.*

Proof. Let k be the degree of the minimal polynomial of A. This implies that no nontrivial linear combination of $\{I, A, A^2, \ldots, A^{k-1}\}$ can equal the zero matrix, so this set is linearly independent of size k. However, the minimal polynomial

witnesses that the list $\{I, A, A^2, \ldots, A^{k-1}, A^k\}$ is linearly dependent. By induction it follows that A^ℓ is in the span of $\{I, A, A^2, \ldots, A^{k-1}\}$ for all $\ell \geq k$. Therefore $\{I, A, A^2, \cdots, A^{k-1}\}$ is a basis of $\mathrm{alg}(A)$. □

Proposition 2.43. *Let $D \in M_n(\mathbb{C})$ be a diagonal matrix. The degree of the minimal polynomial of D is the number of distinct eigenvalues of D.*

Proof. Let λ_i be the ith diagonal entry of D. For any polynomial f, the ith diagonal entry of $f(D)$ is $f(\lambda_i)$. Therefore

$$f(D) = 0 \Leftrightarrow (\forall i)(f(\lambda_i) = 0) \Leftrightarrow \prod{}'(x - \lambda_i) \text{ divides } f\,, \tag{9}$$

where $\prod'$ extends over all *distinct* λ_i. So $\prod'(x - \lambda_i)$ is the minimal polynomial of D. □

Corollary 2.44. *If $A \in M_n(\mathbb{C})$ is diagonalizable, then the degree of the minimal polynomial of A, and therefore the dimension of* $\mathrm{alg}(A)$*, is the number of distinct eigenvalues of A.*

Proof. This follows from Prop. 2.42, Fact 2.41, and Prop. 2.43. □

Proposition 2.45. *Let $E_0, \ldots, E_k$ be the orthogonal projections to the eigenspaces of a symmetric matrix A in $M_n(\mathbb{C})$. Then $E_0, \ldots, E_k$ are in* $\mathrm{alg}(A)$*.*

Proof. Since A is symmetric, we can assume $\mathrm{alg}(A)$ consists of diagonal matrices. Let λ_t be the eigenvalue of A corresponding to the eigenspace to which E_t projects. Let g_t be the Lagrange interpolation polynomial taking λ_t to 1 and all other eigenvalues of A to 0. Then $g_t(A) = E_t$. □

Proposition 2.46. *Let $E_0, \ldots, E_k$ be the orthogonal projections to the eigenspaces of a symmetric matrix A in $M_n(\mathbb{C})$. Then A is in* $\mathrm{alg}(E_0, \ldots, E_k)$*.*

Proof. By transforming to an eigenbasis, we can assume $\mathrm{alg}(E_0, \ldots, E_k)$ consists of diagonal matrices. With respect to this eigenbasis, A is diagonal with eigenvalues along the diagonal. Let λ_t be the eigenvalue of A corresponding to the eigenspace to which E_t projects. Then we have

$$A = \sum_{i=0}^{k} \lambda_i E_i \tag{10}$$

□

2.3. **Relations and graphs**

Sets. For $r \in \mathbb{N}$, let $[r]$ denote the set $\{0, 1, \cdots, r-1\}$. Let Ω be a finite set. We refer to the r-element subsets of Ω as the r-subsets of Ω. Let $\binom{\Omega}{r}$ denote the set of all r-subsets of Ω. The power set of Ω, that is, the set of all subsets of Ω, is denoted by $\mathfrak{P}(\Omega)$.

Relations. Let Ω be a finite set of *vertices* with $|\Omega| = n$. A *relation* on Ω is a subset of $\Omega \times \Omega$. For each relation $R \subseteq \Omega \times \Omega$, we define the *converse relation* $R^- = \{(y, x) : (x, y) \in R\}$. A *relational structure* on Ω is the set Ω paired with a set of relations on Ω. The *diagonal relation* $\mathrm{diag}(\Omega)$ is the set $\{(x, x) : x \in \Omega\}$.

Graphs and Digraphs. A *graph* $X = (\Omega, E)$ is a finite set Ω, called the vertex set, paired with a set of edges $E \subseteq \{\{u, v\} : u, v \in \Omega, u \neq v\}$. In a graph, we say a vertex v is *incident* with an edge e if $v \in e$, and two vertices u and v are *adjacent* if $\{u, v\} \in E$. The degree of a vertex $v \in \Omega$ is the number of edges incident with v. A *directed graph* or *digraph* $X = (\Omega, E)$ is a finite set of vertices Ω along with a set $E \subseteq \Omega \times \Omega$ of directed edges. In a digraph, a vertex v is said to be *incident* with an edge e if $e = (v, w)$ or $e = (w, v)$ for some vertex w. We say a pair of vertices u, v in a digraph are *adjacent* if $(u, v) \in E$ or $(v, u) \in E$. The *indegree* of a vertex v in Ω, denoted $\deg_X^-(v)$ is the number of vertices u such that $(u, v) \in E$; analogously, the *outdegree* of v, denoted $\deg_X^+(v)$, is the number of vertices w such that $(v, w) \in E$. A graph $X = (\Omega, E)$ can be modeled as a digraph $Y = (\Omega, E')$ where $(x, y), (y, x) \in E'$ if $\{x, y\} \in E$. Note that in this case the indegree and outdegree of any vertex in Y are the same, and both are equal to the degree of the vertex in X. We call a graph or digraph *complete* if the edge set is maximal, including all loops. A graph or digraph is called *irreflexive* if it contains no loops.

Definition 2.47. Let $X = (\Omega, E)$ be a graph. If $x, y \in \Omega$, a *walk* of length ℓ from x to y is a sequence of vertices $z_0, z_1, \ldots, z_\ell$ such that $z_0 = x$, $z_\ell = y$, and $\{z_i, z_{i+1}\} \in E$ for $0 \leq i \leq \ell - 1$.

Definition 2.48. Let $X = (\Omega, E)$ be a digraph. If $x, y \in \Omega$, a *directed walk* of length ℓ from x to y is a sequence of vertices $z_0, z_1, \ldots, z_\ell$ such that $z_0 = x$, $z_\ell = y$, and $(z_i, z_{i+1}) \in E$ for $0 \leq i \leq \ell - 1$.

A graph $X = (\Omega, E)$ is said to be *connected* if for all $x, y \in \Omega$, there exists a walk from x to y. However, the concept of connectedness can be defined for digraphs in multiple ways. A digraph $X = (\Omega, E)$ is said to be *weakly connected* if the graph $Y = (\Omega, \widetilde{E})$ defined by

$$\{x, y\} \in \widetilde{E} \Leftrightarrow (x, y) \in E \cup E^- \tag{11}$$

is connected. X is said to be *strongly connected* if for all $x, y \in \Omega$, there exists a directed walk from x to y. It is clear that strong connectedness implies weak connectedness. A digraph X is called *Eulerian* if the indegree of every vertex is equal to its outdegree.

Fact 2.49. In an Eulerian digraph, weak connectedness is equivalent to strong connectedness.

Definition 2.50. The *distance*, denoted by $\mathrm{dist}_X(x, y)$, between two vertices x, y in a graph X is the length of the shortest walk from x to y. If no such walk exists, the distance is said to be infinite.

Definition 2.51. The *diameter* of a graph is the maximum distance between two vertices, ranging over all pairs.

Definition 2.52. If $X = (\Omega, E)$ is a digraph, then the $|\Omega| \times |\Omega|$ *adjacency matrix* $A(X) = (m_{i,j})$ is defined to have entries

$$m_{i,j} = \begin{cases} 1 & \text{if } (v_i, v_j) \in E\,, \\ 0 & \text{otherwise}\,, \end{cases} \tag{12}$$

where v_i, v_j range over all elements of Ω.

Definition 2.53. The adjacency matrix of a graph is the adjacency matrix of its associated digraph.

Fact 2.54. Let R_1, R_2 be relations on Ω. Let A_1 be the adjacency matrix of the digraph (Ω, R_1) and let A_2 be the adjacency matrix of (Ω, R_2). Then $R_1 = R_2^-$ if and only if $A_2 = A_1^{\mathrm{tr}}$.

In this paper, we refer to the eigenvalues of the adjacency matrix of a graph as the *eigenvalues* of the graph.

Fact 2.55. Let X be a graph. The $(i,j)^{th}$ entry of $A(X)^k$ is the number of walks of length k from v_i to v_j.

Proposition 2.56. *Let X be a connected graph of diameter d. The minimal polynomial of $A(X)$ has degree at least $d+1$, hence* $\mathrm{alg}(A(X))$ *has dimension at least $d+1$.*

Proof. Let $A = A(X)$. Since the graph has diameter d, there exist vertices at distance ℓ for all $0 \leq \ell \leq d$. By Fact 2.55, A^ℓ has a nonzero entry where A^j has a zero entry for all $0 \leq j < \ell \leq d$, hence A^ℓ cannot be written as a linear combination of $\{I, A, \ldots, A^{\ell-1}\}$. Thus the list $\{I, A, \cdots, A^d\}$ is linearly independent, so the minimal polynomial has degree at least $d+1$. The second part of the claim follows immediately from Prop. 2.42. □

Corollary 2.57. *A graph of diameter d has at least $d+1$ distinct eigenvalues.*

Proof. Let X be a graph, and let A be its adjacency matrix. By Prop. 2.42, the minimal polynomial of A has degree at least $d+1$. A is symmetric, so by the Spectral Theorem, A is diagonalizable. The conclusion follows by Cor. 2.44. □

Groups. For groups G and H, we write $H \leq G$ to denote that H is a subgroup of G. For a finite set Ω, we let $\mathrm{Sym}(\Omega)$ denote the symmetric group acting on Ω. If $X = (\Omega, E)$ is a graph, let $\mathrm{Aut}(X)$ denote automorphism group of X, that is, the group of permutations of Ω which preserve the adjacency relation of X.

