

---

# MA 862 : COMBINATORICS II

---

**Amit Rajaraman**

Last updated February 23, 2023

## Contents

<b>1</b>	<b>The Delsarte and Schrijver Bounds</b>	<b>2</b>
1.1	*-algebras of matrices . . . . .	2
1.2	A primer on representation theory . . . . .	8
1.3	The Delsarte Bound . . . . .	12
1.4	The Schrijver Bound . . . . .	14
1.5	Johnson schemes . . . . .	20

## §1. The Delsarte and Schrijver Bounds

### 1.1. \*-algebras of matrices

Denote by  $\mathcal{M}_n(\mathbb{C})$  the  $\mathbb{C}$ -vector space of all  $n \times n$  complex matrices.

**Definition 1.1.** A subspace  $\mathcal{A} \subseteq \mathcal{M}_n(\mathbb{C})$  is said to be a *\*-algebra of matrices* if

1.  $\mathcal{A}$  is closed under multiplication, in that if  $A, B \in \mathcal{A}$ , then  $AB \in \mathcal{A}$ , and
2.  $\mathcal{A}$  is closed under conjugate transposes, in that if  $A = (a_{ij}) \in \mathcal{A}$ , then  $A^\dagger = (\overline{a_{ji}}) \in \mathcal{A}$ .
3.  $\text{Id} \in \mathcal{A}$ .

That is, it is a subalgebra that is closed under conjugate transposes. \*-algebras are also sometimes referred to as *self-adjoint algebras*.

Let  $q$  be a prime power. Denote by  $B_q(n)$  the set of all subspaces of  $\mathbb{F}_q^n$  and  $B_q(n, k)$  the set of all  $k$ -dimensional subspaces of  $\mathbb{F}_q^n$ . It is not too difficult to show that

$$|B_q(n, k)| = \binom{n}{k}_q = \frac{(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-k+1})}{(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})}.$$

We had also considered this quantity  $\binom{n}{k}_q$  in Section 1.4 of [Combinatorics I](#). Recall the  $q$ -Pascal recurrence

$$\binom{n+1}{k}_q = \binom{n}{k-1}_q + q^k \binom{n}{k}_q \quad (1.1)$$

for  $n \geq 0, k \geq 1$  with  $\binom{n}{0}_q = 1$  and  $\binom{0}{k}_q = \delta_{0,k}$ . Is there a way to see this recurrence more directly using the subspace perspective of the  $q$ -binomial coefficient? If we have a (size  $k$ ) basis of a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ , and consider the  $k \times n$  matrix with rows equal to the vectors in this basis, we may bring this matrix to a *unique* row-reduced echelon form (independent of the basis used) using row operations wherein

- (i) all rows are nonzero,
- (ii) the first non-zero entry in every row is a 1. Suppose this entry occurs in column  $C_i$  in row  $i$ ,
- (iii)  $C_1 < C_2 < \cdots < C_k$ , and
- (iv) the submatrix comprising the  $\{C_1, \dots, C_k\}$  columns is a  $k \times k$  identity matrix.

So, we can count  $k \times n$  matrices in RREF instead of subspaces. Equation (1.1) then follows immediately by considering whether the last column is pivotal or not.

**Definition 1.2.** Let  $A$  be Hermitian. Then,  $\langle A \rangle$ , the \*-algebra generated by  $A$ , is  $\text{span}\{\text{Id}, A, A^2, \dots\}$ .

Note that this algebra is abelian. Furthermore, by the spectral theorem,  $\dim(\langle A \rangle)$  is the number of distinct eigenvalues of  $A$ .

If  $A \in \mathcal{M}_n(\mathbb{C})$  is such that  $PAP^{-1}$  is Hermitian, then  $P\langle A \rangle P^{-1}$  is also a \*-algebra.

**Example 1** (\*-algebras on graphs). Let  $G = (V, E)$  be a graph and  $A$  its adjacency matrix.  $\langle A \rangle$  is called the *adjacency algebra* of  $G$ .

More specifically, consider the  $n$ -cube graph  $C_n$  with vertex set  $B(n) = 2^{[n]}$  and an edge between  $X, Y$  if  $|X \Delta Y| = 1$ . Although  $\langle A \rangle$  is  $*$ -algebra of  $2^n \times 2^n$  matrices, its dimension turns out to be only  $n + 1$ . The fact that we only require  $n + 1$  parameters to describe an arbitrary element of  $\langle A \rangle$  is key to the Delsarte bound on binary code size we shall study later.

Let  $k \leq n/2$ . The Johnson graph has vertex set  $B(n, k) = \binom{[n]}{k}$  and an edge between  $X, Y$  if  $|X \cap Y| = k - 1$ . The dimension of this graph's adjacency algebra turns out to be  $k + 1$ .

The Grassmann graph  $J_q(n, k)$  has vertex set  $B_q(n, k)$  (see above the example for definition) with  $X, Y \in B_q(n, k)$  adjacent iff  $\dim(X \cap Y) = k - 1$ . It turns out that the dimension of this graph's adjacency algebra is  $k + 1$  as well. Interestingly, the proof for this ends up just being a " $q$ -analogue" of the proof for the Johnson graph.

The  $q$ -analogue of the  $n$ -cube  $C_q(n)$  has vertex set  $B_q(n)$  with  $X, Y$  adjacent iff  $|\dim X - \dim Y| = 1$ . We do not know the dimension of this graph's adjacency algebra! The adjacency matrix seems difficult to study (and is perhaps not even the right object to study). We shall instead study a weighted adjacency matrix of  $C_q(n)$ .

All the above examples are commutative. **Recall** that a *unitary representation* of a group  $G$  is a group homomorphism  $\varphi : G \rightarrow \mathcal{U}_n(\mathbb{C})$ .

**Theorem 1.3.** Let  $\varphi$  be a unitary representation of a group  $G$ . Then,

$$\mathcal{A} = \{A \in \mathcal{M}_n(\mathbb{C}) : A\varphi(g) = \varphi(g)A \text{ for all } g \in G\}$$

is a  $*$ -algebra called the *commutant* of  $\varphi$ .

*Proof.* It is obvious that  $\mathcal{A}$  is a subspace that is closed under multiplication. We have for  $A \in \mathcal{A}, g \in G$  that

$$\varphi(g^{-1}) = \varphi(g)^{-1} = \varphi(g)^\dagger,$$

so

$$A^\dagger \varphi(g) = (\varphi(g)^\dagger A)^\dagger = (\varphi(g^{-1})A)^\dagger = (A\varphi(g)^{-1})^\dagger = \varphi(g)A^\dagger,$$

which easily yields the desideratum. ■

The above  $*$ -algebra may possibly be non-commutative. Suppose that  $G$  acts on a set  $S$ . For each  $g$ , we can denote the group action by an  $S \times S$  permutation matrix  $\rho(g)$ , with  $(\rho(g))_{gs, s} = 1$ . This gives a *representation*  $\rho : G \rightarrow \mathcal{U}_S(\mathbb{C})$  – any group action thus yields a  $*$ -algebra.

We would like to analyze the set of matrices which commute with all  $\rho(g)$ . Let  $G$  act on the sets  $S, T$ , and let  $\rho : G \rightarrow \mathcal{U}_S(\mathbb{C}), \tau : G \rightarrow \mathcal{U}_T(\mathbb{C})$  be the corresponding maps. Consider

$$\mathcal{A} = \{M \in \mathcal{M}_{T \times S}(\mathbb{C}) : M\rho(g) = \tau(g)M \text{ for all } g \in G\}.$$

Finally, we shall set  $S = T$  so that it is a  $*$ -algebra, which we denote  $\text{Hom}_G(S, S)$ .

**Lemma 1.4.** Let  $M \in \mathcal{M}_{T \times S}(\mathbb{C})$ . Defining  $\mathcal{A}$  as above,  $M \in \mathcal{A}$  iff  $M_{t, s} = M_{gt, gs}$  for all  $g \in G, t \in T, s \in S$ .

*Proof.* The  $t, s$ th entry of  $M\rho(g)$  is equal to  $M_{t,gs}$ , and that of  $\tau(g)M$  is  $M_{g^{-1}t,s}$ . The required follows. ■

Now, the two actions induce an action on  $T \times S$ .  $M$  belongs to  $\mathcal{A}$  iff it is constant on the orbits of this action. Consequently, the dimension of  $\mathcal{A}$  is the number of orbits of the action of  $G$  on  $T \times S$ , with a basis being the set of matrices  $M_j$  which are equal to 1 on precisely those cells in the same orbit  $\theta_j$  and 0 elsewhere.

This basis of  $\mathcal{A}$  is called its *orbital basis*.

**Lemma 1.5** (Gelfand's Lemma). Let  $T = S$  in the above discussion. If each  $M_j$  is symmetric,  $\mathcal{A}$  is commutative.

*Proof.* Since each  $M_j$  is symmetric and orthogonal, all matrices in  $\mathcal{A}$  are symmetric. We are done if we show that a \*-algebra of symmetric matrices is commutative. Indeed,  $MN = (MN)^\top = N^\top M^\top = NM$ . ■

Note that the converse does *not* hold; we shall see a counterexample later. Let us get back to our earlier discussion in Example 1. Think of  $B(n)$  as  $\{0, 1\}^n$ . Consider the *hyperoctahedral group*  $H_n$ , which has base set equal to  $S_2^n \times S_n$ , with elements denoted  $(\sigma_1, \sigma_2, \dots, \sigma_n, \pi)$ . This group acts on  $B(n)$  by first permuting the  $n$  coordinates according to  $\pi$ , then deciding whether or not to flip the entries based on the  $(\sigma_i)$ . Note that adjacency is preserved under the group action. In fact,  $H_n$  is the set of all permutations that preserve adjacency.

