Theorem 18.9. *With the above notation,*

$$B_Y^t B_Y = \frac{|Y|}{|X|} P^t \Delta_{a_Y^*} P.$$

Proof. For $0 \le i, j \le d$ we show that the (i,j)-entry of each side is equal to

$$|Y| \sum_{k=0}^{d} p_{i,j}^k a_k.$$

Using Lemma 18.8 the (i,j)-entry of $B_Y^t B_Y$ is equal to

$$(A_i \psi_Y)^t A_j \psi_Y = \psi_Y^t A_i A_j \psi_Y = \sum_{k=0}^{d} p_{i,j}^k \psi_Y^t A_k \psi_Y = |Y| \sum_{k=0}^{d} p_{i,j}^k a_k.$$

The (i,j)-entry of $P^t \Delta_{a_Y^*} P$ is equal to

$$\begin{aligned}
\sum_{\ell=0}^{d} P_{i,\ell}^t a_\ell^* P_{\ell,j} &= \sum_{\ell=0}^{d} P_i(\ell) a_\ell^* P_j(\ell) \\
&= \sum_{\ell=0}^{d} a_\ell^* \sum_{k=0}^{d} p_{i,j}^k P_k(\ell) \\
&= \sum_{k=0}^{d} p_{i,j}^k \sum_{\ell=0}^{d} a_\ell^* P_k(\ell) \\
&= |X| \sum_{k=0}^{d} p_{i,j}^k a_k.
\end{aligned}$$

□

Corollary 18.10. *The rank of the matrix B_Y is equal to the number of nonzero scalars among $\{a_i^*\}_{i=0}^d$.*

Proof. By Theorem 18.9 and since P is invertible. □

Lecture 26

Let us clarify what it means for some a_i^* to be zero.

Lemma 18.11. *For $0 \le i \le d$ the following are equivalent:*

(i) $a_i^* = 0$;

(ii) $E_i \psi_Y = 0$;

(iii) *column i of $B_Y Q$ is zero.*

Proof. By Corollary 18.5 and Lemma 18.8(ii). □

Definition 18.12. We define some parameters as follows.

(i) Define

$$\delta = \min\{i|1 \le i \le d,\ a_i \neq 0\}, \qquad \delta^* = \min\{i|1 \le i \le d,\ a_i^* \neq 0\}.$$

We call δ (resp. δ^*) the *minimum distance* (resp. *dual minimum distance*) of Y.

(ii) Define

$$s = \big|\{i|1 \le i \le d,\ a_i \neq 0\}\big|, \qquad s^* = \big|\{i|1 \le i \le d,\ a_i^* \neq 0\}\big|.$$

We call s (resp. s^*) the *degree* (resp. *dual degree*) of Y.

(iii) Define

$$t = \max\{i|1 \le i \le d,\ a_1^* = a_2^* = \cdots = a_i^* = 0\} = \delta^* - 1.$$

We call t the *strength* of Y.

The above definitions depend on the given orderings $\{R_i\}_{i=0}^d$ and $\{E_i\}_{i=0}^d$.

Our next general goal is to explain the MacWilliams inequality. This inequality will play an important role for codes and designs.

We bring in some notation. For any row vector $u = (u_0, u_1, \ldots, u_d)$ such that $u_0 \neq 0$, define

$$s(u) = \big|\{i|1 \le i \le d,\ u_i \neq 0\}\big|.$$

We also define

$$t(u) = \max\{i|1 \le i \le d,\ u_1 = u_2 = \cdots = u_i = 0\}.$$

If $u_1 \neq 0$ then we define $t(u) = 0$.

Theorem 18.13. (MacWilliams inequality). *Consider a row vector $u = (u_0, u_1, \ldots, u_d)$ such that $u_0 \neq 0$.*

(i) *Assume that the ordering $\{R_i\}_{i=0}^d$ is P-polynomial. Then*

$$s(uQ) \ge \left\lfloor \frac{t(u)}{2} \right\rfloor.$$

(ii) *Assume that the ordering $\{E_i\}_{i=0}^d$ is Q-polynomial. Then*

$$s(uP) \ge \left\lfloor \frac{t(u)}{2} \right\rfloor.$$

Proof. (i) Write $\theta_i = P_1(i)$ for $0 \le i \le d$. For $0 \le k \le d$ there exists a polynomial $v_k(z)$ that has degree k and $P_k(i) = v_k(\theta_i)$ for $0 \le i \le d$. Abbreviate $t = t(u)$. By assumption $u_i = 0$ for $1 \le i \le t$. Abbreviate $s = s(uQ)$. We assume $s < \lfloor t/2 \rfloor$ and get a contradiction. Note that $2s + 2 \le t$. Define the set $S = \{i | 1 \le i \le d, \sum_{\ell=0}^{d} u_\ell Q_i(\ell) \neq 0\}$. So $s = |S|$. Define a polynomial