3. Configurations

3.1. Coherent configurations

In this section, we follow the notation of L. Babai from Section 3 of [2]. We begin with an overview of coherent configurations, which are highly regular combinatorial objects introduced independently several times in different contexts. Coherent configurations were first introduced by I. Schur in 1933 [21] for the purpose of studying finite permutation groups. The term "coherent configuration" was introduced by D. Higman in 1970, who studied them in Schur's context and developed the representation theory of adjacency algebras (see Sec. 3.2). Around the same time (1968), B. Weisfeiler and A. Leman defined an equivalent concept motivated by the Graph Isomorphism problem [24] (see [25]). They also introduced an algebra, which they called a "cellular algebra," that is equivalent to the adjacency algebra. Coherent configurations played a key role in the recent quasipolynomial-time solution of the Graph Isomorphism problem by L. Babai [2].

Let Ω be a finite set of *vertices* with $|\Omega| = n$.

Definition 3.1. A *partition structure* $\mathfrak{X} = (\Omega; \mathscr{R}) = (\Omega; R_0, \cdots, R_{r-1})$ is a relational structure on Ω where each relation $R_i \subseteq \Omega \times \Omega$ for $i \in [r]$ is nonempty and $\mathscr{R} = (R_0, \cdots, R_{r-1})$ partitions $\Omega \times \Omega$. That is,

$$\bigsqcup_{i=0}^{r-1} R_i = \Omega \times \Omega\,, \tag{13}$$

where $\sqcup$ denotes a disjoint union.

Let Y be the complete digraph with vertex set Ω, identifying each loop with the unique vertex incident with it. We can view $\mathscr{R}$ as a coloring on the edges and vertices of Y, letting the *color* of edge (x, y) be i if $(x, y) \in R_i$. We denote the color of edge (x, y) by $c(x, y)$. We call the digraph $X_i = (\Omega, R_i)$ the *color-i constituent*[1] of the partition structure $\mathfrak{X}$. With some abuse of terminology, we also refer to the relation R_i as the color-i constituent.

With every digraph, we can associate a partition structure.

Example 3.2. Let $X = (\Omega, E)$ be a digraph, and define four relations as follows,

$$R_0 = \mathrm{diag}(\Omega) \cap E\,, \qquad R_1 = \mathrm{diag}(\Omega) \backslash E\,,$$
$$R_2 = E \backslash \mathrm{diag}(\Omega)\,, \qquad R_3 = \Omega \times \Omega \backslash (E \cup \mathrm{diag}(\Omega))\,.$$

Then $\mathfrak{X}(X) = (\Omega; R_0, R_1, R_2, R_3)$ is a partition structure.

Definition 3.3. A *(binary) configuration* of rank r is a partition structure $\mathfrak{X} = (\Omega; \mathscr{R}) = (\Omega; R_0, \cdots, R_{r-1})$ satisfying

(1) $(\forall x, y, z \in \Omega)\ (c(x, y) = c(z, z) \Rightarrow x = y)\,,$

(2) $(\forall u, v, x, y \in \Omega)\ (c(u, v) = c(x, y) \Rightarrow c(v, u) = c(y, x))\,.$

Viewing a coloring of a loop as a coloring of a vertex, Condition (1) guarantees that vertices are colored differently from edges. A vertex color is called a *diagonal color*, while an edge color is called an *off-diagonal color*. Condition (2) states that colors are paired, that is, the color of a directed edge (u, v) determines the color of its converse (v, u). For a given color class $R_i \in \mathscr{R}$, Condition (2) guarantees that its converse R_i^- is also included in $\mathscr{R}$. Conditions (1) and (2) together imply that for a color class $R_i \in \mathscr{R}$, R_i and R_i^- are either equal or disjoint.

Definition 3.4. A configuration is called *homogeneous* if all vertices have the same color, i.e., $R_0 = \mathrm{diag}(\Omega)$.

Definition 3.5. We call an irreflexive digraph $X = (\Omega, E)$ a *tournament* if every pair of distinct vertices is adjacent and X is oriented, i.e., $E \cap E^- = \emptyset$ and $E \cup E^- \supseteq \Omega \times \Omega \backslash \mathrm{diag}(\Omega)$.

Example 3.6. The partition structure $\mathfrak{X}(X)$ constructed in Example 3.2 is a configuration if and only if the digraph X satifies one of the following.

(1) X is a tournament.

[1] What we call a constituent is called an "extended constituent" in [2].

(2) $E = E^-$, i.e., X is a graph.

Definition 3.7. A *coherent configuration* of rank r is a binary configuration $\mathfrak{X} = (\Omega; \mathscr{R}) = (\Omega; R_0, \cdots, R_{r-1})$ satisfying the additional condition

(3) There exist r^3 nonnegative integers $p^k_{i,j}$ $(i, j, k \in [r])$ such that $\forall i, j, k \in [r]$ and $\forall (x, y) \in R_k$ we have

$$|\{z \in \Omega : (c(x, z) = i) \wedge (c(z, y) = j)\}| = p^k_{i,j}\,. \tag{14}$$

Thus a coherent configuration is a configuration where the color of a directed edge encodes the number of walks of length 2 from its tail to its head in a given pair of colors. The values $p^k_{i,j}$ are called the **intersection numbers** of $\mathfrak{X}$.

For $i, j < r$ and $x, y \in V$, let $p(x, y, i, j)$ denote the number of $z \in V$ satisfying $c(x, z) = i$ and $c(z, y) = j$. The *Weisfeiler-Leman refinement* is a color refinement process on partition structures satisfying Condition (1) of Definition 3.3. The Weisfeiler-Leman refinement is an iterative process. In one round, it constructs a refined coloring c^0 by setting $c^0(x, y) = c^0(u, v)$ if $c(x, y) = c(u, v)$ and for all $i, j < r$ we have $p(x, y, i, j) = p(u, v, i, j)$. The iteration stops when no proper refinement is obtained.

Remark 3.8. The stable colorings of the Weisfeiler-Leman refinement, those colorings that do not get refined, are precisely the coherent configurations.

Since the information stored in each edge color of a stable coloring of the Weisfeiler-Leman refinement is preserved under isomorphisms, this refinement process can be used as an isomorphism-rejection tool. Let G_1 and G_2 be graphs. If we construct partition structures corresponding to G_1 and G_2 as in Example 3.2, then the resulting refined colorings will have either equal or disjoint color sets. Thus if two graphs produce disjoint color sets when the Weisfeiler-Leman refinement is applied to their corresponding configurations, then the graphs are not isomorphic.

A constituent is called a *diagonal constituent* if its edges belong to the diagonal relation $\mathrm{diag}(\Omega) = \{(x, x) : x \in \Omega\}$. A homogeneous configuration contains exactly one diagonal constituent, namely $(\Omega; \mathrm{diag}(\Omega))$. A constituent is called *off-diagonal* if it is not a diagonal constituent.

Next we show that the color of a vertex determines the outdegree of each constituent at that vertex.

Lemma 3.9. *Let $X = (\Omega; \mathscr{R})$ be a coherent configuration and v be a vertex in Ω. Fix a color i, and let j be such that $R_j = R_i^-$. If $c(v, v) = k$, then $\deg^+_{X_i}(v) = p^k_{i,j}$ and $\deg^-_{X_i}(v) = p^k_{j,i}$.*

Proof. Let $\mathfrak{X} = (\Omega; \mathscr{R})$ be a coherent configuration, and fix $u, v \in \Omega$ such that $c(u, u) = c(v, v) = 0$. Fix a color i, let X_i be the color-i constituent, and let $R_j = R_i^-$. Thus for any $z \in \Omega$, $c(u, z) = i$ implies $c(z, u) = j$, giving us the following equality.

$$|\{z \in \Omega : (c(u, z) = i) \wedge (c(z, u) = j)\}| = |\{z \in \Omega : (c(u, z) = i)\}| = \deg^+_{X_i}(u) \tag{15}$$

The left hand side is the intersection number $p^0_{i,j}$ (see Definition 3.7). Similarly,

$$|\{z \in \Omega : (c(u, z) = j) \wedge (c(z, u) = i)\}| = |\{z \in \Omega : (c(z, u) = i)\}| = \deg^-_{X_i}(u)\,. \tag{16}$$

□

Proposition 3.10. *Every constituent of a homogeneous coherent configuration is Eulerian.*

Proof. Fix a color $i \in [r]$, let X_i be the color-i constituent, and let $R_j = R_i^-$. By Lemma 3.9,

$$p^0_{i,j} \cdot |\Omega| = \sum_{v\in\Omega} \deg^-_{X_i}(v) = \sum_{v\in\Omega} \deg^+_{X_i}(v) = p^0_{j,i} \cdot |\Omega| \,. \tag{17}$$

We can conclude that $p^0_{i,j} = p^0_{j,i}$, so $\forall v \in \Omega$ we have $\deg^+_{X_i}(v) = \deg^-_{X_i}(v)$. □

Prop. 3.10 along with Fact 2.49 show that weak connectedness and strong connectedness for the off-diagonal constituents of a homogeneous coherent configuration are equivalent.

Definition 3.11. A homogeneous coherent configuration $\mathfrak{X}$ is *primitive* if every off-diagonal constituent is weakly (equivalently, strongly) connected. $\mathfrak{X}$ is *uniprimitive* if it is primitive and has rank at least 3.

Coherent configurations can be applied to the study of finite permutation groups. Let $G \leq \mathrm{Sym}(\Omega)$, that is, let G be a permutation group acting on the set Ω. An orbit of the diagonal G-action on $\Omega \times \Omega$ is called an *orbital*.

Definition 3.12. Let $R_1, \cdots, R_{r-1}$ be the orbitals of G. Then $(\Omega; R_1, \cdots, R_{r-1})$ is a partition structure called an *orbital configuration*.

Fact 3.13. An orbital configuration is necessarily a coherent configuration.

A coherent configuration is called *Schurian* if it can be realized as the orbital configuration of some permutation group.

3.2. **The adjacency algebra**

We associate with each constituent of a coherent configuration $\mathfrak{X} = (\Omega; R_0, \cdots, R_{r-1})$ an element of the matrix algebra $M_n(\mathbb{F})$ for an arbitrary field $\mathbb{F}$. This allows us to view the combinatorial construction of coherent configurations as an algebraic structure. Our exposition follows the remarks of Delsarte and Levenshtein [12], as well as Brouwer's exposition [9].

Let A_i denote the adjacency matrix of the color-i constituent of $\mathfrak{X}$.

Observation 3.14. The set of constituent adjacency matrices, $\mathfrak{A} = \{A_i\}_{i\in[r]}$, consists of nonzero $(0,1)$-matrices with the following structural properties.

