# Duality

Chris Godsil

# Preface

Duality in association schemes, related matters.

# Contents

# Chapter 1

# Association Schemes

We offer an introduction to association schemes, starting from an algebriac viewpoint.

## 1.1 Coherent Algebra

schur product

coherent algebra: Schur-closed and $*$-closed matrix algebra (with $J$).

**1.1.1 Lemma.** *A coherent algebra has a unique basis consisting of* 01*-matrices.*

If $\mathscr{A}$ is a coherent algebra, then the identity matrix is the sum of the diagonal matrices from the canonical basis. The algebra is *homogeneous* if $I$ belongs to the standard basis.

**1.1.2 Lemma.** *A commutative coherent algebra is homogeneous.*

An *association scheme* is a set of matrices that form the canonical basis for a commutative coherent algebra.

Axioms

## 1.2 Coherent Algebras as Commutants of Permutations

**1.2.1 Lemma.** *The commutant of a set of permutation $n \times n$ matrices is Schur-closed; equivalently, the commutant of a permutation group is a coherent algebra.*

The commutant of the permutation group $G$ is homogeneous if and only if $G$ is transitive.

examples: generously transitive permutation groups.

## 1.3 Quantum Permutations

Let $P$ be an $n\times$ matrix with entries from some algebra of $d\times d$ matrices (e.g., $\mathrm{Mat}_{d\times d}(\mathbb{C})$).

We say that a matrix $P$ over the ring $\mathrm{Mat}_{d\times d}(\mathbb{C})$ is a *quantum permutation* if:

(a) The entries of $P$ are projections.

(b) Each row and each column of $P$ sums to $I$.

If $R=\mathbb{Z}$, then the only idempotents are 0 and 1 and in this case a quantum permutation is a permutation.

There is a simple construction of quantum permutations based on Latin squares. Let $z_1,\ldots,z_n$ be an orthonormal basis for $\mathbb{C}^n$. If $L$ is an $n\times n$ Latin square, let $P$ be the $n\times n$ matrix we get replacing each entry $i$ of $L$ by $z_i z_i^*$.

**1.3.1 Lemma.** *If $P_1,\ldots,P_k$ are $d\times d$ projections and $\sum_r P_r = I_d$, then $P_rP_s=0$ if $r\neq s$.*

*Proof.* If $\sum_r P_r = I_d$, then

$$P_k=\sum_r P_kP_r = P_k + P_k\Big(\sum r\neq kP_r\Big),$$

and hence

$$P_k\Big(\sum r\neq kP_r\Big)=0$$

and therefore

$$0=\sum_{r\neq k}\mathrm{tr}(P_kP_r)$$

As projections are positive semidefinite, $\mathrm{tr}(P_kP_r)\geq 0$ and equality holds if and only if $P_kP_r=0$. □

**1.3.2 Lemma.** *If $P$ is a quantum permutation, then $P^*P=I$ (i.e., $P$ is unitary).*

Suppose $M$ and $N$ are quantum permutations of order $n\times n$. We define the $n\times n$ block matrix $M\star N$ by

$$(M\star N)_{i,j}=\sum_r M_{i,r}\otimes N_{r,j}$$

We leave the proof of the following as an exercise.

**1.3.3 Lemma.** *If $M$ and $N$ are quantum permutations of order $n\times n$, then $M\star N$ is too. Further, if $M$ and $N$ commute with $A$, so does $M\star N$.* □

## 1.4 Coherent Algebras as Commutants of Quantum Permutations

The matrices $M$ such that $M_\times I_d$ commute with $P$ form a matrix algebra that contains $I$ and $J$.

Since $P^*P = I$, the matrix $P^*$ is a polynomial in $P$ and so if $A \otimes I$ commutes with $P$, it commutes with $P^*$; consequently if $A \otimes I$ commutes with $P$, so does $A^*$.

**1.4.1 Theorem.** *The commutant of a set of $n \times n$ permutation matrices is a coherent algebra.*

*Proof.* We show that if $P$ is a quantum permutation that commutes with $M \otimes I$ and $N \otimes I$, it commutes with $(M \circ N) \otimes I$.

The $ij$-block of $(M \otimes I)P$ is

$$\sum_r M_{i,r} P_{r,j}$$

and, by hypothesis, this is equal to the $ij$-block of $P(M \otimes I)$:

$$\sum_s M_{s,j} P_{i,s}.$$

We have

$$\sum_r M_{i,r} P_{r,j} \sum_s N_{i,s} P_{s,j} = \sum_r (M_{i,r} N_{i,r}) P_{r,j}$$

where the right side is the $ij$-block of $((M \circ N) \otimes I)P$. Similarly

$$\sum_r M_{r,j} P_{i,r} \sum_r N_{r,j} P_{i,r} = \sum_r (M_{r,j} N_{r,j}) P_{i,r}$$

where the right side is the $ij$-block of $P((M \circ N) \otimes I)$. Since the left sides of the previous pair of equations are equal, our result follows. □

This result is easy to prove, and is left to the reader. One consequence of it is that quantum isomorphic graphs are cospectral with cospectral complements.

Following Atserias et al (arXiv:1611.09837v3), we define two graphs $X$ and $Y$ on $n$ vertices to be *quantum isomorphic* if there is a quantum permutation $P$ of order $n \times n$, with entries projections of order $d \times d$, such that

$$(A(X) \otimes I_d)P = P(A(Y) \otimes I_d).$$

If $X = Y$, we have a *quantum automorphism* of $X$. Since $P$ is unitary, the matrices $A(X) \otimes I$ and $A(Y) \otimes I$ are similar, and so we see that quantum isomorphic graphs are cospectral. From Lemma 1.3.3 though, it follows that if $X$ and $Y$ are quantum isomorphic, the coherent algebras generated by $A(X)$ and $A(Y)$ are isomorphic.

There are graphs that are quantum isomorphic but not isomorphic. (See [**?**].)

## 1.5 Type-II Matrices

We use $W^{(-)}$ to denote the Schur inverse of a matrix $W$ (which need not be square). We that an $n \times n$ matrix $W$ is a *type-II* matrix if $WW^{(-)T} = nI$. Hadamard matrices provide one class of type-II matrices. More generally a unitary matrix is type-II if and only if it is flat. For any nonzero complex number $t$, the matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & t & -t \\ 1 & -1 & -t & t \end{pmatrix}$$

is type II.

A *monomial matrix* is the product a permutation matrix and an invertible diagonal matrix. The monomial matrices of a given order form a group. If $M$ and $N$ are monomial and $W$ it type-II, then $MWN$ is type-II. We say that $MWN$ and $W$ are equivalent. If $W$ is type-II so is $W^T$, but in general $W$ and $W^T$ are not equivalent. If $W_1$ and $W_2$ are type-matrices, so is $W_1 \otimes W_2$.

The next result is easy to verify.

**1.5.1 Lemma.** *For an $n \times n$ matrix, any two of the following statements imply the third:*

*(a) $W$ is a type-II matrix.*

*(b) $n^{-1/2}W$ is unitary.*

*(c) $|W_{i,j}| = 1$ for all $i$ and $j$.* □

We say a type-II matrix is *flat* if all its entries have the same absolute value. The character table of an abelian group is a flat type-II matrix. A flat real type-II matrix is a Hadamard matrix.

Nomura [**?**] has shown that there are exactly three equivalence classes of $5 \times 5$ type-II matrices. One class is represented by the character table of the cyclic group of order five, the other two have representatives of the form $\alpha I + J$ (so here $W^{(-)}$ is not equivalent to $W$). Haagerup [**?**] has shown that if $n$ is not prime, there are infinitely many equivalence classes of unitary type-II matrices of order $n$.

For any complex number $t$, the matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & t & -t \\ 1 & -1 & -t & t \end{pmatrix}$$

is type II. Next we have the *Potts models*: if $W$ is $n \times n$ and

$$W = (t-1)I + J,$$

then

$$\begin{aligned} WW^{(-)T} &= ((t-1)I+J)((t^{-1}-1)I+J) \\ &= ((2-t-t^{-1})I+(n-2+t+t^{-1})J, \end{aligned}$$

whence it follows that $W$ is type II whenever $2-t-t^{-1}=n$, i.e., whenever $t$ is a root of the quadratic

$$t^2+(n-2)t+1.$$

As the first example suggests, any Hadamard matrix is a type-II matrix, and it is not unreasonable to view type-II matrices as a generalization of Hadamard matrices.

**1.5.2 Lemma.** *An $n\times n$ matrix $W$ is type-II if and only if for any two diagonal matrices $D_1$ and $D_2$,*

$$\langle D_1, W^{-1}D_2W\rangle = \frac{1}{n}\operatorname{tr}(D_1)\operatorname{tr}(D_2).$$

*Proof.* We have

$$\langle e_ie_i^T, W^{-1}e_je_j^TW\rangle = \operatorname{tr}(e_ie_i^TW^{-1}e_je_j^TW) = e_i^TW^{-1}e_je_j^TWe_i = (W^{-1})_{i,j}W_{j,i},$$

and so our claim for $D_1=e_ie_i^T$ and $D_2=e_je_j^T$ if and only if

$$(W^{-1})_{i,j}W_{j,i}=\frac{1}{n}.$$

It holds for all $i$ and $j$ if and only if $W^{-1}=\frac{1}{n}W^{(-1)T}$, i.e., if $W$ is type II. The result now follows by linearity. □

**1.5.3 Corollary.** *If $W$ is type II of order $n\times n$ and $D$ is diagonal,*

$$(W^{-1}DW)_{i,i}=\frac{1}{n}\operatorname{tr}(D).$$ □

**1.5.4 Lemma.** *Suppose $P_1,\dots,P_k$ are pairwise orthogonal projections summing to $I$. If $W$ is a $k\times k$ type-II matrix and we define*

$$U_i=\sum_j W_{i,j}P_i \qquad (i=1,\dots,k),$$

*then $U_1,\dots,U_k$ are invertible and*

$$\sum_i P_i\otimes P_i=\sum_i U_i\otimes U_i^{-1}.$$

*If $W$ is unitary, so are $U_1,\dots,U_k$.*

## 1.6 Nomura Algebras of Type-II Matrices

If $W$ is an $m \times n$ Schur-invertible matrix, we define $n^2$ vectors $Y_{i,j}(W)$ (for $0 \le i, j \le n$) by

$$W_{i/j} = We_i \circ W^{(-)} e_j.$$

The *Nomura algebra* $\mathscr{N}_W$ of $W$ is the set of $n \times n$ complex matrices for each each of the $n^2$ vectors $W_{i/j}$ is an eigenvector. This is a matrix algebra.

**1.6.1 Lemma.** *The matrix $W$ is type-II if and only if $J \in \mathscr{N}_W$.* □

If $W$ is type-II, it is invertible and therefore for fixed $j$, the vectors

$$W_{i/j} = \partial_j(W)^{-1} We_i$$

are linearly independent. If $M \in \mathscr{N}_W$, we define $\Theta_W(M)$ to be the $n \times n$ matrix such that

$$MW_{i/j} = (\Theta_W(M)_{i,j}) W_{i/j}.$$

The map $\Theta_W$ is linear on $\mathscr{N}_W$ and injective. We also have

$$\Theta_W(MN) = \Theta_W(M) \circ \Theta_W(N).$$

Let $W$ be a type-II matrix of order $n \times n$. Define matrices $\mathscr{F}_{i,j} = \mathscr{F}_{i,j}(W)$ by

$$\mathscr{F}_{i,j} = \frac{1}{n} W_{i/j} (W_{j/i})^T = \frac{1}{n} \partial_i(W)(We_j)^{(-1)} (We_j)^T \partial_i(W)^{-1}.$$

We note that $\mathscr{F}_{i,i} = \frac{1}{n} J$ and

$$\mathscr{F}_{i,j}^T = \mathscr{F}_{j,i},$$

Further

$$\mathscr{F}_{i,j}^{(-)} = n W_{j/i} (W_{i/j})^T = n^2 \mathscr{F}_{j,i}.$$

If $W$ is flat, then $F_{i,j}$ is Hermitian.

If $W$ is a type-II matrix, the columns of $W^{(-)}$ form a dual basis to the set of columns of $W$. It follows that the matrices $F_{i,j}$ are idempotents and that

$$\sum_i F_{i,j} = I = \sum_j F_{i,j}.$$

Now we can prove a very important result due to Nomura:

**1.6.2 Theorem.** *If $M \in \mathscr{N}_W$, then $\Theta_{W^T}(\Theta_W(M)) = nM^T$.*

*Proof.* Assume $M \in \mathscr{N}_W$. Then $M\mathscr{F}_{i,j} = \Theta(M)_{i,j} \mathscr{F}_{i,j}$ and, summing this over $j$ yields

$$M = \sum_j \Theta(M)_{i,j} \mathscr{F}_{i,j}.$$

Therefore

$$M_{r,s} = \frac{1}{n}\sum_j \Theta_W(M)_{i,j}\frac{W_{r,i}}{W_{r,j}}\frac{W_{s,j}}{W_{s,i}} = \frac{1}{n}\frac{W_{r,i}}{W_{s,i}}\sum_j \Theta_W(M)_{i,j}\frac{W_{s,j}}{W_{r,j}}.$$

If follows that

$$nM_{r,s}(W^T)_{s/r} = \Theta_W(M)(W^T)_{s/r}.$$

and this yields our result. □

This theorem tells us many things. First, we see that $\Theta_W$ and $\Theta_{W^T}$ are invertible and that $\mathcal{N}_W$ is closed under transposes. Since $\mathrm{im}(\Theta_{W^T})$ is Schur-closed, we also see that $\mathcal{N}_W$ is Schur-closed. As $\mathcal{N}_W$ is Schur-closed, it has a basis of 01-matrices and, consequently, $\mathcal{N}_W$ is closed under complex conjugation. To sum up, $\mathcal{N}_W$ is the Bose-Mesner algebra of an association scheme, and $\mathcal{N}_{W^T}$ is the Bose-Mesner algebra which we can view as dual to $\mathcal{N}_W$.

## 1.7 Type-II Matrices and Quantum Permutations

Let $\mathscr{F}_W$ be the $n^2 \times n^2$ block matrix with $ij$-block equal to $\mathscr{F}_{i,j}$; we call it the *matrix of idempotents* of $W$. Since $\mathscr{F}_{i,j}^T = \mathscr{F}_{j,i}$, we see that $\mathscr{F}$ is symmetric.

If $\mathscr{F}^\tau$ is the matrix we get by applying the transpose map to each block of $\mathscr{F}$, i.e., the partial transpose. Then

$$\mathscr{F}^\tau = \frac{1}{n}\mathscr{F}^{(-)}.$$

Let $S$ be the operator on $\mathbb{C}^n \otimes \mathbb{C}^n$ that sends $u \otimes v$ to $v \otimes u$ (for all $u$ and $v$).

**1.7.1 Lemma.** *If $W$ is type-II, then $\mathscr{F}_{W^T} = S\mathscr{F}_W S$.*

*Proof.* We have

$$n(\mathscr{F}_{i,j}(W))_{r,s} = \frac{W_{r,i}}{W_{r,j}}\frac{W_{s,j}}{W_{s,i}} = \frac{W_{r,i}}{W_{s,i}}\frac{W_{s,j}}{W_{r,j}} = \frac{W_{i,r}^T}{W_{i,s}^T}\frac{W_{j,s}^T}{W_{j,r}^T} = n(\mathscr{F}_{r,s}(W^T))_{i,j}.$$

Here the left hand and right hand terms are equal respectively to

$$(e_i \otimes e_r)^T \mathscr{F}(W)(e_j \otimes e_s), \qquad (e_r \otimes e_i)^T \mathscr{F}(W^T)(e_s \otimes e_j)$$

and the result follows. □

**1.7.2 Theorem.** *If $W$ is a type-II matrix, then $\mathscr{F}$ is type-II. If in addition $W$ is flat, then $\mathscr{F}$ is flat and is a quantum permutation matrix.*

*Proof.* For fixed $i$, the vectors $We_j$ form a basis of $\mathbb{C}^n$ and the vectors $n^{-1}(We_j)^{(-)}$ form a basis dual to this. Hence the matrices

$$\frac{1}{n}(We_j)^{(-1)}(We_j)^T$$

are pairwise orthogonal idempotents and sum to $I$. Therefore for fixed $i$ the matrices $F_{i,j}$ are pairwise orthogonal idempotents that sum to $I$.

Since $\mathscr{F}^T = \mathscr{F}$, it also follows that each column of $\mathscr{F}_W$ consists of pairwise orthogonal idempotents that sum to $I$. If $W$ is flat, then $F_{i,j}$ is Hermitian. □

**1.7.3 Theorem.** *Let $W$ be a type-II matrix and let $\mathscr{F}_W$ be the associated matrix of idempotents. The set of matrices $M$ such that $[I \otimes M, \mathscr{F}_W] = 0$ is equal to $\mathscr{N}_W$. The set of matrices $N$ such that $[N \otimes I, \mathscr{F}_W] = 0$ is equal to $\mathscr{N}_{W^T}$.*

*Proof.* We have that $[I \otimes M, \mathscr{F}_W] = 0$ if and only if $[M, \mathscr{F}_{i,j}] = 0$ for all $i$ and $j$. Now $M$ commutes with a rank-1 matrix $uv^*$ if and only if $u$ is a right eigenvector for $M$. Hence $[M, \mathscr{F}_{i,j}] = 0$ for fixed $i$ and all $j$ if and only if $M \in \mathscr{N}_W$.

For the second claim,

$$S((N \otimes I)\mathscr{F}_W)S = (I \otimes N)\mathscr{F}_{W^T},$$

from which the assertion follows. □

One consequence of this result is that $\mathscr{N}_W$ is the commutant of the set of matrices

$$\{F_{i,j} : j = 1, \ldots, n\}.$$

We also see that $\mathscr{N}_{W^T} \otimes \mathscr{N}_W$ is contained in the commutant of $\mathscr{F}_W$.

Since the set of matrices $N$ such that $N \otimes I$ commutes with $\mathscr{F}_W$ is Schur-closed, this set of matrices is itself is Schur-closed. Therefore $\mathscr{N}_{W^T}$ and $\mathscr{N}_W$ are Schur-closed.

# Chapter 2

# Products and Tensors

We show how to use the Kronecker product of matrices, or equivalently the tensor product of algebras, to construct new association schemes from old.

## 2.1 Tensor Powers

We consider constructions of association schemes that make use of the tensor product.

**2.1.1 Lemma.** *If $A_o, \ldots, A_d$ and $B_0, \ldots, B_e$ are two association schemes with $d$ and $e$ classes respectively, then the matrices*

$$A_i \otimes B_j, \quad 0 \le i \le d,\ 0 \le j \le e$$

*form an association scheme with $de + d + e$ classes, and that the Bose-Mesner algebra of this product is the tensor product of the Bose-Mesner algebras of its factors.*

*Proof.* This is not hard to verify directly. Alternatively let the two schemes be denoted by $\mathscr{A}$ and $\mathscr{B}$ respectively. It follows from **??** and **??** that the tensor product

$$\mathbb{C}[\mathscr{A}] \otimes \mathbb{C}[\mathscr{B}]$$

is closed under matrix and Schur multiplication. Since it contains $J$ and is transpose-closed, we deduce that it is the Bose-Mesner algebra of a scheme. The dimension of this algebra is $(d+1)(e+1)$ and hence this product scheme has the stated number of classes. □

Similarly we have a power construction:

**2.1.2 Lemma.** *If $\mathscr{A}$ is an association scheme with $d$ classes, then $\mathbb{C}[\mathscr{A}]^{\otimes k}$ is the Bose-Mesner algebra of an association scheme with $(d+1)^k - 1$ classes.* □

It is not hard to construct new association schemes with a large number of classes, hence the previous two constructions are not as useful as we might hope.

However there is an interesting construction based on the tensor power, which we develop now.

Suppose $V$ is a vector space. We define an action of $\mathrm{Sym}(k)$ on $V^{\otimes k}$ by declaring that if

$$x_1 \otimes \cdots \otimes x_k$$

and $\sigma \in \mathrm{Sym}(k)$, then

$$\sigma : x_1 \otimes \cdots \otimes x_k \mapsto x_{1\sigma} \otimes \cdots \otimes x_{k\sigma}.$$

It follows that $\sigma$ induces a linear map from $V^{\otimes k}$ to itself (which we will denote by $\sigma$. If $e_1, \ldots, e_d$ is a basis for $V$, then the products

$$e_{i_1} \otimes \cdots \otimes e_{i_k}$$

form a basis for $V^{\otimes k}$. Since $\sigma$ permutes the elements of this basis, the matrix representing $\sigma$ is a permutation matrix.

Note that some elements of $V^{\otimes k}$ are left fixed by the action of $\mathrm{Sym}(k)$. As examples we have the diagonal terms

$$e_i \otimes \cdots \otimes e_i$$

and, when $k = 2$, the sum

$$e_1 \otimes e_2 + e_2 \otimes e_1$$

is fixed by $\mathrm{Sym}(2)$. We define the *$k$-th symmetric power* of $V$ to be the subspace of $V^{\otimes k}$ formed by the vectors that are fixed by each element of $\mathrm{Sym}(k)$. If $\dim(V) = d$, then its $k$-th symmetric power has dimension $\binom{d+k-1}{k}$.

**2.1.3 Theorem.** *If $\mathscr{A}$ is an association scheme with $d$ classes, then the $k$-th symmetric power of $\mathbb{C}[\mathscr{A}]$ is an association scheme with $\binom{d+k}{k} - 1$ classes.*

*Proof.* The $k$-th symmetric power of $\mathbb{C}[\mathscr{A}]$ is the centralizer of a set of permutation matrices, and therefore it is Schur-closed by **??**. It is closed under matrix multiplication and transpose and contains $I$ and $J$, and it is commutative since $\mathbb{C}[\mathscr{A}]$ is. Therefore it is the Bose-Mesner algebra of an association scheme. □

We call the scheme produced by this construction the *$k$-th symmetric power* of $\mathscr{A}$, and we denote it by $H(k, \mathscr{A})$.

We note the proof of the previous theorem theorem also yields that a symmetric power of a coherent algebra is again a coherent algebra, and this power is homogeneous if the input is.

## 2.2 Generalized Hamming Schemes

In this section we offer an alternative, more concrete, construction of the symmetric power and consider some examples.

Suppose $\mathscr{A}$ is an association scheme with Schur idempotents $A_0, \ldots, A_d$ and vertex set $V$. If $u$ and $v$ are two elements of $V^n$, let $h(u, v)$ be the vector of length $d+1$ whose $i$-th entry $h_i(u, v)$ is the number of coordinates $j$ such that $u_j$ and $v_j$

are $i$-related. The entries of $h(u,v)$ sum to $n$; conversely any non-negative vector of length $n$ whose entries sum to $n$ is equal to $h(u,v)$ for some $u$ and $v$. If $\alpha$ is a non-negative vector of length $d+1$ and $\mathbf{1}^T\alpha = n$, define $A_\alpha$ to be the 01-matrix with rows and columns indexed by $V^n$ and with $(A_\alpha)_{u,v} = 1$ if and only if $h(u,v) = \alpha$. This set of matrices forms the $k$-th symmetric power of $\mathscr{A}$. If $\mathscr{A}$ is the scheme with one class on $q$ vertices, then $H(n,\mathscr{A})$ is the Hamming scheme $H(n,q)$.

By way of a more particular example, suppose $I$, $A_1$ and $A_2$ form an association scheme with two classes, i.e., the association scheme of a strongly regular graph. The Schur idempotents of $\mathscr{A}\otimes\mathscr{A}$ are the nine matrices

$$\begin{array}{ccc} I, & I\otimes A_1, & A_1\otimes I, \\ I\otimes A_2, & A_2\otimes I, & A_1\otimes A_2, \\ A_2\otimes A_1, & A_1\otimes A_1, & A_2\otimes A_2. \end{array}$$

The Schur idempotents of $H(2,\mathscr{A})$ are

$$\begin{array}{ccc} I, & I\otimes A_1 + A_1\otimes I, & I\otimes A_2 + A_2\otimes I, \\ A_1\otimes A_2 + A_2\otimes A_1, & A_1\otimes A_1, & A_2\otimes A_2. \end{array}$$

## 2.3 A Tensor Identity

We use $A\otimes B$ to denote the Kronecker product of two matrices $A$ and $B$. We offer a more exalted version of Seidel's identity, due to Koppinen.