$$f(z) = (z - \theta_0) \prod_{j \in S} (z - \theta_j).$$

The degree of $f(z)$ is $s + 1$. For $0 \le i \le d$,

$$f(\theta_i) = 0 \qquad \text{if and only if} \quad i \in S \cup \{0\}.$$

The degree of $f(z)^2$ is $2s + 2$. Therefore $f(z)^2$ is a linear combination of $\{v_i(z)\}_{i=0}^{2s+2}$. Write

$$f(z)^2 = \sum_{i=0}^{2s+2} b_i v_i(z) \qquad\qquad b_i \in \mathbb{R}.$$

Define

$$b_i = 0 \qquad\qquad (2s + 3 \le i \le d).$$

For $1 \le i \le d$ we have $u_i b_i = 0$, because $u_i = 0$ for $1 \le i \le t$ and $b_i = 0$ for $t + 1 \le i \le d$. Consider the row vector

$$b = (b_0, b_1, \ldots, b_d).$$

Observe that

$$uQ(bP^t)^t = uQPb^t = |X|ub^t = |X| \sum_{i=0}^{d} u_i b_i = |X| u_0 b_0.$$

Observe that for $j \in S \cup \{0\}$,

$$(bP^t)(j) = \sum_{k=0}^{d} b_k P_k(j) = \sum_{k=0}^{d} b_k v_k(\theta_j) = f(\theta_j)^2 = 0.$$

Therefore

$$uQ(bP^t)^t = 0.$$

We have $u_0 b_0 = 0$ and $u_0 \neq 0$, so $b_0 = 0$. Observe that

$$\sum_{i=0}^{d} f(\theta_i)^2 Q_i(0) = \sum_{i=0}^{d} \sum_{j=0}^{d} b_j P_j(i) Q_i(0) = \sum_{j=0}^{d} b_j \sum_{i=0}^{d} Q_i(0) P_j(i) = \sum_{j=0}^{d} b_j (QP)_{0,j} = |X| b_0 = 0.$$

This is impossible because $f(\theta_i)^2 > 0$ and $Q_i(0) = m_i > 0$ for $i \notin S \cup \{0\}$. □

Corollary 18.14. *Assume that the ordering $\{E_i\}_{i=0}^{d}$ is Q-polynomial. Let Y denote a nonempty subset of X that has degree s and strength t. Then*

$$s \ge \lfloor t/2 \rfloor.$$

Proof. Apply Theorem 18.13(ii) with $u = a_Y Q$. □

19 Codes in a P-polynomial association scheme

We continue to discuss a symmetric association scheme $\mathcal{X} = (X, \{R_i\}_{i=0}^d)$. Throughout this section we assume that the ordering $\{R_i\}_{i=0}^d$ is P-polynomial. Recall that the graph $\Gamma = (X, R_1)$ is distance-regular. Let ∂ denote the path-length distance function for Γ. Recall that for $y, z \in X$ and $0 \leq i \leq d$, $\partial(y,z) = i$ if and only if $(y,z) \in R_i$. Abbreviate $A = A_1$ and $\theta_i = P_1(i)$ for $0 \leq i \leq d$. Recall the valencies $\{k_i\}_{i=0}^d$. Abbreviate $k = k_1$.

For $x \in X$ and $0 \leq e \leq d$ we consider the set of vertices

$$\{y \in X | \partial(x,y) \leq e\}.$$

This set has a partition

$$\{y \in X | \partial(x,y) \leq e\} = \cup_{i=0}^e \Gamma_i(x).$$

Therefore

$$\big|\{y \in X | \partial(x,y) \leq e\}\big| = \sum_{i=0}^{e} |\Gamma_i(x)| = \sum_{i=0}^{e} k_i.$$

Let Y denote a subset of X with $|Y| \geq 2$. We call Y a *code*. We consider the minimum distance $\delta = \min\{\partial(y,z) | y, z \in Y,\ y \neq z\}$. We have $1 \leq \delta \leq d$.