(1) The sum of all $A_i \in \mathfrak{A}$ is J_n, the $n \times n$ matrix of all 1's.

(2) The sum of the A_i for the diagonal constituents R_i is I_n.

(3) $(\forall i \in [r])(\exists j \in [r])(A_j = A_i^{tr})$.

(4) For any $i, j \in [r]$, we have

$$A_i A_j = \sum_{k=0}^{r-1} p^k_{ij} A_k \,. \tag{18}$$

In fact, the above four properties are equivalent to the definition of a coherent configuration.

Equation (18) guarantees that $\mathrm{span}(\mathfrak{A})$ is closed under matrix multiplication, hence it is an algebra.

Definition 3.15. The $\mathbb{F}$-*adjacency algebra* $\mathcal{A}$ is the span of $A_0, \ldots, A_{r-1}$.

Remark 3.16. Property (4) of Obs. 3.14 implies that the structure constants of the adjacency algebra (see Definition 2.20) with respect to the basis $A_0, \ldots, A_{r-1}$ are the intersection numbers.

Fact 3.17. $\dim \mathcal{A} = r$.

Remark 3.18. The adjacency algebra is closed under both the usual matrix multiplication and Hadamard (entry-wise) multiplication.

Proposition 3.19. *$\mathcal{A}$ has an identity.*

Proof. By Axiom (1) of Definition 3.3, $I_n \in \mathcal{A}$ (see Property (2) of Obs. 3.14). □

Restricting ourselves to subalgebras of $M_n(\mathbb{F})$ over a field $\mathbb{F} \subseteq \mathbb{C}$ which is closed under complex conjugation, we will show that $\mathcal{A}$ is closed under adjoints.

Proposition 3.20. *The adjacency algebra $\mathcal{A}$ of a coherent configuration over $\mathbb{R}$ or $\mathbb{C}$ is *-closed.*

Proof. It suffices to show that the adjoint of each basis matrix $A_0, \ldots, A_{r-1}$ belongs to $\mathcal{A}$. But $A_i^* = A_i^{\mathrm{tr}} = A_j$ for some j (see Property (3) of Obs. 3.14). □

Corollary 3.21. *The adjacency algebra $\mathcal{A}$ of a coherent configuration over $\mathbb{R}$ or $\mathbb{C}$ is semisimple.*

Proof. This follows immediately from Props. 3.20 and 2.33. □

3.3. **Commutative coherent configurations**

Definition 3.22. A coherent configuration is called *commutative* if $p_{ij}^k = p_{ji}^k$ for all $0 \leq i, j, k < r$.

Proposition 3.23. *A coherent configuration $\mathfrak{X} = (\Omega; R_0, \ldots, R_{r-1})$ is commutative if and only if the associated adjacency algebra $\mathcal{A}$ is commutative.*

Proof. Suppose that $\mathfrak{X}$ is symmetric. By Property (4) of Obs. 3.14, every pair of elements of the basis $A_0, \ldots, A_{r-1}$ of $\mathcal{A}$ commutes. It follows that $\mathcal{A}$ is commutative.

Suppose that the adjacency algebra is commutative. Combining Property (4) of Obs. 3.14 along with the uniqueness of the expression of any $A \in \mathcal{A}$ as a linear combination of the basis $A_0, \cdots, A_{r-1}$, we have

$$A_i A_j = \sum_{k=0}^{r-1} p_{ij}^k A_k = \sum_{k=0}^{r-1} p_{ji}^k A_k = A_j A_i \,. \tag{19}$$

Choosing any pair $i, j \in [r]$, then we must have $p_{ij}^k = p_{ji}^k$ for each $k \in [r]$. Therefore $\mathfrak{X}$ is commutative. □

This constraint on the intersection numbers forces all loops to have the same color.

Proposition 3.24. *A commutative coherent configuration is necessarily homogeneous.*

Proof. Let $\mathfrak{X} = (\Omega, \mathscr{R})$ be a commutative coherent configuration. Suppose, seeking a contradiction, that two vertices $u, v \in \Omega$ are colored differently, so $(u, u) \in R_\ell$ and $(v, v) \in R_m$ for $\ell \neq m$. If $(u, v) \in R_k$, then $p^k_{\ell,k} = 1$ but $p^k_{k,\ell} = 0$, contradicting commutativity. □

Observation 3.25. Let $\mathfrak{X}$ be a commutative coherent configuration. Axiom (2) of Definition 3.3 guarantees that the adjoint of any adjacency matrix $A_0, \ldots, A_{r-1}$ is in the adjacency algebra of $\mathfrak{X}$. Thus for $0 \leq i < r$, A_i commutes with its adjoint, hence is A_i is normal.

We show that commutativity is sufficient to ensure that the entire adjacency algebra is simultaneously diagonalizable.

Corollary 3.26. *The adjacency algebra of a commutative coherent configuration has a common orthonormal eigenbasis.*

Proof. By Prop. 3.23 and Obs. 3.25, the basis $A_0, \cdots, A_{r-1}$ satisfies the hypotheses of Thm. 2.13. Therefore the basis, hence the entire adjacency algebra, has a common orthonormal eigenbasis. □

Two classes of values, known as the p-numbers and q-numbers, associated with the adjacency algebra of commutative coherent configurations were introduced by P. Delsarte in his monumental dissertation [11].

Definition 3.27. Let $\mathfrak{X}$ be a commutative coherent configuration, and let $A_0, \cdots, A_{r-1}$ be the constitutent adjacency matrices. The *p-numbers* $(p_i(j))$, for $i, j \in [r]$, of the adjacency algebra $\mathcal{A}$ of $\mathfrak{X}$ are the unique complex numbers satisfying

$$A_i = \sum_{j=0}^{r-1} p_i(j) E_j \,, \tag{20}$$

where $E_0, \ldots, E_{r-1}$ is the unique basis of orthogonal idempotents from Fact 2.29.

Proposition 3.28. *Let $\mathfrak{X}$ be a commutative coherent configuration. Let A_i be the adjacency matrix of the color-i constituent of $\mathfrak{X}$. Then $p_i(j)$ is the eigenvalue corresponding to the eigenspace of A_i containing U_j.*

Proof. This is immediate from the Spectral Theorem and Cor. 2.37. The projections to eigenspaces form the unique set of minimal idempotents of $\mathcal{A}$. □

Observation 3.29. It follows from Prop. 3.28 that for $\lambda \in \mathbb{R}$ the multiplicity of λ as an eigenvalue of A_i is $\sum\{\mathrm{rk}(E_j) : j \in \{0, \ldots, n\}, p_i(j) = \lambda\}$.

The q-numbers are defined analogously.

Definition 3.30. Let $\mathfrak{X}$ be a commutative coherent configuration, and let $A_0, \cdots, A_{r-1}$ be the constitutent adjacency matrices. The *q-numbers* $(q_j(i))$, for $i, j \in [r]$, of the adjacency algebra $\mathcal{A}$ of $\mathfrak{X}$ are the unique complex numbers satisfying

$$E_j = \sum_{i=0}^{r-1} q_j(i) A_i \,, \tag{21}$$

where $E_0, \ldots, E_{r-1}$ is the unique basis of orthogonal idempotents of $\mathcal{A}$ from Fact 2.29.

4. Association Schemes

We use the term "association scheme" in its original, pre-Delsarte sense (see Remark 4.5 below).

4.1. Association schemes and their adjacency algebras

Definition 4.1. An *association scheme* is a coherent configuration $\mathfrak{X} = (\Omega; \mathscr{R}) = (\Omega; R_0, \cdots, R_{r-1})$ in which every constituent is undirected (self-paired), i.e.,

(4) $(\forall x, y \in \Omega)(c(x, y) = c(y, x))\,.$

Observation 4.2. An equivalent requirement is that each constituent adjacency matrix A_i is symmetric.

An association scheme can be viewed as a coloring on the edges of a complete undirected graph.

Proposition 4.3. *An association scheme is a commutative coherent configuration.*

Proof. Let $\mathfrak{X} = (\Omega; \mathscr{R})$ be an association scheme. Fix $x, y \in \Omega$, and let $k = c(x, y) = c(y, x)$. Then we have

$$p_{ij}^k = |\{z \in \Omega : (c(x, z) = i) \wedge (c(z, y) = j)\}| \tag{22}$$

$$= |\{z \in \Omega : (c(z, x) = i) \wedge (c(y, z) = j)\}| \tag{23}$$

$$= p_{ji}^k \,. \tag{24}$$

□

Corollary 4.4. *Association schemes are homogeneous.*

Proof. This follows directly from Props. 4.3 and 3.24. □

Association schemes have independently been studied in the context of statistical design theory since the late 1940s [8].

Remark 4.5. This definition is more strict than that of Delsarte, who uses the term "association scheme" for commutative coherent configurations.

Remark 4.6. Not every commutative coherent configuration is an association scheme in our (classical) sense. To show that these notions are distinct, consider the coherent configuration on the vertex set $\Omega = \{x, y, z\}$ where $R_0 = \mathrm{diag}(\Omega)$, $R_1 = \{(x, y), (y, z), (z, x)\}$, and $R_2 = R_1^-$.

By Props. 3.23 and 4.3, all association schemes are commutative coherent configurations and the corresponding adjacency algebras are commutative. Moreover, the basis $A_0, \cdots, A_{r-1}$, hence the entire the adjacency algebra, consists of self-adjoint matrices over $\mathbb{R}$ by Obs. 4.2. These conditions are sufficient to find a common *real* orthonormal eigenbasis for the entire adjacency algebra.

Corollary 4.7. *The adjacency algebra of an association scheme has a common real orthonormal eigenbasis.*

Proof. By Prop. 3.23, Prop. 4.3, and Obs. 4.2, the basis $A_0, \cdots, A_{r-1}$ satisfies the hypotheses of Thm. 2.14. Therefore the basis, hence the entire adjacency algebra, has a common real orthonormal eigenbasis. □

4.2. **Metric schemes**

Given an undirected graph $X = (\Omega, E)$, we can define the *distance configuration* $\mathfrak{M}(X)$ as the configuration generated by the distance metric. That is, each pair $(x, y) \in \Omega \times \Omega$ is colored by $\mathrm{dist}_X(x, y)$. Note that Condition (3) in Definition 3.7 does not necessarily hold for distance configurations, e.g., let X be the path on 3 vertices.