The group action can be thought of as first taking the vertex to any other arbitrary vertex, then permuting the  $n$  outgoing edges in some manner – these two together further determine the group element.

Let  $\alpha, \beta, \alpha', \beta' \in B(n)$ . We denote by  $d(\alpha, \beta)$  the set of coordinates where  $\alpha, \beta$  differ. We write  $(\alpha, \beta) \sim (\alpha', \beta')$  if the two are in the same  $H_n$ -orbit.

**Lemma 1.6.**  $(\alpha, \beta)$  and  $(\alpha', \beta')$  are in the same  $H_n$ -orbit iff  $d(\alpha, \beta) = d(\alpha', \beta')$ .

*Proof.* The forward direction is straightforward – permuting the coordinates leaves the distance the same and flipping a select set of coordinates of both also leaves the distance unchanged.

For the backward direction, suppose  $d(\alpha, \beta) = d(\alpha', \beta') = k$ . Consider the permutation applied to  $\alpha$  which has all 0s at the start then all 1s. Then, flip all the 1s in  $\alpha$ . Consider the element  $\beta''$  obtained by performing the same operations on  $\beta$ . Due to the first part,  $\beta''$  has exactly  $k$  1s. Next, permute the coordinates of  $\beta''$  to get  $\beta'''$ , which has all 0s at the start then all 1s.  $(0, \beta''')$  is in the same orbit as  $(\alpha, \beta)$ . By performing similar operations, it is also in the same orbit as  $(\alpha', \beta')$ , completing the proof. ■

Let  $A_0, A_1, \dots, A_n$  be the  $n$  orbital bases of  $B(n) \times B(n)$  under the group action  $H_n$ , defined by

$$A_j(\alpha, \beta) = \begin{cases} 1, & d(\alpha, \beta) = j, \\ 0, & \text{otherwise.} \end{cases}$$

Going back to the perspective of  $B(n)$  containing subsets of  $[n]$ ,

$$A_j(X, Y) = \begin{cases} 1, & |X \triangle Y| = j, \\ 0, & \text{otherwise.} \end{cases}$$

Note that  $A_1$  is the adjacency matrix  $A$  of the  $n$ -cube graph  $C(n)$ !

**Proposition 1.7.** It holds that  $\langle A \rangle = \text{span}\{A_0, A_1, \dots, A_n\}$ .

*Proof.* Denote by  $\mathcal{A}$  the algebra on the right, which is the commutant of the  $H_n$  action on  $B(n)$ . Because  $A_1 = A$  is in  $\mathcal{A}$ ,  $\langle A \rangle \subseteq \mathcal{A}$ . It remains to show the reverse containment, which is implied if we show that  $A_j \in \langle A \rangle$  for each  $j$ . If  $A_j \in \langle A \rangle$ , then  $AA_j$  is just some linear combination of  $A_0, A_1, \dots, A_{j+1}$  (with a positive coefficient on  $A_{j+1}$ ), completing the proof. ■

**Corollary 1.8.** The adjacency matrix  $A$  of the  $n$ -cube graph has  $n + 1$  distinct eigenvalues.

A natural next question is: what are these  $n + 1$  eigenvalues, and what are each of their eigenspaces and multiplicities?

As a little spoiler, we answer these questions: the eigenvectors are  $n - 2k$  for  $k = 0, 1, \dots, n$ , with  $n - 2k$  having multiplicity  $\binom{n}{k}$ . We shall prove this later in \*\*\* SEC ? \*\*\*.

Let us next go back to the example of  $B(n, k)$ .  $S_n$  acts on  $B(n, k)$  with  $\pi \cdot \{i_1, \dots, i_k\} = \{\pi(i_1), \dots, \pi(i_k)\}$ . What are the orbits of this  $S_n$ -action on  $B(n, k) \times B(n, k)$ ?

**Lemma 1.9.** Let  $(X, Y), (X', Y') \in B(n, k) \times B(n, k)$ . Then,  $(X, Y) \sim (X', Y')$  iff  $|X \cap Y| = |X' \cap Y'|$ .

The proof of the above is straightforward, and we omit it. Note in particular that  $(X, Y) \sim (Y, X)$ , so each orbital matrix is symmetric. Therefore,

$$\mathcal{A} = \text{Hom}_{S_n}(B(n, k), B(n, k))$$

is commutative. We have for any sets  $X, Y$  of size  $k$  that

$$\max\{0, 2k - n\} \leq |X \cap Y| \leq k.$$

Therefore,  $\dim \mathcal{A} = 1 + \min\{k, n - k\}$ . Let  $\{A_k, A_{k-1}, \dots, A_{\max\{0, 2k-n\}}\}$  be the orbital basis of  $\mathcal{A}$  with  $A_j(X, Y) = 1$  if  $|X \cap Y| = j$  and 0 otherwise. Then,  $A_k = \text{Id}$  and  $A_{k-1} = A$  is the adjacency matrix of the Johnson graph  $J(n, k)$ !

**Proposition 1.10.** It holds that  $\langle A \rangle = \text{span}\{A_k, A_{k-1}, \dots, A_{\max\{0, 2k-n\}}\}$ .

The proof is very similar to that of Proposition 1.7.

**Corollary 1.11.** The adjacency matrix  $A$  of the Johnson graph  $J(n, k)$  has  $1 + \min\{k, n - k\}$  distinct eigenvalues.

In the case where  $k \leq n - k$ , the multiplicities of the eigenvalues of the graph are  $\binom{n}{0}, \binom{n}{1} - \binom{n}{0}, \binom{n}{2} - \binom{n}{1}, \dots, \binom{n}{k} - \binom{n}{k-1}$ . We shall prove this and find the corresponding eigenspaces later in \*\*\* SEC ? \*\*\*.

When we deal with  $B_q(n, k)$ , the collection of  $k$ -dimensional subspaces of  $\mathbb{F}_q^n$ , we shall take the action of  $\text{GL}_n(\mathbb{F}_q)$  defined by

$$MX = M(X) = \{Mv : v \in X\}$$

Once more, we get results as in the Johnson graph.

**Lemma 1.12.** Let  $(X, Y), (X', Y') \in B_q(n, k) \times B_q(n, k)$ . Then,  $(X, Y) \sim (X', Y')$  iff  $\dim(X \cap Y) = \dim(X' \cap Y')$ .

So, the Grassmann graph with adjacency matrix  $A$  and corresponding adjacency algebra  $\mathcal{A}$  has  $\dim \mathcal{A} = 1 + \max\{k, n-k\}$  as well. Letting  $\{A_k, A_{k-1}, \dots, A_{\max\{0, 2k-n\}}\}$  be the orbital basis of  $\mathcal{A}$  with  $A_j(X, Y) = 1$  if  $\dim(X \cap Y) = j$  and 0 otherwise, we again get that  $\langle A \rangle = \text{span}\{A_k, \dots, A_{\max\{0, 2k-n\}}\}$ .

**Proposition 1.13.** It holds that  $\langle A \rangle = \text{span}\{A_k, A_{k-1}, \dots, A_{\max\{0, 2k-n\}}\}$ .

**Corollary 1.14.** The adjacency matrix  $A$  of the Grassmann graph  $J_q(n, k)$  has  $1 + \min\{k, n-k\}$  distinct eigenvalues.

The multiplicity of the eigenvalues (when  $k \leq n/2$ ) end up being  $\binom{n}{0}_q, \binom{n}{1}_q - \binom{n}{0}_q, \binom{n}{2}_q - \binom{n}{1}_q, \dots, \binom{n}{k}_q - \binom{n}{k-1}_q$ .

So far, all examples have been commutative.

**Example 2** (Non-commutative  $*$ -algebras). Consider the action of  $S_n$  on  $B(n)$ , with  $\pi\{i_1, \dots, i_k\} = \{\pi(i_1), \dots, \pi(i_k)\}$ . Similar to what we have already seen,  $(X, Y) \sim (X', Y')$  iff  $|X| = |X'|$ ,  $|Y| = |Y'|$ , and  $|X \cap Y| = |X' \cap Y'|$ . Consider the  $B(n) \times B(n)$  matrix  $M_{i,j,t}$  defined by

$$M_{i,j,t}(X, Y) = \begin{cases} 1, & |X| = i, |Y| = j, |X \cap Y| = t, \\ 0, & \text{otherwise,} \end{cases}$$

for any choice of  $i - t \geq 0, j - t \geq 0$ , and  $i + j - t \leq n$ . The number of ways of choosing such  $i, j, t$  is  $\binom{n+3}{3}$  – we would like to find the number of solutions to  $(i - t) + (j - t) + t + r = n$ , where  $i - t, j - t, t, r \geq 0$ . Therefore, setting  $\mathcal{A} = \text{Hom}_{S_n}(B(n), B(n))$ , we have  $\dim \mathcal{A} = \binom{n+3}{3}$ . Further note that  $\mathcal{A}$  is non-commutative. Indeed,  $M_{2,3,1}M_{3,4,2} \neq 0$  but  $M_{3,4,2}M_{2,3,1} = 0$ .

The  $q$ -analogue of the above example is as follows. Let  $\text{GL}_n(\mathbb{F}_q)$  act on  $B_q(n)$ , and define  $M_{i,j,t}(q)$  by

$$M_{i,j,t}(q)(X, Y) = \begin{cases} 1, & \dim X = i, \dim Y = j, \dim(X \cap Y) = t, \\ 0, & \text{otherwise.} \end{cases}$$

Again, we have  $\dim \mathcal{A} = \binom{n+3}{3}$ .