**2.3.1 Theorem.** *Let $\mathscr{A}$ be an association scheme with $d$ classes. Then*

$$\sum_{i=0}^{d} \frac{1}{v v_i} A_i \otimes A_i^T = \sum_{i=0}^{d} \frac{1}{m_i} E_i \otimes E_i.$$

*Proof.* Suppose that $V$ is an inner product space and $u_1,\ldots,u_k$ and $v_1,\ldots,v_k$ are two orthogonal bases for a subspace $U$ of $V$. If

$$R = \sum_{i=1}^{k} \frac{1}{\langle u_i, u_i\rangle} u_i u_i^*$$

and

$$S = \sum_{i=1}^{k} \frac{1}{\langle v_i, v_i\rangle} v_i v_i^*,$$

and $x \in V$, then $Rx$ and $Sx$ are both the orthogonal projection of $x$ onto $U$. So $Rx = Sx$ for all $x$ and therefore $R = S$. Since

$$xy^* = x\otimes y^*,$$

we thus have

$$\sum_{i=1}^{k} \frac{1}{\langle u_i, u_i\rangle} u_i \otimes u_i^* = \sum_{i=1}^{k} \frac{1}{\langle v_i, v_i\rangle} v_i \otimes v_i^*. \tag{2.3.1}$$

Now let $\mathrm{vec} : \mathrm{Mat}_{m\times n}(\mathbb{C}) \to \mathbb{C}^{mn}$ be the linear map given by

$$\mathrm{vec}(A) = \begin{pmatrix} Ae_1 \\ \vdots \\ Ae_n \end{pmatrix}.$$

If $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$, let $M^{\#}$ denote the linear map from $\mathrm{Mat}_{n\times n}(\mathbb{C})$ to $\mathbb{C}$ given by

$$M^{\#}(X) := \mathrm{tr}(M^* X).$$

Note that

$$M^{\#}(X) = \mathrm{vec}(M)^* \,\mathrm{vec}(X).$$

Then (2.3.1) yields that

$$\sum_{i=0}^{d} \frac{1}{v v_i} A_i \otimes A_i^{\#} = \sum_{i=0}^{d} \frac{1}{m_i} E_i \otimes E_i^{\#}.$$

Consequently

$$\sum_{i=0}^{d} \frac{1}{v v_i} A_i \otimes \mathrm{vec}(A_i)^T = \sum_{i=0}^{d} \frac{1}{m_i} E_i \otimes \mathrm{vec}(\overline{E}_i)^T$$

and therefore

$$\sum_{i=0}^{d} \frac{1}{v v_i} A_i \otimes A_i = \sum_{i=0}^{d} \frac{1}{m_i} E_i \otimes \overline{E}_i.$$

Let $I$ denote the identity map on $\mathrm{Mat}_{v\times v}(\mathbb{C})$ and $\tau$ the transpose map. If we apply $I \otimes \tau$ to both sides of this identity, the result follows. □

We let $\mathscr{K}$ denote either of the two sums in the statement of 2.3.1. Since $E_j \otimes E_j$ is self-adjoint, we have $\mathscr{K}^* = \mathscr{K}$ and therefore we also have

$$\mathscr{K} = \sum_{i=0}^{d} \frac{1}{v v_i} A_i^T \otimes A_i.$$

## 2.4 Applications

We present three applications of our tensor identity.

First, suppose $X \in \mathrm{Mat}_{v\times v}(\mathbb{C})$ and $T : \mathbb{C}[\mathscr{A}] \otimes \mathbb{C}[\mathscr{A}] \to \mathbb{C}[\mathscr{A}]$ is the linear mapping given by

$$T(C \otimes D) = \mathrm{tr}(DX)C.$$

Therefore

$$T(\mathscr{K}) = \sum_{i=0}^{d} \frac{1}{v v_i} \mathrm{tr}(A_i^T X) A_i = \sum_{i=0}^{d} \frac{1}{m_i} \mathrm{tr}(E_i X) E_i.$$

An association scheme $\mathscr{A}$ with $d$ classes is *pseudocyclic* if its valencies $v_1, \ldots, v_d$ are all equal and its multiplicities $m_i$ are all equal. If we denote the common value of these parameters by $m$, then $v = dm + 1$. Koppinen's identity yields that

$$\mathscr{K} = \frac{1}{v} I + \frac{1}{vm} \sum_{i=1}^{d} A_i^{\otimes 2} = E_0 + \frac{1}{m} \sum_{i=1}^{d} E_i^{\otimes 2}.$$

Here

$$\sum_{i=1}^{d} A_i^{\otimes 2}$$

is the adjacency matrix of a regular graph. The previous equality shows that it has exactly three eigenvalues ($vm-m$, $v-m$ and $-m$), and therefore it is the adjacency matrix of a strongly regular graph.

The simplest example of a pseudocyclic scheme is the scheme with $d$ classes associated to the odd cycle $C_{2d+1}$. (In this case the strongly regular graph is $L(K_{2d+1,2d+1})$.)

We offer another proof of the inequality (**??**).

**2.4.1 Theorem.** *Let $\mathscr{A}$ be an association scheme with $d$ classes on $v$ vertices and let $R$ be a subset of $\{1,\dots,d\}$. If $C$ is an $R$-clique and $D$ is an $R$-coclique, then $|C||D| \le v$.*

*Proof.* Let $C$ be an $R$-clique and $D$ an $R$-coclique, with characteristic vectors $y$ and $z$ respectively. Let $S$ be the subset $C \times D$ of $V \times V$, with characteristic vector $x$. Then $x = y \otimes z$ and

$$x^T(A_i \otimes A_i)x = y^T A_i y\, z^T A_i z = 0$$

if $i \neq 0$. So

$$x^T x = x^T \left( \sum_i \frac{1}{v v_i} A_i \otimes A_i \right) x = \sum_{j=0}^{d} \frac{1}{m_j} x^T (E_j \otimes \overline{E_j}) x.$$

The matrices $E_i$ are positive-semidefinite, and therefore so are the matrices $E_i \otimes \overline{E_i}$. Consequently each term in the last sum is non-negative, and thus

$$|S| = xx^T \ge x^T (E_0 \otimes E_0) x = \frac{|S|^2}{v^2}.$$

Therefore $|S| \le v$. □

## Notes

Bailey [**?**] also offers a detailed treatment of constructions based on tensor products. Delsarte [**?**, ???] introduced what we called the generalised Hamming schemes, calling them ???. Its applications in 2.4 are new, although the results themselves are not. (In particular the pseudocyclic schemes we present were first found by [**?**].)

# Chapter 3

# Translation Schemes

Suppose $\Gamma$ is an abelian group of order $v$. The conjugacy class scheme on $\Gamma$ is a scheme with $v-1$ classes, and each minimal Schur idempotent is a permutation matrix. Many interesting schemes arise as subschemes of these; they are known as translation schemes.

## 3.1 Characters

Let $\Gamma$ be a finite abelian group. A *character* of $\Gamma$ is a homomorphism from $\Gamma$ into the multiplicative group formed by the non-zero complex numbers. The set of all characters of $\Gamma$ is denoted by $\Gamma$, and is called the *character group* of $\Gamma$. If $\psi \in \Gamma^*$ and $g \in \Gamma$, then $g^k$ for some integer $k$. Therefore

$$\psi(1) = \psi(g^k) = \psi(g)^k,$$

whence we see that $\psi(g)$ is a $k$-root of unity. It follows that

$$\psi(g^{-1}) = \overline{\psi(g)}.$$

The *trivial* character is the map that sends each element of $\Gamma$ to 1. If $\varphi$ and $\psi$ are characters, we define the map $\varphi\psi$ by

$$\varphi\psi(g) := \varphi(g)\psi(g).$$

Using this definition it follows that $\Gamma^*$ is an abelian group. If $\psi \in \Gamma^*$, then $\psi^{-1} = \overline{\psi}$.

To give an example, suppose $\Gamma = \mathbb{Z}_n$. Let $\theta$ be an $n$-th root of unity in $\mathbb{C}$ and let $g$ be a generator for $\Gamma$. Then the map

$$g^k \mapsto \theta^k$$

is readily seen to be a character of $\Gamma$. Thus each $n$-th root of unity determines a character of $\Gamma$, and these characters form a subgroup of $\Gamma^*$ with order $n$. For further progress, we need the following.

**3.1.1 Lemma.** *If $\psi$ is a non-trivial character of the finite abelian group $\Gamma$, then*

$$\sum_{g\in\Gamma}\psi(g)=0.$$

*Proof.* If $a\in G$ then

$$\sum_{g\in\Gamma}\psi(g)=\sum_{g\in\Gamma}\psi(ag)=\psi(a)\sum_{g\in\Gamma}\psi(g),$$

whence we see that if $\psi(a)\neq 1$, then $\sum_g\psi(g)=0$. □

If $S\subseteq\Gamma$ and $\psi\in\Gamma^*$, we define

$$\psi(S)=\sum_{g\in S}\psi(g).$$

The previous result thus states that if $\psi$ is not trivial, then $\psi(\Gamma)=0$.

**3.1.2 Corollary.** *If $\varphi$ and $\psi$ are characters of $\Gamma$, then*

$$\sum_{g\in\Gamma}\varphi(g)\overline{\psi(g)}=\begin{cases}|\Gamma|, & \text{if } \varphi=\overline{\psi};\\ 0, & \text{otherwise.}\end{cases}$$

*Proof.* Apply the lemma to the product $\varphi\overline{\psi}$. □

We define the sum in this corollary to be the *inner product* of $\varphi$ and $\psi$; we see that distinct characters are orthogonal. It follows that the elements of $\Gamma^*$ are linearly independent elements of the vector space $\mathbb{C}^G$ of complex-valued functions of $\Gamma$. Since this space has dimension $|\Gamma|$, we conclude that

$$|\Gamma^*|\leq|\Gamma|.$$

We can now show that $\Gamma^*$ and $\Gamma$ are isomorphic abelian groups. We saw above that $\mathbb{Z}_n^*$ contains a subgroup isomorphic to $\Gamma$, and therefore

$$\mathbb{Z}_n^*\cong\mathbb{Z}_n.$$

A finite abelian group is the direct product of cyclic groups. If $A$ and $B$ are finite abelian groups then we may assume inductively that

$$(A\times B)^*\cong A^*\times B^*,$$

and so our claim follows.

Let $\Gamma$ be a finite abelian group of order $n$. A *character table* of $\Gamma$ is the $n\times n$ matrix with $ij$-entry equal to the value of the $i$-character on the $j$-th element of $\Gamma$. By 3.1.2,

$$HH^*=nI.$$

Also

$$H\circ\overline{H}=J.$$

For example, the character table of $\mathbb{Z}_2^n$ may be taken to be the Kronecker product of $n$ copies of

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

For another example, let $\Gamma$ be $\mathbb{Z}_n$ and suppose $\eta$ is a primitive $n$-th root of unity. The matrix $P$ with rows and columns indexed by $\Gamma$ and with

$$P_{i,j} = \eta^{ij}$$

is a character table for $\Gamma$. Since this is symmetric, any finite abelian group has a symmetric character table.

## 3.2 Translation Graphs

Let $G$ be a group and suppose $C \subseteq G$. The *Cayley graph* $X(C)$ is the graph with vertex set $G$ and arc set

$$\{(g,h) : hg^{-1} \in C\}.$$

Define

$$C^{-1} = \{c^{-1} : c \in C\}$$

and call $C$ *inverse-closed* if $C = C^{-1}$. Then $X(C)$ is a directed graph if and only if $C$ is not inverse-closed, and it will contain loops if $1 \in C$. We do not insist that Cayley graphs be undirected, but we do insist that they do not have loops.

If $a \in G$, let $\rho_a$ be the map that sends $x$ in $G$ to $xa$. Then $\rho_a$ is a permutation of $G$ and an automorphism of $X(C)$. Hence $G$ acts as a regular group of automorphisms of $X(C)$. Conversely, if $G$ acts as a regular group of automorphisms of a graph $X$, we may choose a vertex $v$ in $X$ and define $C$ to be the set of elements $g$ of $G$ such that $(v, gv)$ is an arc in $X$. Then $X$ is isomorphic to the Cayley graph $X(C)$.

We define a *translation graph* to be a Cayley graph for an abelian group. One advantage of translation graphs is that their eigenvalues and eigenvectors are more accessible, as we show now.

Suppose $\Gamma$ is an abelian group of order $v$. Each character of $G$ can be extended to a function on the subsets of $\Gamma$ as follows. Suppose $\psi \in \Gamma^*$ and $S \subseteq \Gamma$. Then

$$\psi(S) := \sum_{g \in S} \psi(g).$$

**3.2.1 Lemma.** *Let $X$ be a Cayley graph for the abelian group $\Gamma$, relative to the subset $C$. Each character $\psi$ of $\Gamma$ is an eigenvector for $A(X)$ with eigenvalue $\psi(C)$.*

*Proof.* A function $\psi$ on $V(X)$ is an eigenvector if there is a complex number $\lambda$ such that

$$\lambda\psi(g) = \sum_{h \sim g} \psi(h)$$

Since

$$\sum_{h \sim g} \psi(h) = \sum_{c \in C} \psi(cg) = \psi(g) \sum_{c \in C} \psi(c) = \psi(g)\psi(C),$$

we see that $\psi$ is an eigenvector with eigenvalue $\psi(C)$.

Assume $V = V(d,\mathbb{F})$ is a vector space. A Cayley graph for $V$ is a translation graph. A Cayley graph for $V$ is *linear* if its connection set is closed under multiplication by the non-zero elements of $\mathbb{F}$. Any Cayley graph for $V(d,GF(2))$ is linear, as is any undirected Cayley graph for $V(d,GF(3))$.

## 3.3 Translation Schemes and their Duals

Let $\Gamma$ be a finite abelian group of order $v$. Each element of $\Gamma$ gives rise to a permutation of $\Gamma$—the permutation corresponding to $a$ maps $g$ in $\Gamma$ to $ga$. Hence for each element $g$ in $\Gamma$ we have a permutation matrix $P(g)$; the map $g \mapsto P(g)$ is a group homomorphism. Therefore

$$P(g)P(h) = P(h)P(g), \qquad P(g^{-1}) = P(g)^T.$$

We have $P(1) = I$ and $\sum_g P(g) = J$. Hence the matrices $P(g)$ form an association scheme with $v-1$ classes. (This is in fact the conjugacy class scheme on $\Gamma$, but the description we have just presented may be more transparent.) We call it the *abelian group scheme* on $\Gamma$.

**3.3.1 Lemma.** *Let $\mathscr{A}$ be an association scheme with $v$ vertices. Then $\mathscr{A}$ has $v-1$ classes if and only if it is the association scheme of an abelian group.*

*Proof.* Suppose $\mathscr{A}$ has $v$ vertices and $v$ classes $A_0,\ldots,A_{v-1}$. Since $\sum_i A_i = J$, we have $v_i = 1$ for each $i$. It follows that $A_i$ is a permutation matrix, and that together they form an abelian group of order $v$. □

We define a *translation scheme* to be a subscheme of an abelian group scheme. The Hamming schemes and the bilinear forms schemes are translation schemes.

Let $\mathbb{F}$ be a finite field of order $q$ and suppose $K$ is a subgroup of $F^*$, the multiplicative group of $\mathbb{F}$. The *cyclotomic scheme* has the elements of $\mathbb{F}$ as its vertices, and $(u,v)$ is $i$-related if and only if $v-u$ lies in the $i$-th coset of $K$. Hence if $k = |K|$, this scheme has $(q-1)/k$ classes each of valency $k$. This scheme is symmetric if and only if $-1 \in K$. It is a translation scheme relative to the additive group of $\mathbb{F}$. If $q = p^n$ for some prime $n$, then the scheme is linear if and only if $K$ contains $GF(p)^*$.

Let $\mathscr{A}$ be a subscheme of the scheme coming from the abelian group $\Gamma$. Then $\Gamma$ acts by right multiplication as a group of permutations on itself, and thus $\Gamma$ acts transitively on the vertices of $\mathscr{A}$. In particular, $\Gamma \le \mathrm{Aut}(X_i)$ for $i = 1,\ldots,d$ and therefore each $X_i$ is a Cayley graph for $\Gamma$ relative to a subset $C_i$. The sets $C_i$ partition $\Gamma\setminus 1$ and are closed under inverses, that is, for each $i$ we have $C_i^{-1} = C_j$ for some $j$.

The matrix of eigenvalues $P$ of an abelian group scheme is the character table of the group. Thus the columns of $P$ are indexed by the elements of the group, the rows by the characters and the $ij$-entry is the value of the $i$-th character on the $j$ element. Assume $\pi$ is a partition $C_0,\ldots,C_d$ of $\Gamma$ such that $C_0 = \{1\}$ and the set of cells is inverse-closed. Let $S$ be the characteristic matrix of $\pi$. Then by **??**, the dimension of the algebra generated by the matrices $A_i = A(X(C_i))$ is equal to the number of distinct rows of $PS$. Further, by **??**, is this dimension is $e+1$, then $e \ge d$ and equality

holds if and only if $A_0, \ldots, A_d$ form an association scheme. (We will discuss this from a somewhat different viewpoint in Section 4.7.)

If equality holds then $\pi$ determines a partition of $\Gamma^*$ into $d+1$ cells, $D_0, \ldots, D_d$ say. It is not hard to show that one of these cells consists of the trivial character, and that the set of cells in inverse-closed. Hence we obtain an association scheme on $\Gamma^*$. We call this scheme the *dual* of the scheme determined by $\pi$. Thus translation schemes come in dual pairs.

## 3.4 Geometry, Codes and Graphs

Let $V$ be the vector space of dimension $d$ over the finite field $GF(q)$. The 1-dimensional subspaces of $V$ are the points of the projective space $PG(d-1,q)$. Suppose $\Omega \subseteq PG(d-1,q)$. We can represent the set $\Omega$ by the columns of a $d \times |\Omega|$ matrix $M$ whose columns are homogeneous coordinate vectors for the elements of $\Omega$. We call the row space of $M$ the *code* of $\Omega$. The kernel of $M$ is the *dual code* of $\Omega$. We will usually denote the code of $\Omega$ by $C(\Omega)$, or by $C$. The dual code of $C$ is $C^\perp$.

If $\Omega \subseteq PG(d-1,q)$, then $\langle\Omega\rangle$ denotes the smallest projective subspace that contains $\Omega$. The *dimension* of $\Omega$ is the projective dimension of $\langle\Omega\rangle$; the *rank* $\mathrm{rk}(\Omega)$ is the dimension of the subspace of $V$ corresponding to the projective subspace $\langle\Omega\rangle$. (The rank is one greater than the projective dimension.) We note that $\mathrm{rk}(\Omega)$ is equal to the dimension of its code.

Using the machinery we have just defined, we can translate geometric questions about $\Omega$ into questions about its code. However there is also a translation into graph theory. Suppose $M$ is a matrix representing $\Omega$. Let $X(\Omega)$ denote the Cayley graph for the additive group of $V$ with the non-zero scalar multiples of the columns of $M$ as its connection set. Thus $X$ is a Cayley graph on $q^d$ vertices, with valency $(q-1)|\Omega|$. It is connected if and only $\mathrm{rk}(M) = d$, and this holds if and only if $\mathrm{rk}(\Omega) = d$. These Cayley graphs are the most important examples of linear Cayley graphs (as defined at the end of Section 3.2).

If $C$ is a subspace of $V$, its *coset graph* is the graph with the cosets of $C$ as its vertices, and the number of edges joining two cosets $C_1$ and $C_2$ is equal to the number of vectors in $C_2$ at Hamming distance one from a given vector in $C_1$. This definition allows a coset graph to have loops as well as multiple edges.

**3.4.1 Lemma.** *The coset graph of a code $C$ is simple if and only if the minimum distance of $C$ is at least three.* □

Note that the columns of $M$ are distinct, and so the dual code of $\Omega$ has minimum distance at least three. (A code with minimum distance at least three is often called a *projective code*.)

**3.4.2 Lemma.** *If $\Omega \subseteq PG(d-1,q)$, then $X(\Omega)$ is the coset graph of the dual code of $\Omega$.* □

There is also a direct geometric description of $X(\Omega)$. View $PG(d-1,q)$ as the hyperplane at infinity of the affine geometry $AG(d,q)$. The vertices of $AG(d,q)$ are

the elements of $V$ and its subspaces are the cosets of the linear subspaces of $V$. Construct a graph with vertex set $V$ by defining two distinct points to be adjacent if the unique line through them meets the hyperplane at infinity in a point of $\Omega$; this graph is $X(\Omega)$.

We will see that there are many interesting connections between the properties of $\Omega$, its code $C$ and its graph $X(\Omega)$. Before we can develop these, we need information about the eigenvalues and eigenvectors of $X$.

Let tr denote the trace map from the field $\mathbb{F}$ of order $q$ to its prime field (of order $p$). If $\theta$ is a complex primitive $p$-th root of 1, then the map

$$x \mapsto \theta^{\mathrm{tr}(a^T x)}$$

is a character of the additive group of $V$, which we denote by $\psi_a$. If $a \in V$, then

$$a^\perp := \{x : a^T x = 0\}.$$

Usually we will view $a^\perp$ as a subset of $PG(d-1,q)$.

**3.4.3 Theorem.** *If $\Omega \subseteq PG(d-1,q)$ and $\psi_a$ is as above, then $\psi_a$ is an eigenvector for $X(\Omega)$ with eigenvalue $q|\Omega \cap a^\perp| - |\Omega|$.*

*Proof.* The connection set $\mathscr{C}$ of $X(\Omega)$ consists of the vectors $\gamma x$, where $\gamma$ varies over the non-zero elements of $\mathbb{F}$ and $x$ varies over the columns of $M$. Then

$$x \mapsto \mathrm{tr}(\gamma a^T x)$$

is a linear map from $\mathbb{F}$ to $GF(p)$. It is onto, and so takes each possible value exactly $q/p$ times as $\gamma$ varies over $\mathbb{F}$. Since the sum of the distinct powers of $\theta$ is zero,

$$\sum_{\gamma \in \mathbb{F} \setminus 0} \theta^{\mathrm{tr}(\gamma a^T x)} = \begin{cases} -1, & x \neq 0; \\ q-1, & x = 0. \end{cases}$$

Therefore $\psi_a(\mathscr{C}) = q|\Omega \cap a^\perp| - |\Omega|$. □

Geometrically $|\Omega \cap a^\perp|$ is the number of points of $\Omega$ that lie on the hyperplane of $PG(d-1,q)$ with coordinate vector $a^T$. If $\gamma \neq 0$, then

$$q|\Omega \cap a^\perp| = q|\Omega \cap (\gamma a)^\perp|,$$

whence we see that each hyperplane gives rise to $q-1$ eigenvectors for $X(\Omega)$, all with the same eigenvalue.

## 3.5 Language

In this section we develop a set of dictionaries, allowing us to translate between the languages of finite geometry, coding theory and graph theory.

We assume that $\Omega$ is a subset of $PG(d-1,q)$ with rank $d$ and size $m$, represented by a matrix $M$. We denote the code of $\Omega$ by $C$ and its graph by $X$.

Suppose $H$ is a hyperplane in $PG(d-1,q)$, with coordinate vector $h^T$. The elements of $\Omega \cap h^T$ index the zero entries of $h^T M$. If $\mathrm{wt}(x)$ denote the weight of the code word $x$, then

$$|\Omega \cap h^T| = m - \mathrm{wt}(h^T M).$$

Thus a hyperplane of $PG(d-1,q)$ that intersects $\Omega$ in exactly $i$ points determines $q-1$ code words of weight $m-i$, and $q-1$ eigenvectors of $X$ with eigenvalue $qi-m$. In particular, the eigenvalues of $X$ and their multiplicities are determined by the weight enumerator of the code of $\Omega$.