Definition 4.8. A connected undirected graph X is called *distance-regular* if the distance configuration $\mathfrak{M}(X)$ generated by X is an association scheme. If so, we call $\mathfrak{M}(X)$ the *metric scheme* generated by X.

Definition 4.9. A graph X is called *strongly regular* with parameters (n, k, λ, μ) if X is a k-regular graph on n vertices, each pair of adjacent vertices has λ common neighbors, and each pair of nonadjacent vertices has μ common neighbors.

Fact 4.10. The distance-regular graphs of diameter at most 2 are precisely the connected strongly regular graphs.

Definition 4.11. A connected undirected graph X is called *distance-transitive* if for each pair $((u, v), (x, y)) \in \Omega^4$ of pairs of vertices such that $\mathrm{dist}_X(u, v) = \mathrm{dist}_X(x, y)$ the following holds

$$(\exists \sigma \in \mathrm{Aut}(X))(u^\sigma = x \text{ and } v^\sigma = y)\,. \tag{25}$$

Every distance-transitive graph is distance-regular, since distances and the number of common neighbors are preserved by automorphisms. The converse is false; in fact, there exist large families of strongly regular graphs with no nontrivial automorphisms. For example, consider the line graphs of Steiner triple systems. These are strongly regular graphs, and it is shown in Cor. 1.13(a) of [3] that any automorphism on the line graph is inherited from the Steiner triple system that generated it, provided the Steiner triple system has at least 15 points. Almost all Steiner triple systems are shown to have no nontrivial automorphisms in [4], thus the line graphs of almost all Steiner triple systems admit no nontrivial automorphisms. Another class of examples can be generated from Latin squares, as mentioned in Thm. 1.20 of [3].

Next, we show that the adjacency algebras of metric schemes are generated by the adjacency matrix of the corresponding distance-regular graph. We also prove a spectral property of distance-regular graphs.

Proposition 4.12. *The adjacency matrix of a distance-regular graph generates the adjacency algebra of its corresponding metric scheme.*

Proof. Let X be a distance-regular graph of diameter d and let $A = A(X)$. The adjacency algebra has dimension $d+1$ (see Definition 3.15). Since A is contained in the adjacency algebra and generates an algebra of dimension at least $d+1$ by Prop. 2.56, we conclude that $\mathrm{alg}(A)$ is the adjacency algebra. □

Theorem 4.13. *A distance-regular graph of diameter d has exactly $d+1$ distinct eigenvalues.*

Proof. Let X be a distance-regular graph of diameter d and let $A = A(X)$. By Prop. 4.12, A spans the adjacency algebra of X with dimension $d+1$. Thus, by Prop. 2.42, the degree of the minimal polynomial of A is exactly $d+1$. By Cor. 2.44, X has exactly $d+1$ eigenvalues. □

We are now ready to prove our main structural theorem concerning the adjacency algebra of metric schemes.

Theorem 4.14. *The orthogonal projections to eigenspaces of a distance-regular graph form a basis of symmetric orthogonal idempotents for the adjacency algebra of its corresponding metric scheme.*

Proof. Let X be a distance-regular graph of diameter k, and let $A = A(X)$. By Prop. 4.13, X has $k+1$ distinct eigenvalues. Let $U_0, \ldots, U_k$ be the eigenspaces corresponding to the eigenvalues $\lambda_0, \ldots, \lambda_k$ of X. Let $E_0, \ldots, E_k$ be the orthogonal projections to $U_0, \ldots, U_k$. Since $U_0, \ldots, U_k$ are orthogonal, $E_0, \ldots, E_k$ are mutually orthogonal. Each E_t is a projection, hence idempotent. The operators $E_0, \ldots, E_k$ are symmetric by Fact 2.10. Prop. 4.12 implies $\mathscr{A} = \mathrm{alg}(A)$, where $\mathscr{A}$ is the adjacency algebra of the metric scheme generated by X. By Prop. 2.45, $E_0, \ldots, E_t \in \mathscr{A}$. By Prop. 2.46, the $k+1$ matrices $E_0, \ldots, E_k$ span $\mathscr{A}$. Since $\mathscr{A}$ has dimension $k+1$ by Prop. 2.44, we conclude that $E_0, \ldots, E_k$ is a basis of $\mathscr{A}$. □

Corollary 4.15. *Let $E_0, \ldots, E_k$ be the orthogonal projections to eigenspaces of a distance-regular graph X of diameter k. Let A be the algebra generated by $A(X)$ (and therefore the adjacency algebra of the metric scheme $\mathfrak{M}(X)$). Then for each B in the adjacency algebra of $\mathfrak{M}(X)$, we have*

$$B = \sum_{i=0}^{k} \mu_i E_i \,, \tag{26}$$

where the subspace onto which E_i projects is a subspace of the eigenspace of B corresponding to μ_i.

Proof. Let A be the adjacency matrix of the distance-regular graph X of diameter k. Let λ_j be the eigenvalue of A corresponding to the eigenspace U_j onto which E_j

projects. By Prop. 4.12, $B = \sum_{i=0}^{k} c_i A^i$ for some $c_0, \ldots, c_k \in \mathbb{C}$. By Thm. 4.14,

$$B = \sum_{i=0}^{k} c_i \left(\sum_{j=0}^{k} \lambda_j E_j \right)^i = \sum_{i=0}^{k} c_i \left(\sum_{j=0}^{k} \lambda_j^i E_j \right) = \sum_{j=0}^{k} \left(\sum_{i=0}^{k} c_i \lambda_j^i \right) E_j \tag{27}$$

The value $\sum_{i=0}^{k} c_i \lambda_j^i$ is the eigenvalue of B whose eigenspace contains U_j. □

4.3. **Hamming schemes**

The Hamming schemes are a class of metric schemes which arose from the framework of error-correcting "block codes."

Definition 4.16. The *Hamming graph* $H(n,k)$ is a graph with vertices labeled by strings $B \in [k]^n$, the set of ordered n-tuples of elements from the set $\{0, \ldots, k-1\}$. Given two such strings B_1 and B_2, the vertices v_{B_1} and v_{B_2} are adjacent in $H(n,k)$ if B_1 and B_2 differ in exactly one coordinate.

Observe that the distance between vertices in the Hamming graph is the number of coordinates in which their corresponding strings differ. This is called the *Hamming distance* of the strings.

Fact 4.17. The Hamming graph $H(n,k)$ is distance-transitive.

Corollary 4.18. *The Hamming graph $H(n,k)$ has exactly $n+1$ distinct eigenvalues.*

Proof. The Hamming graph has diameter n, so this follows from Prop. 4.13. □

Definition 4.19. The *Hamming scheme* $\mathfrak{H}(n,k)$ is the metric scheme induced by the distance function on the Hamming graph $H(n,k)$. That is, for $B_1, B_2 \in [k]^n$, we have $c(v_{B_1}, v_{B_2}) = \mathrm{dist}_{H(n,k)}(B_1, B_2)$.

4.4. **Johnson schemes**

A class of metric schemes central to this paper is the Johnson schemes. In statistical literature, Johnson schemes are often referred to as *triangular association schemes*. We begin by defining the underlying graph $J(n,k)$ whose distance function determines the colors of edges in the Johnson scheme $\mathfrak{J}(n,k)$.

Definition 4.20. Let X be a finite set satisfying $|X| = n \geq 2k+1$. The *Johnson graph* $J(X,k) = (\Omega, E)$ is a graph with $\binom{n}{k}$ vertices labeled by the k-subsets of X,

$$\Omega = \left\{ v_T : T \in \binom{X}{k} \right\}. \tag{28}$$

For $S, T \in \binom{X}{k}$ the vertices v_S and v_T are joined by an edge if $|S \backslash T| = |T \backslash S| = 1$, i.e., their intersection is maximal. Since this construction only depends on the size of X up to isomorphism, we write $J(n,k) = J(X,k)$ when we do not want to specify the underlying n-set.

Observation 4.21. For $S, T \in \binom{[n]}{k}$, the distance between v_S and v_T in $J(n,k)$ is

$$\mathrm{dist}_{J(n,k)}(v_S, v_T) = |T \backslash S| = |S \backslash T| \,. \tag{29}$$

Fact 4.22. The Johnson graph $J(n,k)$ is distance-transitive.

Corollary 4.23. *The Johnson graph $J(n,k)$ has exactly $k+1$ distinct eigenvalues.*

Proof. The Johnson graph has diameter k, so this follows from Prop. 4.13. □

Definition 4.24. The *Johnson scheme* $\mathfrak{J}(n,k)$ is the metric scheme generated by the Johnson graph $J(n,k)$. That is, given a finite set X satisfying $|X| = n \geq 2k+1$, the Johnson scheme $\mathfrak{J}(X,k) = \mathfrak{J}(n,k)$ is an association scheme with $\binom{n}{k}$ vertices identified with k-subsets of X. For $S, T \in \binom{X}{k}$, the edge (v_S, v_T) is colored by $|S \backslash T| = i$.

Remark 4.25. For $k \geq 2$, the Johnson scheme $\mathfrak{J}(n,k)$ is a uniprimitive coherent configuration.

5. Full-Rank Inclusion Matrices

5.1. Gottlieb's theorem

In order to construct a common eigenbasis for the Johnson adjacency algebra in Sec. 6, we make use of a full-rank property, known as Gottlieb's theorem, concerning a certain class of systems of linear equations. The matrices corresponding to such systems are *inclusion matrices*, defined in a special case as follows.

Definition 5.1. Fix $k, \ell, n \in \mathbb{Z}$ such that $0 \leq k \leq \ell \leq n$. We define the *Boolean inclusion matrix* to be the $\binom{n}{k} \times \binom{n}{\ell}$ matrix $I_n(k,\ell) = (\zeta_{AB})$ with rows labeled by k-subsets A of $[n]$, columns labeled by ℓ-subsets B of $[n]$, and entries given by

$$\zeta_{AB} = \begin{cases} 1 & \text{if } A \subseteq B \,, \\ 0 & \text{otherwise} \,. \end{cases} \tag{30}$$

Theorem 5.2 (Gottlieb's Theorem)**.** *If $k \leq \ell$ and $k + \ell \leq n$, then the Boolean inclusion matrix $I_n(k,\ell)$ has full row rank.*

A closely related full-rank property for lattices of subspaces of projective geometries that arise from vector spaces over finite fields is Kantor's theorem. In order to state Kantor's theorem., we introduce the general notion of an inclusion matrix.