So far, this idea of translating proofs to proofs in the setting of  $q$ -analogues seems pretty straightforward. However, things don't work out as well when we try to go from  $C(n)$  to  $C_q(n)$ . The issue is that  $H_n$  does not have a neat  $q$ -analogue. Later, we shall look at a  $q$ -analogue of  $\text{Hom}_{H_n}(B(n), B(n))$  that does not come from a graph action.

**Example 3.** Let  $G$  be a finite group.  $G \times G$  acts on  $G$  by  $(g, h) \cdot a = gah^{-1}$ . What is the orbital basis of the commutant of this action?

Let  $(a, b), (c, d) \in G \times G$ . Then,  $(a, b) \sim (c, d)$  iff  $ab^{-1}$  and  $cd^{-1}$  are conjugates in  $G$ .

The former is true iff for some  $g, h \in G$ ,  $gah^{-1} = c$  and  $gbh^{-1} = d$ . Equivalently,  $ga = ch$  and  $b^{-1}g^{-1} = h^{-1}d^{-1}$ . Multiplying the two, this implies that  $gab^{-1}g^{-1} = cd^{-1}$ , that is,  $ab^{-1}$  and  $cd^{-1}$  are conjugates. For the backward direction, if we have  $gab^{-1}g^{-1} = cd^{-1}$ . Setting  $h = gac^{-1}$ , the previous equation implies that  $h = d^{-1}gb$ . This directly implies that  $gah^{-1} = c$  and  $gbh^{-1} = d$ .

Let the conjugacy classes of  $G$  be  $C_1, \dots, C_t$ . Consider the  $G \times G$  matrices  $A_j$  by

$$A_j(g, h) = \begin{cases} 1, & gh^{-1} \in C_j, \\ 0, & \text{otherwise.} \end{cases}$$

In the case where each element of the group is conjugate to its inverse, we can use **Gelfand's Lemma** to conclude that each  $A_j$  is symmetric so  $\mathcal{A}$  is abelian. An example of such a group is the symmetric group  $S_n$ , and the dimension of the resulting  $\mathcal{A}$  is  $p(n)$ , the number of number partitions of  $n$ . However, it turns out that  $\mathcal{A}$  is commutative for *any*  $G$ ! This shows that Gelfand's lemma is sufficient but not necessary. \*\*\* EXERCISE \*\*\*

**Example 4.** Consider  $K_{2n}$ , the complete graph on  $2n$  vertices. It is not too difficult to show that the number of perfect matchings of  $K_{2n}$  is  $\frac{(2n)!}{n!2^n} = (2n)!!$ . Denote the set of all perfect matchings on  $K_{2n}$  by  $\text{PM}_{2n}$ .  $S_{2n}$  acts on  $\text{PM}_{2n}$  in an obvious manner, by mapping the matching  $\{i_1j_1, i_2j_2, \dots, i_nj_n\}$  to  $\{\pi(i_1)\pi(j_1), \dots, \pi(i_n)\pi(j_n)\}$ . What are the  $K_{2n}$  orbits on  $\text{PM}_{2n} \times \text{PM}_{2n}$ ?

Let  $M_1, M_2 \in \text{PM}_{2n}$ . It is not too difficult to see that  $M_1 \cup M_2$  comprises of "alternating cycles", namely even cycles whose edges alternate between being in  $M_1, M_2$  (such a cycle may also be a 2-cycle with two edges between two vertices, one of which is in  $M_1$  and the other in  $M_2$ ). This induces a number partition of  $n$ , based on the number of cycles of size  $2k$  for  $1 \leq k \leq n$ . Call this partition  $d(M_1, M_2)$ .

We claim that  $(M_1, M_2) \sim (M_3, M_4)$  iff  $d(M_1, M_2) = d(M_3, M_4)$ .

The forward direction is direct since if we have  $\pi(M_1, M_2) = (M_3, M_4)$ , then  $\pi$  applied to the vertices of the multigraph  $M_1 \cup M_2$  gives  $M_3 \cup M_4$  while having the same graph (up to isomorphism), so the partition remains the same. For the backward direction, just match up  $M_1 \cup M_2$  and  $M_3 \cup M_4$  in a way that cycle sizes agree.

Therefore, the dimension of this  $*$ -algebra is  $p(n)$ , the number of partitions of  $n$ . Recall that this is the same as the number of partitions as the previous example when  $G = S_n$ . Further, since  $d(M_1, M_2) = d(M_2, M_1)$ , this algebra is abelian by **Gelfand's Lemma**.

Much like the spectral theorem of normal matrices, there is a spectral theorem of  $*$ -algebras which "diagonalizes" them.

**Theorem 1.15** (Spectral theorem for commutative  $*$ -algebras). Let  $\mathcal{A} \subseteq \mathcal{M}_n(\mathbb{C})$  be a commutative  $*$ -algebra. Then, there exists an  $n \times n$  unitary matrix  $U$  and positive integers  $q_1, \dots, q_m$  (determined up to permutation) such that  $U^\dagger \mathcal{A} U$  is the set of all  $(q_0, \dots, q_m)$ -block diagonal matrices, that is, the set of all matrices

$$\begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_m \end{pmatrix},$$

where  $C_k$  is a  $q_k \times q_k$  scalar matrix. In particular, any element of  $U^\dagger \mathcal{A} U$  is determined by the  $m$  scalars corresponding to these blocks, so  $\dim \mathcal{A} = m$  and  $q_1 + \dots + q_m = n$ .

*Proof.* ■

**Corollary 1.16.** Let  $\mathcal{A}$  be a commutative  $*$ -algebra. Then there exist subspaces  $W_1, \dots, W_m$  of  $\mathbb{C}^n$  that are (common) eigenspaces of any  $A \in \mathcal{A}$ .

There is also a more general spectral theorem for (not necessarily commutative)  $*$ -algebras, that we state without proof.

**Theorem 1.17** (Spectral theorem for  $*$ -algebras). Let  $\mathcal{A} \subseteq \mathcal{M}_n(\mathbb{C})$  be a commutative  $*$ -algebra. Then, there exists an  $n \times n$  unitary matrix  $U$  and positive integers  $p_1, \dots, p_m$  and  $q_1, \dots, q_m$  (determined up to permutation) such that  $U^\dagger \mathcal{A} U$  is the set of all  $((p_0, q_0), \dots, (p_m, q_m))$ -block diagonal matrices, that is, the set of all matrices

$$U^\dagger \mathcal{A} U = \left( \begin{array}{cccc} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_m \end{array} \right),$$

where  $C_k$  is a block diagonal matrix

$$C_k = \left( \begin{array}{cccc} B_k & & & \\ & B_k & & \\ & & \ddots & \\ & & & B_k \end{array} \right)$$

consisting of  $q_k$  repeated blocks of a  $p_k \times p_k$  matrix  $B_k$ . Furthermore,  $\dim \mathcal{A} = p_1^2 + \dots + p_m^2$  and  $n = p_1 q_1 + \dots + p_m q_m$ .

In either spectral theorem, we say that we have a *diagonalization* of  $\mathcal{A}$  if we know the images  $A \mapsto U^\dagger A U$  explicitly, and an *explicit diagonalization* if we further know  $U$ .

## 1.2. A primer on representation theory

**Definition 1.18.** A *representation* of a group  $G$  is a group homomorphism  $\varphi : G \rightarrow \text{GL}(V)$  for some finite-dimensional vector space  $V$  over  $\mathbb{C}$ . Given such a representation, we say that  $V$  is a  $G$ -module.

The image of  $g$  under  $\varphi$  is denoted  $\varphi_g$ , but we usually abuse notation it like a group action. That is, we denote  $(\varphi(g))(v)$  as  $\varphi_g(v)$  or merely  $g \cdot v$  or even  $gv$  when the representation is clear from context.



**Example 5.** Let  $G$  be a group and  $S$  a finite set such that  $G$  acts on  $S$ . Consider the *linearization* of  $S$  or the *permutation module* corresponding to  $S$ , which is the vector space with  $S$  as a basis, that is,

$$\mathbb{C}[S] = \left\{ \sum_{s \in S} \alpha_s s : \alpha_s \in \mathbb{C} \right\}.$$

The action of  $G$  induces a representation on  $\mathbb{C}[S]$ , namely

$$g \cdot \left( \sum_s \alpha_s s \right) = \sum_s \alpha_s (g \cdot s).$$

**Definition 1.19.** Given a  $G$ -module  $V$ , a subspace  $W \subseteq V$  is said to be a *submodule* of  $V$  if for all  $w \in W$  and  $g \in G$ ,  $gw \in W$ .

That is, it is invariant with respect to the representation.

**Definition 1.20.** A  $G$ -module  $V$  is said to be *irreducible* if  $\dim V > 0$  and it has no submodules other than  $\{0\}$  and  $V$ .

More succinctly, an irreducible  $G$ -module is one with exactly two submodules. In particular, any one-dimensional module is irreducible

**Example 6.** Consider the obvious action of  $S_n$  on  $X = [n]$ . Considering the permutation module  $\mathbb{C}[X]$ , the subspaces

$$V_1 = \text{span}\{1 + 2 + \cdots + n\} \text{ and} \\ V_2 = \{c_1 1 + c_2 2 + \cdots + c_n n : c_1 + \cdots + c_n = 0\}.$$

Clearly,  $V_1$  is irreducible. It turns out that  $V_2$  is irreducible as well! Suppose instead that  $W \neq 0$  is a submodule of  $V_2$ , containing  $w = c_1 1 + \cdots + c_n n$  for some  $(c_i)$  adding up to 0. Suppose that  $c_1 \neq 0$ . We must have that some other  $c_i$  is also nonzero and unequal to  $c_1$ ; suppose that  $c_2$  is so. Then,

$$w = c_1 1 + c_2 2 + \cdots + c_n n \in W \\ (1 \ 2)w = c_2 1 + c_1 2 + \cdots + c_n n \in W$$

since  $W$  is a submodule. Subtracting the two, we get that  $(1 - 2) \in W$ . Applying  $(2 \ j)$  for  $j \geq 3$ , we get that  $(1 - j) \in W$  for any  $j = 2, 3, \dots, n$ . Therefore,  $\dim W = n - 1$  so  $W$  must be  $V_2$ .