**3.5.1 Lemma.** *Let $\Omega$ be a set of $m$ points in $PG(d-1,q)$ and let $\tau$ be the least eigenvalue of $X(\Omega)$. Then $\tau \geq -m$, and equality holds if and only if the code of $\Omega$ contains a word of weight $n$.* □

**3.5.2 Theorem.** *Let $\Omega$ be a set of $n$ points in $PG(d-1,q)$ with code $C$. Then $X(\Omega)$ is $q$-colourable if and only if $C^\perp$ contains a word of weight $n$.*

*Proof.* If there is no word of weight $n$ in $C^\perp$, then the least eigenvalue of $X(\Omega)$ is greater than $-n$. The valency of $X(\Omega)$ is $n(q-1)$ and so the ratio bound yields that

$$\alpha(X(\Omega)) < \frac{|V(X)|}{1+\frac{n(q-1)}{n}} = \frac{|V(X)|}{q}.$$

Hence $\chi(X(\Omega)) > q$.

Conversely, let $M$ be a matrix that represents $\Omega$ and suppose $a^T M$ is a word of weight $n$ in the code of $\Omega$. If $x$ and $y$ are vertices of $X(\Omega)$ and $a^T x = a^T y$, then $a^T(x-y) = 0$ and therefore $x$ and $y$ are not adjacent in $X(\Omega)$. Hence the map $x \mapsto a^T x$ is a proper colouring of $X(\Omega)$ using the elements of $\mathbb{F}$. □

**3.5.3 Corollary.** *Let $\Omega$ be a set of points in $PG(d-1,q)$. To determine the least eigenvalue of $X(\Omega)$ from $\Omega$ is NP-hard.*

*Proof.* Take $M$ to be the incidence matrix of an orientation of a graph $Y$. If $a^T M$ has no zero entries, the vector $a$ determines a proper colouring of $Y$ with $q$ colours. If $q = 3$, then $Y$ is 3-colourable if and only if the code over $GF(3)$ generated by $M$ contains a word of weight $n$. Hence $X(M)$ is 3-colourable if and only if $Y$ is 3-colourable. Since it is NP-hard to decide if a graph is 3-colourable, we are done. □

We also see that it is NP-hard to decide if the adjacency matrix of a Cayley graph for $\mathbb{Z}_2^n$ is invertible (over $\mathbb{R}$).

The connection between eigenvalues of the coset graph and the weight distribution of the code appears to be folk-lore. Some information appears in Delorme and Solé (European J. Comb. 12 (1991)) [***but I have not checked this yet***].

The *covering radius* of a code $C$ is the least integer $r$ such that every word is at distance at most $r$ from a word of $C$.

**3.5.4 Lemma.** *The covering radius of $C^\perp(\Omega)$ is equal to the diameter of $X$.* □

A *cap* in projective space is a set of points such that no three are collinear.

**3.5.5 Lemma.** *Suppose* $\Omega \subseteq PG(d-1,q)$. *Then the following are equivalent:*

*(a)* $\Omega$ *is a cap.*

*(b) The minimum distance of* $C^{\perp}$ *is at least four.*

*(c)* $X(\Omega)$ *is triangle-free.* □

# Chapter 4

# Duality

## 4.1 The Discrete Fourier Transform

The set $\mathscr{C}_n$ of $n \times n$ circulants over $\mathbb{F}$ is closed under matrix and Schur multiplication and contains $I$ and $J$, the units for these multiplications. (Thus it is the Bose-Mesner algebra of the association scheme of the cyclic group of order $n$.) We introduce an important endomorphism of this algebra.

Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ that contains a primitive $n$-th root of unity. Equivalently, $\mathbb{E}$ is a splitting field for $t^n - 1$. Let $\theta$ be a fixed $n$-th root of unity in $\mathbb{E}$. If $M = p(R)$, define

$$\Theta(M) = \sum_{i=0}^{n-1} p(\theta^i) R^i.$$

Thus $\Theta$ is an endomorphism, a linear operator on $\mathscr{C}_n$. We call it a *duality map*.

**4.1.1 Lemma.** *If $M \in \mathscr{C}_n$ then $\Theta^2(M) = nM^T$.*

*Proof.* It is enough to show that $\Theta^2(R^k) = nR^T$. We have

$$\begin{aligned}\Theta^2(R^k) = \sum_j \theta^{kj} \Theta(R^j) &= \sum_{i,j} \theta^{kj} \theta^{ij} R^i \\ &= \sum_i \Big( \sum_j \theta^{j(i+k)} \Big) R^i.\end{aligned}$$

The inner sum is zero unless $i = -k$, when it is $n$. Therefore $\Theta^2(R^k) = R^{-k}$ and since $R^{-1} = R^T$, the result follows. □

**4.1.2 Theorem.** *If $M, N \in \mathscr{C}_n$ then $\Theta(MN) = \Theta(M) \circ \Theta(N)$ and $\Theta(M \circ N) = \frac{1}{n}\Theta(M)\Theta(N)$.*

*Proof.* We have

$$\Theta(p(R)q(R)) = \sum_i p(\theta^i) q(\theta^i) R^i = \Big( \sum_i p(\theta^i) R^i \Big) \circ \Big( \sum_i q(\theta^i) R^i \Big),$$

which is the first claim. The second follows from this and the previous lemma. □

**4.1.3 Theorem.** *If $M^T = \sum_\nu \mu_i R^i$, then $M\Theta(R^i) = \mu_i \Theta(R^i)$.*

*Proof.* We have

$$\begin{aligned} M\Theta(R^i) &= v^{-1}\Theta^2(M^T)\Theta(R^i) \\ &= \Theta(\Theta(M^T) \circ R^i) \\ &= \Theta(\mu_i R^i) \\ &= \mu_i \Theta(R^i). \end{aligned}$$ ] □

It follows from this that the entries of $\Theta(M)$ are eigenvalues of $M$, and the columns of $\Theta(R_i)$ are eigenvectors for all circulants.

Define the *weight* of a circulant to be the number of non-zero entries in a column.

**4.1.4 Lemma.** *If $\deg(q(t)) = \ell$, then $\Theta(q(R))$ has weight at least $n - \ell$.*

*Proof.* If $\deg(q(t)) = \ell$, then at most $\ell$ distinct powers of $\theta$ are zeros of $q$ and so $\Theta(q(R))$ has at most $\ell$ zero entries in any column. □

The following result is the BCH-bound.

**4.1.5 Theorem.** *If $M = \varphi(R)$ and $\varphi(t)$ vanishes on $k$ consecutive powers of $\theta$, the minimum distance of the column space of $M$ is at least $k+1$.*

*Proof.* Suppose $M = p(R)$. If $p(t)$ has $k$ consecutive powers of $\theta$ as zeros, then $\Theta(M)$ has $k$ cyclically consecutive zeros in its first column. Hence there is an integer $s$ such that last $k$ entries in $R^s\Theta(M)$ are zero, and therefore there is a polynomial $q(t)$ with degree at most $n-1-k$ such that

$$R^s\Theta(M) = q(R).$$

Consequently

$$\Theta(q(R)) = \Theta(R^s) \circ \Theta^2(M)$$

has weight at least $k+1$. Since $\Theta(R^s) = \Theta(R)^{\circ s}$ has no zero entries and $\Theta^2(M) = M^T$, it follows that $M$ has weight at least $k+1$.

If $g(t)$ is a polynomial, then $g(R)M = g(R)p(R)$ and $g(t)p(t)$ vanishes on $k$ consecutive powers of $\theta$. Therefore $g(R)M$ has weight at least $k+1$, for any polynomial $g$. This implies that the minimum weight of the column space of $M$ is at least $k+1$. □

$M$ is diagonalisable if and only $n \cdot 1 \neq 0$ in $\mathbb{F}$.

The subset $\{0,3,4,9,11\}$ in $\mathbb{Z}_{21}$ is a cyclic difference set for a projective plane of order four. Hence if

$$\psi(t) = 1 + t^3 + t^4 + t^9 + t^{11}$$

then $N = p(R)$ is the incidence matrix of a plane of order four. Since $\deg(p) = 11$, we see that $\mathrm{rk}(N) \geq 10$ over $\mathbb{Z}_2$. We can check though that $\psi$ divides $t^{21} - 1$: in fact

$$(t-1)\psi(t)\psi^*(t) = t^{21} - 1$$

and consequently $\mathrm{rk}(N) = 10$.

## 4.2 The Hadamard Transform

In the previous we worked with a duality related to the cyclic group. Here we introduce an analogous duality map related to the elementary abelian group $\mathbb{Z}_2^n$. It may help to view this as the additive group of a vector space of dimension $n$ over $\mathbb{Z}_2$.

When working with the cyclic group we used circulant matrices, which are linear combinations of the powers of $R$, where $R$ is a cyclic permutation matrix. We introduce the analagous matrices for $\mathbb{Z}_2^n$. First define a matrix $P$

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If $u \in \mathbb{Z}_2$, define $A_u$ to be the Kronecker product

$$A_u := P^{u_1} \otimes \cdots \otimes P^{u_n}.$$

Then $A_0 = I$,

$$A_u A_v = A_{u+v}$$

(and in particular $A_u^2 = I$). It follows that the map

$$u \mapsto A_u$$

is a group isomorphism. A simple induction argument on $n$ yields that

$$\sum_u A_u = J.$$

(Partition the sum over the vectors $u$ such that $u_1 = 0$ and the vectors $u$ with $u_1 = 1$.)

It follows that the matrices in

$$\mathscr{A} := \{A_u : u \in \mathbb{Z}_n\}$$

are linearly independent. Define $\mathbb{F}[\mathscr{A}]$ to be vector space over $\mathbb{F}$ spanned by the matrices in $\mathscr{A}$. (For our purposes here, $\mathbb{F} = \mathbb{R}$ will suffice.)

If $u \in \mathbb{Z}_n$, define the function $\psi_u : \mathbb{Z}_n \to \{-1, 1\}$ by

$$\psi_u(v) = (-1)^{u^T v}.$$

Define a duality map $\Theta$ on $\mathbb{F}[\mathscr{A}]$ by setting

$$\Theta(A_u) = \sum_v \psi_u(v) A_v$$

and extend $\Theta$ to $\mathbb{F}[\mathscr{A}]$ by linearity. We have at once that

$$\Theta(I) = J.$$

Then

$$\begin{aligned} \Theta(A_u)\Theta(A_v) &= \sum_x \sum_y \psi_u(x)\psi_v(y) A_x A_y \\ &= \sum_{x,y} (-1)^{u^T x + v^T y} A_{x+y} \\ &= \sum_{x, x+y} (-1)^{(u-v)^T x} (-1)^{v^T (x+y)} A_{x+y}. \end{aligned}$$

Since

$$\sum_x (-1)^{(u-v)^T x} = \begin{cases} 2^n, & u = v; \\ 0, & \text{otherwise} \end{cases}$$

we conclude that

$$\Theta(A_u)\Theta(A_v) = \delta_{u,v} 2^n \Theta(A_u).$$

Consequently, for all $M$ and $N$ in $\mathbb{F}[\mathscr{A}]$,

$$\Theta(M)\Theta(N) = 2^{-n}\Theta(M \circ N).$$

We also have $\Theta(A_u) \circ \Theta(A_v) = \Theta(A_{u+v})$, whence $\Theta(A_u A_v) = \Theta(A_u) \circ \Theta(A_v)$ and

$$\Theta(MN) = \Theta(M) \circ \Theta(N).$$

Next

$$\begin{aligned} A_u \Theta(A_v) = A_u \sum_w \psi_v(w) A_w &= \sum_w (-1)^{v^T w} A_{u+w} \\ &= (-1)^{v^T u} \sum_w (-1)^{v^T (u+w)} A_{u+w} \\ &= \psi_u(v) \Theta(A_v) \end{aligned}$$

which shows that the columns of $\Theta(A_v)$ are eigenvectors for $A_u$. Moreover, we see that the entries of $\Theta(M)$ are the eigenvalues of $M$.

We leave the proof of the next result as an exercise.

**4.2.1 Theorem.** *If $M \in \mathbb{F}[\mathscr{A}]$, then $\Theta^2(M) = 2^n M$.* □

Since $\Theta(I) = J$, it follows that $\Theta(J) = 2^n I$. The proof of 4.1.3 is easily modified to yield our next result.

**4.2.2 Theorem.** *If $M \in \mathbb{F}[\mathscr{A}]$, then the entries of $\Theta(M)$ are the eigenvalues of $M$.* □

**4.2.3 Lemma.** *If $M \in \mathbb{F}[\mathscr{A}]$, then* $\operatorname{tr}(\Theta(M)) = \operatorname{sum}(M)$.

*Proof.* Let $\rho$ denote the sum of a row of $M$. We have

$$\begin{aligned} I \circ \Theta(M) &= 2^{-n}\Theta^2(I) \circ \Theta(M) \\ &= 2^{-n}\Theta(\Theta(I)M) \\ &= 2^{-n}\Theta(JM) \\ &= 2^{-n}\Theta(\rho J) \\ &= \rho I \end{aligned}$$

Therefore $\operatorname{tr}(\Theta(M)) = \operatorname{sum}(M)$. □

## 4.3 Two Matrix Duals

Let $C$ be a linear code of length $n$ and let $a_i$ denote the number of words in $C$ of weight $i$. The *weight enumerator* $W_C(x,y)$ is the polynomial

$$W_C(x,y) = \sum_{i=0}^{n} a_i x^{n-i} y^i.$$

It is a surprising fact that $W_{C^\perp}$ can be obtained from $W_C(x,y)$, and in a simple way.

If $C$ is a linear binary code of length $n$, define the matrix $A_C$ by

$$A_C := \sum_{u \in C} A_u.$$

**4.3.1 Lemma.** *If $C$ is a binary linear code, then $\Theta(A_C) = |C| A_{C^\perp}$.*

*Proof.* If $\beta$ is a basis for $C$, then

$$\prod_{u \in \beta} (I + A_u) = A_C.$$

and accordingly $\Theta(A_C)$ is the Schur product of the matrices

$$\Theta(I + A_u) = J + \Theta(A_u),$$

where $u$ runs over $\beta$. Now

$$J + \Theta(A_u) = \sum_v (1 + (-1)^{u^T v}) A_v = 2 \sum_{v \in u^\perp} A_v$$

and therefore the Schur product of the matrices $J + \Theta(A_u)$ is $2^{|\beta|} A_{C^\perp}$, as required. □

Let $K$ be the matrix

$$K := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If $M$ is a matrix $M^{\otimes n}$ denotes the Kronecker product of $n$ copies of $M$.

**4.3.2 Lemma.** *We have*

$$\sum_u x^{n-\mathrm{wt}(u)} y^{\mathrm{wt}(u)} A_u = (xI + yK)^{\otimes n}.$$

*Proof.* Let $e_1, \ldots, e_n$ denote the standard basis for $\mathbb{Z}_2^n$. If $u \in \mathbb{Z}_2^n$, then

$$u = \sum_i u_i e_i.$$

Then

$$A_u = K^{u_1} \otimes \cdots \otimes K^{u_n}$$

and so $x^{n-\mathrm{wt}(u)} y^{\mathrm{wt}(u)} A_u$ is the Kronecker product of the $n$ terms $x^{1-u_i} y^{u_i} K^{u_i}$ for $i = 1, \ldots, n$. This implies the lemma. □

**4.3.3 Lemma.** *We have* $\Theta(M \otimes N) = \Theta(M) \otimes \Theta(N)$.

*Proof.* The entries of $\Theta(M) \otimes \Theta(N)$ are the products of the entries of $\Theta(M)$ and $\Theta(N)$, and these are the eigenvalues of $M$ and $N$. The products of the eigenvalues of $M$ and $N$ are the eigenvalues of $M \otimes N$, and these are the entries of $\Theta(M \otimes N)$. [We have neglected some bookkeeping, you are welcome to supply it. :-)] □

**4.3.4 Corollary.** *We have*

$$\Theta\Big(\sum_u x^{n-\mathrm{wt}(u)} y^{\mathrm{wt}(u)} A_u\Big) = \sum_u (x+y)^{n-\mathrm{wt}(u)} (x-y)^{wt(u)} A_u.$$

*Proof.* We have $\Theta(I) = J$. Since $K = J - I$,

$$\Theta(K) = \Theta(J) - \Theta(I) = 2I - J.$$

Therefore

$$\Theta(xI + yK) = xJ + 2yI - yJ = (x-y)(J-I) + (x+y)I = (x+y)I + (x-y)K.$$

We now obtain the result by applying Lemmas 4.3.2 and 4.3.3. □

## 4.4 MacWilliams Theorem

We apply the results from the previous section to derive MacWilliams theorem, a fundamental result in Coding Theory.

**4.4.1 Theorem.** *Let $C$ be a binary linear code of length $n$. Then*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y).$$

*Proof.* Set $M$ equal to $\sum_u x^{n-\mathrm{wt}(u)} y^{\mathrm{wt}(u)} A_u$. Then the diagonal entries of $A_{C^\perp} M$ are each equal to $W_{C^\perp}(x,y)$, whence

$$\mathrm{tr}(A_{C^\perp} M) = 2^n W_{C^\perp}(x,y).$$

Using 4.2.3, we have

$$\begin{aligned}
\mathrm{tr}(A_{C^\perp} M) &= 2^{-n} \mathrm{tr}(\Theta^2(A_{C^\perp} M)) \\
&= 2^{-n} \mathrm{sum}(\Theta(A_{C^\perp} M)) \\
&= 2^{-n} \mathrm{sum}(\Theta(A_{C^\perp}) \circ \Theta(M)) \\
&= 2^{-n} |C^\perp| \mathrm{sum}(A_C \circ \Theta(M)) \\
&= |C|^{-1} \mathrm{sum}(A_C \circ \Theta(M)).
\end{aligned}$$

Since the row sum of $A_C \circ \Theta(M)$ is $W_C(x+y, x-y)$, the last term above is equal to $2^n |C|^{-1} W_C(x+y, x-y)$, and so the theorem is proved. □

By way of example, suppose $C$ is the code of the plane of order four. Our computations in **??** yield that the weight enumerator of $C$ is

$$x^{21} + 21x^{16}y^5 + 210x^{13}y^8 + 280x^{12}y^9 + 280x^9y^{12} + 210x^8y^{13} + 21x^5y^{16} + y^{21}.$$

Using MacWilliams theorem, we find the weight enumerator of the dual is

$$x^{21} + 168x^{15}y^6 + 210x^{13}y^8 + 1008x^{11}y^{10} + 280x^9y^{12} + 360x^7y^{14} + 21x^5y^{16}.$$

**4.4.2 Theorem.** *The length of a doubly even binary self-dual code is divisible by 8.*

*Proof.* If $C$ is self-dual with length $n$, then $|C| = 2^{n/2}$ and

$$W_C(x,y) = 2^{-n/2}W_C(x+y, x-y) = W_C\Big(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\Big).$$

Therefore $W_C(x,y)$ is invariant under the substitution represented by the matrix

$$\tau = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Since $C$ is doubly even, it is also invariant when we replace $y$ by $iy$ (with $i^2 = -1$). Equivalently it is invariant under the substitution represented by

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

We find that

$$(\tau\sigma)^3 = \frac{1+i}{\sqrt{2}}I.$$

Hence if $\theta := (1+i)/\sqrt{2}$, the substitution

$$x \mapsto \theta x, \quad y \mapsto \theta y$$

leaves $W_C(x,y)$ invariant. But

$$W_C(\theta x, \theta y) = \theta^n W_C(x,y)$$

and as $\theta$ is a primitive 8-th root of unity, this implies that $8 \mid n$. □

## 4.5 Projective Planes

We use the theory at hand to prove that there is no projective plane of order $n$, where $n \equiv 6$ modulo 8.

We work with linear codes over $GF(2)$. A code is *even* if all its word have even weight, and it is *doubly even* if all words have weight divisible by four. If $C$ is a binary code of length $n$, the *extended code* by adding an $(n+1)$-th coordinate to each code word, such that the weight of the extended code word is even. (Thus we are adding a parity check; the operation is trivial if $C$ is even.)

**4.5.1 Theorem.** *Let $N$ be the incidence matrix of a projective plane with order $n$ and let $C$ be the linear code spanned by the rows of $N$ over $GF(2)$. Then the extended code is self-dual and doubly even.*

*Proof.* Let $N$ be the incidence matrix of our projective plane. Let $N_1$ denote the matrix we get by adding a final column equal to $\mathbf{1}$ to $N$. Since $n$ is even and since equal row of $N$ has weight $n+1$, the rows of $N_1$ have even weight. One consequence is that each word in row$(N)$ has even weight.

Further

$$NN^T = nI + J$$

and hence

$$N_1 N_1^T = (nI + J) + J = 0 \mod 2.$$

It follows that the code generated by the rows of $N_1$ is self-orthogonal. As $n \equiv 2$ modulo four, each row of $N_1$ has weight divisible by four, whence it follows that all code words in row$(N_1)$ have weight divisible by four.

Each row of $N_1$ has length $n^2+n+2$, and it remains for us to show that

$$\mathrm{rk}(N_1) = \frac{1}{2}(n^2+n+2).$$

Since $\mathbf{1}$ lies in col$(N)$ over $GF(2)$, we see that $N_1$ and $N$ have the same rank. We will therefore compute rk$(N)$.

Let $v = n^2+n+1$ and let $H$ be a parity check matrix for $C$—in other words, $H$ is a binary matrix with linearly independent rows such that $NH^T = 0$ and

$$\mathrm{rk}(N) + \mathrm{rk}(H) = v.$$

(Or to put it yet another way, the rows of $H$ are a basis for ker$(N)$.) Permuting columns of $N$ and $H$ if needed, we may assume that $H$ has the form

$$\begin{pmatrix} I_r K \end{pmatrix}$$

where $r = \mathrm{rk}(H)$. Let $H_1$ be given by

$$H_1 = \begin{pmatrix} I_r & K \\ 0 & I_{v-r} \end{pmatrix}.$$

Now view $N$ and $H_1$ as 01-matrices over $\mathbb{Q}$.

Since $\det(H_1) = 1$, we have

$$\det(N) = \det(NH_1^T).$$

Since $NH^T = 0$ modulo two, each entry in the first $r$ columns of $NH_1^T$ is even, and therefore $2^r$ divides $\det(N)$. Now

$$NN^T = nI + J,$$

from which it follows that

$$\det(N) = (n+1)n^{n(n+1)/2}.$$

As both $n+1$ and $n/2$ are odd, we conclude that $r \le n(n+1)/2$. This implies that

$$\mathrm{rk}(N) = v - r \ge \frac{1}{2}(n^2+n+2);$$

since $\mathrm{rk}(N_1) = \mathrm{rk}(N)$ and since $\mathrm{row}(N_1)$ is self-orthogonal,

$$\mathrm{rk}(N_1) = (n^2+n+2)/2. \qquad \square$$

If $n \equiv 6$ modulo eight, then $n^2+n+2 \equiv 4$ modulo eight. Consequently by 4.4.2, there is no binary doubly even self-dual code of this length. Thus we have the following result.

**4.5.2 Corollary.** *If $n \equiv 6$ modulo eight, there is no projective plane of order $n$.*

This condition is weaker than the Bruck-Ryser-Chowla theorem, but certainly easier to use.

## 4.6 Duality

We say an association scheme $\mathscr{A}$ is *formally self-dual* if $Q = \overline{P}$.

If $i \in \{0,1,\ldots,d\}$, we define $i^T$ to be the element of $i \in \{0,1,\ldots,d\}$ such that $A_{i^T} = A_i^T$. We recall that $p_j(k) = \overline{p_j(k^T)}$.

**4.6.1 Theorem.** *Let $\mathscr{A}$ be an association scheme on $v$ vertices such that $\overline{Q} = P$ and let $\Theta$ be the linear mapping from $\mathbb{C}[\mathscr{A}]$ to itself such that $\Theta(A_i) = \sum_j p_i(j)A_j$. Then:*

*(a)* $\Theta(A_i) = v\overline{E_i}$.