Definition 5.3. Let $\mathcal{P}$ be a ranked poset, and fix $k, \ell \in \mathbb{Z}$ such that $0 \leq k \leq \ell$. Let w_i denote the number of elements in $\mathcal{P}$ of rank i. Then the *inclusion matrix* $I_{\mathcal{P}}(k,\ell) = (\zeta_{ab})$ is a $w_k \times w_\ell$ matrix with rows labeled by rank k elements and columns labeled by rank ℓ elements. The entries of $I_{\mathcal{P}}(k,\ell)$ are given by

$$\zeta_{ab} = \begin{cases} 1 & \text{if } a \leq b \,, \\ 0 & \text{otherwise} \,, \end{cases} \tag{31}$$

where $a, b \in \mathcal{P}$, $\mathrm{rk}(a) = k$, and $\mathrm{rk}(b) = \ell$.

Theorem 5.4 (Kantor's Theorem)**.** *Let $\mathscr{L}$ be the lattice of subspaces of a finite-dimensional vector space over a finite field. If $k \leq \ell$ and $k + \ell \leq n$, then $I_{\mathscr{L}}(k,\ell)$ has full row rank.*

A lattice-theoretic generalization of both Gottlieb's and Kantor's theorems was found by Barry Guiduli, which we describe in Sec. 5.4.

5.2. **Lattices**

We begin by introducing some concepts in lattice theory.

Definition 5.5. A *lattice* is a poset $\mathscr{L} = (\mathscr{L}, \leq)$ such that every element has a unique meet and join, that is,

$$a \wedge b = \max\{c \in \mathscr{L} : c \leq a, b\}\,, \tag{32}$$

$$a \vee b = \min\{c \in \mathscr{L} : c \geq a, b\}\,. \tag{33}$$

Definition 5.6. A lattice $\mathscr{L}$ is called *bounded* if there exists two elements, denoted by 0 and 1, such that for all $a \in \mathscr{L}$, we have

(1) $a \wedge 1 = a$ and $a \vee 1 = 1\,,$

(2) $a \wedge 0 = 0$ and $a \vee 0 = a\,.$

We will only be considering finite lattices, which are necessarily bounded. A meet-semilattice is a poset where every element need only have a unique meet. A join-semilattice is defined analogously, and its dual is a meet-semilattice.

Definition 5.7. Fix two distinct elements a, b of the lattice $\mathscr{L}$. We say that b *covers* a if $b > a$ and there is no $c \in \mathscr{L}$ such that $b > c > a$.

Definition 5.8. A lattice $\mathscr{L}$ is called *ranked* if it can be equipped with a rank function $\mathrm{rk} : \mathscr{L} \to \mathbb{Z}_{\geq 0}$ compatible with the ordering, i.e, $a < b$ implies $\mathrm{rk}(a) < \mathrm{rk}(b)$, such that if b covers a, then $\mathrm{rk}(b) = \mathrm{rk}(a) + 1$. The *rank* of an element $a \in \mathscr{L}$ is the value of the rank function when evaluated at a.

Definition 5.9. Let a be an element of a lattice $\mathscr{L}$. An element b is called a *complement* of a if $a \wedge b = 0$ and $a \vee b = 1$.

Definition 5.10. We call a bounded lattice *complemented* if every element has a complement.

Definition 5.11. A lattice is called *modular* if it satisfies the modular law

$$x \leq b \Rightarrow x \vee (a \wedge b) = (x \vee a) \wedge b\,. \tag{34}$$

Remark 5.12. An equivalent dual statement of the modular law is

$$x \geq b \Rightarrow x \wedge (a \vee b) = (x \wedge a) \vee b\,. \tag{35}$$

Next, we will look at two examples of modular complemented lattices which will have particular relevance to our later results.

Definition 5.13. Let X be any set of size n. The Boolean lattice $\mathcal{B}_n$ is the lattice of subsets of X, ordered by inclusion.

Observation 5.14.

$$I_n(k, \ell) = I_{\mathcal{B}_n}(k, \ell) \tag{36}$$

Proposition 5.15. *Fix $k > t > s$. Then*

$$I_{\mathcal{B}_n}(s,k) = \binom{k-t}{t-s} I_{\mathcal{B}_n}(k,t) I_{\mathcal{B}_n}(t,s) \tag{37}$$

Proof. Fix an s-subset S and a k-subset K. There are $\binom{k-t}{t-s}$ t-subsets contained in K which contain S. □

This will be used later in Cor. 6.5

The Boolean lattice is ranked, and the rank of an element $S \subseteq X$ is $|S|$. The Boolean lattice is also complemented, and the complement of an element S is $X \backslash S$. The "meet" operation is the intersection, and analogously the "join" operation is the union.

We will also consider the lattices of subspaces of finite-dimensional projective geometries, ordered by inclusion. For the definition of a projective geometry, see Sec. 1.2 of [6]. We describe the special case of projective geometries over finite fields.

Example 5.16. Let V be a vector space of dimension $n+1$ over a finite field $GF(q)$. The subspaces of this space form a projective geometry, and the lattice of the subspaces ordered by inclusion, denoted $PG(n,q)$, is ranked, modular, and complemented.

It is known that any finite projective geometry of dimension at least 3 arises from a vector space, but this is false for dimension 2.

Definition 5.17. A *finite projective plane* is a finite set Ω of points along with a set $\mathscr{S} \subseteq \mathfrak{P}(\Omega)$ of lines. The points and lines must satisfy the following axioms.

(1) Every pair of points is contained in a line.

(2) Two lines intersect in exactly one point.

(3) There exists a set of four points, no three of which are contained in a line.

The projective geometries of dimension 2 are precisely the projective planes.

The lattice of subspaces of any finite-dimensional projective geometry is ranked, and the rank of an element is its dimension. Such a lattice is also complemented. In the case that the projective geometry arises from a vector space W, a complement of a subspace is found by extending a basis B of the subspace to a basis B' of W and taking the span of the extension $B' \backslash B$. In the case of projective planes, a line and any point not contained in that line are complements.

Both $\mathcal{B}_n$ and the lattice of subspaces of any finite-dimensional projective geometry are modular.

Fact 5.18. All bounded modular lattices are ranked.

The finite-dimensional modular complemented lattices were entirely classified in the 1930s.

Theorem 5.19 (Birkhoff–Menger)**.** *Every finite-dimensional complemented modular lattice is isomorphic to the direct product of simple finite-dimensional complemented modular lattices, which are the two-element Boolean lattice and lattices of subspaces of finite-dimensional projective geometries.*

For the proof of Thm. 5.19, see Dilworth's "Note on Modular Complemented Lattices" [13].

5.3. **A property of modular complemented lattices**

We shall derive Gottlieb's and Kantor's theorems from a theorem of B. Guiduli, which uses a somewhat technical hypothesis on semilattices ("rank-regularity"). In this section we show that rank-regular modular complemented lattices satisfy a positivity condition required by Guiduli's result.

The following definition is a condition on the symmetry of a semi-lattice that is a critical hypothesis for the main result of this section.

Definition 5.20 (Guiduli)**.** We call a ranked semi-lattice *rank-regular* if for every $(i, j, k, \ell) \in \mathbb{Z}^4$ there exists a value $s_{ijk\ell}$ such that for every a and b, if $\mathrm{rk}(a) = \mathrm{rk}(c) = k$ and $\mathrm{rk}(a \wedge c) = i$ then we have

$$\#\{b : \mathrm{rk}(b) = \ell, b \geq a, \mathrm{rk}(b \wedge c) = j\} = s_{ijk\ell}\,. \tag{38}$$

Proposition 5.21. *Let $\mathscr{L}$ be a ranked meet-semilattice. Suppose $\mathscr{L}$ admits a group G of automorphisms such that for all k and i, G is transitive on the pairs $\{(a, b) : rk(a) = rk(b) = k, rk(a \wedge b) = i\}$. Then $\mathscr{L}$ is rank-regular.*

This is a classic example of a symmetry condition which implies regularity. It follows that the Boolean lattice $\mathcal{B}_n$ and the lattice of subspaces over a finite field $PG(n)$ are rank-regular. However, symmetry is not necessary; e.g., consider the finite projective planes.

Fact 5.22. Every point in a projective plane is contained in the same number of lines. If every point is contained in m lines, then every line has m points, there are $n = m^2 - m + 1$ points, and the number of lines is the same as the number of points.

Proposition 5.23. *Every finite projective plane is rank-regular.*

Proof. Let P be a projective plane with vertex set Ω, and let m denote the number of lines through any point. Note that we require $i \leq j \leq k \leq \ell$ for $s_{ijk\ell}$ to be nonzero. Moreover, if $k = \ell$, $i < k - 1$, or $\ell = 3$ then the value of s_{ijkl} is either 0 or 1. There are four remaining cases to check. We have $s_{1112} = m$, where b (as in Definition 5.20) ranges over all lines, and $s_{0001} = |\Omega| = m^2 - m + 1$, where b ranges over all points. Moreover, $s_{0012} = m - 1$ and $s_{0112} = 1$ because there is a unique line through each pair of distinct points. □

While the main results of this paper are direct consequences of existing theory, the next observation appears to be new.While the main results of this paper are direct consequences of existing theory, the next observation appears to be new.