Ideally, we would like some result in the spirit of the prime factorization theorem, saying that any module can be decomposed into a direct sum of irreducible submodules in a “unique” fashion. We shall spend the remainder of this section developing this theorem.

**Definition 1.21.** Let  $V$  be a finite-dimensional vector space with an inner product  $\langle \cdot, \cdot \rangle$ . A *unitary* representation is a group homomorphism  $\varphi : G \rightarrow \mathcal{U}(V)$ . In such a case,  $V$  is called a *unitary  $G$ -module*.

Above  $\mathcal{U}(V)$  is the subgroup of matrices in  $\text{GL}(V)$  under which the inner product is preserved. That is,  $\mathcal{U}(V)$  is the set of all matrices  $A$  such that for any  $v, w \in V$ ,  $\langle v, w \rangle = \langle Av, Aw \rangle$ .

**Lemma 1.22.** Let  $V$  be a unitary  $G$ -module with  $\dim V > 0$ . Then,  $V$  is a direct sum of irreducible submodules.

*Proof.* If  $V$  is irreducible, we are done. Suppose otherwise, and let  $W \neq 0$  be a proper submodule of  $V$ . Consider  $W^\perp = \{v \in V : \langle v, w \rangle = 0\}$ . For any  $v \in W^\perp$ ,  $g \in G$ , and  $w \in W$ , since  $W$  is a submodule,  $\langle gv, w \rangle = \langle v, g^{-1}w \rangle = 0$ , so  $gv \in W^\perp$ . It follows that  $W^\perp$  is a proper submodule of  $V$ . Induction on dimension completes the proof. ■

**Lemma 1.23.** Let  $V$  be a  $G$ -module with  $\dim V > 0$ . Then,  $V$  is a direct sum of irreducible submodules.

*Proof.* Let  $(\cdot, \cdot)$  be any inner product on  $V$ . Consider the inner product  $\langle \cdot, \cdot \rangle$  defined by

$$\langle v, w \rangle = \sum_{h \in G} (hv, hw).$$

Note that  $V$  is a unitary  $G$ -module with respect to  $\langle \cdot, \cdot \rangle$ . The desideratum follows by the previous lemma. ■

This completes the first part of the statement we made earlier, showing that any module can be decomposed into a direct sum of irreducibles. Now, we would like to show that this decomposition is also unique in some sense.

**Definition 1.24.** Given  $G$ -modules  $V, W$ , a linear map  $f : V \rightarrow W$  is said to be  $G$ -linear if  $f$  commutes with the action of  $G$ , that is,  $f(gv) = gf(v)$ . We denote

$$\text{Hom}_G(V, W) = \{f : V \rightarrow W : f \text{ is } G\text{-linear}\}.$$

In some settings,  $W$  may be a vector space of functions; in such cases, take care with the definition of  $G$ -linearity.

**Lemma 1.25.** Let  $V, W$  be irreducible  $G$ -modules and  $f : V \rightarrow W$  be  $G$ -linear. Then, either  $f \equiv 0$  or  $f$  is an isomorphism.

*Proof.* Note that  $\ker f$  and  $\text{im } f$  are respectively submodules of  $V$  and  $W$ , so by irreducibility, they must each be equal to 0 or the entire vector space. If  $\ker f = V$ , then  $f \equiv 0$ . If  $\ker f = 0$ , we must also have  $\text{im } f = W$  so  $f$  is an isomorphism. ■

**Lemma 1.26** (Schur's Lemma). Let  $V$  be an irreducible  $G$ -module and  $f : V \rightarrow V$  be  $G$ -linear. Then,  $f = \lambda I$  for some  $\lambda \in \mathbb{C}$ .

*Proof.* Let  $\lambda$  be some eigenvalue of  $f$ . Then,  $f - \lambda I$  is also  $G$ -linear and has nonzero kernel; by the previous lemma, it follows that it is identically 0, completing the proof. ■

**Corollary 1.27.** Let  $V, W$  be irreducible  $G$ -modules. Then,

$$\dim \text{Hom}_G(V, W) = \begin{cases} 1, & V \cong W, \\ 0, & \text{otherwise.} \end{cases}$$

**Corollary 1.28.** A  $G$ -invariant inner product on an irreducible  $G$ -module is unique up to scaling.

*Proof.* Let  $\langle \cdot, \cdot \rangle$  and  $[\cdot, \cdot]$  be two  $G$ -invariant inner products on an irreducible  $G$ -module  $V$ . Consider the linear map  $\varphi : V \rightarrow V^*$  (where  $V^*$  is the dual of  $V$ ) defined by

$$\varphi(v)(u) = \langle v, u \rangle,$$

and similarly  $\psi : V \rightarrow V^*$  defined by  $\psi(v)(u) = [v, u]$ . Note that both  $\varphi$  and  $\psi$  are  $G$ -linear isomorphisms, where for  $f \in V^*$  we define

$$(g \cdot f)(v) = f(g^{-1} \cdot v).$$

It follows that  $\psi^{-1} \circ \varphi : V \rightarrow V$  is a  $G$ -linear isomorphism. Irreducibility of  $V$  with **Schur's Lemma** implies that  $\psi^{-1} \circ \varphi = \lambda \text{Id}$ , which yields the desired. ■

**Lemma 1.29.** Let  $V, W$  be  $G$ -modules, and  $W_1, W_2$  be  $G$ -submodules of  $W$  such that  $W = W_1 \oplus W_2$ . Then,

$$\text{Hom}_G(V, W_1 \oplus W_2) \cong \text{Hom}_G(V, W_1) \oplus \text{Hom}_G(V, W_2).$$

In particular,

$$\dim \text{Hom}_G(V, W_1 \oplus W_2) = \dim \text{Hom}_G(V, W_1) + \dim \text{Hom}_G(V, W_2).$$

*Proof.* Let  $\pi_1 : W \rightarrow W_1$  and  $\pi_2 : W \rightarrow W_2$  denote the respective projection maps. Given  $T \in \text{Hom}_G(V, W_1 \oplus W_2)$ , we have  $\pi_1 \circ T \in \text{Hom}_G(V, W_1)$  and  $\pi_2 \circ T \in \text{Hom}_G(V, W_2)$ . For the backward inclusion, given  $T_1 \in \text{Hom}_G(V, W_1), T_2 \in \text{Hom}_G(V, W_2)$ , the map  $T$  defined by  $T(v) = (T_1(v), T_2(v))$  is in  $\text{Hom}_G(V, W)$ . This establishes an isomorphism between  $\text{Hom}_G(V, W)$  and  $\text{Hom}_G(V, W_1) \oplus \text{Hom}_G(V, W_2)$ , proving the claim. ■

Given a vector space  $V$ , denote by  $nV$  the direct sum of it with itself  $n$  times. Also denote  $0V = 0$ .

**Corollary 1.30.** Let  $V_1, \dots, V_r$  be irreducible  $G$ -modules and  $V, W$  be  $G$ -modules such that

$$\begin{aligned} V &\cong n_1 V_1 \oplus n_2 V_2 \oplus \dots \oplus n_r V_r \text{ and} \\ W &\cong m_1 V_1 \oplus m_2 V_2 \oplus \dots \oplus m_r V_r, \end{aligned}$$

where  $n_i, m_i \geq 0$ . Then,

$$\dim \text{Hom}_G(V, W) = n_1 m_1 + n_2 m_2 + \dots + n_r m_r.$$

**Corollary 1.31.** Let  $V$  be a  $G$ -module such that

$$V \cong n_1 V_1 \oplus n_2 V_2 \oplus \dots \oplus n_r V_r,$$

where  $V_1, \dots, V_r$  are irreducible  $G$ -modules, and  $n_i > 0$  for each  $i$ . Then, the  $(n_i, V_i)$  are determined by  $V$  up to permutation and isomorphism.

*Proof.* This is immediate on noting that by the previous corollary, for any irreducible  $W$ ,  $W$  appears with multiplicity  $n$  in a decomposition of  $V$  iff  $\dim \text{Hom}_G(V, W) = n$ . ■

**Definition 1.32.** A  $G$ -module  $V$  is *multiplicity-free* iff for any irreducible  $W$ ,  $\dim \text{Hom}_G(V, W) \in \{0, 1\}$ .

**Lemma 1.33.** Let  $G$  act on a set  $S$  and consider  $\mathcal{A} = \text{Hom}_G(S, S)$ . Then,  $\mathbb{C}[S]$  is multiplicity-free iff  $\mathcal{A}$  is commutative.

Suppose that  $\mathbb{C}[S] \cong n_1 V_1 \oplus \cdots \oplus n_r V_r$ . It is easy to see that

$$\mathcal{A} \cong \text{Hom}_G(n_1 V_1, n_1 V_1) \oplus \cdots \oplus \text{Hom}_G(n_r V_r, n_r V_r)$$

is commutative iff each of the  $r$  parts of the direct sum are commutative. The idea behind the proof is that each  $\text{Hom}_G(n_i V_i, n_i V_i)$  is essentially a  $n_i \times n_i$  matrix, which is commutative iff  $n_i = 1$ .