*(b)* $\Theta(I) = J$, $\Theta(J) = vI$.

*(c)* $\Theta(MN) = \Theta(M) \circ \Theta(N)$ *for all $M$ and $N$ in $\mathbb{C}[\mathscr{A}]$.*

*(d)* $\Theta(M \circ N) = \frac{1}{v}\Theta(M)\Theta(N)$ *for all $M$ and $N$ in $\mathbb{C}[\mathscr{A}]$.*

*(e) If $\mathscr{B}$ is a subscheme of $\mathscr{A}$, then $\Theta(\mathscr{B})$ is also a subscheme.*

*Proof.* Since $\overline{p_i(j)} = q_i(j)$, we have

$$\Theta(A_i) = \sum_{j=0}^{d} \overline{q_i(j)}A_j = v\overline{E_i}.$$

In particular, $\Theta(I) = J$.

Next

$$\Theta(v\overline{E_i})) = \sum_j \overline{q_i(j)}\Theta(A_j) = \sum_{j,k} \overline{q_i(j)}p_j(k)A_k = \sum_{j,k} q_i(j)p_j(k^T)A_k^T.$$

Since $QP = vI$, it follows that

$$\Theta(vE_i) = vA_i^T.$$

Hence

$$\Theta^2(M) = vM^T \tag{4.6.1}$$

for all $M$ in $\mathbb{C}[\mathscr{A}]$. (Note that $\Theta(J) = vI$.)

Since the entries of $\Theta(A_i)$ are the eigenvalues of $A_i$, we see that $\Theta(A_iA_j) = \Theta(A_i) \circ \Theta(A_j)$ and hence

$$\Theta(MN) = \Theta(M) \circ \Theta(N), \tag{4.6.2}$$

for all $M$ and $N$ in $\mathbb{C}[\mathscr{A}]$.

Finally

$$\Theta(A_i \circ A_j) = \delta_{i,j} v\overline{E_i} = \frac{1}{v}\Theta(A_i)\Theta(A_j).$$

and thus

$$\Theta(M \circ N) = \frac{1}{v}\Theta(M)\Theta(N). \tag{4.6.3}$$

for all $M$ and $N$ in $\mathbb{C}[\mathscr{A}]$. □

If $\Theta$ is a map satisfying the conditions of this theorem, we call it a *duality map*. The matrix representing $\Theta$ relative to the basis $A_0, \ldots, A_d$ is $P$.

Suppose $\mathscr{A}$ is the scheme of the cyclic group of order $v$. If $\theta$ is a primitive $v$-th root of 1 then we may assume that

$$P_{i,j} = \theta^{(i-1)(j-1)}. \tag{4.6.4}$$

It is easy to verify that $P\overline{P} = vI$, so this scheme is formally self-dual. The map $\Theta$ is essentially the discrete Fourier transform. We may take $\theta$ from any field $\mathbb{F}$ that contains a primitive $v$-th root of 1, and thus we may define $\Theta$ on $\mathbb{F}[\mathscr{A}]$.

It seems reasonable to define an association scheme on $v$ vertices to be *self-dual* if there is an endomorphism $\Theta$ of $\mathrm{Mat}_{n\times n}(\mathbb{C})$ such that $\Theta(A_i) = v\overline{E_i}$ for $i = 0, 1, \ldots, d$.

If $\mathscr{A}$ and $\mathscr{B}$ are schemes and the matrix of eigenvalues of $\mathscr{B}$ is the complex conjugate of the matrix of dual eigenvalues of $\mathscr{A}$, we say that $\mathscr{A}$ and $\mathscr{B}$ are *formally dual*. In this case we can define a map $\Theta$ as above, and a slightly modified version of 4.6.1 still holds. If $\Theta$ is induced by an endomorphism of $\mathrm{Mat}_{n\times n}(\mathbb{C})$, we say the pair of schemes is *dual*.

De Caen observed that if $\mathscr{A}$ and $\mathscr{B}$ are dual, then the product scheme $\mathscr{A} \otimes \mathscr{B}$ is self-dual. Hence we might choose to view self-duality as the fundamental concept.

Each translation scheme is either self-dual or has a distinct dual translation scheme. The only known examples of dual pairs of non-isomorphic schemes arise in this way. The Higman-Sims scheme is self-dual and is not a translation scheme.

## 4.7 Dual Partitions

Let $G$ be an abelian group. Then $G$ is isomorphic to its character group $G^*$ and we use $\psi_a$ to denote the character corresponding to $a$ in $G$.

Assume $\pi$ is a partition of $G$ with $\{0\}$ as one cell. If $C_0 = \{0\}$ and

$$\pi = \{C_0, C_1, \ldots, C_r\}$$

then we have Cayley graphs $X_1, \ldots, X_r$ with connection sets $C_1, \ldots, C_r$. Their adjacency matrices $A_1, \ldots, A_d$ commute and sum to $J - I$. If $a \in G$, the *profile* of $a$ is the vector

$$(\psi_a(C_0)), \ldots, \psi_a(C_r).$$

We say that $a$ and $b$ are equivalent if their profiles are equal, and the equivalence classes of this relation form a partition

$$\pi^* = \{D_0, \ldots, D_s\}$$

with $D_0 = \{0\}$.

**4.7.1 Lemma.** *We have $|\pi^*| \geq |\pi|$. Equality holds if and only if the graphs $X_1, \ldots, X_r$ form an association scheme, in which case we also get an association scheme with $r$ classes on the characters.*

*Proof.* See "Algebraic Combinatorics". □

Now let $V = V(d, \mathbb{F})$ be a vector space, where $|\mathbb{F}| = q$ and the characteristic of $\mathbb{F}$ is $p$. Set $\mathscr{C} = \{0\}$ and let

$$\mathscr{C}_1, \ldots, \mathscr{C}_r$$

be a partition of the non-zero elements of $V$, such that each cell is closed under multiplication by the non-zero elements of $\mathbb{F}$. (So each Cayley graph $X(\mathscr{C}_i)$ is linear.) As in the previous section, this partition of $V$ determines a partition of the characters of $V$ into $s$ classes, where $s \geq r$ and $s = r$ if and only if the graphs $X(\mathscr{C}_i)$ form an association scheme.

To get further, we need more information on the characters of $V$. Assume $\eta$ is a primitive $p$-th root of unity in $\mathbb{C}$ and let tr be the trace map from $\mathbb{F}$ to $GF(p)$. Then the map

$$\psi_a : x \mapsto \eta^{\mathrm{tr}(a^T x)}$$

is a character and all characters of $V$ arise in this way. The next result is a restatement of Theorem 3.4.3.

**4.7.2 Theorem.** *Let $M$ be a $d \times m$ matrix of $\mathbb{F}$ such that no two columns are linearly independent. Let $\mathscr{C}$ be the set of $(q-1)m$ non-zero scalar multiples of the columns of $M$. If $a \in V$, then*

$$\psi_a(\mathscr{C}) = (q-1)m - q\mathrm{wt}(a^T M).$$ □

If $\mathscr{C}$ is closed under multiplication by non-zero elements of $\mathbb{F}$, then $\mathscr{C} \cup \{0\}$ is the union of 1-dimensional subspaces of $V = V(d, \mathbb{F})$. Therefore any partition of the complete graph on the vectors of $V$ into $r$ linear Cayley graphs corresponds to a partition of the 1-dimensional subspaces of $V$, and thus can be represented by matrices $M_1, \ldots, M_r$, each with $d$ rows, such that the matrix

$$\mathscr{M} = \begin{pmatrix} M_1 & \ldots & M_r \end{pmatrix}$$

has exactly $(q^d - 1)/(q-1)$ columns, no two linearly independent. If $a \in V$, we define its profile to be the vector of length $r$ with $i$-th entry $\mathrm{wt}(a^T M_i)$. This gives a

partition of $V \setminus 0$ with at least $r$ classes. If there are exactly $r$ classes we get a pair of association schemes on $V$. The first consists of the graphs $X_1, \ldots, X_r$. The second, dual, scheme consists of the Cayley graphs with the "profile classes" as connection sets.

Note that if $a \neq 0$, then

$$\sum_i \mathrm{wt}(a^T M_i) = \mathrm{wt}(a^T \mathscr{M}),$$

where $(q-1)\mathrm{wt}(a^T \mathscr{M})$ is the number of non-zero vectors $x$ such that $a^T x \neq 0$. So the profile of $a$ is determined by the its first $r-1$ entries.

## 4.8 Difference Sets in Schemes

Let $\mathscr{A}$ denote an association scheme on $v$ vertices. A *difference set* in $\mathscr{A}$ is 01-matrix $A$ such that

$$AA^T = nI + \lambda J$$

for some positive integers $n$ and $\lambda$. Hence $A$ is an incidence matrix for a symmetric design. It is easy to verify that if $A$ is a difference set then so is $J - A$, and thus we may assume $A \circ I = 0$ is we like. If $k$ is the row sum of $A$, then $n = k - \lambda$.

Consider the case where $A$ is a difference set and $A = A^T$. Then the squares of the eigenvalues of $A$ are $\lambda v + n$ and $n$. If $k$ denotes the row sum of $A$, then $k$ is an eigenvalue of $A$ and

$$k^2 = \lambda(v-1) + k;$$

the remaining eigenvalues of $A$ are $\pm\sqrt{n}$. If $\mathrm{tr}(A) = 0$, there are positive integers $a$ and $b$ such that $1 + a + b = v$ and

$$k + a\sqrt{n} - b\sqrt{n} = \mathrm{tr}(A) = 0.$$

Accordingly

$$b - a = \frac{k}{\sqrt{k-\lambda}},$$

from which it follows that $k-\lambda$ is a perfect square. Since $A$ has exactly three distinct eigenvalues, it is the adjacency matrix of a strongly regular graph with $a = c$.

The case where $A$ is not symmetric is more complex. Since $A$ lies in the Bose-Mesner algebra of the scheme, $AA^T = A^T A$ and therefore $A$ is normal. A normal matrix is symmetric if and only if its eigenvalues are real, consequently some eigenvalues of $A$ are complex. The valency aside, all eigenvalues of $A$ have absolute value $\sqrt{k-\lambda}$. The matrix $A$ is still an incidence matrix of a symmetric design.

Suppose $A$ is a 01-matrix in $\mathscr{A}$ with each row summing to $k$. Since $A$ is normal, $A = LDL^*$ where $L$ is unitary. Hence

$$A^T = A^* = L\overline{D}L^*$$

and thus if $Az = \theta z$, then $A^T z = \overline{\theta} z$ and $AA^T z = |\theta|^2 z$. If the valency $k$ is a simple eigenvalue of $A$ and its remaining eigenvalues each have absolute value $\sqrt{k-\lambda}$, then $AA^T - (k-\lambda)I$ has rank one. It follows that $A$ is a difference set.

Classical difference sets arise as difference sets in the association scheme of an abelian group $\Gamma$. In this case we can view the first row of $A$ as the characteristic function of a subset $S$ of $\Gamma$, and the eigenvalues are the complex numbers

$$\psi(S) + \sum_{g \in \Gamma} \psi(g).$$

# Chapter 5

# Bent Functions

We consider bent functions from the point of view of association schemes. We develop the connections with continuous quantum walks and with covers. We study crooked functions, which are closely associated with bent functions, and which give rise to interesting drackns.

## 5.1 Functions and Schemes

Suppose $\mathscr{A}$ is an association scheme with $d$ classes where, as usual, we use $\mathbb{C}[\mathscr{A}]$ to denote its Bose-Mesner algebra. If $f$ is a complex function on $\{0,\ldots,d\}$, we define a matrix $f(\mathscr{A})$ in $\mathbb{C}[\mathscr{A}]$ by

$$f(\mathscr{A}) = \sum_{i=0}^{d} f_i A_i.$$

If $M \in \mathbb{C}[\mathscr{A}]$, then $e_1^T M$ can be viewed as a function on $\{0,\ldots,d\}$. We note that

$$(fg)(\mathscr{A}) = f(\mathscr{A}) \circ g(\mathscr{A})$$

and so the mapping $f \mapsto f(\mathscr{A})$ is an isomorphism. Thus complex functions on $\{0,\ldots,d\}$ correspond to elements of $\mathbb{C}[\mathscr{A}]$, and multiplication of functions becomes Schur products of matrices.

This becomes more interesting if $\mathscr{A}$ is the group scheme for an abelian group $\Gamma$. In this case

$$A_x A_y = A_{x+y}.$$

Now

$$f(\mathscr{A})g(\mathscr{A}) = \sum_{x,y} f_x g_y A_x A_y = \sum_z \left( \sum_x f_x g_{z-x} \right) A_z$$

and the function on $\Gamma$ whose value on $z$ is $\sum_x f_x g_{z-x}$ is called the *convolution* of $f$ and $g$, denoted $f \star g$.

The group scheme for an abelian group admits a duality map $\Theta$, which (as we recall from Section 4.6) satisfies the following conditions:

(a) $\Theta(A_i) = |\Gamma|\overline{E_i}$.

(b) $\Theta(I) = J$, $\Theta(J) = |\Gamma| I$.

(c) $\Theta(MN) = \Theta(M) \circ \Theta(N)$ for all $M$ and $N$ in $\mathbb{C}[\mathscr{A}]$.

(d) $\Theta(M \circ N) = |\Gamma|^{-1}\Theta(M)\Theta(N)$ for all $M$ and $N$ in $\mathbb{C}[\mathscr{A}]$.

(e) $\Theta^2(M) = vM$

It follows that

$$\Theta(f(\mathscr{A})) = |\Gamma| \sum_i f_i \overline{E_i}$$

and therefore the eigenvalues of $|G|^{-1}\Theta(f(\mathscr{A}))$ are the entries of $f(\mathscr{A})$, that is, they are the values of $f$.

We observe that the eigenvalues of $\Theta(M)$ are the entries of $\Theta^2(M)$, i.e., they are the entries of $vM$.

If $\Gamma = \mathbb{Z}_n$, then $\Theta$ is the *discrete Fourier transform*, and if $\Gamma = \mathbb{Z}_2^d$, it is the *Hadamard transform*.

If $M$ is flat, then the eigenvalues of $\Theta(M)$ all have the same absolute value, and so some scalar multiple of $\Theta(M)$ is unitary (and if the entries of $M$ have absolute value 1, then $\Theta(M)$ is unitary). Similarly if $M$ is unitary, $\Theta(M)$ is flat.

## 5.2 Bent Functions

Let $\Gamma$ be an abelian group and let $\mathscr{A}$ denote its association scheme. A *bent function* on $\Gamma$ is a function $f$ such that $f(\mathscr{A})$ is a flat unitary matrix.

The original, and usual, definition of a bent function is that it is a function $f$ from $\mathbb{Z}_2^d$ to $\mathbb{Z}_2$ such that $f(\mathscr{A})$ is a Hadamard matrix. Bent functions were introduced by Rothaus (the first published paper is: O. S. Rothaus On "Bent" Functions, *Journal of Combinatorial Theory, Series A.* **20**, 300–305.)

Bent functions on the cyclic group $\mathbb{Z}_n$ are also known as "cyclic $n$-roots". Haagerup [**?**] proved that if $p$ is prime, only finitely many cyclic $p$-roots exist. (If they exist, their entries are algebraic numbers.)

Although it is not immediately clear that it is useful, we could extend our definition to general schemes. We are then close to the problem of identifying the type-II matrices that lie in the Bose-Mesner algebra of an association scheme. Ada and I solved this for strongly regular graphs, and she used this solution to determine the flat unitary matrices that lie in the Bose-Mesner algebra of a strongly regular graph.

Using the duality map on translation schemes, we see that each bent function $f$ has a dual $\hat{f}$, such that

$$\Theta(f(\mathscr{A})) = \hat{f}(\mathscr{A})$$

This dual is a bent function. (For the Boolen case, this was alreqdy observed by Rothaus.)

Since the Kronecker product of flat unitaries is a flat unitary matrix, we have a product operation on bent functions.

## 5.3 Boolean Functions

Formally, a *Boolean function of arity $d$* is a function from subsets of $\{1,\dots,d\}$ to $\mathbb{Z}_2$. It follows that Boolean function is the characteristic function of a subset of the power set of $\{1,\dots,d\}$. If $f_{\mathscr{S}}$ and $f_{\mathscr{T}}$ are respectively the characteristic functions of subsets $\mathscr{S}$ and $\mathscr{T}$, then

$$f_{\mathscr{S}} f_{\mathscr{T}} = f_{\mathscr{S}\cup\mathscr{T}}$$

and, using $\oplus$ to denote symmetric difference,

$$f_{\mathscr{S}} + f_{\mathscr{T}} = f_{\mathscr{S}\oplus\mathscr{T}}.$$

Any Boolean function of arity $d$ can be expressed as a polynomial in the variables $x_1,\dots,x_d$; we simply define $x_i$ to be $f_{\{i\}}$. If $f$ is Boolean, then

$$x \mapsto (-1)^{f(x)}$$

is a $\pm1$-valued function on $\mathbb{Z}_2^d$.

The polynomial $x_1x_2$ is a bent function in two variables. If $f = x_1x_2$, then

$$f(\mathscr{A}) = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

Since the Kronecker product of two symmetric Hadamard matrices with constant diagonal is a symmetric Hadamard matrix with constant diagonal, it is a bent function. We see that

$$x_1x_2 + x_3x_4$$

is a bent function on $\mathbb{Z}_2^4$, it is the Kronecker square of the previous example. If $d > 2$ and we view $f = x_1x_2$ as a function on $\mathbb{Z}_2^d$, then

$$f(\mathscr{A}) = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix} \otimes J_{d-e}$$

If $f$ is expressed as a polynomial, then $f(\mathscr{A})$ is the Schur product of matrices $f_i(\mathscr{A})$, where $f_i$ runs over the monomials in $f$. (Schur multiplication of $\pm1$-valued functions corresponds to symmetric difference.) The polynomial

$$x_1x_2 + x_3x_4 + x_1x_3 + x_2x_4 + x_1x_4 + x_2x_3$$

is a bent function on $\mathbb{Z}_2^4$ (check this), its Hadamard matrix is the Schur product of three bent functions, each isomorphic to our first example.

Suppose $f : \mathbb{Z}_2^d \to \mathbb{Z}_2$. We can use the support of $f$ as the connection set of a Cayley graph. (If we are feeling fussy, we might assume $f(0) = 0$, but one loop per

vertex is not a problem.) There is a second subset we might reasonably use, namely the set

$$\mathscr{D} = \{(x, f(x) : x \in \mathbb{Z}_2^d).$$

(This is the graph of $f$, in the Calculus sense of the word 'graph'.) Let $\mathscr{D}$ denote the elements of $\mathscr{D}$ with last entry 0, and let $\mathscr{D}_1$ consist of the elements with last entry 1. The Cayley graph $X(\mathbb{Z}_2^{d+1}, \mathscr{D})$ is then is the superposition of two Cayley graphs $X(\mathbb{Z}_2^{d+1}, \mathscr{D}_0)$ and $X(\mathbb{Z}_2^{d+1}, \mathscr{D}_1)$. The first of these is isomorphic to two vertex-disjoint copies of the Cayley graph $X(\mathbb{Z}_2^d, f^{-1}(0))$, the second is isomorphic to $K_2 \times X(\mathbb{Z}_2^d, \mathrm{supp}(f))$. Note that one of these two Cayley graphs will have a loop on each vertex. If $f(0) = 0$, it will be the first and in this $X(\mathbb{Z}_2^{d+1}, \mathscr{D})$ is the switching graph of $X(\mathbb{Z}_2^d, f^{-1}(0))$.

The first is $X(\mathbb{Z}_2^{d+1}, \mathscr{C}_0)$, which is isomorphic to two disjoint copies of the Cayley graph of $\mathbb{Z}_d$ with the complement of $\mathrm{supp}(f)$ as its connection set. The second is $X(\mathbb{Z}_2^{d+1}, \mathscr{C}_1)$, isomorphic to the direct product of $K_2$ with the Cayley graph for $\mathbb{Z}_2^d$ with connection set $\mathrm{supp}(f)$. [*** Switching graph of complement ***]

We can extend all this to the case where our abelian group is the additive group of the vector space $V(d, \mathbb{F})$, where $|\mathbb{F}|$ has order $q$ and characteristic $p$. In place of Boolean functions, we consider functions $f$ from $V$ to $\mathbb{F}$. To obtain complex-valued functions, choose a (non-identity) $p$-th root of unity in $\mathbb{C}$, and work with the function

$$x \mapsto \theta^{\mathrm{tr}(x)};$$

in other words, choose a character $\chi$ in the additive group of $\mathbb{F}$ and work with the compositions $\chi \circ f$.

## 5.4 Sage Code for Boolean Functions

```
# convert an integer to a binary vector of length d
def bin(n,d):
    res = []
    i = 0
    while i < d:
        n,r = divmod(n,2)
        res = [r] + res
        i += 1
    return VectorSpace(GF(2),d)(res)

# inverse of above
def num( bvec):
    num = 0
    twop = 1
    for digit in bvec:
        if digit != 0:
            num = num + twop
        twop = 2*twop
    return num
```

```
from sage.crypto.boolean_function import BooleanFunction
R.<x0, x1, x2, x3, x4> = BooleanPolynomialRing()
g=BooleanFunction(x0*x1+x2*x3+x0*x3*x4+x1*x2*x4+x2*x3*x4)
# g.is_plateaued()

# It's not clear to me what the domain of a Boolean function is, but
    they seem
# to accept integers

# compute support of boolean function
def bfnconn(bfun):
    op = []
    n = bfun.nvariables()
    VS = VectorSpace(GF(2),n)
    return [ bin(k,n) for k in range(2^n) if bfun(k)]

# get the eigenvalues
# g.walsh_hadamard_transform()

# get cubelike graph with bfnconn as connection set
# X = cubelike(bfnconn)

# compute unscaled weighing matrix from a plateaued function, i.e,
    compute dual
def Theta(bfun):
    n = bfun.nvariables()
    VS = VectorSpace(GF(2),n)
    op = 0
    for va in VS:
        vec = vector([(-1)^(vx.dot_product(va)) for vx in VS])
        op += (-1)^(bfun(num(va)))*vec.outer_product(vec)
    return op
```

## 5.5 Weighing Matrices

We study weighing matrices, which are a generalization of Hadamard matrices.

We say that a $v \times v$ matrix $W$ with entries $\pm 1$ is a *weighing matrix* with *weight* $w$ if $W^T W = wI$. A weighing matrix of weight $v$ is a Hadamard matrix and you might prove that a weighing matrix of weight $v-1$ is permutation equivalent to a conference matrix. If $H$ is a Hadamard matrix, then the matrices

$$\begin{pmatrix} 0 & H \\ H^T & 0 \end{pmatrix}$$

is a weighing matrix. If $W_1$ and $W_2$ are weighing matrices of the same order and

weight, then

$$\begin{pmatrix} W_1 & 0 \\ 0 & W_2 \end{pmatrix}$$

is a weighing matrix. The Kronecker product of two weighing matrices is a weighing matrix.

If $W$ is a weighing matrix $W$ with weight $w$, then $w^{-1/2}W$ is orthogonal, whence its eigenvalues have absolute value 1.

We say $W$ is *regular* if its row sums are all equal. If $W\mathbf{1} = \rho\mathbf{1}$, then

$$\rho W^T\mathbf{1} = W^T W\mathbf{1} = w\mathbf{1}$$

and so each column of $W$ sums to $w/\rho$. By the "findamental theorem of accountancy", the sum of the row sums of a matrix is equal to the sum of its column sums, and hence $\rho = w/\rho$. Therefore $w$ is a perfect square and $\rho = \pm\sqrt{w}$.

