MA 862 : Combinatorics II

Amit Rajaraman

Last updated February 3, 2023

Contents

§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. $\mathrm{Id} \in \mathcal{A}$.

That is, it is a subalgebra that is closed under conjugate transposes.
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

$$\binom{n+1}{k}_q = \binom{n}{k-1}_q + q^k \binom{n}{k}_q \tag{1.1}$$

for $n \geq 0, k \geq 1$ with $\binom{n}{0}_q = 1$ and $\binom{0}{k} = \delta_{0,k}$. 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 $\{C_1, \ldots, C_k\}$ 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 $\mathrm{span}\{\mathrm{Id}, A, A^2, \ldots\}$.

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

For $A \in \mathcal{M}^n(\mathbb{C})$ similar to a Hermitian matrix, that is, PAP^{-1} is Hermitian for some P, $P\langle A \rangle P^{-1}$ is 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 $|X \triangle Y| = 1$. 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 $\varphi : G \to \mathcal{U}_n(\mathbb{C})$.

Theorem 1.3. Let φ be a unitary representation as above. 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 φ.

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* $\rho : G \to \mathcal{U}_S(\mathbb{C})$ – 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 $\rho : G \to \mathcal{U}_S(\mathbb{C}), \tau : G \to \mathcal{U}_T(\mathbb{C})$ be the corresponding maps. Consider

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

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

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, sth 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 θ_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 $(\sigma_1, \sigma_2, \ldots, \sigma_n, \pi)$. This group acts on $B(n)$ by first permuting the n coordinates according to π, then deciding whether or not to flip the entries based on the (σ_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 α, β differ. We write $(\alpha, \beta) \sim (\alpha', \beta')$ if the two are in the same H_n-orbit.

Lemma 1.6. (α, β) and (α', β') 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 α which has all 0s at the start then all 1s. Then, flip all the 1s in α. Consider the element β'' obtained by performing the same operations on β. Due to the first part, β'' has exactly k 1s. Next, permute the coordinates of β'' to get β''', which has all 0s at the start then all 1s. $(0, \beta''')$ is in the same orbit as (α, β). By performing similar operations, it is also in the same orbit as (α', β'), completing the proof. ■

Let $A_0, A_1, \ldots, A_n$ 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 $\langle A \rangle = \operatorname{span}\{A_0, A_1, \ldots, A_n\}$.

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 $A_0, A_1, \ldots, A_{j+1}$ (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 $k = 0, 1, \ldots, n$, 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 $\pi \cdot \{i_1, \ldots, i_k\} = \{\pi(i_1), \ldots, \pi(i_k)\}$. 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,

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

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

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

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 $\binom{n}{0}, \binom{n}{1} - \binom{n}{0}, \binom{n}{2} - \binom{n}{1}, \ldots, \binom{n}{k} - \binom{n}{k-1}$. 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 $\mathrm{GL}_n(\mathbb{F}_q)$ 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 $\langle A \rangle = \operatorname{span}\{A_k, \dots, A_{\max\{0,2k-n\}}\}$.

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

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 $k \le n/2$) 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 $i-t \ge 0$, $j-t \ge 0$, and $i+j-t \le n$. 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 $i-t, j-t, t, r \ge 0$. Therefore, setting $\mathcal{A} = \operatorname{Hom}_{S_n}(B(n), B(n))$, we have $\dim \mathcal{A} = \binom{n+3}{3}$. Further note that $\mathcal{A}$ is non-commutative. Indeed, $M_{2,3,1}M_{3,4,2} \ne 0$ but $M_{3,4,2}M_{2,3,1} = 0$.

The q-analogue of the above example is as follows. Let $\mathrm{GL}_n(\mathbb{F}_q)$ 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 $\operatorname{Hom}_{H_n}(B(n), B(n))$ 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 PM_{2n}. S_{2n} acts on PM_{2n} in an obvious manner, by mapping the matching $\{i_1j_1, i_2j_2, \dots, i_nj_n\}$ to $\{\pi(i_1)\pi(i_2), \dots, \pi(i_n)\pi(j_n)\}$. What are the K_{2n} orbits on $\mathrm{PM}_{2n} \times \mathrm{PM}_{2n}$?
Let $M_1, M_2 \in \mathrm{PM}_{2n}$. 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 edgees 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 $1 \le k \le n$. 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 π 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 $W_1, \ldots, W_m$ 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 $p_1, \ldots, p_m$ and $q_1, \ldots, q_m$ (determined up to permutation) such that $U^\dagger \mathcal{A} U$ is the set of all $((p_0, q_0), \ldots, (p_m, q_m))$*-block diagonal matrices*, that is, the set of all matrices

$$U^\dagger \mathcal{A} U = \begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_m \end{pmatrix},$$

where C_k is a block diagonal matrix

$$C_k = \begin{pmatrix} B_k & & & \\ & B_k & & \\ & & \ddots & \\ & & & B_k \end{pmatrix}$$