### 1.3. The Delsarte Bound

**Definition 1.34.** A *binary code*  $C$  (of length  $n$ ) is a non-empty proper subset of  $B(n)$ . Given  $X, Y \in B(n)$ , the *Hamming distance*  $d$  defined by  $d(X, Y) = |X \triangle Y|$ . The Hamming distance of a code  $C$  is  $d(C) = \min_{\substack{X, Y \in C \\ X \neq Y}} d(X, Y)$ .

Codes are studied in great detail in coding theory, with the distance of a code being an indicator of how resistant it is to “corruption”.

**Definition 1.35.** Given  $n, d$ ,  $A(n, d)$  is the size of a largest binary code of length  $n$  whose distance is at least  $d$ .

Given the previous paragraph, it should be of no surprise that  $A(n, d)$  is of great interest to coding theorists. However, it turns out that computing it is NP-hard. We shall give an efficient algorithm to compute an upper bound on  $A(n, d)$ . While we do not provide any theoretical guarantee on how good this bound is, it turns out to be surprisingly effective in practice.

Consider the graph  $G$  on vertex set  $B(n)$ , where  $X, Y$  are adjacent iff  $d(X, Y) < d$ .  $A(n, d)$  is then precisely the size of a largest independent set on  $G$ . For  $S \subseteq B(n)$  an independent set, let  $\chi(S) \in \mathbb{R}^V$  be the indicator vector of  $S$ . Consider

$$M = \frac{1}{|S|} \chi(S) \chi(S)^\top.$$

Then,  $M$  is positive semidefinite,  $M_{ij} = 0$  if  $ij \notin E$ ,  $\text{Tr}(M) = 1$ , and  $|S| = \sum_{i,j} M_{ij}$ .

**Definition 1.36 (Semidefinite Program).** Given matrices  $C, X$ , denote  $\langle C, X \rangle = \sum_{i,j} C_{ij} X_{ij}$ . A *semidefinite program* is a program of the form

$$\begin{aligned} & \text{maximize} && \langle C, X \rangle \\ & \text{subject to} && X \succeq 0 \\ & && \langle A_i, X \rangle = b_i, i \in [m] \end{aligned}$$

where  $X$  is a  $n \times n$  matrix of variables  $x_{ij}$ ,  $A_i$  and  $C$  are matrices (that are also part of the input of the program), and the  $b_i$  are constants.

That is, a semidefinite program is just a linear program with an additional constraint that a matrix defined by the variables is positive semidefinite. It turns out that optima to semidefinite programs can be found in polynomial time (up to an error of  $\epsilon$ ).

Given the earlier discussion, it follows that the size of a largest independent set is bounded from above by the solution to the following semidefinite program.

$$\begin{aligned} & \text{maximize} && \langle J, M \rangle \\ & \text{subject to} && M \succeq 0, \\ & && \text{Tr}(M) = 1, \\ & && M_{ij} = 0, \quad ij \in E. \end{aligned} \tag{1.2}$$

However, note that for our graph  $G$  on  $B(n)$ , this SDP is of exponential size in the input parameter  $n$ ! The Delsarte bound takes advantage of the symmetries of the graph to bring this down to a *linear* program whose size is polynomial in  $n$ .

Recall the hyperoctahedral group  $H_n$ . For  $\tau \in H_n$ , let  $\rho_\tau$  be the  $B(n) \times B(n)$  permutation matrix that permutes vertices according to  $\tau$ . The key idea is that since  $\tau$  is distance-preserving, if  $C$  is a code with minimum distance at least  $d$ , so is  $\tau(C)$ . Therefore, for a given code  $C$ , instead of the  $\chi(S)\chi(S)^\top$  we considered earlier, we shall instead look at

$$M = \frac{1}{|C|} \sum_{\tau \in H_n} \rho_\tau \chi(C) \chi(C)^\top \rho_\tau^\top, \tag{1.3}$$

which is positive semidefinite. Furthermore, since  $M$  lives in a far lower-dimensional space than the  $2^n \times 2^n$  space we had earlier. In fact,  $M \in \text{Hom}_{H_n}(B(n), B(n))$ , so lives in only a  $(n+1)$ -dimensional space (recall that we had proved this back in Proposition 1.7)! Indeed, it is easy to show that for any  $\sigma \in H_n$ ,  $M$  commutes with the unitary matrix  $P_\sigma$ , since

$$P_\sigma M P_\sigma^\top = P_\sigma \left( \frac{1}{|C|} \sum_{\tau \in H_n} P_\tau \chi(C) \chi(C)^\top P_\tau^\top \right) P_\sigma^\top = \frac{1}{|C|} \sum_{\tau \in H_n} P_{\sigma \circ \tau} \chi(C) \chi(C)^\top P_{\sigma \circ \tau}^\top = M. \tag{1.4}$$

Let  $A_0, \dots, A_n$  be the orbital basis of  $\text{Hom}_{H_n}(B(n), B(n))$ , so any element in the commutant is of the form  $\sum_{i=0}^n x_i A_i$ . Let us next express the  $x_i$  in terms of the code itself.

**Proposition 1.37.** Let  $\lambda_i$  be the number of pairs  $(X, Y) \in C^2$  with  $d(X, Y) = i$ , and  $\alpha_i = \lambda_i / |C| \binom{n}{i}$ . With  $M$  defined as above,

$$M = n! (\alpha_0 A_0 + \alpha_1 A_1 + \dots + \alpha_n A_n).$$

*Proof.* The number of 1s in  $A_i$  is  $2^n \binom{n}{i}$ . The number of 1s in  $\chi(C)\chi(C)^\top$  in the nonzero positions of  $A_i$  is precisely  $\lambda_i$ . When we sum over the elements of  $H_n$ , this implies that the sum of elements of  $M$  in the nonzero positions of  $A_i$  is  $2^n n! \lambda_i = 2^n n! \binom{n}{i} \alpha_i |C|$ . Therefore, the  $A_i$  term in  $M$  has a coefficient of  $(2^n n! \binom{n}{i} \alpha_i |C|) / (|C| 2^n \binom{n}{i}) = n! \alpha_i$ , as desired. ■

Therefore, the upper bound yielded by eq. (1.2) is at most that of the following semidefinite program.

$$\begin{aligned} & \text{maximize} && \sum_{i=0}^n \binom{n}{i} x_i \\ & \text{subject to} && x_i \geq 0 \quad \text{for all } i, \\ & && x_0 = 1, x_1 = \dots = x_{d-1} = 0, \\ & && x_0 A_0 + x_1 A_1 + \dots + x_n A_n \succeq 0. \end{aligned}$$

However, the positive semidefiniteness constraint is still exponentially large! To get around this, recall that the  $A_i$  have the same eigenspaces, and only  $(n+1)$  distinct eigenvalues, so we can just manually check that all the eigenvalues of  $\sum_{i=0}^n x_i A_i$  are non-negative. To do this, we must compute the eigenvalues of each  $A_i$ .

Now, consider  $\mathbb{C}^2$  with the basis  $e_0 = \begin{pmatrix} 1 & 0 \end{pmatrix}$  and  $e_1 = \begin{pmatrix} 0 & 1 \end{pmatrix}$ . The matrix  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  has eigenvalues  $1, -1$  with the respective eigenvectors being

$$u = \frac{e_0 + e_1}{\sqrt{2}} \text{ and } v = \frac{e_0 - e_1}{\sqrt{2}}.$$

Now, consider the isomorphism  $\mathbb{C}[B(n)] \rightarrow (\mathbb{C}^2)^{\otimes n}$  where each basis vector  $X$  maps to  $a_1 \otimes \cdots \otimes a_n$ , with  $a_i = e_1$  if  $i \in X$  and  $e_0$  otherwise.

An alternate orthonormal basis of  $\mathbb{C}[B(n)]$  is the set of  $u_1 \otimes \cdots \otimes u_n$ , where each  $u_i$  is either  $u$  or  $v$ .

Now, consider the subspace  $W_j$  spanned by all  $u_1 \otimes \cdots \otimes u_n$ , where exactly  $j$  of the  $u_i$  are  $v$  (and the remaining are  $u$ ). It may be checked that  $W_j$  is an eigenspace of  $A_i$ , with the eigenvalue

$$\sum_{k=0}^i (-1)^k \binom{j}{k} \binom{n-j}{i-k}.$$

In particular, the eigenvalues of  $A = A_1$  are  $n - 2j$  with multiplicity  $\dim W_j = \binom{n}{j}$ . Therefore, an upper bound on  $A(n, d)$  is given by the linear program

$$\begin{aligned} & \text{maximize} && \sum_{i=0}^n \binom{n}{i} x_i \\ & \text{subject to} && x_i \geq 0 \text{ for all } i, \\ & && x_0 = 1, x_1 = \cdots = x_{d-1} = 0, \\ & && \sum_{i=0}^n x_i \left( \sum_{k=0}^i (-1)^k \binom{j}{k} \binom{n-j}{i-k} \right) \geq 0 \quad j \in [n]. \end{aligned}$$

#### 1.4. The Schrijver Bound

The idea behind the Schrijver bound is that we split the sum in eq. (1.3) into two parts as

$$|C| \cdot M = |\Pi| \cdot \frac{1}{|\Pi|} \sum_{\tau \in \Pi} \rho_\tau \chi(C) \chi(C)^\top \rho_\tau^\top + |H_n \setminus \Pi| \cdot \frac{1}{|H_n \setminus \Pi|} \sum_{\tau \in H_n \setminus \Pi} \rho_\tau \chi(C) \chi(C)^\top \rho_\tau^\top,$$

where each of the two matrices live in a space of dimension polynomial in  $n$ . It is clear that the two are positive semidefinite.