**5.5.1 Lemma.** *Assume $W$ is a $v \times v$ weighing matrix with sign $\epsilon$ in the Bose-Mesner algebra of the group scheme of $\mathbb{Z}_2^d$. Then $w$ is an even power of two, and the eigenvalues of $W$ are $\pm\sqrt{w}$. The row sum of $W$ is $\frac{1}{2}(w \pm \sqrt{w})$. Further:*

*(a) If $\mathrm{tr}(W) \neq 0$, the multiplicity of $\sqrt{w}$ is*

$$\frac{1}{2}\left(v + \frac{\mathrm{tr}(W)}{\sqrt{w}}\right).$$

*(b) If $\mathrm{tr}(W) = 0$, then the two eigenvalues have the same multiplicity.*

*Proof.* Since $W$ is symmetric, its eigenvalues are $\pm\sqrt{w}$. The row sum of $W$ is an eigenvalue of $W$, whence it is equal to $\pm\sqrt{w}$. The number of non-zero entries in a row is $w$ and, if exactly $b$ entries are positive, the row sum is $2b - w$, so $b = (w + \pm\sqrt{w})/2$.

If $\sqrt{w}$ has multiplicity $a$ as an eigenvalue of $W$, then

$$\mathrm{tr}(W) = a\sqrt{w} - (v-a)\sqrt{w} = (2a - v)\sqrt{w}.$$

If $\mathrm{tr}(W) \neq 0$, it follows that $\sqrt{w}$ divides $v$ and

$$a = \frac{1}{2}\left(v + \frac{\mathrm{tr}(W)}{\sqrt{w}}\right). \qquad \square$$

We remark that $W$ determines a 2-ev double cover of the graph with adjacency matrix $W^{\circ 2}$.

## 5.6 Dual Weighing Matrices

Define the *sign* of a weighing matrix $W$ to be $\mathrm{tr}(W)\,\mathrm{sum}(W)$. (This is an abuse, because it could be zero.) The matrices $W$ and $-W$ have the same sign.

**5.6.1 Lemma.** *Assume $W$ is a $v\times v$ weighing matrix of weight $w$ in the group scheme of $\mathbb{Z}_2^d$. Then $w^{-1/2}\Theta(W)$ is a $\pm1$-matrix with eigenvalues $0$ and $\pm w^{-1/2}v$. Let $B$ be the $01$-matrix in the scheme such that $w^{-1/2}\Theta(W) = 2B - J$. If $\epsilon = W_{1,1}$, the eigenvalues of $B$ are*

$$\frac{v}{2}(1+\epsilon w^{-1/2}), \quad 0, \quad \pm\frac{v}{2}w^{-1/2},$$

*where the first eigenvalue is simple and the multiplicity of $0$ is $v-w$ if $\epsilon = 0$ and is otherwise $v-1-w$.*

*Proof.* We see that $\Theta(W)$ is a matrix with entries $\pm\sqrt{w}$. The eigenvalues of $\Theta(W)$ are the entries of $\Theta^2(W)$, i.e., the entries of $vW$. Accordingly $w^{-1/2}\Theta(W)$ is a $\pm1$-matrix with eigenvalues $0$ and $\pm w^{-1/2}v$.

There is a $01$-matrix $B$ in $\mathbb{C}[\mathscr{A}]$ such that

$$w^{-1/2}\Theta(W) = 2B - J$$

and then

$$2\Theta(B) - vI = \Theta(2B-J) = w^{-1/2}\Theta^2(W) = w^{-1/2}vW,$$

which implies that

$$\Theta(B) = \frac{v}{2}(I + w^{-1/2}W).$$

If $W\circ I = 0$, it follows that the eigenvalues of $B$ are

$$\frac{v}{2}, \quad 0, \quad \pm\frac{v}{2}w^{-1/2}.$$

If $W\circ I = I$, the eigenvalues of $B$ are

$$\frac{v}{2}(1+w^{-1/2}), \quad 0, \quad \pm\frac{v}{2}w^{-1/2}$$

and if $W\circ I = -I$, they are

$$\frac{v}{2}(1-w^{-1/2}), \quad 0, \quad \pm\frac{v}{2}w^{-1/2}. \qquad \square$$

We will refer to the graph with adjacency matrix $B$ as the graph of the dual weighing matrix.

A $\pm1$-valued function $\mathbb{Z}_2^d$ on $G$ is said to be *plateaued* if the non-zero eigenvalues of $H = f(\mathscr{A})$ all have the same absolute value. If the non-zero eigenvalues of $H$ are $\pm\rho$, then the entries of $\rho^{-1}\Theta(H)$ are $0,\pm1$ and its eigenvalues are $\pm v/\rho$. Therefore

$$(\rho^{-1/2}\Theta(H))^2 = \frac{v^2}{\rho^2}I,$$

which implies that $\rho^{-1}\Theta(H)$ is a weighing matrix with weight $v^2/\rho^2$. Hence $\rho^2 \geq v$ (and if $\rho^2 = v$, then $\rho^{-1}\Theta(H)$ is a Hadamard matrix). Thus plateaued functions are dual to weighing matrices.

If $\rho^2 = 2v$, then $f$ is said to be a *semibent* function. (Plateaued, semibent, you can't make this stuff up, hmm, well...) When $d$ is odd, a semibent function is dual to a weighing matrix of order $2^d \times 2^d$ with weight $2^{(d+1)/2}$. The Boolean functions

$$x_0x_1 + x_0x_2 + x_1x_2, \quad x_0x_1 + x_2x_3 + x_0x_3x_4 + x_1x_2x_4 + x_2x_3x_4$$

are semi-bent. The graph underlying the weighing matrix of the second function is a drackn.

We could generalize the idea of a weighing matrix to general abelian group schemes by assuming only that its non-zero elements all have the same absolute value. So if $W$ were a weighing matrix in a scheme of the finite abelian group $G$, its scaled dual would be a matrix with entries $\pm 1$ and with all non-zero eigenvalues having the same absolute value.

[Apparently any Boolean function of degree at most two is plateaued—see Section 5.1 in Claude Carlet1 and Emmanuel Prouff: "On plateaued functions and their constructions".) It seems that the dual of a linear function is a permutation.

## 5.7 Walk-Regular Graphs

A regular graph with at most four distinct eigenvalues is walk regular, and so by Lemma 5.6.1, the graph of a dual weighing matrix is walk regular. We can say a little more (following van Dam and Omidi).

**5.7.1 Lemma.** *Let $X$ be a connected regular graph with exactly four eigenvalues*

$$k, \quad \theta, \quad 0, \quad -\theta.$$

*Then $A^{2m+1}$ lies in* span$\{I, J, A\}$ *for all non-negative integers $m$.*

*Proof.* Assume $p(t) = t(t^2 - \theta^2)$. Then (by spectral decomposition)

$$\frac{1}{n}p(k)J = p(A) = A^3 - \theta^2 A$$

and therefore $A^3 \in$ span$\{I, J, A\}$. But this equation also implies that

$$A^{2m+3} - \theta^2 A^{2m+1} = \frac{1}{n}p(k)k^{2m}J$$

and the lemma follows. □

A graph is said to be *strongly $\ell$-walk regular* if $\ell > 1$ and $A^\ell \in$ span$\{I, J, A\}$. So the graph of a dual weighing matrix is strongly $\ell$-walk regular for all odd integers $\ell$ (with $\ell > 1$). (It's not clear what we might do with this information.)

For more on strongly $\ell$-walk regular graphs, see van Dam and Omidi.

## 5.8 Hadamard Matrices

A Hadamard matrix is a $v \times v$ weighing matrix with weight $v$, so the theory above from the previous section implies that if $H$ is a regular Hadamard matrix, then $v$ is a perfect square and the row sum of $H$ is $\pm\sqrt{v}$.

If $H$ lies in the Bose-Mesner algebra of $\mathbb{Z}_2^d$, it is a bent function. Replacing $H$ by $-H$ if needed, there is a 01-matrix $B$ in the scheme (with zero diagonal) such that $H = J - 2B$. Let $\sigma$ be the row sum of $H$. Then $2B = J - H$ and since $HJ = J$, the eigenvalues of $J - H$ are

$$v - \sigma, \quad \pm\sqrt{v}.$$

Here $\sigma = \pm\sqrt{v}$ and therefore the eigenvalues of $B$ are

$$\frac{1}{2}(v \pm \sqrt{v}), \quad \pm\frac{1}{2}\sqrt{v}.$$

The first eigenvalue here is the row sum of $B$, since it is simple we see that $B$ is the adjacency matrix of a connected regular graph with exactly three eigenvalues. Thus $B$ is the adjacency matrix of a strongly regular graph.

## 5.9 Projective Two-Weight Codes

A linear code is a *two-weight* code if its non-zero code words have only two different weights. A code $C$ is *projective* if the minimum weight of its dual code as at least three; equivalently $C$ is projective if no column of its generator matrix is a scalar multiple of another. If $M$ is the generator matrix of a projective code, the Cayley graph $X(M)$ has $\mathrm{col}(M)$ as its vertex set, with two elements of $\mathrm{col}(M)$ adjacent if their difference is a scalar multiple of a column of $M$. (So $X(M)$ is a linear Cayley graph.) In the absence of warnings, assume that the rows of $M$ are linearly independent.

Any cubelike graph can be expressed as $X(M)$ for a suitable $d \times m$ matrix over $\mathbb{Z}_2$. In this case, $X(M)$ is strongly regular if and only if $\mathrm{row}(M)$ is a projective two-weight code. Therefore any weighing matrix in the group scheme of $\mathbb{Z}_2^d$ determines a projective two-weight code.

## 5.10 Hamming Schemes

We work with Hamming schemes. We choose a finite commutative ring $R$ and identify the vertices of the Hamming scheme with the elements of $R^d$. (Our rings will be finite fields and $\mathbb{Z}_4$.) If $\chi$ is a character of the additive group of $R$, we can define a *pairing*, a bi-additive map $\beta$ from $R^d \times R^d$ to $\mathbb{C}$ by mapping $(u, v)$ in $R^d \times R^d$ to

$$\chi\Big(\sum_i u_i v_i\Big).$$

If $a$ is fixed, the map

$$x \mapsto \beta(ax)$$

is a character of $\mathbb{R}^d$; we denote it by $\beta_a$. The distinct characters $\beta_a$ (for $a \in R^d$) form an orthogonal basis for the space of complex functions on $R^d$. We define the *weight* of $\beta_a$ to be the Hamming weight of $a$. The advantage of this is that the characters of weight $r$ form an orthogonal basis for the $r$-th eigenspace of the Hamming scheme.

$$\sum_z (-1)^{f(z)}(-1)^{a\cdot z} = \sum_z (-1)^{f(z)+a\cdot z}$$

[*** goal is to show that bent functions are at max distance from affine functions ***]

## 5.11 Uniform Mixing and PST

A continuous quantum walk is a family of unitary matrices $U(t)$ of the form

$$U(t) := \exp(i\,t\,A).$$

(So it's a 1-parameter subgroup of the unitary group.) The matrix $A$ is the *Hamiltonian* of the walk, and is required to be hermitian; for us it will be the adjacency matrix of a graph. A quantum walk admits uniform mixing if there is a time $\tau$ such that $U(\tau)$ is flat. The simplest example is when $A$ is the adjacency matrix of $K_2$, where uniform mixing occurs at time $\pi/4$.

If our walk is based on a graph in a translation scheme and uniform mixing occurs at time $\tau$, then $U(\tau)$ is a flat unitary. Hence we have a bent function. It is important to note though that a given bent function need not be of the form $\exp(i\,t\,A)$ for some 01-matrix $A$.

If $\Gamma = \mathbb{Z}_2^d$ and $f$ is a real-valued bent function, then $H = f(\mathscr{A})$ is a symmetric Hadamard matrix with constant diagonal and $H^2 = 2^d I$. Thus if $U(\tau)$ flat and real, then $U(2\tau) = I$. If we have uniform mixing at time $\tau$ and pst at time $2\tau$, then there is a complex root of unity $\gamma$ such that $U(\tau)^4 = \gamma I$. So $H = \gamma^{-1/4}U(\tau)$ is a flat unitary and $\Theta(H)$ is a flat unitary with entries in $\{\pm 1, \pm i\}$. Therefore $H$ is a bent function over $\mathbb{Z}_4^e$ (for some $e$).

[*** Cao, Feng. Uniform mixing on abelian Cayley graphs. (`https://arxiv.org/abs/1911.07495`): real bent functions in $\mathbb{Z}_2^d$ admit fast uniform mixing ***]

[*** Tan, Feng, Cao. Perfect state transfer on abelian Cayley graphs. (`https://arxiv.org/abs/1712.09260`): real bent functions in $\mathbb{Z}_2^d$ give fast pst ***]

## 5.12 Crooked Functions

## 5.13 Now for $\mathbb{Z}_4$

We consider functions from $\mathbb{Z}_4^d$ to $\{\pm 1, \pm i\}$; we refer to these as *quaternary functions*. We work in the association scheme over $\mathbb{Z}_4^d$. Any quaternary function determines a matrix in the scheme with entries $\{\pm 1, \pm i\}$, and so we have a flat matrix. We want this to be unitary, which means it is a flat unitary matrix, and in this case the dual will be a flat unitary matrix with entries roots of unity and eigenvalues in $\{\pm 1, \pm i\}$.

Suppose $H$ is an $n \times n$ matrix with entries from $\{\pm 1, \pm i\}$ and $H_0, H_1$ are the real matrices such that $H = H_0 + iH_1$. Then

$$nI = (H_0 + iH_1)^*(H_0 + iH_1) = H_0^T H_0 + H_1^T H_1 + i(H_0^T H_1 - H_1^T H_0),$$

implying that $H_0^T H_1$ is symmetric. This also implies that $H_0^T H_0 + H_1^T H_1 = nI$. Further, the $2n \times 2n$ matrix

$$\begin{pmatrix} H_0 + H_1 & H_0 - H_1 \\ H_1 - H_0 & H_0 + H_1 \end{pmatrix}$$

is a Hadamard matrix if and only $H$ is a complex Hadamard matrix.

Let $H$ be an $n \times n$ complex Hadamard matrix, and let $S_i$ denote the sum of the entries in the $i$-th row of $H$. Then $\sum_i |S_i|^2 = n^2$ (exercise) and, using Cauchy-Schwarz, we deduce that $\sum_i |S_i| \leq n\sqrt{n}$ and with equality if and only if $|S_i| = \sqrt{n}$ for all $i$. Now suppose each row of $H$ sums to $\sigma$. Since $H^* H = nI$ and $H$ is normal, all eigenvalues of $H$ have absolute value $\sqrt{n}$. As $\sigma$ is an eigenvalue, $|\sigma| = \sqrt{n}$. Now there are integers $a, b, c, d$ such that

$$\sigma = (a - b) + i(c - d)$$

and therefore

$$n = |\sigma|^2 = \sigma\overline{\sigma} = (a - b)^2 + (c - d)^2$$

## 5.14 To Do

1. Get examples of plateaued functions.
2. Study the graphs associated with these functions. (Cayley graph on support of functions, four graphs from weighing matrix).
3. Does a plateaued function give rise to a 3-class scheme?
4. BH4 matrices in abelian group schemes, please.
5. Study duals of BH4 matrices.
6. If $H$ is BH4, is $H \circ H$ a Hadamard matrix? (Sometimes? When?)

# Chapter 6

# Type-II Matrices

## 6.1 Eigenspaces

The algebra $\mathcal{N}_W$ determines a scheme consisting of $n \times n$ matrices. We describe how we can determine the eigenmatrix of the scheme. Let us say that vectors $Y_{a,b}$ and $Y_{r,s}$ *overlap* if $Y_{a,b}^T Y_{r,s} \neq 0$.

**6.1.1 Lemma.** *If $Y_{a,u}$ and $Y_{b,c}$ overlap then $(\Theta(M))_{u,a} = (\Theta(M))_{b,c}$.*

*Proof.* As the vectors $Y_{u,i}$ for fixed $u$ form a basis, $Y_{b,c}$ lies in their span. In fact

$$Y_{b,c} = \frac{1}{n} \sum_i (Y_{i,u}^T Y_{b,c}) Y_{u,i}.$$

So

$$(\Theta(M))_{b,c} Y_{b,c} = M Y_{b,c} = \frac{1}{n} \sum_i (Y_{i,u}^T Y_{b,c}) (\Theta(M))_{u,i} Y_{u,i}.$$

Multiply both sides of this by $Y_{a,u}^T$ to get

$$\begin{aligned}(\Theta(M))_{b,c} Y_{a,u}^T Y_{b,c} &= \frac{1}{n} (Y_{a,u}^T Y_{b,c}) (\Theta(M))_{u,a} Y_{a,u}^T Y_{u,a} \\ &= Y_{a,u}^T Y_{b,c} (\Theta(M))_{u,a}.\end{aligned}$$

If $Y_{a,u}^T Y_{b,c} \neq 0$, this implies that $(\Theta(M))_{u,a} = (\Theta(M))_{b,c}$. □

We define a graph with vertex set $\Omega$. Define $i$ and $j$ to be adjacent if there are $b$ and $c$ such that $Y_{b,c}$ overlaps both $Y_{u,i}$ and $Y_{u,j}$. Note $u$ is adjacent to itself, and to no other vertex. Any matrix $\sum F_i$, where $i$ ranges over the vertices in a component of this graph, is a matrix idempotent of the scheme belonging to $\mathcal{N}_W$. (The key point is that this sum lies in $\mathcal{N}_W$.)

We have the following observation, due to Jaeger et al [**?**].

**6.1.2 Lemma.** *Let $W$ be a Hadamard matrix of order $n$. If $\mathcal{N}_W$ is non-trivial, then $n$ is divisible by eight.*

*Proof.* Let $w_i$ denote $We_i$. Normalize $W$ so that $w_1 = \mathbf{1}$ and assume $1$, $i$, $j$ and $k$ are distinct. Then

$$(w_1 + w_i) \circ (w_1 + w_j) \circ (w_1 + w_j)$$

is the Schur product of three vectors with entries $0, \pm 2$. The sum of the entries of this vector is

$$\langle \mathbf{1}, w_1^{\circ 3} \rangle + \langle \mathbf{1}, w_1^{\circ 2} \circ (w_i + w_j + w_k) \rangle \\ + \langle \mathbf{1}, w_1 \circ (w_i \circ w_j + w_i \circ w_k + w_j \circ w_k) \rangle + \langle \mathbf{1}, w_i \circ w_j \circ w_k \rangle$$

Since $W$ is a Hadamard matrix, the second and third terms here are zero, whence we deduce that, modulo 8,

$$n + \langle \mathbf{1}, w_i \circ w_j \circ w_k \rangle = 0$$

and therefore, if $n$ is not divisible by 8, then $w_i$ cannot be orthogonal to $w_j \circ w_k$. □

## 6.2 Hadamard Matrices

A Hadamard matrix is a $\pm 1$-matrix of order $n \times n$ such that

$$H^T H = nI.$$

Since $H \circ H = J$ it follows that $H$ is a type-II matrix. Hadamard matrices have long been of interest to combinatorialists. Since they are the simplest examples of type-II matrices, we summarize what is known about their Nomura algebras here.

**6.2.1 Lemma.** *If $W$ is real then all matrices in $\mathcal{N}_W$ are symmetric.*

*Proof.* If $W$ is real then the eigenvectors $Y_{a,b}$ are real. Hence the Schur idempotents of the scheme have only real eigenvalues. Since $\mathcal{N}_W$ is closed under transposes and is a commutative algebra, the Schur idempotents are real normal matrices. A real normal matrix is symmetric if and only if its eigenvalues are real. □

The following is a new proof of a result due to Jaeger et al [**?**].

**6.2.2 Lemma.** *Let $W$ be a Hadamard matrix of order $n$. If $\mathcal{N}_W$ is non-trivial, then $n$ is divisible by eight.*

*Proof.* Let $w_i$ denote $We_i$. Normalise $W$ so that $w_1 = \mathbf{1}$ and assume $1$, $i$, $j$ and $k$ are distinct. Then

$$(w_1 + w_i) \circ (w_1 + w_j) \circ (w_1 + w_k)$$

is the Schur product of three vectors with entries $0, \pm 2$. The sum of the entries of this vector is

$$\langle \mathbf{1}, w_1^{\circ 3} \rangle + \langle \mathbf{1}, w_1^{\circ 2} \circ (w_i + w_j + w_k) \rangle \\ + \langle \mathbf{1}, w_1 \circ (w_i \circ w_j + w_i \circ w_k + w_j \circ w_k) \rangle + \langle \mathbf{1}, w_i \circ w_j \circ w_k \rangle \quad (6.2.1)$$

Since $W$ is a Hadamard matrix, the second and third terms here are zero, whence we deduce that, modulo 8,

$$n + \langle \mathbf{1}, w_i \circ w_j \circ w_k \rangle = 0$$

and therefore, if $n$ is not divisible by 8, then $Y_{i,1} = w_i$ cannot be orthogonal to $Y_{j,k} = w_j \circ w_k$. □

If $H$ is a Hadamard matrix of order less than 32, its Nomura algebra is a product of Potts models. (Unpublished computations by Allan Roberts and the second author.)

Hadamard matrices form a special case of a more general class of type-II matrices. A complex matrix is *flat* if all its entries have the same absolute value. The following result is easy to prove.

**6.2.3 Lemma.** *For an $n \times n$ matrix, any two of the following statements imply the third:*

*(a) $W$ is a type-II matrix.*

*(b) $n^{-1/2}W$ is unitary.*

*(c) $|W_{i,j}| = 1$ for all $i$ and $j$.* □

In other words, a unitary matrix is type-II if and only if it is flat. The character table of an abelian group is flat, type-II and unitary. Flat unitary matrices appear in quantum physics in connection to mutually unbiased sets of orthogonal bases.

## 6.3 Symmetric Designs

We consider the type-II matrices with exactly two distinct entries that are not Hadamard matrices.

**6.3.1 Theorem.** *Suppose $W = aJ + (b-a)N$, where $N$ is a 01-matrix and $a \neq \pm b$. Then $W$ is type II if and only if $N$ is the incidence matrix of a symmetric design.*

*Proof.* Let $N$ be the incidence matrix of a symmetric $(v,k,\lambda)$-design, and let $W$ be given by

$$W = J + (t-1)N,$$

where

$$t = \frac{1}{2(k-\lambda)}\left(2(k-\lambda) - v \pm \sqrt{v(v-4(k-\lambda))}\right).$$

We show that $W$ is a type-II matrix.

We have

$$W^{(-)} = (t^{-1}-1)N + J$$

and, as $NJ = N^T J = kJ$ and $J^2 = vJ$,

$$\begin{aligned} WW^{(-)T} &= (t-1)(t^{-1}-1)NN^T + (k(t+t^{-1}-2)+v)J \\ &= (t-1)(t^{-1}-1)(k-\lambda)I + ((k-\lambda)(t+t^{-1}-2)+v)J. \end{aligned}$$

The coefficient of $J$ is zero if

$$(k-\lambda)(t-1)^2 + v(t-1) + v = 0,$$

which yields sufficiency.

We now prove the converse. If $W$ has exactly two distinct entries, there is no harm in assuming that we have

$$W = J + (t-1)N$$

for some 01-matrix $N$ and some complex number $t$ such that $t \neq \pm 1$. Then $W^{(-)T} = J + (t^{-1}-1)N^T$ and so, if $W$ is $v \times v$, we have

$$WW^{(-)T} = vJ + (t-1)NJ + (t^{-1}-1)JN^T + (t-1)(t^{-1}-1)NN^T.$$

Since $WW^{(-)T} = vI$ and $NN^T$ is symmetric, this implies that

$$M := (t-1)NJ + (t^{-1}-1)JN^T$$

is symmetric. We work with this. Note that this equation yields

$$M - M^T = (t-t^{-1})NJ + (t^{-1}-t)JN^T = (t-t^{-1})(NJ - (NJ)^T).$$

Since $M = M^T$ and $t \neq \pm 1$, this forces us to conclude that $NJ$ is symmetric. Hence there is a positive integer $k$ such that

$$NJ = JN^T = kJ.$$

Returning to our expression for $WW^{(-)T}$, we now have

$$WW^{(-)T} = (v + k(t+t^{-1}-2))J + (2-t-t^{-1})NN^T. \tag{6.3.1}$$

Since $(2-t-t^{-1}) = -(t-1)^2/t$ and $t \neq 1$, it follows that $NN^T$ is a linear combination of $I$ and $J$, and consequently $N$ is the incidence matrix of a symmetric design. □

Note that if $v + k(t+t^{-1}-2) = 0$ in 6.3.1) then we get $NN^T = kI$. Since $N$ is a square 01-matrix, $NN^T = kI$ only when $k = 1$. In this case, $N$ is the incidence matrix of the complement of the complete design, and $W = J + (t-1)N$ is equivalent to the Potts model.