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

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 $\varphi : G \to \mathrm{GL}(V)$ 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 φ is denoted φ_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

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

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,

$$\begin{aligned} w &= c_1 1 + c_2 2 + \cdots + c_n n \in W \\ (1\ 2)w &= c_2 1 + c_1 2 + \cdots + c_n n \in W \end{aligned}$$

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 $j = 2, 3, \ldots, n$. 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 $\varphi : G \to \mathcal{U}(V)$. In such a case, V is called a *unitary G-module*.

Above $\mathcal{U}(V)$ is the subgroup of matrices in $\mathrm{GL}(V)$ 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 $f : V \to W$ is said to be *G-linear* if f commutes with the action of G, that is, $f(gv) = gf(v)$. We denote

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

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 $f : V \to W$ be G-linear. Then, either $f \equiv 0$ or f is an isomorphism.

Proof. Note that $\ker f$ and $\operatorname{im} f$ 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 $\operatorname{im} f = W$ so f is an isomorphism. ■

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

Proof. Let λ 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,

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

Lemma 1.28. 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,

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

In particular,

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

Proof. Let $\pi_1 : W \to W_1$ and $\pi_2 : W \to W_2$ denote the respective projection maps. Given $T \in \mathrm{Hom}_G(V, W_1 \oplus W_2)$, we have $\pi_1 \circ T \in \mathrm{Hom}_G(V, W_1)$ and $\pi_2 \circ T \in \mathrm{Hom}_G(V, W_2)$. For the backward inclusion, given $T_1 \in \mathrm{Hom}_G(V, W_1), T_2 \in \mathrm{Hom}_G(V, W_2)$, the map T defined by $T(v) = (T_1(v), T_2(v))$ is in $\mathrm{Hom}_G(V, W)$. This establishes an isomorphism between $\mathrm{Hom}_G(V, W)$ and $\mathrm{Hom}_G(V, W_1) \oplus \mathrm{Hom}_G(V, W_2)$, 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 1.29. Let $V_1, \ldots, V_r$ be irreducible G-modules and V, W be G-modules such that

$$V \cong n_1 V_1 \oplus n_2 V_2 \oplus \cdots \oplus n_r V_r \text{ and}$$
$$W \cong m_1 V_1 \oplus m_2 V_2 \oplus \cdots \oplus m_r V_r,$$

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

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

Corollary 1.30. Let V be a G-module such that

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

where $V_1, \ldots, V_r$ 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 $\dim \mathrm{Hom}_G(V, W) = n$. ■

Definition 1.31. A G-module V is *multiplicity-free* iff for any irreducible W, $\dim \mathrm{Hom}_G(V, W) \in \{0, 1\}$.

Lemma 1.32. Let G act on a set S and consider $\mathcal{A} = \mathrm{Hom}_G(S, S)$. 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

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

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

1.3. The Delsarte Bound

Definition 1.33. 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 1.34. 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 $ij \notin E$, $\mathrm{Tr}(M) = 1$, and $|S| = \sum_{i,j} M_{ij}$.

Definition 1.35 (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

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

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 ϵ).

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.

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

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 ρ_τ be the $B(n) \times B(n)$ permutation matrix that permutes vertices according to τ. The key idea is that since τ 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, $M \in \mathrm{Hom}_{H_n}(B(n), B(n))$, 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_σ, 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 $A_0, \ldots, A_n$ be the orbital basis of $\mathrm{Hom}_{H_n}(B(n), B(n))$, 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 1.36. Let λ_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,

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

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 λ_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.

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

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 $\mathbb{C}[B(n)] \to (\mathbb{C}^2)^{\otimes n}$ 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

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

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, Π 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 $\mathcal{A} = \mathrm{Hom}_{S_n}(B(n), B(n))$ – 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 1.37. 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 $\alpha_{i,j,t} = \lambda_i / |C| \binom{n}{i-t,t,j-t}$. 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 1.36, 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 $\alpha_{i,j,t}$.

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