Lemma 5.24 (Babai-Burcroff)**.** *Let $\mathscr{L}$ be a modular complemented rank-regular lattice such that $|\mathscr{L}| = n$. Then for any fixed $k \leq \ell \leq \frac{n}{2}$, we have $s_{iik\ell} > 0$ for all $i \leq k$.*

Proof. This is equivalent to showing that for any a, b of rank k such that $\mathrm{rk}(a \wedge b) = i$ there exists some $c \geq a$ of rank ℓ such that $c \wedge b = a \wedge b$. Let e be a complement of $(a \vee b)$, and let $d \stackrel{\text{def}}{=} e \vee a$. Immediately we have $d \geq a$ so $d \wedge b \geq a \wedge b$. It is enough to show that $d \wedge b \leq a$, or equivalently $(d \wedge b) \vee a = a$. Using the dual modular law, since $d \geq a$ we have

$$(d \wedge b) \vee a = d \wedge (b \vee a)\,. \tag{39}$$

Rewriting this, and using the dual modular law on $a \vee b \geq a$, we have

$$(b \vee a) \wedge d = (a \vee b) \wedge (e \vee a) = ((a \vee b) \wedge e) \vee a = 0 \vee a = a\,. \tag{40}$$

Thus $d \wedge b = a \wedge b$. Taking any path from a to d, let c be the unique element of rank ℓ along this path. Then $a \wedge b = d \wedge b \geq c \wedge b \geq a \wedge b$, so c is as desired. □

Importantly, our two main examples of lattices, the $\mathcal{B}_n$ and the lattice of subspaces of a projective geometry, satisfy $s_{iik\ell} > 0$, allowing us to apply the next theorem of Guiduli.

5.4. **Inclusion matrices of full rank**

The following theorem of B. Guiduili, which can be found in Chapter 9 Section 2 of [5], combined with Lemma 5.24, includes both Gottlieb's Theorem and Kantor's Theorem (see Thms.5.2 and 5.4). The proof generalizes the approach of Graver and Jurkat [16] (1973). For the definition of an inclusion matrix, see Definition 5.3.

Theorem 5.25 (Guiduli, 1992)**.** *Let $\mathscr{L}$ be a rank-regular semi-lattice and fix $0 \leq k \leq \ell \leq \frac{n}{2}$. Let $s_{ij} = s_{ijk\ell}$ and assume that $s_{ii} > 0$ for all $i = 0, \cdots, k$. Then the matrix $I_{\mathscr{L}}(k, \ell)$ has full row rank.*

Proof. Let $M = I_{\mathscr{L}}(k, \ell)$. To show that M has full row rank, it is enough to construct a $w_\ell \times w_k$ matrix N such that $MN = I_{w_k}$. Let $N = (n_{bc})$, where $b, c \in \mathcal{P}$, $\mathrm{rk}(b) = \ell$, and $\mathrm{rk}(c) = k$. In other words, it is sufficient to choose the entries of N such that

$$(MN)_{ac} = \delta_{ac}\,, \tag{41}$$

where $\mathrm{rk}(a) = \mathrm{rk}(c) = k$ and δ_{ac} is the Kronecker delta function on rank k elements of $\mathcal{P}$. Moreover, our construction of N will satisfy the additional restraint that n_{bc} depends only on $\mathrm{rk}(b \wedge c)$, i.e., $n_{bc} = t_{\mathrm{rk}(b \wedge c)}$. Fix a, c of rank k in $\mathcal{P}$, and let $i = \mathrm{rk}(a \wedge c)$. We have:

$$(MN)_{ac} = \sum_{\substack{b \\ \mathrm{rk}(b)=\ell}} m_{ab} n_{bc} = \sum_{j=0}^{k} t_j \sum_{\substack{b \\ \mathrm{rk}(b)=\ell \\ \mathrm{rk}(b \wedge c)=j}} m_{ab} = \sum_{j=0}^{k} s_{ij} t_j\,, \tag{42}$$

where the last inequality follows because the number of b such that $b \geq a$, $\mathrm{rk}(b) = \ell$, $\mathrm{rk}(b \wedge c) = j$, and $rk(a \wedge c) = i$ is precisely s_{ij}. We want to show the existence of

a solution to the system of $k+1$ linear equations in the $k+1$ unknowns $t_0, \ldots, t_k$ given by

$$\sum_{j=0}^{k} s_{ij} t_i = \delta_{ik} \quad (\text{for } 0 \le i \le k)\,. \tag{43}$$

If $i > 0$ then $s_{ij} = 0$, and by hypothesis if $i = j$ then $s_{ij} > 0$. This shows that the matrix corresponding to this system $S = (s_{ij})$ is an upper triangular matrix with nonzero diagonal entries. Therefore this system is solvable, hence such an N exists. We can conclude that M has full row rank. □

Corollary 5.26 (Gottlieb's Theorem)**.** *Let $\mathscr{L}$ be the Boolean lattice $\mathcal{B}_n$. If $k \le \ell$ and $k + \ell \le n$, then $I_{\mathscr{L}}(k, \ell)$ has full row rank.*

Corollary 5.27. *Let $\mathscr{L}$ be the lattice of subspaces of a finite-dimensional projective geometry. If $k \le \ell$ and $k + \ell \le n$, then $I_{\mathscr{L}}(k, \ell)$ has full row rank.*

Proof. In both cases, $\mathscr{L}$ is rank-regular. By Lemma 5.24, $s_{iik\ell} > 0$ for every $i \in \{0, \cdots, k\}$. □

Remark 5.28. Kantor's theorem (see Thm. 5.4) is a special case of Cor. 5.27. However, the only additional information in Cor. 5.27 is that the incidence matrices of finite projective planes are non-singular, a well-known fact that can be easily verified directly.

6. Common Eigenbasis Construction for the Johnson Adjacency Algebra

6.1. Matrices in the Johnson adjacency algebra

Let A_i be the adjacency matrix of the color-i constituent of the Johnson scheme $\mathfrak{J}(n, k)$. Our goal is to calculate the eigenvalues of any linear combination M of the matrices $A_0, \cdots, A_{r-1}$. These linear combinations are precisely the matrices in the adjacency algebra of the Johnson scheme. To do so, it is sufficient to find a common eigenbasis for the adjacency algebra of the Johnson scheme and compute the eigenvalues of the basis $A_0, \ldots, A_{r-1}$.

Let X be a set of size n, and let $\binom{X}{k}$ be the set of k-subsets of X. The entries of matrices in the Johnson adjacency algebra, where the rows and columns are indexed by $A, B \in \binom{X}{k}$, depend only on the intersection size $|A \cap B|$ of the subsets.

Notation 6.1. Fix $n, k \in \mathbb{N}$ such that $k \le \lfloor \frac{n}{2} \rfloor$. Let $f : [k] \to \mathbb{C}$ be an arbitrary function. Define the $\binom{n}{k} \times \binom{n}{k}$ matrix M by

$$M = (m_{AB}) = (f(|A \cap B|))\,, \tag{44}$$

where A and B range over all elements of $\binom{[n]}{k}$.

We are interested in which functions f will result in an integral spectrum for M. The original question, asked by Tusnády, was the case $f(\ell) = \dbinom{\ell}{r}$ for some $r \in \mathbb{Z}_{\ge 0}$.

The next few sections are devoted to constructing a common eigenbasis for $\mathscr{A}$ and computing the eigenvalues of M.

6.2. **Construction of eigenspaces via a subset-weight system**

We think of vectors in $\mathbb{C}^{\binom{n}{k}}$ as weightings on the k-subsets of $[n]$. For $t < k$, a weighting on the k-subsets induces a weighting on the t-subsets by setting the weight of a t-subset T to be the sum of the weights of all the k-subsets containing T. We call a weighting on t-subsets *trivial* if the weight of every t-subset is 0. In this section, we construct $k+1$ mutually orthogonal subspaces $U_0, \cdots, U_k$ of $\mathbb{C}^{\binom{n}{k}}$ such that the weighting on k-subsets associated with each vector in U_t induces the trivial weighting on $(t-1)$-subsets. It will be shown in Sec. 7.1 that $U_0, \ldots, U_k$ are precisely the eigenspaces of the Johnson graph.

In his famous paper "On the Shannon Capacity of a Graph" [18], Lovász computed the eigenvalues of the Kneser graph, the color-k constituent of the Johnson scheme, in order to prove an upper bound on its Shannon capacity. We follow Lovász's construction of eigenvectors to construct the subspaces $U_0, \cdots, U_k$.

Definition 6.2. We call a function $w : \binom{X}{t} \to \mathbb{C}$ a *weight system on t-tuples.*

Definition 6.3. Fix $s, t \in \mathbb{Z}_{\geq 0}$ such that $s < t$. Given a weight system w on t-tuples, the *induced weight system* $\widehat{w} : \mathfrak{P}(X) \to \mathbb{C}$ is defined by

$$\widehat{w}(S) = \sum_{\substack{T \supseteq S \\ T \in \binom{X}{t}}} w(T) \tag{45}$$

if $|S| \leq t$, and by

$$\widehat{w}(S) = \sum_{T \in \binom{S}{t}} w(T) \tag{46}$$

if $|S| > t$.

Observation 6.4. Fix $s \in [k+1]$. Let $\widehat{w}_s$ denote the restriction of $\widehat{w}$ to $\binom{X}{s}$. Given a weight system w on t-tuples, then

$$\widehat{w}_s = I_{\mathcal{B}_n}(s,t) \tag{47}$$

if $s \leq t$, and

$$\widehat{w}_s = I_{\mathcal{B}_n}(t,s)^{\mathrm{tr}} \tag{48}$$

if $s > t$.

Corollary 6.5. *Let $k > t \geq 0$. If w is a good weight system on t-subsets, then by Prop. 5.15 the induced weight system on k-subsets induces the trivial weight system on $(t-1)$-subsets.*

Proof. This follows from Prop. 5.15. □

Definition 6.6. We call a weight system w on t-tuples *good* if the induced weight system $\widehat{w}$ on $(t-1)$-tuples satisfies

$$\widehat{w}(S) = 0 \tag{49}$$

for each $S \in \binom{X}{t-1}$.

Proposition 6.7. *The system* $\{\widehat{w}(S) = 0\}_{S\in\binom{X}{t-1}}$ *of equations has full row rank, where the values of the weight system* w *on* t*-tuples are treated as the unknowns.*

Proof. The matrix associated with this system is precisely $I_{\mathcal{B}_n}(t-1,t)$. Since $t \le k \le \frac{n}{2}$, by Thm. 5.2 (Gottlieb's Theorem), this system has full row rank. □

Corollary 6.8. *The good weight systems on* t*-tuples form a subspace of* $\mathbb{C}^{\binom{n}{t}}$ *of dimension* $\binom{n}{t} - \binom{n}{t-1}$.