If $H$ is a Hadamard matrix, we may multiply it fore and aft by diagonal matrices, thus setting all entries in the first row and column to 1. If $H_1$ is the matrix we get from this by deleting the first row and column, then

$$\frac{1}{2}(H_1 + J)$$

is the incidence matrix of a symmetric design. This gives a large class of examples of symmetric designs.

**6.3.2 Lemma.** *Suppose $W$ is a type-II matrix of the form $(t-1)N+J$, where $N$ is the incidence matrix of a symmetric $(v,k,\lambda)$-design. If $v>3$, then all matrices in $\mathcal{N}_{W^T}$ are symmetric.*

*Proof.* We show that $\langle Y_{i,j}, Y_{i,j}\rangle \neq 0$ when $v>3$. By **??**, it follows that $\Theta(M)_{i,j} = \Theta(M)_{j,i}$ for all $M$ in $\mathcal{N}_W$ and for all $i$ and $j$.

We have

$$\begin{aligned}\langle Y_{i,j}, Y_{i,j}\rangle &= (k-\lambda)(t^2+t^{-2})+v-2k+2\lambda\\ &= (k-\lambda)(t^2-2+t^{-2})+v,\end{aligned}$$

and so, if $\langle Y_{i,j}, Y_{i,j}\rangle = 0$ then

$$t^2-2+t^{-2} = \frac{-v}{(k-\lambda)}.$$

From our computations in the proof of the previous theorem,

$$(k-\lambda)(t-2+t^{-1})+v=0, \tag{6.3.2}$$

and so

$$t-2+t^{-1} = \frac{-v}{(k-\lambda)}.$$

As

$$t^2-2+t^{-2} = (t-2+t^{-1})(t+2+t^{-1}),$$

these equations imply that, if $\langle Y_{i,j}, Y_{i,j}\rangle = 0$, then

$$t+1+t^{-1}=0,$$

whence (6.3.2) implies that $v=3(k-\lambda)$.

Since $v(v-1)\lambda = vk(k-1)$, if $v=3(k-\lambda)$, then

$$k^2 = k+(v-1)\lambda = (3\lambda+1)(k-\lambda)$$

and therefore

$$k^2-(3\lambda+1)k+3\lambda^2+\lambda=0$$

This discriminant of this quadratic is

$$1+2\lambda-3\lambda^2 = (1-\lambda)(1+3\lambda),$$

which is negative if $\lambda>1$. The lemma follows. □

**6.3.3 Lemma.** *Let $N$ be the incidence matrix of a symmetric design, and let $W$ be a type-II matrix of the form $(t-1)N+J$. If $t\neq -1$, then the difference of two distinct columns of $N$ is an eigenvector for the Nomura algebra of $W$.*

*Proof.* If $u$ is a point in the design and $\alpha$ and $\beta$ are the $i$-th and $j$-th blocks in the design, then

$$(Y_{i,j})_u = \begin{cases} t, & \text{if } u \in \alpha \setminus \beta; \\ t^{-1}, & \text{if } u \in \beta \setminus \alpha; \\ 1, & \text{otherwise.} \end{cases}$$

By the previous lemma, $Y_{i,j}$ and $Y_{j,i}$ have the same eigenvalues for any matrix in $\mathcal{N}_W$. Therefore the vector

$$(t - t^{-1})^{-1}(Y_{i,j} - Y_{j,i})$$

is an eigenvector for each matrix in $\mathcal{N}_W$, but this vector is just the difference of the $i$-th and $j$-th columns of $N$. □

We note that if $t = -1$ then $(t-1)N + J$ is type II if and only if it is a Hadamard matrix. The previous lemmas lead to the following disappointing consequence.

**6.3.4 Theorem.** *Suppose $W$ is a type-II matrix of the form $(t-1)N + J$, where $N$ is the incidence matrix of a symmetric $(v,k,\lambda)$-design. If $v > 3$ and $t \neq -1$, then the Nomura algebra of $W$ is trivial.*

Let $Z_{i,j} := Ne_i - Ne_j$ for some $i \neq j$. If $k$ is distinct from $i$ and $j$ then

$$\langle Z_{i,j}, Ne_k \rangle = \langle Ne_i, Ne_k \rangle - \langle Ne_j, Ne_k \rangle = \lambda - \lambda = 0$$

while

$$\langle Z_{i,j}, Ne_i \rangle = k - \lambda.$$

We conclude that $\langle Z_{i,j}, Z_{i,k} \rangle = k - \lambda$ and therefore at least one of

$$Y_{i,k}^T Y_{i,j}, \quad Y_{k,i}^T Y_{i,j}, \quad Y_{i,k}^T Y_{j,i} \quad \text{and} \quad Y_{k,i}^T Y_{j,i}$$

is non-zero. It follows from **??** and 6.3.2 that

$$\Theta(M)_{i,k} = \Theta(M)_{i,j}$$

for any matrix $M$ from $\mathcal{N}_W$. It follows that $\mathcal{N}_W$ must be trivial. □

## 6.4 Equiangular Lines

We consider sets of lines in $\mathbb{C}^d$. A set of lines in $\mathbb{C}^d$ spanned by the unit vectors $x_1, \ldots, x_n$ is *equiangular* if there is a real number $\alpha$ such that

$$|\langle x_i, x_j \rangle| = \alpha$$

whenever $i \neq j$. Note that it is reasonable to take the absolute value here, because if $\lambda \in \mathbb{C}$ and $|\lambda| = 1$ then $\lambda x_i$ and $x_i$ are unit vectors spanning the same line. We will refer to $\alpha$ as the *angle* between the lines. We are also interested in equiangular sets of lines in $\mathbb{R}^d$; the above definition still works in this case. We have the following result, due to [**?**].

**6.4.1 Theorem.** *If there is a set of $n$ equiangular lines in $\mathbb{C}^d$ or $\mathbb{R}^d$ with angle $\alpha$ and $d\alpha^2 < 1$, then*

$$n \leq \frac{d(1-\alpha^2)}{1-d\alpha^2}.$$

*Proof.* Suppose $x_1, \ldots, x_n$ are unit vectors spanning a set of equiangular lines in $\mathbb{C}^d$ and suppose $X_i := x_i x_i^*$. Then $X_i$ is a Hermitian matrix that represents orthogonal projection onto the line spanned by $x_i$. Assume that $|\langle x_i, x_j\rangle| = \alpha$ when $i \neq j$. The space of Hermitian matrices is a real inner product space with inner product $\langle X, Y\rangle$ given by

$$\langle X, Y\rangle = \operatorname{tr}(XY).$$

Then $\langle X_i, X_i\rangle = 1$ and if $i \neq j$ then

$$\begin{aligned}\langle X_i, X_j\rangle = \operatorname{tr}(X_i X_j) &= \operatorname{tr}(x_i x_i^* x_j x_j^*)\\ &= \operatorname{tr}(x_j^* x_i x_i^* x_j)\\ &= |x_i^* x_j|^2\\ &= \alpha^2.\end{aligned}$$

If

$$Z := \sum_i X_i$$

then

$$\langle Z, Z\rangle = n + (n^2 - n)\alpha^2$$

and if $\gamma \in \mathbb{R}$, then

$$\langle Z - \gamma I, Z - \gamma I\rangle = n + (n^2 - n)\alpha^2 - 2\gamma n + \gamma^2 d.$$

Here the right side is a quadratic in $\gamma$, and is non-negative for all real $\gamma$. Its minimum value occurs when $\gamma = n/d$, which implies that

$$-\frac{n^2}{d} + n(1 + \alpha^2(n-1)) \geq 0.$$

The theorem follows from this. □

Note that the above proof still works if we replace $\mathbb{C}$ by $\mathbb{R}$ and 'Hermitian' by 'symmetric'.

We say a set of lines is *tight* if equality holds in the bound of the previous theorem. We say that an $n \times n$ matrix $C$ is a *generalized conference matrix* if:

(a) $C$ is Hermitian

(b) $C_{i,i} = 0$ for all $i$.

(c) $|C_{i,j}| = 1$ if $i \neq j$.

(d) The minimal polynomial of $C$ is quadratic.

Note that a conference matrix is an $n \times n$ matrix with diagonal entries zero and off-diagonal entries $\pm 1$, such that $CC^T = (n-1)I$. It is known that a conference matrix is equivalent to a symmetric or skew symmetric conference matrix. If $C$ is symmetric then it is Hermitian and $C^2 - (n-1)I = 0$. If $C$ is skew symmetric, then $iC$ is Hermitian and $(iC)^2 - (n-1)I = 0$.

**6.4.2 Corollary.** *Suppose $x_1, \ldots, x_n$ are unit vectors that span a set of equiangular lines in $\mathbb{C}^d$ with angle $\alpha$ and Gram matrix $G$, and suppose $G = I + \alpha C$. Then the set of lines is tight if and only if $C$ is a generalized conference matrix.*

*Proof.* Suppose $x_1, \ldots, x_n$ span a set of equiangular lines in $\mathbb{C}^d$, let $X_i$ be the orthogonal projection onto the line spanned by $x_i$ and set $Z = \sum_i X_i$. If this set of lines is tight, then

$$\langle Z - \gamma I, Z - \gamma I \rangle = 0$$

and consequently

$$\sum_i X_i = \frac{n}{d} I.$$

Let $U$ be the $n \times d$ matrix with $i$-th row equal to $x_i^*$. Then

$$U^* U = \sum_i X_i = \frac{n}{d} I.$$

Now $G := UU^*$ is the Gram matrix of the unit vectors $x_1, \ldots, x_n$; since $UU^*$ and $U^*U$ have the same non-zero eigenvalues with the same multiplicities it follows that the eigenvalues of $G$ are 0 and $n/d$. Since our set of lines is equiangular, we may write

$$G = I + \alpha C.$$

Here $C$ is Hermitian, its diagonal entries are zero, its off-diagonal entries all have absolute value 1, and its minimal polynomial is quadratic. Thus it is a generalized conference matrix.

For the converse, suppose that $C$ is a non-zero Hermitian matrix with zero diagonal and

$$C^2 - \beta C - \gamma I = 0.$$

Then the diagonal entries of $C^2$ are positive, whence $\gamma \neq 0$ and $C$ is invertible. If $\tau$ is the least eigenvalue of $C$, then

$$G := I - \frac{1}{\tau} C$$

is Hermitian and all its eigenvalues non-negative. Assume $\mathrm{rk}(G) = d$. Since $\mathrm{tr}(G) = n$ it follows that the eigenvalues of $G$ are 0 and $n/d$. Hence there is an $n \times d$ matrix $U$ such that

$$U^* U = \frac{n}{d} I, \quad UU^* = G.$$

Thus $G$ is Gram matrix of the columns of $U^*$, and so these columns span a set of equiangular lines in $\mathbb{C}^d$. Since $U^*U = (n/d)I$, the set of lines is tight. □

Conditions (a) and (c) in the definition of generalized conference matrix imply that $(C^2)_{i,i} = (n-1)I$, whence the minimal polynomial of $C$ has the form $z^2 - \beta z - (n-1)$, for some $\beta$.

**6.4.3 Theorem.** *Suppose $C$ is a generalized conference matrix of order $n \times n$ with minimal polynomial $z^2 - \beta z - (n-1)$. If $t + t^{-1} + \beta = 0$, then $tI + C$ is type II.*

*Proof.* If $C$ is a generalized conference matrix, then

$$(tI + C)^{(-)T} = t^{-1}I + C$$

and therefore

$$\begin{aligned}(tI + C)(tI + C)^{(-)T} &= I + t^{-1}C + tC^{(-)T} + CC^{(-)T} \\ &= I + (t + t^{-1})C + C^2 \\ &= I + (t + t^{-1})C + \beta I + (n-1)I \\ &= nI + (t + t^{-1} + \beta)C.\end{aligned}$$

Hence $tI + C$ is type-II if

$$t + t^{-1} + \beta = 0. \qquad \square$$

We derive a converse to this result, under weaker conditions.

**6.4.4 Theorem.** *Let $W$ be a type-II matrix with all diagonal entries equal to $c$ and with quadratic minimal polynomial. If $W - cI$ is Hermitian, it is a scalar multiple of a generalized conference matrix.*

*Proof.* Suppose that $W$ is $n \times n$ and

$$W^2 - \beta W - \gamma I = 0.$$

Since $W$ is invertible, $\gamma \neq 0$ and

$$W^{-1} = -\frac{1}{\gamma}(\beta I - W).$$

Hence

$$J = nW \circ W^{-T} = -\frac{n}{\gamma}(\beta W \circ I - W \circ W^T),$$

from which we find that

$$W \circ W^T = \beta W \circ I + \frac{\gamma}{n}J. \tag{6.4.1}$$

It follows that all off-diagonal entries of $W$ have the same absolute value (namely $\sqrt{\gamma/n}$). $\square$

## 6.5 Strongly Regular Graphs

A graph $X$ is strongly regular if it is not complete and there are integers $k$, $a$ and $c$ such that the number of common neighbours of an ordered pair of vertices $(u,v)$ is $k$, $a$ or $c$ according as $u$ and $v$ are equal, adjacent or distinct and not adjacent. Trivial examples are provided by the graphs $mK_n$ and their complements. The Petersen graph provides a less trivial example. A strongly regular graph $X$ is *primitive* if both $X$ and its complement are connected; an imprimitive strongly regular graph is isomorphic to $mK_n$ or its complement. A strongly regular graph $X$ gives rise to an association scheme with two classes, corresponding to $X$ and its complement. Conversely each association scheme with two classes determines a complementary pair of strongly regular graphs.

**6.5.1 Theorem.** *Let $X$ be a primitive strongly regular graph with $v$ vertices, valency $k$, and eigenvalues $k$, $\theta$ and $\tau$, where $\theta > \tau$. Let $A_1$ be the adjacency matrix of $X$ and $A_2$ the adjacency matrix of its complement. Suppose*

$$W := I + xA_1 + yA_2.$$

*Then $W$ is a type-II matrix if and only if one of the following holds*

*(a)* $y = x = \frac{1}{2}(2 - v \pm \sqrt{v^2 - 4v})$.

*(b)* $x = 1$ *and* $y = 1 + \frac{1}{2(\bar{k}-\lambda)}(-v \pm \sqrt{v^2 - 4(\bar{k}-\lambda)v})$ *and $A_2$ is the incidence matrix of a symmetric $(v, \bar{k}, \lambda)$-design where $\bar{k} = v - k - 1$.*

*(c)* $x = -1$ *and* $y = \frac{1}{2}(\lambda \pm \sqrt{\lambda^2 - 4})$ *(where $\lambda = (1+\theta\tau)^{-1}(2 - 2\theta\tau - v)$), and $A_1$ is the incidence matrix of a symmetric design.*

*(d)* $x + x^{-1}$ *is a zero of the quadratic $z^2 - \alpha z + \beta - 2$ with*

$$\alpha = \frac{1}{\theta\tau}[v(\theta+\tau+1) + (\theta+\tau)^2],$$
$$\beta = \frac{1}{\theta\tau}[-v - v(1+\theta+\tau)^2 + 2\theta^2 + 2\theta\tau + 2\tau^2]$$

*and*

$$y = \frac{1}{(x - x^{-1})}\left(\frac{\theta\tau x - 1}{(\theta+1)(\tau+1)}(x + x^{-1} - 2 + v) - (v-2)x - 2\right).$$

*Proof.* We use $\ell$ to denote valency $v - 1 - k$ of the complement of $X$. Then the eigenvalues of $A_2$ are $v - 1 - k$, $-1 - \tau$ and $-1 - \theta$ and the equation $WW^{(-)T} = vI$ is equivalent to

$$(1 + kx + \ell y)(1 + kx^{-1} + \ell y^{-1}) = v,$$
$$(1 + \theta x + (-\theta - 1)y)(1 + \theta x^{-1} + (-\theta - 1)y^{-1}) = v,$$
$$(1 + \tau x + (-\tau - 1)y)(1 + \tau x^{-1} + (-\tau - 1)y^{-1}) = v.$$

Note that this set of equations is invariant under the substitutions

$$x \mapsto x^{-1}, \quad y \mapsto y^{-1}$$

and also under the substitutions

$$x \mapsto y, \quad y \mapsto x, \quad \theta \mapsto -\theta - 1, \quad \tau \mapsto -\tau - 1.$$

The missing details in the following calculations were performed in Maple.

If we set

$$X := x + \frac{1}{x}, \quad Y := y + \frac{1}{y}, \quad Z := \frac{x}{y} + \frac{y}{x}$$

then, from our three equations we get

$$k\ell Z + kX + \ell Y = v - 1 - k^2 - \ell^2,$$

$$-\theta(\theta+1)Z + \theta X - (\theta+1)Y = v - 1 - \theta^2 - (\theta+1)^2, \tag{6.5.1}$$

$$-\tau(\tau+1)Z + \tau X - (\tau+1)Y = v - 1 - \tau^2 - (\tau+1)^2. \tag{6.5.2}$$

These three equations are linearly dependent: if $\theta$ has multiplicity $m$ and $\tau$ has multiplicity $n$ as an eigenvalue of $A_1$, then the first equation plus $m$ times the second plus $n$ times the third is zero. In fact, our three equations are equivalent to the following pair.

$$Y - 2 + v = \frac{\theta\tau}{(\theta+1)(\tau+1)}(X - 2 + v), \tag{6.5.3}$$

$$Z - 2 = \frac{1}{(\theta+1)(\tau+1)}(X - 2 + v). \tag{6.5.4}$$

Given the definitions of $Y$ and $Z$, we can view this as a pair of linear equations in $y$ and $y^{-1}$, whence we find that

$$y(x - x^{-1}) = \frac{\theta\tau x - 1}{(\theta+1)(\tau+1)}(x + x^{-1} - 2 + v) - (v-2)x - 2.$$

Assume $x^2 \neq 1$. If we define

$$p(x) := \tau\theta x^3 + (1 - v + 2\theta + 2\tau - \theta v - \tau v)x^2 - (2\theta + \tau\theta + 2\tau + v)x - 1,$$

then (6.5.3) and (6.5.4) hold if and only if

$$y = \frac{p(x)}{(\theta+1)(\tau+1)(x^2-1)}, \qquad y^{-1} = \frac{-x^2 p(x^{-1})}{(\theta+1)(\tau+1)(x^2-1)}.$$

Then the previous expressions for $y$ and $y^{-1}$ hold if and only if

$$-x^2 p(x) p(x^{-1}) = [(\theta+1)(\tau+1)(x^2-1)]^2.$$

We deduce that $x$ must be a root of the polynomial

$$(x^2 + (v-2)x + 1)(x^4 - \alpha x^3 + \beta x^2 - \alpha x + 1) \tag{6.5.5}$$

where

$$\alpha = \frac{1}{\theta\tau}[v(\theta+\tau+1)+(\theta+\tau)^2],$$
$$\beta = \frac{1}{\theta\tau}[-v-v(1+\theta+\tau)^2+2\theta^2+2\theta\tau+2\tau^2].$$

If $x$ is a root of the quadratic factor in (6.5.5), then $X-2+v=0$ and so Equations (6.5.3) and (6.5.4) imply that $Y=2-v$ and $Z=2$. Since

$$Z-2=\frac{(x-y)^2}{xy},$$

it follows that

$$y=x=\frac{1}{2}(2-v\pm\sqrt{v^2-4v}).$$

This is the Potts model solution.

We turn to the quartic factor in (6.5.5), which is equal to

$$x^2\left(\left(x+x^{-1}\right)^2-\alpha\left(x+x^{-1}\right)+\beta-2\right).$$

From this we see that $X$ must be a zero of the quadratic

$$z^2-\alpha z+\beta-2 \tag{6.5.6}$$

and thus (d) holds.

To complete the proof we consider the cases where $x^2=1$. If $x=1$ then Table **??** yields that $A_2$ is the incidence matrix of a symmetric design. So we assume $x=-1$.

Equations (6.5.3) and (6.5.4) imply that

$$Y-2+v=\theta\tau(Z-2).$$

Since $Z=-Y$ if $x=-1$, we find that

$$(1+\theta\tau)Y=2-2\theta\tau-v$$

whence

$$y=\frac{1}{2}(\lambda\pm\sqrt{\lambda^2-4}),$$

where

$$\lambda=\frac{2-2\theta\tau-v}{1+\theta\tau}.$$

(The denominator cannot be zero because $\tau\le-2$ and $\theta\ge1$ for any primitive strongly regular graph.)

If $x=-1$ then $Z=-Y$ and $X=-2$; if we add equations (6.5.3) and (6.5.4) we get

$$v-4=\frac{(\theta\tau+1)(v-4)}{(\theta+1)(\tau+1)}.$$

whence we find that $v-4$ or $\theta+\tau=0$. Since, for any strongly regular graph,

$$A^2-(\theta+\tau)A+\theta\tau I=(k+\theta\tau)J,$$

we see that if $\theta+\tau=0$, then $A^2=-\theta\tau I+(k+\theta\tau)J$. Therefore $A$ is the incidence matrix of a symmetric design (with zero diagonal and symmetric incidence matrix). □

Jaeger [**?**] showed that if $W$ is a spin model then $X$ is formally self-dual. If $X$ is formally self-dual then $v = (\theta - \tau)^2$ and the quadratic (6.5.6) becomes

$$\left(z - \frac{\tau^2 - \theta^2 + 2\tau}{\theta}\right)\left(z - \frac{\theta^2 - \tau^2 + 2\theta}{\tau}\right).$$

In addition to the Potts model solutions, Equations (6.5.3) and (6.5.4) give

$$\begin{aligned} x &= \frac{1}{2\tau}\left(\theta^2 - \tau^2 + 2\theta \pm \sqrt{(\theta-\tau)(\theta-\tau+2)(\theta+\tau)(\theta+\tau+2)}\right) \quad \text{and} \\ y &= \frac{1}{2(\theta+1)}\left(\theta^2 - \tau^2 + 2(\theta+1) \pm \sqrt{(\theta-\tau)(\theta-\tau+2)(\theta+\tau)(\theta+\tau+2)}\right), \end{aligned}$$

or

$$\begin{aligned} x &= \frac{1}{2\theta}\left(\tau^2 - \theta^2 + 2\tau \pm \sqrt{(\theta-\tau)(\theta-\tau-2)(\theta+\tau)(\theta+\tau+2)}\right) \quad \text{and} \\ y &= \frac{1}{2(\tau+1)}\left(\tau^2 - \theta^2 + 2(\tau+1) \pm \sqrt{(\theta-\tau)(\theta-\tau-2)(\theta+\tau)(\theta+\tau+2)}\right). \end{aligned}$$

Hence there are at most six type-II matrices, up to equivalence, in the Bose-Mesner algebra of a formally self-dual strongly regular graph.

We now determine what happens to the imprimitive strongly regular graphs, which will arise in the next section.