Here,  $\Pi$  is defined as

$$\Pi = \{\tau \in H_n : \tau(C) \ni \mathbf{0}\}.$$

For  $X \in B(n)$ , consider

$$\Pi_X = \{\tau \in H_n : \tau(X) = \mathbf{0}\}.$$

Then, setting

$$R_X = \frac{1}{|\Pi_X|} \sum_{\tau \in \Pi_X} \rho_\tau \chi(C) \chi(C)^\top \rho_\tau^\top,$$

we have

$$R = \frac{1}{|\Pi|} \sum_{\tau \in \Pi} \rho_\tau \chi(C) \chi(C)^\top \rho_\tau^\top = \frac{1}{|C|} \sum_{X \in C} R_X.$$

Set  $\Pi' = H_n \setminus \Pi$ . We similarly have

$$R' = \frac{1}{|\Pi'|} \sum_{\tau \in \Pi'} \rho_\tau \chi(C) \chi(C)^\top \rho_\tau^\top,$$

so

$$M = |\Pi| \cdot R + |\Pi'| \cdot R'.$$

The space we shall consider is  $\mathcal{A} = \text{Hom}_{S_n}(B(n), B(n))$  – recall from Example 2 that this is a non-commutative  $\binom{n+3}{3}$ -dimensional  $*$ -algebra with basis  $(M_{i,j,t})$ . It is reasonably easy to show that  $R, R' \in \mathcal{A}$  by a proof similar to eq. (1.4).

**Proposition 1.38.** Let  $\lambda_{i,j,t}$  be the number of pairs  $(X, Y, Z) \in C^3$  with  $d(X, Y) = i, d(Y, Z) = j, d(Z, X) = i + j - 2t$ , and  $\alpha_{i,j,t} = \lambda_{i,j,t} / \binom{n}{i-t, t, j-t}$ . With  $R, R'$  defined as above,

$$R = \sum_{i,j,t} \alpha_{i,j,t} M_{i,j,t}$$

and

$$R' = \frac{|C|}{2^n - |C|} \sum_{i,j,t} (\alpha_{i+j-2t,0,0} - \alpha_{i,j,t}) M_{i,j,t}.$$

*Proof.* The sum of elements of  $R_X$  in the nonzero positions of  $M_{i,j,t}$  is precisely the number of  $(Y, Z) \in C^2$  such that for some  $\tau \in \Pi$ ,  $|\tau(Y)| = i, |\tau(Z)| = j$ , and  $d(\tau(Y), \tau(Z)) = i + j - 2t$ , which is precisely the number of  $(Y, Z) \in C^2$  such that  $d(X, Y) = i, d(X, Z) = j$ , and  $d(Y, Z) = i + j - 2t$ . Summing over  $X$  and dividing by  $|C|$ , this is exactly  $\binom{n}{i-t, t, j-t} \alpha_{i,j,t}$ . On the other hand, the sum of elements of  $M_{i,j,t}$  on the other hand is  $\binom{n}{i-t, t, j-t}$ . The first equation follows.

Now, by Proposition 1.37, we have

$$\begin{aligned} M &= n! \sum_{t=0}^n \alpha_t A_t \\ &= n! \sum_{t=0}^n \alpha_{t,0,0} A_t \\ &= n! \sum_{t=0}^n \alpha_{t,0,0} \sum_{i,j} M_{i,j,(i+j-t)/2} \\ &= n! \sum_{i,j,t} \alpha_{i+j-2t,0,0} M_{i,j,t}. \end{aligned}$$

Therefore, using the expansion of  $R$ , we have

$$\begin{aligned} |\Pi|R + |\Pi'|R' &= |C| \cdot M \\ n!|C|R + n!(2^n - |C|)R' &= n!|C| \sum_{i,j,t} \alpha_{i+j-2t,0,0} M_{i,j,t} \\ R' &= \frac{|C|}{2^n - |C|} \sum_{i,j,t} (\alpha_{i+j-2t,0,0} - \alpha_{i,j,t}) M_{i,j,t}. \end{aligned}$$

■

Now, note that  $|C| = \sum_{i=0}^n \binom{n}{i} \alpha_{i,0,0}$ . So, the upper bound yielded by eq. (1.2) is at most that by the following semidefinite program, where we have added a couple more constraints that may be proved using the definitions of  $\alpha_{i,j,t}$ .

$$\begin{aligned} &\text{maximize} && \sum_{i=0}^n \binom{n}{i} x_{i,j,t} \\ &\text{subject to} && x_{i,j,t} = 0 \\ & && x_{i,j,t} = x_{i',j',t'} \\ & && 0 \leq x_{i,j,t} \leq x_{i,0,0} \\ & && x_{i,0,0} + x_{j,0,0} \leq 1 + x_{i,j,t} \\ & && \sum_{i,j,t} x_{i,j,t} M_{i,j,t} \succcurlyeq 0, \\ & && \sum_{i,j,t} (x_{i+j-2t,0,0} - x_{i,j,t}) M_{i,j,t} \succcurlyeq 0. \end{aligned} \quad \begin{aligned} & \{i, j, i+j-2t\} \cap [d-1] \neq \emptyset, \\ & (i, j, i+j-2t) \text{ is a permutation of } (i', j', i'+j'-2t'), \\ & \text{for all } i, j, t, \\ & \text{for all } i, j, t, \end{aligned} \quad (1.5)$$

To conclude, we must, as in the Delsarte bound, take advantage of symmetries to bring down the size of the PSD constraint. This is far more complicated here, however, since the algebra is non-commutative so we must deal with the *block* diagonalization (recall the [Spectral theorem for \\*-algebras](#)).

**Theorem 1.39** (Schrijver). Let  $\mathcal{A}_n = \text{Hom}_{S_n}(B(n), B(n))$ . Set  $\mathcal{M} = \lfloor n/2 \rfloor$ , and  $p_k = n - 2k + 1$  and  $q_k = \binom{n}{k} - \binom{n}{k-1}$  for  $k = 0, 1, \dots, m$ . Then, the following are true.

- (a) There exists a  $B(n) \times S$  real unitary matrix  $V$  (for some indexing set  $S$  of size  $2^n$ ) such that  $V^\dagger \mathcal{A}_n V$  is equal to the set of all  $S \times S$   $((p_0, q_0), (p_1, q_1), \dots, (p_m, q_m))$ -block-diagonal matrices.  
In particular, this implies that  $p_0^2 + \dots + p_m^2 = \dim \mathcal{A}_n = \binom{n+3}{3}$  and  $p_0 q_0 + \dots + p_m q_m = 2^n$ .

- (b) “Dropping” the duplicated blocks in the above block-diagonalization, we get a PSDness-preserving \*-algebra isomorphism

$$\Phi : \mathcal{A}_n \rightarrow \bigoplus_{k=0}^m \mathcal{M}_{p_k}(\mathbb{C}).$$

- (c) Suppose that

$$\Phi \left( \sum_{r,s,t=0}^n x_{r,s,t} M_{r,s,t} \right) = (R_0, \dots, R_m),$$

where the rows and columns of  $R_k \in \mathcal{M}_{p_k}(\mathbb{C})$  are indexed by  $k, k+1, \dots, n-k$ . Then, for  $k \leq i, j \leq n-k$ ,

$$(R_k)_{ij} = \frac{1}{\sqrt{\binom{n-2k}{i-k} \binom{n-2k}{j-k}}} \sum_{u,t=0}^n (-1)^{u-t} \binom{u}{t} \binom{n-2k}{u-k} \binom{n-k-u}{i-u} \binom{n-k-u}{j-u} x_{i,j,t}.$$

We shall spend the remainder of this section proving the above monster of a theorem.

**Definition 1.40.** The *up* linear operator  $U : \mathbb{C}[B(n)] \rightarrow \mathbb{C}[B(n)]$  is defined by

$$X \mapsto \sum_{\substack{Y \supseteq X \\ |Y|=|X|+1}} Y.$$

Similarly, the *down* linear operator  $D : \mathbb{C}[B(n)] \rightarrow \mathbb{C}[B(n)]$  is defined by

$$X \mapsto \sum_{\substack{Y \subset X \\ |Y|=|X|-1}} Y.$$

Despite the deceptive names,  $U$  and  $D$  are *not* inverses of each other.

**Definition 1.41.** An element  $v \in \mathbb{C}[B(n)]$  is said to be *homogeneous* if  $v \in \mathbb{C}[B(n, k)]$  for some  $0 \leq k \leq n$ . In this case, we say that the *rank* of  $v$  is  $k$  and write  $r(v) = k$ .

A *symmetric Jordan chain* (SJC) is a sequence  $(v_k, v_{k+1}, \dots, v_{n-k})$  of non-zero homogeneous elements of  $\mathbb{C}[B(n)]$  such that  $r(v_i) = i$  for  $i = k, k+1, \dots, n-k$ ,  $U(v_i) = v_{i+1}$  for  $i = k, k+1, \dots, n-k-1$ , and  $U(v_{n-k}) = 0$ .

A *symmetric Jordan basis* (SJB) of  $\mathbb{C}[B(n)]$  is a basis of  $\mathbb{C}[B(n)]$  consisting of a disjoint union of SJCs.



It is not difficult to see that in an SJB, the number of SJC's going from rank  $k$  to  $n - k$  is  $\binom{n}{k} - \binom{n}{k-1}$  – the chains starting at lower levels account for a  $\binom{n}{k-1}$ -dimensional subspace of  $B(n, k) \subseteq B(n)$ , so an appropriate number of SJC's have to start at this level.