Definition 19.1. For $0 \leq e \leq d$, the code Y is e *error correcting* whenever $\partial(y,z) \geq 2e+1$ for distinct $y, z \in Y$.

Lemma 19.2. *The code Y is e error correcting for $0 \leq e \leq \lfloor(\delta-1)/2\rfloor$.*

Proof. Clear. □

Lemma 19.3. *Write $e = \lfloor(\delta-1)/2\rfloor$. Then the dual degree s^* of Y satisfies*

$$s^* \geq e.$$

Proof. Apply the first MacWilliams inequality to the inner distribution of Y. □

Lemma 19.4. *Write $e = \lfloor(\delta-1)/2\rfloor$.*

(i) *The following subsets are mutually disjoint:*

$$\{z \in X | \partial(y,z) \leq e\} \qquad y \in Y. \tag{78}$$

(ii) *We have*

$$|Y|(k_0 + k_1 + \cdots + k_e) \leq |X|. \tag{79}$$

(iii) *Equality holds in* (79) *if and only if the subsets* (78) *partition X.*

Proof. By our above comments. □

Definition 19.5. The code Y is called *perfect* whenever equality holds in (79).

Recall the characteristic vector ψ_Y. Recall the Bose-Mesner algebra $\mathcal{M}$ and the vector $\mathbf{1} = \sum_{x \in X} \hat{x}$.

Theorem 19.6. (Lloyd type theorem, I). *Write $e = \lfloor (\delta - 1)/2 \rfloor$, and assume that Y is perfect.*

(i) *The vectors $\{A_i \psi_Y\}_{i=0}^{e}$ are linearly independent;*

(ii) $(A_0 + A_1 + \cdots + A_e)\psi_Y = \mathbf{1}$;

(iii) $(A - kI)(A_0 + A_1 + \cdots + A_e)\psi_Y = 0$;

(iv) *the vectors $\{A_i \psi_Y\}_{i=0}^{e}$ span $\mathcal{M}\psi_Y$;*

(v) $\dim \mathcal{M}\psi_Y = 1 + e$;

(vi) *the dual degree $s^* = e$.*

Proof. (i) For these vectors the nonzero coordinates are in disjoint locations.
(ii) Because X is partitioned by the subsets

$$\{z \in X | \partial(y, z) \le e\} \qquad\qquad y \in Y.$$

(iii) The graph Γ is regular with valency k, so $A\mathbf{1} = k\mathbf{1}$. The result follows by this and (ii).
(iv) Let W denote the span of $\{A_i \psi_Y\}_{i=0}^{e}$. Note that $\psi_Y \in W$. We show that $W = \mathcal{M}\psi_Y$. To do this, it suffices to show that $AW \subseteq W$. For $0 \le i \le e-1$ we have $AA_i\psi_Y \in W$, because AA_i is a linear combination of A_{i-1}, A_i, A_{i+1}. Also, $AA_e\psi_Y \in W$ in view of (iii).
(v) By (i), (iv) above.
(vi) We show that the dimension of $\mathcal{M}\psi_Y$ is equal to $1 + s^*$. The vector space $\mathcal{M}$ has a basis $\{E_i\}_{i=0}^{d}$. The vector space $\mathcal{M}\psi_Y$ has a basis consisting of the nonzero vectors among $\{E_i\psi_Y\}_{i=0}^{d}$. The cardinality of this basis is $1+s^*$, in view of Lemma 18.11. So the dimension of $\mathcal{M}\psi_Y$ is equal to $1 + s^*$. The result follows by this and (v). $\square$

Theorem 19.7. (Lloyd type theorem, II). *Write $e = \lfloor (\delta - 1)/2 \rfloor$, and assume that Y is perfect. Define a polynomial*

$$\Psi_e(z) = \sum_{i=0}^{e} v_i(z),$$

where the polynomial $v_i(z)$ has degree i and $A_i = v_i(A)$. Then the roots of $\Psi_e(z)$ are

$$\{\theta_i | 1 \le i \le d,\ E_i\psi_Y \ne 0\}.$$

Proof. The polynomial $\Psi_e(z)$ has degree e. There are e many integers i $(1 \le i \le d)$ such that $E_i\psi_Y \ne 0$. For these i we show that $\Psi_e(\theta_i) = 0$. We have

$$\begin{aligned} 0 &= (A - kI)(A_0 + A_1 + \cdots + A_e)\psi_Y \\ &= (A - kI)\Psi_e(A)\psi_Y. \end{aligned}$$