**6.5.2 Theorem.** *Let $A_1$ be the adjacency matrix of $mK_{k+1}$ and $A_2$ the adjacency matrix of its complement. Suppose*

$$W := I + xA_1 + yA_2.$$

*Then $W$ is a type-II matrix if and only if one of the following holds*

*(a) $W$ is equivalent to the Potts model,*

*(b)*

$$x = \frac{(kv - 2k - 1)y^2 - (v - 2k - 2)y - 1}{k(1 - y^2)}$$

*and*

$$y + y^{-1} = \frac{2(k+1)^2 - v(k^2+1)}{(k+1)^2 - kv}$$

*where $v = m(k+1)$.*

*Proof.* The eigenvalues of $A_1$ are $k$ and $-1$, so $\theta = k$ and $\tau = -1$. The equation $WW^{(-)T} = vI$ are equivalent to Equations (6.5.1) and (6.5.2):

$$\begin{aligned} -k(k+1)Z + kX - (k+1)Y &= v - 1 - k^2 - (k+1)^2 \\ X &= -v + 2. \end{aligned}$$

Solving this as a pair of linear equations in $x$ and $x^{-1}$ gives

$$k(1 - y^2)x = (kv - 2k - 1)y^2 - (v - 2k - 2)y - 1.$$

Assume $y^2 \neq 1$. Then Equations (6.5.1) and (6.5.2) are equivalent to

$$x = \frac{p(y)}{k(1-y^2)}$$

and

$$x^{-1} = \frac{-y^2 p(y^{-1})}{k(1-y^2)}$$

where

$$p(y) = (kv - 2k - 1)y^2 - (v - 2k - 2)y - 1.$$

Now these expressions for $x$ and $x^{-1}$ hold if and only if

$$-y^2 p(y^{-1})p(y) = k^2(1-y^2)^2.$$

We deduce that $y$ must be a root of the quartic

$$\left(y^2 + (v-2)y + 1\right)\left(y^2 - \beta y + 1\right)$$

where

$$\beta = \frac{2(k+1)^2 - v(k^2+1)}{(k+1)^2 - kv}.$$

If $y$ is a root of $y^2 + (v-2)y + 1$ then we deduce from Equation (6.5) that $x = y$ and $W$ is the Potts model.

If $y = 1$ then $Y = 2$, $Z = X$ and Equation (6.5.1) becomes $X = \frac{-v}{k^2} + 2$. Equations (6.5.1) and (6.5.2) imply $k = 1$. In this case, $A_1$ is a permutation matrix and $W = J + (x-1)A_1$ is equivalent to the Potts model.

If $y = -1$ then $Y = -2$, $Z = -X$ and Equation (6.5.1) becomes

$$X = \frac{v - 2k^2 - 4k - 4}{k^2 + 2k}.$$

Equations (6.5.1) and (6.5.2) imply

$$2 - v = \frac{v - 2k^2 - 4k - 4}{k^2 + 2k},$$

which leads to $v = 4$ and $x = -1$. In this case, $-W = J - 2I$ is the Potts model. □

## 6.6 Covers of Complete Graphs

Now we know that the Bose-Mesner of algebra of an association scheme with two classes contains type-II matrices different from the Potts models. Given this, it is natural to ask what happens in schemes with more than two classes; in this section we consider the next simplest case. We will see that non-trivial type-II matrices do arise, and that the amount of effort required to establish this increases considerably.

We say a graph of diameter $d$ is *antipodal* if whenever $u$, $v$ and $w$ are vertices and

$$\mathrm{dist}(u,v) = \mathrm{dist}(v,w) = d,$$

then $u = w$ or $\mathrm{dist}(u,w) = d$. If $X$ is antipodal, then the relation "at distance 0 or $d$" is an equivalence relation. The cube and the line graph of the Petersen graph provide two examples with $d = 3$. If $X$ is antipodal with $d = 2$, then it is the complement of a collection of complete graphs. If $X$ is an antipodal graph with diameter $d$, then its 'antipodal classes' form the vertices of a distance-regular graph with the same valency and diameter $\lfloor \frac{d}{2} \rfloor$.

Here we are interested in distance-regular antipodal graphs with diameter three. To each such graph there is a set of four parameters $(n, r, a_1, c_2)$. The integer $n$ is the number of antipodal classes, and $r$ is the number of vertices in each class. If $(u,v)$ is a pair of vertices from $X$ and $\mathrm{dist}(u,v) = 1$ then $u$ and $v$ have exactly $a_1$ common neighbours; if $\mathrm{dist}(u,v) = 2$ they have exactly $c_2$ common neighbours. The value of $a_1$ is determined by $n$, $r$ and $c_2$, so it is conventional to provide only the triple $(n, r, c_2)$.

**6.6.1 Theorem.** *Suppose $X$ is an antipodal distance regular graph of diameter three with parameters $(n, r, c_2)$ and let $A_i$ be the $i$-th distance matrix of $X$, for $i = 1, 2, 3$. Then the matrix*

$$W = I + xA_1 + yA_2 + zA_3$$

*is type-II if and only if*

*(a) $x = y$ and $W$ is a type-II matrix in the Bose-Mesner algebra of $rK_n$.*

*(b) $y = -x^{-1}$ and $x$ is a solution of a quadratic equation.*

*(c) $y \neq -x^{-1}$ and the possible values of $(x, y)$ are the points of intersection of two quartics in $x$ and $y$.*

*Proof.* We use $\theta$ and $\tau$ to denote eigenvalues of $X$ not equal to $-1$ or $n-1$. Now $W$ is a type-II matrix if and only if the following system of equations are satisfied:

$$(1 - x - (r-1)y + (r-1)z)\left(1 - \frac{1}{x} - \frac{(r-1)}{y} + \frac{(r-1)}{z}\right) = nr, \tag{6.6.1}$$

$$(1 + \theta x - \theta y - z)(1 + \theta x^{-1} - \theta y^{-1} - z^{-1}) = nr, \tag{6.6.2}$$

$$(1 + \tau x - \tau y - z)(1 + \tau x^{-1} - \tau y^{-1} - z^{-1}) = nr. \tag{6.6.3}$$

Subtracting (6.6.3) from (6.6.2) gives

$$(x-y)z^{-1} + (x^{-1} - y^{-1})z = (x-y) + (x^{-1} - y^{-1}) + (\theta + \tau)(x-y)(x^{-1} - y^{-1}). \tag{6.6.4}$$

Adding $\theta$ times this to (6.6.2) yields

$$z^{-1} + z = -\theta\tau(x-y)(x^{-1} - y^{-1}) + 2 - nr. \tag{6.6.5}$$

Solving (6.6.4) and (6.6.5) as two linear equations in $z$ and $z^{-1}$, we get

$$(x-y)\left((1+xy)z - \theta\tau(x-y)^2 - (\theta+\tau)(x-y) + (nr-1)xy - 1\right) = 0. \tag{6.6.6}$$

There are three cases. First if $x = y$ we are lead to type-II matrices contained in the Bose-Mesner algebra of $rK_n$ (including the Potts models). Second, if $xy = -1$ then (6.6.6) yields a quadratic in $X := x + x^{-1}$:

$$-\theta\tau X^2 - (\theta+\tau)X - nr = 0 \tag{6.6.7}$$

and (6.6.5) gives

$$\begin{aligned} z^{-1} + z &= -\theta\tau X^2 - nr + 2 \\ &= (\theta+\tau)X + 2. \end{aligned} \tag{6.6.8}$$

Solving (6.6.1) and (6.6.8) as two linear equations in $z$ and $z^{-1}$ gives

$$z = \frac{p(x)}{rx(x+1)(x-1)(r-1)}$$

and

$$z^{-1} = \frac{-x^4 p(x^{-1})}{rx(x+1)(x-1)(r-1)}$$

where

$$\begin{aligned} p(x) = {} & (r-1)(\theta+\tau+1)x^4 + (\theta+\tau+r-r\theta-r\tau)x^3 + \\ & (3r\theta - r^2\tau - r^2\theta + 3r - r\theta\tau + 3r\tau - 2 - 2\theta - 2\tau - 2r^2)x^2 + \\ & (-r\theta - r\tau + 3r + \theta + \tau - 2r^2)x - (r-1)(r\theta + r\tau - 1 - \tau - \theta). \end{aligned}$$

Now these expressions for $z$ and $z^{-1}$ hold if and only if

$$-x^4 p(x^{-1})p(x) = [rx(x+1)(x-1)(r-1)]^2$$

which gives a quartic in $X$. Applying (6.6.7) to this quartic, we can express $X = x + x^{-1}$ in $r$, $\theta$, and $\tau$. Hence $x$ is a solution of a quadratic equation.

Finally if $x \neq y$ or $-y^{-1}$, Equations (6.6.4) and (6.6.5) are equivalent to

$$z = \frac{1}{(1+xy)}\left(\theta\tau(x-y)^2 + (\theta+\tau)(x-y) - (nr-1)xy + 1\right),$$

and

$$z^{-1} = \frac{1}{xy(1+xy)}\left(\theta\tau(x-y)^2 - (\theta+\tau)(x-y)xy - (nr-1)xy + x^2y^2\right).$$

Now substituting these two expressions into (6.6.1) gives a quartic in variables $x$ and $y$ while $zz^{-1} = 1$ gives another one. □

Note that $rK_n$ is a strongly regular graph, so the possible type-II matrices are determined by the results of the previous section.

Calculations performed in Maple showed that the resultant with respect to $x$ of the two quartics in case (c) is a non-zero polynomial in $y$ of degree at most 30. By the elimination property of resultants [**?**], the resultant vanishes at any common

solution of the two quartics. Hence these two quartics vanish at no more than thirty values for $y$. Similarly, the resultant with respect to $y$ of these two quartics is a non-zero polynomial in $x$ of degree at most 30 and they vanish at no more than thirty values for $x$. Consequently there are finitely many type-II matrices, up to scalar multiplication, in the Bose-Mesner algebra of an antipodal distance regular graph of diameter three.

As a final remark, it could be true that each Bose-Mesner algebra is equal to the set of all polynomials in some type-II matrix. The results of the last two sections imply this is true for schemes with at most two classes, and for antipodal schemes with three classes. (Since we do not have strong evidence either way, we will not make any conjecture.)

# Chapter 7

# Quantum Latin Squares, Quantum Automorphisms

## 7.1 Quantum Latin Squares from Flat Unitaries

We can use flat unitary matrices to construct quantum Latin squares, as we now describe. Suppose $H$ is flat and $n \times n$ and $H^*H = I$. If $M$ is a matrix, let $\partial_i(M)$ denote the diagonal matrix such that

$$(\partial_i(M))_{r,r} = (Me_i)_r.$$

Note that if $H$ is flat and unitary, then $\sqrt{n}\partial_i(H)$ is unitary.

As customary, $M \circ N$ denotes the Schur product of the matrices $M$ and $N$ (except, unfortunately, in Musto and Vicary [**?**], where it denotes the usual matrix multiplication).

**7.1.1 Theorem.** *If $H$ is a flat unitary of order $n \times n$, the matrices $\sqrt{n}H\partial_i(H)H^*$ (for $i = 1, \ldots, n$) define a quantum latin square.*

*Proof.* Set $D_i = \sqrt{n}\partial_i(H)$ and define matrices

$$R_i = H^* D_i H, \quad (1, \ldots, d).$$

We observe that these matrices are unitary (because they are products of unitary matrices).

We need to show that, if $i \neq j$, then $R_i^* R_j$ is a derangement. We have

$$R_i^* R_j = H^* \overline{D_i} H H^* D_j H = H^* \overline{D_i} D_j H$$

and so

$$(R_i^* R_j)_{k,k} = e_k^T H^* \overline{D_i} D_j H e_k = \langle He_i \circ He_k, He_j \circ He_k \rangle.$$

Since $H$ is flat,

$$\langle He_i \circ He_k, He_j \circ He_k \rangle = \langle He_i, He_j \rangle$$

and we're done. □

## 7.2 Unitary Error Bases

A *unitary error basis* is a set of $n^2$ matrices from $U(n)$, such that each pair of elements is trace-orthogonal. The canonical example is the set of four Pauli matrices with $n = 2$. Unitary error bases provide a useful tool in quantum computing. For the first part, our discussion follows Klappenecker and Rötteler [**?**] and we refer you to this for more information—we will focus on constructions.

The example provided by the Pauli matrices can be generalized, using the Weyl-Heisenberg group. To define this, let $\theta$ be a primitive complex $d$th root of 1. Let $Z$ be the diagonal matrix with $(Z)_{r,r} = \theta^{r-1}$ for $r = 1, \ldots, d$, and let $X$ be the $d \times d$ permutation matrix such $Xe_r = e_{r-1}$ (with the subscripts evaluated mod $d$). Let $\mathscr{E}$ denote the set of $d^2$ matrices $X^i Z^j$ for $0 \leq i, j \leq d-1$. To see that $\mathscr{E}$ is a unitary error basis, first note that $\mathrm{tr}(X^i)$ and $\mathrm{tr}(Z^i)$ are both zero unless $i = 0$ and, since $Z$ is diagonal, $\mathrm{tr}(X^i Z^j) = 0$ unless $i = j = 0$. Now note that $XZ = \theta ZX$, and from this it is easy to verify that we have unitary error basis.

There is a second construction, producing *shift-and-multiply bases*. Let $L$ be a Latin square of order $d \times d$, and let $H_1, \ldots, H_d$ be a sequence of flat unitary matrices. Each row of $L$ corresponds to a permutation matrix $Q_i$; define permutation matrices $P_i$ by $P_i = Q_1^{-1} Q_i$. Then $P_1 = I$ and if $i \neq j$, then $P_i^{-1} P_j$ is a derangement. (In particular $P_2, \ldots, P_d$ are derangements.)

Now let $\mathscr{E}$ denote the set of matrices $\sqrt{d} P_i \partial_j(H)$ with $1 \leq i, j \leq d$. Then $\mathscr{E}$ is a unitary error basis.

## 7.3 Magic Unitary Matrices

Let $V$ be a fixed vector space. A *magic unitary* is a square matrix whose entries are projections on $V$, such that the projections in each row and each column sum to $I$. For us, $\dim(V)$ will be finite, and under this assumption it follows that the projections in a row or column will be pairwise orthogonal. If $\dim(V) = d$, it will often be convenient to view an $n \times n$ magic unitary as a block matrix of order $nd \times nd$. We will not distinguish notationally between the magic unitary and the block matrix.

As one example, if $\mathscr{L}$ is a quantum Latin square then we obtain a magic unitary by replacing each unit vector $x$ with the projection $xx^*$. (In fact the array of vectors is a quantum Latin square if and only if this construction produces a magic unitary.) We also see that if $\dim(V) = 1$, then a magic unitary is just a permutation matrix.

**7.3.1 Lemma.** *Suppose $P$ is an $n \times n$ magic unitary with entries projections on $V$ and assume $\dim(V) = d$. Then the $nd \times nd$ matrix associated with $P$ is unitary.*

*Proof.* Easy exercise. □

Following Roberson et al [**?**], we define two graphs $X$ and $Y$ on $n$ vertices to be *quantum isomorphic* if there is a magic unitary $P$ of order $n \times n$, with entries projections of order $d \times d$, such that

$$(A(X) \otimes I_d)P = P(A(Y) \otimes I_d).$$

If $X = Y$, we have a *quantum automorphism* of $X$. Since $P$ is unitary, the matrices $A(X) \times I$ and $A(Y) \times I$ are similar, and so we see that quantum isomorphic graphs are cospectral. We'll see that more is true, but there are graphs that are quantum isomorphic but not isomorphic. (See [**?**].)

**7.3.2 Lemma.** *If $P$ is a magic unitary, it commutes with $J \otimes I_d$.*

This result is easy to prove, and is left to the reader. One consequence of it is that quantum isomorphic graphs are cospectral with cospectral complements.

**7.3.3 Lemma.** *If $P$ is a magic unitary that commutes with $M \otimes I$ and $N \otimes I$, it commutes with $(M \circ N) \otimes I$.*

*Proof.* The $ij$-block of $(M \otimes I)P$ is

$$\sum_r M_{i,r} P_{r,j}$$

and, by hypothesis, this is equal to the $ij$-block of $P(M \otimes I)$:

$$\sum_s M_{s,j} P_{i,s}.$$

We have

$$\sum_r M_{i,r} P_{r,j} \sum_s N_{i,s} P_{s,j} = \sum_r (M_{i,r} N_{i,r}) P_{r,j}$$

where the right side is the $ij$-block of $((M \circ N) \otimes I)P$. Similarly

$$\sum_r M_{r,j} P_{i,r} \sum_r N_{r,j} P_{i,r} = \sum_r (M_{r,j} N_{r,j}) P_{i,r}$$

where the right side is the $ij$-block of $P((M \circ N) \otimes I)$. Since the left sides of the previous pair of equations are equal, our result follows. □

From this lemma it follows that if $X$ and $Y$ are quantum isomorphic, the coherent algebras generated by $A(X)$ and $A(Y)$ are isomorphic. But for this comment to be useful we will need to define coherent algebras, and isomorphisms thereof. (And it's the second part that needs care.)

## 7.4 Coherent Algebras

A *coherent algebra* is a matrix algebra that is *-closed, contains $J$, and is closed under Schur multiplication. (If it's commutative, it's an association scheme.)

**7.4.1 Lemma.** *The commutant of a set of permutation matrices is a coherent algebra.*

*Proof.* Note that if $P$ is a permutation matrix, then

$$P(A \circ B) = (PA) \circ (PB)$$

and it follows that if $A$ and $B$ commute with $P$, so does $A \circ B$. □

The full matrix algebra is Schur-closed and so if $\mathscr{A}$ is a *-closed matrix algebra, the intersection of the *-closed and Schur-closed subalgebras that contain $\mathscr{A}$ is the unique minimal coherent algebra that contains $\mathscr{A}$. It is the coherent algebra generated by $\mathscr{A}$. If $A$ is the adjacency matrix of a graph, the coherent algebra of $X$ is the coherent algebra generated by $A$ or, more precisely, by the algebra of polynomials in $A$. Any permutation matrix that commutes with $A$ must commute with each element of this coherent algebra, and so it should not be surprising that coherent algebras are a useful tool in the theory of graph isomorphism.

**7.4.2 Lemma.** *A coherent algebra has a unique basis that is *-closed and consists of Schur-orthogonal* 01*-matrices.* □

The sum of the elements in this basis is $J$, and the identity matrix will be the sum of elements of the basis that are diagonal. The coherent algebra is *homogeneous* if $I$ is an element of the basis. The commutant of a permutation group is a coherent algebra; it is homogeneous if and only if the group is transitive. A commutative coherent algebra is necessarily homogeneous.

The above lemma implies that coherent algebras can be viewed as arising from special partitions of the arc set of a complete directed graph.

## 7.5 Isomorphism of Coherent Algebras

We discuss isomorphism now. In a sense there is no issue: once we agree on what maps we allow between coherent algebras, an isomorphism is an invertible map. The problem is that even when we consider just matrix algebras, we have three choices.

Clearly maps should be linear and a general linear map $\Phi$ will have the form

$$\Phi(M) = \sum_r A_r M B_r^*$$

for suitable matrices $A_r$ and $B_r$. We want $\Phi(I) = I$, which imposes the condition $\sum_r A_r B_r^* = I$. Of course we also want

$$\Phi(MN) = \Phi(M)\Phi(N)$$

for all $M$ and $N$. These constraints give us what we will call algebra homomorphisms.

The second alternative is to restrict ourselves to maps of the form

$$\Phi(M) = A^{-1} M A$$

Let us temporarily call these *conjugacies*.

The third alternative is to specialize our conjugacies to the cases where the invertible matrices $A$ are permutations.

The Noether-Skolem theorem states that any automorphism of a full matrix algebra over a field is a conjugacy. Wedderburn's theorem says that any semisimple

matrix algebra is conjugate to a direct sum of matrix algebras. Together these results imply that isomorphic coherent algebras similar, i.e., the isomorphism is conjugacy.

Finally note that a coherent algebra can be viewed as a matrix algebra with a distinguished basis—thus we are working with pairs (algebra,basis). If we are given an ordered basis $\beta_1, \ldots, \beta_m$, we can define a multiplication by setting

$$\beta_i * \beta_j = \delta_{i,j}\beta_i$$

and then extending $*$ by linearity. We take our maps to linear maps that take ordered bases to ordered bases.

## 7.6 Type-II Matrices

We denote the Schur inverse, if it exists, of the matrix $W$ by $W^{(-)}$. A complex $n \times n$ matrix $W$ is a *type-II matrix* if

$$WW^{(-1)T} = nI.$$

For any complex number $t$, the matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & t & -t \\ 1 & -1 & -t & t \end{pmatrix}$$

is type II. Real Hadamard matrices provide further examples. A unitary matrix is a type-II matrix if and only if it is flat. The Kronecker product of two type-II matrices is a type-II matrix.

If $W$ is an $m \times n$ Schur-invertible matrix, we define $n^2$ vectors $Y_{i,j}(W)$ (for $0 \le i, j \le n$) by

$$W_{i/j} = We_i \circ W^{(-)}e_j.$$

The *Nomura algebra* $\mathcal{N}_W$ of $W$ is the set of $n \times n$ complex matrices for each each of the $n^2$ vectors $W_{i/j}$ is an eigenvector. This is a matrix algebra.

**7.6.1 Lemma.** *The matrix $W$ is type-II if and only if $J \in \mathcal{N}_W$.* □

If $W$ is type-II, it is invertible and therefore for fixed $j$, the vectors

$$W_{i/j} = \partial_j(W)^{-1}We_i$$

are linearly independent. If $M \in \mathcal{N}_W$, we define $\Theta_W(M)$ to be the $n \times n$ matrix such that

$$MW_{i/j} = (\Theta_W(M)_{i,j})W_{i/j}.$$

The map $\Theta_W$ is linear on $\mathcal{N}_W$ and injective. We also have

$$\Theta_W(MN) = \Theta_W(M) \circ \Theta_W(N).$$

## 7.7 Duality for Nomura Algebras

Type-II Matrices and Magic Unitaries

Let $W$ be a type-II matrix of order $n \times n$. Define matrices $\mathscr{F}_{i,j} = \mathscr{F}_{i,j}(W)$ by

$$\mathscr{F}_{i,j} = \frac{1}{n} W_{i/j}(W_{j/i})^T = \frac{1}{n} \partial_i(W)(We_j)^{(-1)}(We_j)^T \partial_i(W)^{-1}.$$

We note that $\mathscr{F}_{i,i} = \frac{1}{n}J$ and

$$\mathscr{F}_{i,j}^T = \mathscr{F}_{j,i},$$

Further

$$\mathscr{F}_{i,j}^{(-)} = nW_{j/i}(W_{i/j})^T = n^2 \mathscr{F}_{j,i}.$$

If $W$ is flat, then $F_{i,j}$ is Hermitian.

If $W$ is a type-II matrix, the columns of $W^{(-)}$ form a dual basis to the set of columns of $W$. It follows that the matrices $F_{i,j}$ are idempotents and that

$$\sum_i F_{i,j} = I = \sum_j F_{i,j}.$$

Now we can prove a very important result due to Nomura:

**7.7.1 Theorem.** *If $M \in \mathscr{N}_W$, then $\Theta_{W^T}(\Theta_W(M)) = nM^T$.*

*Proof.* Assume $M \in \mathscr{N}_W$. Then $M\mathscr{F}_{i,j} = \Theta(M)_{i,j}\mathscr{F}_{i,j}$ and, summing this over $j$ yields

$$M = \sum_j \Theta(M)_{i,j}\mathscr{F}_{i,j}.$$

Therefore

$$M_{r,s} = \frac{1}{n}\sum_j \Theta_W(M)_{i,j}\frac{W_{r,i}}{W_{r,j}}\frac{W_{s,j}}{W_{s,i}} = \frac{1}{n}\frac{W_{r,i}}{W_{s,i}}\sum_j \Theta_W(M)_{i,j}\frac{W_{s,j}}{W_{r,j}}.$$

If follows that

$$nM_{r,s}(W^T)_{s/r} = \Theta_W(M)(W^T)_{s/r}.$$

and this yields our result. □

This theorem tells us many things. First, we see that $\Theta_W$ and $\Theta_{W^T}$ are invertible and that $\mathscr{N}_W$ is closed under transposes. Since $\mathrm{im}(\Theta_{W^T})$ is Schur-closed, we also see that $\mathscr{N}_W$ is Schur-closed. As $\mathscr{N}_W$ is Schur-closed, it has a basis of 01-matrices and, consequently, $\mathscr{N}_W$ is closed under complex conjugation. To sum up, $\mathscr{N}_W$ is the Bose-Mesner algebra of an association scheme, and $\mathscr{N}_{W^T}$ is the Bose-Mesner algebra which we can view as dual to $\mathscr{N}_W$.