**Example 7.** An SJB of  $\mathbb{C}[B(3)]$  consists of the chains  $(\emptyset, \{1\} + \{2\} + \{3\}, 2(\{1, 2\} + \{1, 3\} + \{2, 3\}), 6\{1, 2, 3\}), (2\{3\} - \{1\} - \{2\}, \{1, 3\} + \{2, 3\} - 2\{1, 2\}),$  and  $(\{2\} - \{1\}, \{2, 3\} - \{1, 3\})$ .

We endow  $\mathbb{C}[B(n)]$  with the standard inner product defined by  $\langle X, Y \rangle = \delta_{XY}$  for  $X, Y \in B(n)$ . The primary lemma in our proof will be the following.

**Lemma 1.42.** There exists an SJB  $J(n)$  of  $\mathbb{C}[B(n)]$  satisfying

- (a) The vectors in  $J(n)$  are orthogonal with respect to the standard inner product  $\langle \cdot, \cdot \rangle$ .
- (b) Let  $0 \leq k \leq n/2$  and let  $(v_k, \dots, v_{n-k})$  be an SJC in  $J(n)$  starting at rank  $k$  and going to rank  $n - k$ . Then,

$$\frac{\|v_{i+1}\|}{\|v_i\|} = \sqrt{(i+1-k)(n-k-i)}$$

for  $k \leq i \leq n - k$ .

**Lemma 1.43.** For  $0 \leq k \leq n$ , set  $m(k) = \min\{k, n - k\}$ . For any  $0 \leq k \leq n$ ,  $\mathbb{C}[B(n, k)]$  can be decomposed into orthogonal mutually non-isomorphic irreducibles as  $W_{k,0} \oplus W_{k,1} \oplus \dots \oplus W_{k,m(k)}$ , where  $W_{k,r}$  is of dimension  $\binom{n}{k} - \binom{n}{k-1}$ . Furthermore,  $W_{k,m(k)}$  and  $W_{j,m(k)}$  are  $S_n$ -isomorphic for any  $k \leq j \leq n - k$ .

Before proving this, let us first establish some consequences of this result. The proof of Theorem 1.39 just uses the change-of-basis matrix associated with the SJB  $J(n)$ .

If we write the up operator  $U$  with respect to the SJB  $J(n)$ , we get  $q_k$  identical blocks of size  $p_k \times p_k$ . Each of these  $p_k \times p_k$  blocks has a 1 at the  $ij$ th entry if  $j - i = 1$  and 0 elsewhere. It turns out that something similar is also true for the  $M_{i,j,t}$ , as we shall show in the proof of Schrijver.

Suppose we normalize  $J(n)$  to get an orthonormal basis  $J'(n)$  of  $\mathbb{C}[B(n)]$ . Let  $(v_k, \dots, v_{n-k})$  be an SJC in  $J(n)$ . For  $i = k, \dots, n - k$ , set

$$v'_i = \frac{v_i}{\|v_i\|} \in J'(n)$$

and

$$\alpha_i = \frac{\|v_{i+1}\|}{\|v_i\|} = \sqrt{(i+1-k)(n-k-i)},$$

with  $\alpha_k = 0$ . Then,

$$U(v'_i) = \alpha_i v'_{i+1}.$$

So, with respect to  $J'(n)$ , the matrix  $U$  is again block-diagonal, with the block corresponding to  $(v'_k, \dots, v'_{n-k})$  having  $\alpha_i$  at the  $ij$ th block if  $j - i = 1$ .

Now, observe that with respect to the standard basis  $B(n)$  of  $\mathbb{C}[B(n)]$ , the matrices for  $U$  and  $D$  are real and transposes of each other. Because  $J'(n)$  is orthonormal, the corresponding matrices are adjoints even here! Therefore,  $D(v'_{i+1}) = \alpha_i v'_i$ , and the subspace spanned by the normalized SJC  $(v'_k, \dots, v'_{n-k})$  is closed under  $D$ .

**Proposition 1.44.** Let  $(v_k, \dots, v_{n-k})$  be an SJC in  $J(n)$ . Then, for  $i = k, \dots, n - k - 1$ , setting  $\alpha_i = \|v_{i+1}\|/\|v_i\|$ ,  $D(v_{i+1}) = \alpha_i^2 D(v_i)$ .

The proof is immediate from the previous discussion.

*Proof of Lemma 1.43.* Recall that  $\text{Hom}_{S_n}(B(n, k), B(n, k))$  is commutative and has dimension  $1 + \{k, n - k\}$ . It follows by Lemma 1.33 that  $\mathbb{C}[B(n, k)]$  is the direct sum of  $1 + \{k, n - k\}$  mutually non-isomorphic irreducibles. Further note that because the  $S_n$  action on  $B(n, k)$  results in a unitary representation of  $\mathbb{C}[B(n, k)]$ , these irreducibles can be taken to be orthogonal.

For  $0 \leq k \leq j \leq n - k \leq n$ , it is easily checked that the  $S_n$  action on  $B(n, k) \times B(n, j)$  has  $1 + k$  irreducibles; the idea is the same as that in Example 2, where  $(X, Y) \sim (X', Y')$  iff  $|X \cap Y| = |X' \cap Y'|$ . This implies that every irreducible occurring in  $\mathbb{C}[B(n, k)]$  also occurs in  $\mathbb{C}[B(n, j)]$ , and in particular,  $\mathbb{C}[B(n, k)]$  and  $\mathbb{C}[B(n, n - k)]$  are isomorphic as  $S_n$ -modules. The desideratum follows. ■

For example, when  $k = 0$ , we get only the trivial irreducible representation. When  $k = 1$ , we get the trivial irreducible as well as that mentioned in Example 6, which is of dimension  $n - 1$ . For  $k = 2$ , we get these two irreducible and another irreducible, which is forced to have dimension  $\binom{n}{2} - n$  (since we know the dimensions of the first two irreducibles).

*Proof of Lemma 1.42.* Now, let us play with these irreducibles in order to get an SJB. If we manage to show that  $U$  maps  $W_{j,m(k)}$  to  $W_{j+1,m(k)}$  bijectively for  $k \leq j < n - k$ , we are done – Schur's Lemma would imply that it then acts like some multiple of  $\text{Id}$ , so if we take some orthogonal basis of  $W_{k,m(k)}$ , applying  $U$  repeatedly maps this basis to an orthogonal basis of  $W_{j,m(k)}$  for any  $k \leq j \leq n - k$ .

Note that  $U : W_{j,m(k)} \rightarrow W_{j+1,m(k)}$  is, by Schur's Lemma, either a multiple of the identity or 0.

\*\*\*\*\* INCOMPLETE \*\*\*\*\*

Let  $(v_k, \dots, v_{n-k})$  be an SJB in  $J(n)$ . To complete the proof, it remains to find  $\alpha_i = \|v_{i+1}\|/\|v_i\|$ . Consider the linear operator  $H : \mathbb{C}[B(n)] \rightarrow \mathbb{C}[B(n)]$  defined by  $X \mapsto (n - 2|X|)X$ . First off, observe that  $UD - DU = H$ . This can be proved easily using a combinatorial argument. For  $X \in B(n)$  of size  $k$ , applying  $UD$  gives  $X$  back in  $n - k$  ways (since we must choose one of the elements not in  $X$  to add and subsequently remove), and applying  $DU$  gives  $X$  back in  $k$  ways. Furthermore, the component for any other set  $Y$  is 0, since it can be arrived at in at most one way for  $UD$  (or  $DU$ ) – removing the element in  $X \setminus Y$  and adding the element in  $Y \setminus X$ .

Now, recall from Proposition 1.44 that  $D(v_{i+1}) = \alpha_i^2 v_i$ . We determine the value of  $\alpha_i^2$  by induction on  $i$ . First off,

$$\alpha_k^2 v_k = D(v_{k+1}) = (DU)(v_k) = (UD - H)(v_k) = -H(v_k) = (n - 2k)v_k,$$

where we used the fact that  $D(v_k) = 0$ . Therefore,  $\alpha_k^2 = n - 2k$ .

For  $k < i \leq n - k$ , we have

$$\alpha_i^2 v_i = (DU)(v_i) = (UD - H)(v_i) = U(\alpha_{i-1}^2 v_{i-1}) - H(v_i) = \alpha_{i-1}^2 v_i - (n - 2i)v_i,$$

and the claim follows by induction. ■

**Lemma 1.45** (Binomial inversion). Let  $a_0, \dots, a_n$  and  $b_0, \dots, b_n$  be sequences. Then,

$$a_t = \sum_{u=0}^n \binom{u}{t} b_u$$

for  $t = 0, \dots, n$  iff

$$b_t = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} a_u$$

for  $t = 0, \dots, n$ .

*Proof.* Let  $M$  be the  $n \times n$  matrix with  $t$ uth entry equal to  $\binom{u}{t}$ , and  $N$  the matrix with  $t$ uth entry equal to  $(-1)^{u-t} \binom{u}{t}$ . The question asks to show that  $M = N^{-1}$ . Consider the vector space spanned by  $\{1, x, x^2, \dots, x^n\}$ . Another basis for this space is  $\{1, (x-1), (x-1)^2, \dots, (x-1)^n\}$ . We have

$$x^u = \sum_{t=0}^n \binom{u}{t} (x-1)^t$$

and

$$(x-1)^u = \sum_{t=0}^n (-1)^{n-t} \binom{u}{t} x^t.$$

The desideratum follows since the two resulting change-of-basis matrices, equal to  $M, N$ , are inverses of each other. ■

**Proposition 1.46.** It holds that

$$M_{i,j,t} = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} M_{i,u,u} M_{u,j,u}.$$

*Proof.* Note that

$$M_{i,t,t} M_{t,j,t} = \sum_{u=0}^n \binom{u}{t} M_{i,j,t}.$$

The  $XY$ th entry of the left is equal to the number of size  $u$  sets  $Z$  such that  $Z \subseteq X, Y$ , assuming  $|X| = i$  and  $|Y| = j$ . If  $X \cap Z = u$ , this number is precisely  $\binom{u}{t}$ . This is exactly equal to the  $XY$ th entry of the right.