Proof. The set of good weight systems is the kernel of $\{\widehat{w}(S) = 0\}_{S\in\binom{X}{t-1}}$. □

Lemma 6.9. *Let* w *be a good weight system. For any* $m < t$*, the induced weight system* $\widehat{w}$ *maps every* m*-subset to* 0.

Proof. Fix $U \in \binom{X}{m}$. Then

$$(t-m)\sum_{\substack{T\in\binom{X}{t}\\ T\supseteq U}} w(T) = \sum_{\substack{S\in\binom{X}{t-1}\\ S\supseteq U}}\ \sum_{\substack{T\in\binom{X}{t}\\ T\supseteq S}} w(T) = \sum_{\substack{S\in\binom{X}{t-1}\\ S\supseteq U}} \widehat{w}(S) = 0\,. \tag{50}$$

Since $t-m>0$, dividing by $t-m$ shows that the induced weight on any m-subset is 0. □

Definition 6.10. For $t = 0,\dots,k$, define the subspace U_t of $\mathbb{C}^{\binom{n}{k}}$ as follows. If w is a good weight system on t-tuples, then let $(\overline{x}(w)) \in \mathbb{C}^{\binom{n}{k}}$ be a weight system on k-tuples with entry $\overline{x}(w)_A = \widehat{w}(A)$ for $A \in \binom{X}{k}$. Then we define

$$U_t = \{\overline{x}(w) :\ w \text{ is a good weight system on } t\text{-tuples}\}. \tag{51}$$

Proposition 6.11. *The dimension of* U_t *is* $\binom{n}{t} - \binom{n}{t-1}$.

Proof. The map from $\mathbb{C}^{\binom{X}{t}}$ to $\mathbb{C}^{\binom{X}{k}}$ defined by $w \mapsto \overline{x}(w)$ is injective on all weight systems on t-tuples. This follows from Gottlieb's theorem, since the matrix associated with map $w \mapsto \overline{x}(w)$ is $I_{\mathcal{B}_n}(t,k)$, which has full column rank. The restriction of this map to good weight systems on t-tuples is also injective, so the result follows from Cor. 6.8. □

Lemma 6.12. *Let* w *be a good weight system on* t*-tuples. Fix* $s \in \mathbb{Z}_{\ge 0}$ *such that* $s < t$*, and let* S *be an* s*-subset of* X*. Then*

$$\sum_{\substack{T\in\binom{X}{t}\\ |S\cap T|=m}} w(T) = 0 \tag{52}$$

Proof. Let $c_m = \sum_{\substack{T\in\binom{X}{t}\\ |S\cap T|=m}} w(T)$ for all $m \in [s+1]$. The equality

$$0 = \sum_{R\in\binom{S}{m}}\ \sum_{\substack{T\in\binom{X}{t}\\ T\supseteq R}} w(T) = \sum_{i=m}^{s}\binom{i}{m}c_i \tag{53}$$

follows from calculating the coefficient of $w(T)$ on each side for $T \in \binom{X}{k}$ such that $|T\cap S| = i$ and from noting that the inner sums in the second expression are all 0

by Lemma 6.9. The last expression is a triangular linear system with all diagonal entries being 1, so we can conclude that $c_0 = \cdots = c_s = 0$. □

Theorem 6.13. *The subspaces $U_0, \ldots, U_k$ are mutually orthogonal.*

Proof. Fix $s, t \in [k+1]$ such that $s < t$. Let $\overline{x}_u \in U_s$ and $\overline{y}_w \in U_t$. Then

$$\overline{x}_u \cdot \overline{y}_w = \sum_{A \in \binom{X}{k}} \left(\sum_{S \in \binom{A}{s}} u(S) \right) \left(\sum_{T \in \binom{A}{t}} w(T) \right) \tag{54}$$

$$= \sum_{S \in \binom{A}{s}} u(S) \sum_{m=0}^{t} \binom{n-s-t+m}{k-s-t+m} \sum_{\substack{T \in \binom{X}{t} \\ |S \cap T| = m}} w(T)\,. \tag{55}$$

The inner sums in Equation (55) are all 0 by Lemma 6.12. Thus $\overline{x}_u \cdot \overline{y}_w = 0$. □

7. Eigenvalues of Matrices in the Johnson Adjacency Algebra

7.1. Computing eigenvalues

In this section, we show that the union of bases of $U_0, \ldots, U_k$ forms a common eigenbasis for $A_0, \ldots, A_k$. Thus to find the eigenvalues of any matrix in the adjacency algebra, it is enough to find the eigenvalues of the basis $A_0, \ldots, A_k$. Let $\overline{x} \in \mathbb{C}^{\binom{n}{k}}$ be any nonzero vector in U_t, constructed as in Sec. 6.2, with corresponding weight function w, and let $\overline{y} = A_{k-\ell}\overline{x}$. We can expand the entry of $\overline{y}$ labeled by $A \in \binom{X}{k}$ by

$$\overline{y}_A = \sum_{\substack{B \in \binom{X}{k} \\ |A \cap B| = \ell}} \sum_{T \in \binom{B}{t}} w(T)\,. \tag{56}$$

The number of occurences of $w(T)$ in the right hand side of the above sum is determined by $m \stackrel{\text{def}}{=} |T \cap A|$. In particular, $w(T)$ will occur $\binom{k-m}{\ell-m}\binom{n-k+m-t}{k-\ell+m-t}$ times. This coefficient comes from choosing $\ell - m$ elements from $A \backslash T$, followed by $k - \ell - (t-m)$ elements from $X \backslash (A \cup T)$. Note that $m \leq \ell \leq k$. Reindexing the above rightmost sum by m gives us the following.

$$\overline{y}_A = \sum_{m=0}^{\ell} \binom{k-m}{\ell-m}\binom{n-k+m-t}{k-\ell+m-t} \sum_{\substack{T \in \binom{X}{t} \\ |T \cap A| = m}} w(T) \tag{57}$$

It remains to compute the rightmost sum above. For $m \leq t$, we denote this term by

$$s_m = \sum_{\substack{T \in \binom{X}{t} \\ |T \cap A| = m}} w(T)\,. \tag{58}$$

Observe that $S_t = \overline{x}_A$. Summing the weights of all t-subsets containing a given m-subset of A, for $m < t$, then summing this quantity over all m-subsets of A, we

find that $w(T)$ is counted with multiplicity $\binom{|T \cap A|}{m}$. The inner sums must all evaluate to 0 by Lemma 6.9, since this quantity is merely the induced weight on the given m-subset. This results in the following identity for $m < t$.

$$\sum_{R \in \binom{A}{m}} \sum_{\substack{T \in \binom{X}{t} \\ T \supseteq R}} w(T) = \sum_{i=0}^{t-m} \binom{t-i}{m} s_{t-i} = 0\,. \tag{59}$$

Proceeding with the inductive step, we have

$$s_m = -\sum_{i=0}^{t-m-1} \binom{t-i}{m} s_{t-i} \tag{60}$$

$$= -\sum_{i=0}^{t-m-1} (-1)^i \binom{t-i}{m} \binom{t}{i} \overline{x}_A \tag{61}$$

$$= -\overline{x}_A \cdot \sum_{i=0}^{t-m-1} (-1)^i \binom{t}{m} \binom{t-m}{i} \tag{62}$$

$$= -\binom{t}{m} \overline{x}_A \cdot \sum_{i=0}^{t-m-1} (-1)^i \binom{t-m}{i} \tag{63}$$

$$= -\binom{t}{m} \overline{x}_A \cdot (-1)^{t-m-1} \binom{t-m-1}{t-m-1} \tag{64}$$

$$= (-1)^{t-m} \binom{t}{m} \overline{x}_A\,, \tag{65}$$

where we use the identity $\binom{n}{h}\binom{n-h}{k} = \binom{n}{k}\binom{n-k}{h}$ in Equation (62) and $\sum_{j=0}^{k}(-1)^j\binom{n}{j} = (-1)^k\binom{n-1}{k}$ in Equation (64).

Combining the above equations gives us

$$\overline{y}_A = \sum_{m=0}^{\ell} \binom{k-m}{\ell-m} \binom{n-k+m-t}{k-\ell+m-t} s_m \tag{66}$$

$$= \sum_{m=0}^{\ell} (-1)^{t-m} \binom{k-m}{\ell-m} \binom{n-k+m-t}{k-\ell+m-t} \binom{t}{m} \overline{x}_A\,. \tag{67}$$

Proposition 7.1. *The union of bases of the subspaces $U_0, \ldots, U_k$, constructed as in Sec. 6.2, forms a common eigenbasis for the Johnson adjacency algebra.*

Proof. By Equation (67), each $U_0, \ldots, U_k$ is a subspace of an eigenspace of $A_{k-\ell}$. Moreover, the subspaces $U_0, \ldots, U_k$ are mutually orthogonal by Prop. 6.13, and their dimensions sum to $\binom{n}{k}$ by Cor. 6.8. Therefore the union of bases for $U_0, \ldots, U_k$ forms a basis for $\mathbb{C}^{\binom{n}{k}}$ and each member is a common eigenvector for $A_0, \ldots, A_k$, hence the entire Johnson adjacency algebra. □

Corollary 7.2. *$U_0, \ldots, U_k$ are precisely the eigenspaces of A_1.*

Proof. By Prop. 7.1, each U_t ($t \in [k+1]$) is a subspace of an eigenspace of A_1 and $U_0, \ldots, U_k$ form a basis for $\mathbb{C}^{\binom{n}{k}}$. By Prop. 4.13, A_1 has precisely $k+1$ eigenvalues. Thus each U_t is an eigenspace, and every eigenspace must contain U_t for some t. □

We now summarize the main structural theorem for the adjacency algebra of the Johnson scheme.

