MA 862 : Combinatorics II

Amit Rajaraman

Last updated January 6, 2023

Contents

§1. Introduction

1.1. The Delsarte bound

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 $\{C_1, \ldots, C_k\}$ rows 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 is 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 in this section.

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 f 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 be possible 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

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

Finally, we shall set $S = T$ so that it is a $*$-algebra.

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 $\{A\}$, $\langle A \rangle \subseteq \mathcal{A}$. 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?