To complete the proof, apply binomial inversion. ■

*Proof of Schrijver.* For  $i, j, k, t$ , define

$$\beta_{i,j,k,t} = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} \binom{n-2k}{u-k} \binom{n-k-u}{i-u} \binom{n-k-u}{j-u}.$$

For  $0 \leq k \leq m$  and  $k \leq i, j \leq n-k$ , define  $E_{i,j,k}$  to be the  $p_k \times p_k$  matrix, with rows and columns indexed by  $k, k+1, \dots, n-k$ , with the entry in row  $i$  and column  $j$  equal to 1 and all other entries 0.

The block-diagonalizing unitary matrix  $V$  is the change-of-basis matrix to the basis described by Lemma 1.42. (a) follows near-immediately by Lemma 1.43 and the proof of Lemma 1.42, and (b) is immediate from (a).

For (c), suppose that  $x_{i,j,t} = 1$  and all others are 0, so we have

$$\Phi(M_{i,j,t}) = (R_0, \dots, R_m).$$

We claim that for  $0 \leq k \leq m$ ,

$$R_k = \begin{cases} \binom{n-2k}{i-k}^{-1/2} \binom{n-2k}{j-k}^{1/2} \beta_{i,j,k,t} E_{i,j,k}, & k \leq i, j \leq n-k, \\ 0, & \text{otherwise.} \end{cases}$$

Now, the  $S_n$ -linear map  $M_{i,j,t}$  maps homogeneous vectors at the  $i$ th level to some (possibly zero) vector at the  $j$ th level, and everything else to 0. Since all the vectors in our basis  $J(n)$  are homogeneous, all the irreducibles except those at the  $i$ th level are certainly mapped to 0. In particular, the irreducible  $W_{i,m(k)}$  must map to  $W_{j,m(k)}$ , and  $W_{r,m(k)}$  maps to 0 for any  $r \neq i$ .

In more concrete terms, this implies that  $R_k = 0$  if  $i$  or  $j$  is not in  $k, k+1, \dots, n-k$ . So, suppose  $k \leq i, j \leq n-k$ . The above observation again implies that  $R_k$  is some multiple of  $E_{i,j,k}$ .

This is where Proposition 1.46 enters the picture. Consider the simpler case where  $j = t = u$  with  $i \geq u$ , so

$$\Phi(M_{i,u,u}) = (A_0^u, \dots, A_m^u).$$

Again,  $A_k^u$  is some multiple of  $E_{i,u,k}$ . Now,  $M_{i,u,u}$  just takes a set  $X \in B(n)$  of size  $i$  to all subsets  $Y \subseteq X$  of size  $u$ . Such a subset can be constructed by taking a “path” from  $X$  down to  $Y$ , removing one element at a time. Each level of such a path is constructed precisely by  $D$ ! Since each  $Y$  is repeated by  $(i-u)!$  paths,  $M_{i,u,u}$  is just equal to  $D^{i-u}/(i-u)!$ . Recall Proposition 1.44. It follows that

$$\begin{aligned} (A_k^u)_{iu} &= \frac{1}{(i-u)!} \prod_{w=u}^{i-1} \sqrt{(w+1-k)(n-k-w)} \\ &= \frac{1}{(i-u)!} \prod_{w=u}^{i-1} (n-k-w) \binom{n-2k}{w-k}^{1/2} \binom{n-2k}{w+1-k}^{-1/2} \\ &= \binom{n-k-u}{i-u} \binom{n-2k}{u-k}^{1/2} \binom{n-2k}{i-k}^{-1/2} \end{aligned}$$

and therefore,

$$A_k^u = \begin{cases} \binom{n-k-u}{i-u} \binom{n-2k}{u-k}^{1/2} \binom{n-2k}{i-k}^{-1/2} E_{i,u,k}, & k \leq u \leq n-k, \\ 0, & \text{otherwise.} \end{cases}$$

Similarly, if  $\Phi(M_{u,j,u}) = (B_0^u, \dots, B_m^u)$ ,

$$B_k^u = \begin{cases} \binom{n-k-u}{j-u} \binom{n-2k}{u-k}^{1/2} \binom{n-2k}{j-k}^{-1/2} E_{u,j,k}, & k \leq u \leq n-k, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, using Proposition 1.46,

$$\begin{aligned} (R_k)_{ij} &= \sum_{u=k}^{n-k} (-1)^{u-t} \binom{u}{t} \sum_{\ell=k}^{n-k} (A_k^u)_{i\ell} (B_k^u)_{\ell j} \\ &= \sum_{u=k}^{n-k} (-1)^{u-t} \binom{u}{t} (A_k^u)_{iu} (B_k^u)_{uj} \\ &= \binom{n-2k}{i-k}^{-1/2} \binom{n-2k}{j-k}^{1/2} \beta_{i,j,k,t} \end{aligned}$$

as desired, proving the theorem. Here, for the final equality, we substituted the expressions for  $A_k^u$  and  $B_k^u$  as proved above. ■

### 1.5. Johnson schemes

Following on from the previous subsection, let  $0 \leq k \leq \lfloor n/2 \rfloor$ , and consider  $\mathcal{A} = \text{Hom}_{S_n}(B(n, k), B(n, k))$ . Recall that unlike  $\text{Hom}_{S_n}(B(n), B(n))$ , this  $*$ -algebra is commutative and of dimension  $k+1$ . The orbital basis of this algebra is  $\{M_t\}_{0 \leq t \leq k}$ , where  $(M_t)_{XY} = 1$  if  $|X \cap Y| = t$  and 0 otherwise. Note that this is essentially just (an appropriate submatrix of)  $\bar{M}_{k,k,t}$ . Let us determine the eigenvalues of the  $M_t$  on each of its  $k+1$  eigenspaces.

We have already discovered these  $k+1$  eigenspaces in the previous subsection! Indeed, we can decompose  $\mathbb{C}[B(n, k)] = W_0 \oplus \dots \oplus W_k$ , where

$$W_j = \text{span}\{v \in J(n) : r(v) = k \text{ and the SJC on which } v \text{ lies starts at rank } j\}.$$

As argued earlier,  $\dim W_j = \binom{n}{j} - \binom{n}{j-1}$ .

We would like to determine the eigenvalues of  $M_{k,k,t}$  on these eigenspaces. Recalling binomial inversion Proposition 1.46, we have

$$M_{k,k,t} = \sum_{u=0}^n (-1)^{u-t} \binom{u}{t} M_{k,u,u} M_{u,k,u}.$$

\*\*\*\*\* INCOMPLETE \*\*\*\*\*

This implies that the eigenvalue of  $M_t$  on  $W_j$  is

$$\sum_{u=0}^n (-1)^{u-t} \binom{u}{t} \binom{k-j}{k-u} \binom{n-j-u}{k-u}.$$

This has an interesting application in counting the number of spanning trees of the Johnson graph.

**Definition 1.47.** A *rooted spanning tree* of a graph  $G = (V, E)$  is a pair  $(T, v)$ , where  $T$  is a spanning tree and  $v$  is a vertex in the graph.

Note that the number of rooted spanning trees of a graph is  $|V|$  times the number of spanning trees of the graph.

**Definition 1.48.** Given a graph  $G = (V, E)$ , the *Laplacian* of  $G$  is the  $V \times V$  matrix  $L = D - A$ , where  $D$  is the diagonal matrix with  $D_{uu}$  equal to the degree of  $u$ , and  $A$  is the adjacency matrix of the graph.

**Theorem 1.49** (Matrix Tree Theorem). Let  $G$  be a connected graph with Laplacian  $\mathcal{L}$ . Then, the number of rooted spanning trees of  $G$  is equal to the product of nonzero eigenvalues of  $\mathcal{L}$ .

It may also be shown that 0 is an eigenvalue of  $\mathcal{L}$  of multiplicity 1. We do not prove the matrix tree theorem.

**Corollary 1.50.** The complete graph  $K_n$  has  $n^{n-2}$  spanning trees.

This is direct using the spanning tree theorem, and there are also several bijective proofs known – see Section 1.2 of the author's [Combinatorics I notes](#) for more details.

**Corollary 1.51.** The number of spanning trees of the  $n$ -hypercube is  $(1/n) \prod_{k=1}^n (2k)^{\binom{n}{k}}$ .

We had studied the eigenvalues of the adjacency matrix of  $n$ -hypercube when studying the Delsarte bound. Since the graph is  $n$ -regular, this also gives the eigenvalues of the Laplacian.

**Corollary 1.52.** The number of spanning trees of the Johnson graph  $J(n, k)$  for  $k \leq n/2$  is

$$\frac{1}{n} \prod_{j=1}^k (j(n-j+1))^{\binom{n}{j} - \binom{n}{j-1}}.$$

Again, we had studied the eigenvalues of the adjacency matrix of  $J(n, k)$  earlier in this section (and indirectly in the Schrijver bound), and the graph is  $k(n-k)$ -regular.

For the last two corollaries, no bijective proof is known.