Corollary 7.3. *Let E_i denote the orthogonal projection to U_i. Then $E_0, \ldots, E_k$ form the basis of symmetric orthogonal idempotents of the adjacency algebra of the Johnson scheme.*

Proof. This follows directly from Cor. 7.2 and Thm. 4.14. □

7.2. **Eigenvalues and Eberlein polynomials**

Theorem 7.4. *The eigenvalues $\lambda_1, \ldots, \lambda_k$, not necessarily distinct, of $A_{k-\ell}$ are given by*

$$\lambda_t = \sum_{m=0}^{t} (-1)^{t-m} \binom{k-m}{\ell-m} \binom{n-k+m-t}{k-\ell+m-t} \binom{t}{m} . \tag{68}$$

Proof. This follows from Equation (67) and Prop. 7.1. Note that the last term in the inner sum is 0 for $m > t$, so we have reindexed the inner sum from its form in Equation (67). □

Corollary 7.5. *The eigenvalues of a matrix M in the adjacency algebra of $\mathfrak{J}(n,k)$, where*

$$M = \sum_{\ell=0}^{k} f(\ell) A_{k-\ell} , \tag{69}$$

are given by $\lambda_0, \cdots, \lambda_k$, not necessarily distinct, where

$$\lambda_t = \sum_{\ell=0}^{k} f(\ell) \sum_{m=0}^{t} (-1)^{t-m} \binom{k-m}{\ell-m} \binom{n-k+m-t}{k-\ell+m-t} \binom{t}{m} . \tag{70}$$

The dimension of the eigenspace corresponding to an eigenvalue μ is

$$\sum_{\substack{t \in \{0,\ldots,k\} \\ \lambda_t = \mu}} \binom{n}{t} - \binom{n}{t-1} . \tag{71}$$

Proof. Since the eigenbasis we constructed is a common eigenbasis of the Johnson adjacency algebra, the eigenvalues of any element are given by the associated linear combination of λ_t, computed in Thm. 7.4, for each element of the basis $A_0, \cdots, A_k$. The dimension of the eigenspace follows from Props. 6.11 and 7.1. □

Definition 7.6. The *Eberlein polynomial* $\mathcal{E}_k^{\ell,n}(t)$ is defined by

$$\mathcal{E}_k^{\ell,n}(t) = \sum_{m=0}^{t} (-1)^{t-m} \binom{k-m}{\ell-m} \binom{k-t}{m} \binom{n-k+m-t}{m} \tag{72}$$

$$= \sum_{m=0}^{\ell} (-1)^{m} \binom{t}{m} \binom{k-t}{\ell-m} \binom{n-k-t}{\ell-m}, \tag{73}$$

where $\ell \leq k \leq n$. The second form is also referred to as the *dual-Hahn polynomial*.

Corollary 7.7. *The eigenvalues $\lambda_1, \ldots, \lambda_k$ of A_i are given by*

$$\lambda_t = \mathcal{E}_k^{k-i,n}(t) \tag{74}$$

for $0 \leq t \leq k$.

Proof. Compare with the result of Thm. 7.4. □

Corollary 7.8. *Certain values of the Eberlein polynomials produce the p-numbers (see Definition 3.27) of the adjacency algebra of the Johnson scheme $\mathfrak{J}(n,k)$. Specifically,*

$$p_i(j) = \mathcal{E}_k^{i,n}(j)\,. \tag{75}$$

Proof. This follows from Prop. 3.28 and Cor. 7.7. □

It is proven in the "Association Schemes and Coding Theory" Sec. of Chapter 5 in [1] that the Eberlein polynomials are an orthogonal family with respect to the weight concentrated on the finite set $\{t_i = i(n+1-i) : i = 0, \ldots, n\}$ with weighting function $w(t_i) = \binom{n}{i} - \binom{n}{i-1}$.

7.3. **Conditions for the integrality of eigenvalues**

The formula in Thm. 7.5 for the eigenvalues of matrices in the Johnson adjacency algebra gives us some nice conditions for the integrality of spectra.

Corollary 7.9. *If f is integer-valued, then the spectrum is integral.*

In particular, Tusnády's matrix where $f(\ell) = \binom{\ell}{r}$ for some parameter r will always have integral eigenvalues.

Corollary 7.10. *If*

$$f(\ell) \cdot \mathcal{E}_k^{k-\ell,n}(t) \in \mathbb{Z} \tag{76}$$

for all $t, \ell \leq k$, then the spectrum is integral.

Corollary 7.11. *There is a infinite class of matrices over $\mathbb{R}$, each in the adjacency algebra of a Johnson scheme, with at least one non-integer entry whose eigenvalues are integral.*

Proof. For fixed values of k_0,t_0, and ℓ_0 satisfying $0 < t_0, \ell_0 < k_0$, the Eberlein polynomial $\mathcal{E}_{k_0}^{k_0-\ell_0,n}(t_0)$ has finite degree in the variable n. Therefore there exist infinitely many n such that $|\mathcal{E}_{k_0}^{k_0-\ell_0,n}(t_0)| \geq 2$. Let $f(\ell_0) = \left(\mathcal{E}_{k_0}^{k_0-\ell_0,n}(t_0)\right)^{-1}$ and set $f(\ell) = 0$ for all $\ell \neq \ell_0$. Then the matrix M, constructed as in Cor. 7.5, has integer eigenvalues with at least one non-integer entry. □

Corollary 7.12. *If we allow f to depend on the parameter n, so $f = f_n$, then to have all $\lambda_t \in \mathbb{Z}$ it is necessary that $f_n(0), f_n(n) \in \mathbb{Z}$.*

Proof. This is observed from evaluating λ_0 and λ_k, respectively. □

Corollary 7.13. *If f is independent of n and k, then the condition that f is integer-valued is both necessary and sufficient.*

Proof. By Cor. 7.12, we must have $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}_{\geq 0}$. □

Acknowledgments

I would like to thank my mentor, Prof. László Babai, for his incredible patience and guidance. He has been more than generous with his time in advising me, capturing my interest through challenge problems, and answering my many questions. In addition, he has worked tirelessly to help edit this paper, and his suggestions have made all the difference. I am grateful to the Budapest Semesters in Mathematics program, which I attended in the summer of 2016, for introducing me to the fascinating field of combinatorics. In particular, I extend my gratitude to Prof. Dezső Miklós for his mentorship during the summer of 2016. I would also like to thank Professor Peter May and all the lecturers for the work they have put in to make this wonderful UChicago Math REU program a reality for the past 18 years.

References

[1] Richard Askey (ed.). Theory and Application of Special Functions: Proceedings of an Advanced Seminar sponsored by the Mathematics Research Center. *The University of Wisconsin-Madison*, 1975.

[2] László Babai. Graph Isomorphism in Quasipolynomial Time. `arXiv:1512.03547 [cs.DS]`, 2016. Updated version (`http://people.cs.uchicago.edu/~laci/17groups/version2.1.pdf`). Downloaded Aug 25, 2017.

[3] László Babai. Automorphism Groups, Isomorphism, Reconstruction. *The Handbook of Combinatorics (Chapter 27)*, 1995.

[4] László Babai. Almost All Steiner Triple Systems Are Asymmetric. *Annals of Discrete Mathematics*, Vol 7, pages 37-39,1980.

[5] László Babai and Péter Frankl. Linear Algebra Methods in Combinatorics (Preliminary Version 2). *The University of Chicago Dept. of Computer Science*, 1992.

[6] Albrecht Beutelspacher and Ute Rosenbaum. Projective Geometry: From Foundations to Applications. *Cambridge University Press*, 1998.

[7] Garrett Birkhoff. Combinatorial Relations in Projective Geometries. *Annals of Mathematics*, Vol 36, pages 743-748, 1935.

[8] Raj Bose. A Note on Fisher's Inequality for Balanced Incomplete Block Designs. *Annals of Mathematical Statistics*, Vol 20, pages 619-620, 1949.

[9] Andries E. Brouwer. Coherent Configurations (Course Notes). *Technische Universiteit Eindhoven*, `https://www.win.tue.nl/~aeb/2WF02/cohconf.pdf`, 2002.

[10] Henry Cohn and Christopher Umans. Fast Matrix Multiplication Using Coherent Configurations. *Proc. 24th ACM-SIAM Symp. on Discrete Algorithms (SODA'13)*, pages 1074-1086, 2013.

[11] Philippe Delsarte. An Algebraic Approach to the Association Schemes of Coding Theory. *Philips Res. Rep. Suppl.*, Vol 10, 1973.

[12] Philippe Delsarte and Vladimir I. Levenshtein. Association Schemes and Coding Theory. *IEEE Transactions on Information Theory*, Vol 44, pages 2477 - 2504, 1998.

[13] Robert Dilworth. Note on Modular Complemented Lattices. *Bulletin of the American Mathematical Society*, Vol 46, pages 74-76, 1940.

[14] Douglas R. Farenick. Algebras of Linear Transformations. *Springer*, 2001.

[15] Daniel Henry Gottlieb. A Certain Class of Incidence Matrices. *Proceedings of the American Mathematical Society*, Vol 17, pages 1233-1237, 1966.

[16] J.E. Graver and W.B. Jurkat. The Module Structure of Integral Designs. *J. Combin. Th. A*, Vol 15, pages 75-90, 1973.

[17] Donald Higman. Coherent configurations I. *Rendiconti del Seminario Matematico della Universita di Padova*, Vol 44, pages 1-25, 1970.

[18] László Lovász. On the Shannon Capacity of a Graph. *IEEE Transactions in Information Theory*, Vol 25, pages 1-7, 1979.

[19] Raghu Meka and Avi Wigderson. Association Schemes, Non-Commutative Polynomial Concentration, and Sum-of-Squares Lower Bounds for Planted Clique. *Electronic Colloquium on Computational Complexity*, Report No. 105, 2013.

[20] Karl Menger. New Foundations of Projective and Affine Geometry. *Annals of Mathematics*, Vol 37, pages 456-482, 1936.

[21] Issai Schur. A Contribution to Theory of Transitive Permutation Groups. *Sitzungsberichte der Preussischen Akademie der Wissenschaften*, Vol 301, pages 5-34, 1933.

[22] B.L. van der Waerden. Algebra, Vol II. *Springer*, 1991.

[23] Joseph Wedderburn. On Hypercomplex Numbers. *Proceedings of the London Mathematical Society*, Vol s2-6, pages 77-118, 1908.

[24] Boris Weisfeiler and A. A. Leman. Reduction of a Graph to a Canonical Form and an Algebra which appears in the Process (in Russian). *Scientific-Technological Investigations*, Vol 9, pages 12-16, 1968.

[25] Boris Weisfeiler (ed.). On Construction and Identification of Graphs. *Springer Lect. Notes in Math*, Vol 558, 1976.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109

E-mail address: burcroff@umich.edu