## 7.8 Type-II Matrices and Magic Unitaries

Let $\mathscr{F}_W$ be the $n^2 \times n^2$ block matrix with $ij$-block equal to $\mathscr{F}_{i,j}$; we call it the *matrix of idempotents* of $W$. Since $\mathscr{F}_{i,j}^T = \mathscr{F}_{j,i}$, we see that $\mathscr{F}$ is symmetric.

If $\mathscr{F}^\tau$ is the matrix we get by applying the transpose map to each block of $\mathscr{F}$, i.e., the partial transpose. Then

$$\mathscr{F}^\tau = \frac{1}{n}\mathscr{F}^{(-)}.$$

Let $S$ be the operator on $\mathbb{C}^n \otimes \mathbb{C}^n$ that sends $u \otimes v$ to $v \otimes u$ (for all $u$ and $v$).

**7.8.1 Lemma.** *If $W$ is type-II, then $\mathscr{F}_{W^T} = S\mathscr{F}_W S$.*

*Proof.* We have

$$n(\mathscr{F}_{i,j}(W))_{r,s} = \frac{W_{r,i}}{W_{r,j}}\frac{W_{s,j}}{W_{s,i}} = \frac{W_{r,i}}{W_{s,i}}\frac{W_{s,j}}{W_{r,j}} = \frac{W_{i,r}^T}{W_{i,s}^T}\frac{W_{j,s}^T}{W_{j,r}^T} = n(\mathscr{F}_{r,s}(W^T))_{i,j}.$$

Here the left hand and right hand terms are equal respectively to

$$(e_i \otimes e_r)^T \mathscr{F}(W)(e_j \otimes e_s), \qquad (e_r \otimes e_i)^T \mathscr{F}(W^T)(e_s \otimes e_j)$$

and the result follows. □

**7.8.2 Theorem.** *If $W$ is a type-II matrix, then $\mathscr{F}$ is type-II. If in addition $W$ is flat, then $\mathscr{F}$ is flat and is a magic unitary matrix.*

*Proof.* For fixed $i$, the vectors $We_j$ form a basis of $\mathbb{C}^n$ and the vectors $n^{-1}(We_j)^{(-)}$ form a basis dual to this. Hence the matrices

$$\frac{1}{n}(We_j)^{(-1)}(We_j)^T$$

are pairwise orthogonal idempotents and sum to $I$. Therefore for fixed $i$ the matrices $F_{i,j}$ are pairwise orthogonal idempotents that sum to $I$.

Since $\mathscr{F}^T = \mathscr{F}$, it also follows that each column of $\mathscr{F}_W$ consists of pairwise orthogonal idempotents that sum to $I$. If $W$ is flat, then $F_{i,j}$ is Hermitian. □

**7.8.3 Theorem.** *Let $W$ be a type-II matrix and let $\mathscr{F}_W$ be the associated matrix of idempotents. The set of matrices $M$ such that $[I \otimes M, \mathscr{F}_W] = 0$ is equal to $\mathscr{N}_W$. The matrices $N$ such that $[N \otimes I, \mathscr{F}_W] = 0$ is equal to $\mathscr{N}_{W^T}$.*

*Proof.* We have that $[I \otimes M, \mathscr{F}] = 0$ if and only if $[M, \mathscr{F}_{i,j}] = 0$ for all $i$ and $j$. Now $M$ commutes with a rank-1 matrix $uv^*$ if and only if $u$ is a right eigenvector for $M$. Hence $[M, \mathscr{F}_{i,j}] = 0$ for fixed $i$ and all $j$ if and only if $M \in \mathscr{N}_W$.

For the second claim,

$$S((N \otimes I)\mathscr{F}_W)S = (I \otimes N)\mathscr{F}_{W^T},$$

from which the assertion follows. □

One consequence of this result is that $\mathscr{N}_W$ is the commutant of the set of matrices

$$\{F_{i,j} : j = 1, \ldots, n\}.$$

Questions and remarks:

- We might hope that the commutant of $\mathscr{F}_W$ is $\mathscr{N}_{W^T} \otimes \mathscr{N}_W$. Can we at least show that this commutant is commutative? Is

$$\mathscr{F}_W = S(W \otimes W^{(-)T})?$$

- Survey magic unitaries. Examples which do not come from type-II matrices? (There are many.) Can we characterize the magic unitaries of the form $\mathscr{F}_W$ (where $W$ is type-II)? Note that the diagonal blocks of $\mathscr{F}_W$ are equal to $J$.
- Relation between $\mathscr{F}_W$ and $\mathscr{F}_{W^T}$? What does $\Theta$ do?
- If $W$ is a (real) Hadamard matrix, then $\mathscr{F}_W$ is a Bush-type Hadamard.
- If $F_{i,j} \in \mathscr{N}_W$, then $\Theta_W(F_{i,j})$ is a permutation matrix.

$$[\![ \Xi \mid \Xi ]\!]$$

# Chapter 8

# Spin

## 8.1 Braids

The *braid group on n strands* $B_n$ is the group generated by elements

$$\sigma_1, \ldots, \sigma_{n-1}$$

subject to the relations:

$$\sigma_i \sigma_j = \sigma_j \sigma_i, \text{ if } |i-j| \geq 2$$
$$\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j, \text{ if } |i-j| = 1.$$

[braids, closure]

The map that takes $\sigma_i$ to the transposition $(i\ i{+}1)$ in the symmetric group $\mathrm{Sym}(n)$ extends to a homomorphism from $B_n$. (Its kernel consists of the *pure braids*.)

The Temperley-Lieb algebra $TL_n(\beta)$ contains a homomorphic image of the Braid group.

## 8.2 Nomura Algebras

Let $A$ and $B$ be $v \times v$ matrices and suppose $B$ is Schur invertible. The *Nomura algebra* $\mathcal{N}_{A,B}$ consists of all $v \times v$ matrices for which all the vectors

$$Ae_i \circ Be_j^{(-)}$$

are eigenvectors. If $M \in \mathcal{N}_{A,B}$, we define $\Theta_{A,B}(M)$ to be the $v \times v$ matrix with $ij$-entry equal to eigenvalue of $M$ associated to $Ae_i \circ Be_j$. Thus $I \in \mathcal{N}_{A,B}$ and $\Theta_{A,B} = J$.

If $M, N \in \mathcal{N}_{A,B}$, then

$$\Theta_{A,B}(MN) = \Theta_{A,B}(M) \circ \Theta_{A,B}(N).$$

Thus $\mathcal{N}_{A,B}$ is an algebra under matrix multiplication, and the image of $\mathcal{N}_{A,B}$ under $\Theta_{A,B}$ is an algebra under Schur multiplication. We note that

$$\mathcal{N}_{A,B} = \mathcal{N}_{B,A}$$

while

$$\Theta_{B,A}(M) = \Theta_{A,B}(M)^T.$$

**8.2.1 Lemma.** *If $A$ is invertible and $B$ is Schur invertible, then $\Theta_{A,B}$ is injective and $\mathcal{N}_{A,B}$ is a commutative algebra.*

A $v \times v$ matrix $W$ is a *type-II matrix* if it is Schur invertible and

$$WW^{(-)T} = vI.$$

Hadamard matrices provide one class of examples. If $W$ is a type-II matrix, then $W$ is invertible and

$$W^{-1} = \frac{1}{v} W^{(-)T}.$$

**8.2.2 Lemma.** *The matrix $W$ is a type-II matrix if and only if $J \in \mathcal{N}_{W,W^{(-)}}$.*

The Nomura algebra $\mathcal{N}_{W,W^{(-)}}$ will play an important role in our work and so we will denote it by $\mathcal{N}_W$. We also write $\Theta_W$ for $\Theta_{W,W^{(-)}}$.

## 8.3 Braids

Let $A$, $B$ and $C$ be $v \times v$ matrices. We define endomorphisms $X_A$, $\Delta_B$ and $Y_C$ of the vector space $\mathrm{Mat}_{n\times n}(\mathbb{C})$ by

$$X_A(M) := AM, \qquad \Delta_B(M) := B \circ M, \qquad Y_C(M) := MC^T.$$

(We could instead use respectively $A \otimes I$, $D_B$ and $I \otimes C$, where $D_B$ is a diagonal matrix with the entries of $B$ as its diagonal entries and all three matrices are viewed as elements of $\mathrm{End}(\mathrm{Mat}_{v\times v}(\mathbb{C}))$.)

**8.3.1 Lemma.** *Suppose $A, B \in \mathrm{Mat}_{v\times v}(\mathbb{C})$. Then $R \in \mathcal{N}_{A,B}$ and $\Theta_{A,B}(R) = S$ if and only*

$$X_R \Delta_B X_A = \Delta_B X_A \Delta_S.$$

We see that $A \in \mathcal{N}_{A,B}$ and $\Theta_{A,B}(A) = B$ if and only if

$$X_A \Delta_B X_A = \Delta_B X_A \Delta_B;$$

we call this the *braid relation*. [If $A$ is invertible and $B$ is Schur invertible and $A \in \mathcal{N}_{A,B}$, does it follow that $\Theta_{A,B}(A) = B$?]

We note the following result, which we call the *exchange identity*.

**8.3.2 Theorem.** *Let $A$, $B$, $C$, $Q$, $R$, $S$ be $v \times v$ matrices. Then*

$$X_A \Delta_B X_C = \Delta_Q X_R \Delta_S$$

*if and only if*

$$X_A \Delta_C X_B = \Delta_R X_Q \Delta_{S^T}.$$

*Proof.* Apply each of the four products to the matrix $e_i e_j^T$. □

The bilinear form $\mathrm{tr}(MN^T)$ on $\mathrm{Mat}_{v\times v}(\mathbb{C})$ is non-degenerate and hence allows to define the adjoint of elements of $\mathrm{End}(\mathrm{Mat}_{v\times v}(\mathbb{C}))$. We denote the adjoint by transpose and observe that

$$(X_A)^T = X_{A^T}, \quad (\Delta_B)^T) = \Delta_B.$$

Thus the braid relation implies that

$$X_{A^T}\Delta_B X_{A^T} = \Delta_B X_{A^T}\Delta_B.$$

## 8.4 Jones Pairs

We say that $v\times v$ matrices $A$ and $B$ form a *one-sided Jones pair* if $A$ is invertible, $B$ is Schur invertible and $A \in \mathcal{N}_{A,B}$. They form a *Jones pair* if $(A, B^T)$ is also a one-sided Jones pair.

**8.4.1 Lemma.** *If $(A,B)$ is a one-sided Jones pair, so are each of the following:*

*(a)* $(A^T, B)$.

*(b)* $(A^{-1}, B^{(-)})$.

*(c)* $(D^{-1}AD, B)$, *where $D$ is diagonal and invertible.*

*(d)* $(A, BP)$, *where $P$ is a permutation matrix.*

*(e)* $(\lambda A, \lambda B)$, *for any non-zero complex number $\lambda$.*

**8.4.2 Lemma.** *The matrices $A$ and $B$ form a one-sided Jones pair if and only if for all $i$ and $j$ we have*

$$A(Ae_i \circ Be_j) = B_{i,j}(Ae_i \circ Be_j).$$

**8.4.3 Corollary.** *Let $(A,B)$ be a pair of $v\times v$ matrices and let $D_j$ be the diagonal matrix formed from the $j$-th column of $B$. Then $(A,B)$ is a one-side Jones pair if and only if, for $j = 1,\ldots,v$,*

$$AD_jA = D_jAD_j.$$

**8.4.4 Lemma.** *If $(A,B)$ is a one-sided Jones pair, then each column of $B$ sums to* $\mathrm{tr}(A)$.

*Proof.* From the previous result we have

$$A^{-1}D_jA = D_jAD_j^{-1}$$

whence $A$ and $D_j$ are similar and $\mathrm{tr}(A) = \mathrm{tr}(D_j)$. Therefore each column of $B$ sums to $\mathrm{tr}(A)$. □

We say a Jones pair $(A,B)$ is *invertible* if $A$ is Schur invertible and $B$ is invertible.

**8.4.5 Theorem.** *Suppose $(A,B)$ is a one-sided Jones pair and $B$ is invertible, then $A$ and $B$ are type-II matrices and the diagonal of $A$ is constant.*

*Proof.* If $A \in \mathcal{N}_{A,B}$ then $A^{-1} \in \mathcal{N}_{A,B}$ and so

$$\Theta_{B,A}(A^{-1}) = B^{(-)T}.$$

This implies that

$$X_{A^{-1}} \Delta_A X_B = \Delta_A X_B \Delta_{B^{(-)T}} \tag{8.4.1}$$

and taking the transpose of this, we get

$$X_{B^T} \Delta_A X_{A^{-T}} = \Delta_{B^{(-)T}} X_{B^T} \Delta_A.$$

If we apply the right side to $I$ we get $B^T(A \circ A^{-T})$, if we apply the left side to $I$ the result is

$$B^{(-)T} \circ (B^T(A \circ I)) = J(A \circ I)$$

and hence

$$B^T(A \circ A^{-T}) = J(A \circ I).$$

Since $B$ is invertible and its row sums are all equal t some constant $\beta$, this implies that

$$A \circ A^{-T} = B^{-T} J(A \circ I) = \beta J(A \circ I).$$

The sum of the entries in the $i$-th column of $A \circ A^{-T}$ is

$$\sum_r (A^{-1})_{r,i} (A^T)_{r,i} = \sum_r (A^{-1})_{r,i} A_{i,r} = 1$$

and therefore all columns of $J(A \circ I)$ must be equal. It follows that $vA \circ A^{-T} = J$ and so $A$ is a type-II matrix with constant diagonal.

To complete the proof we multiply each side of (8.4.1) on the left by $\Delta_{A^{(-)}}$ and on the right by $X_{B^{-1}}$ to obtain

$$\Delta_{A^{(-)}} X_{A^{-1}} \Delta_A = X_B \Delta_{B^{(-)T}} X_{B^{-1}}.$$

Taking inverses on both sides yields

$$\Delta_{A^{(-)}} X_A \Delta_A = X_B \Delta_{B^T} X_{B^{-1}}$$

and applying each side to $I$ gives

$$A^{(-)} \circ (A(A \circ I)) = B(B^T \circ B^{-1}).$$

Since the diagonal of $A$ is constant, the left side here is equal to $aJ$ for some $a$ and so

$$B^T \circ B^{-1} = aB^{-1}J$$

Arguing as before, the sum of a row of $B^T \circ B^{-1}$ is 1. Therefore $B^{-1}J$ is a multiple of $J$; from this we see that $B$ is a type-II matrix. □

**8.4.6 Lemma.** *If $(A,B)$ is Jones pair and $A$ is Schur invertible, then $B$ is invertible.*

*Proof.* Apply both sides of (8.4.1) to $J$; this yields

$$A^{-1}(A\circ(BJ)) = A\circ(BB^{(-)T}).$$

Since $(A,B^T)$ is a Jones pair the row sums of $B$ equal $\mathrm{tr}(A)$ and so the left side here is equal to $\mathrm{tr}(A)I$. As $A$ is Schur invertible it follows that $BB^{(-)T}$ is diagonal. However the diagonal entries of $BB^{(-)T}$ are all equal and so it is a scalar matrix. We conclude that $B$ is type II and invertible. □

## 8.5 Gauge Equivalence

If $D$ is an invertible diagonal matrix we say that $D^{-1}JD$ is a *dual permutation matrix*. The Schur inverse of a dual permutation matrix is a dual permutation matrix.

**8.5.1 Lemma.** *If $A$, $C$ and $M$ are Schur invertible and $X_A\Delta_M = \Delta_M X_C$, then $C^{(-)}\circ A$ is a dual permutation matrix. If $B$, $C$ and $M$ are invertible and $\Delta_B X_M = X_M\Delta_C$, then $CB^{-1}$ is a permutation matrix.*

**8.5.2 Corollary.** *If $(A,B)$ and $(C,B)$ are one-sided Jones pairs, then $C = D^{-1}AD$ where $D$ is invertible and diagonal.*

**8.5.3 Corollary.** *If $(A,B)$ and $(A,C)$ are one-sided Jones pairs, then $C = BP$ where $P$ is a permutation matrix.*

## 8.6 Nomura Algebras of Type-II matrices

A type-II matrix $W$ is called a *spin model* if $(W,W^{(-)})$ is a Jones pair. If $W\in\mathcal{N}_W$, then $(W,W^{(-)})$ need not be a Jones pair, because the columns of $W^{(-)}$ might not sum to $\mathrm{tr}(A)$. If $\sigma$ denotes the sum of a column of $W^{(-)}$ and we choose $\gamma$ so that

$$\gamma^2\,\mathrm{tr}(W) = \sigma$$

then $\gamma W$ is a spin model.

**8.6.1 Theorem.** *Let $A$ be a $v\times v$ type-II matrix. Then $\Theta_A$ is a bijection from $\mathcal{N}_A$ to $\mathcal{N}_{A^T}$ and $\Theta_{A^T}$ is a bijection from $\mathcal{N}_{A^T}$ to $\mathcal{N}_A$. If $R\in\mathcal{N}_A$ then $\Theta_{A^T}(\Theta_A(R)) = vR^T$.*

*Proof.* Suppose $R\in\mathcal{N}_A$ and $\Theta_A(R) = S$. Then

$$X_R\Delta_{A^{(-)}}X_A = \Delta_{A^{(-)}}X_A\Delta_S$$

and the transpose of this is

$$X_{A^T}\Delta_{A^{(-)}}X_{R^T} = \Delta_S X_{A^T}\Delta_{A^{(-)}}$$

and applying the exchange identity to this yields

$$X_{A^T}\Delta_{R^T}X_{A^{(-)}} = \Delta_{A^T}X_S\Delta_{A^{(-)T}}.$$

If we multiply both sides of this on the left by $\Delta_{A^{(-)T}}$ and on the right by $X_{A^{(-)-1}}$ we get

$$X_S \Delta_{A^{(-)T}} X_{A^{(-)-1}} = \Delta_{A^{(-)T}} X_{A^T} \Delta_{R^T}.$$

Since $A^{(-)-1} = \frac{1}{v} A^T$, this yields

$$X_S \Delta_{A^{(-)T}} X_{A^T} = \Delta_{A^{(-)T}} X_{A^T} \Delta_{vR^T}$$

whence $S \in \mathcal{N}_{A^T}$ and $\Theta_{A^T}(S) = vR^T$.

As $\Theta_{A^T}(\Theta_A(R)) = vR^T$, we see that $\Theta_A$ and $\Theta_{A^T}$ are bijections. □

This proof shows that the composite map

$$\frac{1}{v} \Theta_{A^T} \Theta_A$$

is the transpose map on $\mathcal{N}_A$. Hence $\frac{1}{v}\Theta_A \Theta_{A^T}$ is the transpose map on $\mathcal{N}_{A^T}$. In fact $\Theta_A$ and $\Theta_{A^T}$ commute with the transpose.

**8.6.2 Corollary.** *If $A$ is a type-II matrix and $R \in \mathcal{N}_A$, then $R^T \in \mathcal{N}_A$ and $\Theta_A(R^T) = \Theta_A(R)^T$.*

*Proof.* If $R \in \mathcal{N}_A$ then $vR^T = \Theta_{A^T}(\Theta_A(R) \in \mathcal{N}_A$ and

$$\Theta_A(vR^T) = \Theta_A(\Theta_{A^T}(\Theta_A(R))) = v\Theta_A(R)^T.$$ □

**8.6.3 Corollary.** *If $A$ is a $v \times v$ type-II matrix and $M, N \in \mathcal{N}_A$, then*

$$\Theta_A(M \circ N) = \frac{1}{v} \Theta_A(M) \Theta(N).$$

**8.6.4 Corollary.** *If $A$ is a type-II matrix then its Nomura algebra is closed under matrix multiplication, Schur multiplication, transpose and complex conjugation.*

*Proof.* We know that $\mathcal{N}_A$ is closed under matrix multiplication and that

$$\Theta_A(MN) = \Theta_A(M) \circ \Theta_A(N),$$

from which it follows that the image of $\Theta_A$ is Schur-closed. Therefore $\mathcal{N}_{A^T}$ is Schur-closed. Swapping $A$ and $A^T$, we deduce that $\mathcal{N}_A$ is Schur-closed.

We saw above that $\mathcal{N}_A$ is closed under transpose. Since it is Schur-closed it has a basis consisting of 01-matrices, and the complex span of these matrices is closed under complex conjugation. □

This corollary asserts that $\mathcal{N}_A$ is the Bose-Mesner algebra of an association scheme.

## 8.7 Spin Models

By definition, $W$ is a spin model if $(W, W^{(-)})$ is a one-sided Jones pair.

**8.7.1 Lemma.** *If $A$ is a type-II matrix and $(A, A^{(-)})$ is a one-sided Jones pair, then it is a Jones pair.*

*Proof.* Since $(A, A^{(-)})$ is a one-sided Jones pair, we have

$$X_A \Delta_{A^{(-)}} X_A = \Delta_{A^{(-)}} X_A \Delta_{A^{(-)}}$$

and taking the transpose of this yields

$$X_{A^T} \Delta_{A^{(-)}} X_{A^T} = \Delta_{A^{(-)}} X_{A^T} \Delta_{A^{(-)}}.$$

Using the exchange identity we obtain

$$X_{A^T} \Delta_{A^T} X_{A^{(-)}} = \Delta_{A^T} X_{A^{(-)}} \Delta_{A^{(-)T}}$$

and inverting both sides yields

$$X_{A^{(-)-1}} \Delta_{A^{(-)T}} X_{A^{-T}} = \Delta_{A^T} X_{A^{(-)-1}} \Delta_{A^{(-)T}}.$$

If we multiply on the left by $\Delta_{A^{(-)T}}$ and on the right by $X_{A^T}$, the result is

$$\Delta_{A^{(-)T}} X_{A^{(-)-1}} \Delta_{A^{(-)T}} = X_{A^{(-)-1}} \Delta_{A^{(-)T}} X_{A^T}.$$

We observe that $A^{(-)-1} = \frac{1}{v} A^T$, whence the last equation yields

$$\Delta_{A^{(-)T}} X_{A^T} \Delta_{A^{(-)T}} = X_{A^T} \Delta_{A^{(-)T}} X_{A^T}$$

and therefore $(A^T, A^{(-)T})$ is a one-sided Jones pair. From the transpose of this we see that $(A, A^{(-)T})$ is one-sided Jones pair, and thus it follows that $(A, A^{(-)})$ is a Jones pair. □

**8.7.2 Theorem.** *If $A$ is spin model, then $\mathcal{N}_A = \mathcal{N}_{A^T}$ and $\Theta_A = \Theta_{A^T}$.*

*Proof.* We use gauge equivalence. If $(A, A^{(-)})$ and $A, A^{(-)T}$ are one-sided Jones pairs, there is a permutation matrix $P$ such that $A^{(-)T} = A^{(-)}P$, and consequently

$$\mathcal{N}_{A,A^{(-)T}} = \mathcal{N}_{A,A^{(-)}P} = \mathcal{N}_{A,A^{(-)}}$$

Now $A \in \mathcal{N}_A$ if and only if

$$A^T \in \mathcal{N}_{A^T,A^{(-)}} = \mathcal{N}_{A^T,A^{(-)T}}.$$

Since $\mathcal{N}_A$ is closed under transposes, the result holds.

Suppose $R \in \mathcal{N}_A$ and $\Theta_A(R) = S$ then

$$X_R \Delta_{A^{(-)}} X_A = \Delta_{A^{(-)}} X_A \Delta_S$$

and if $R \in \mathcal{N}_{A^T}$ and $\Theta_{A^T} = T$ then

$$X_R \Delta_{A^{(-)T}} X_{A^T} = \Delta_{A^{(-)T}} X_{A^T} \Delta_T.$$

Consequently

$$(\Delta_{A^{(-)T}} X_{A^T} \Delta_T)^{-1} \Delta_{A^{(-)}} X_A \Delta_S = X_{A^{-T}} \Delta_{A^T \circ A^{(-)}} X_A.$$

The left side here equals

$$\Delta_{T^{(-)}} X_{A^{-T}} \Delta_{A^T} \Delta_{A^{(-)}} X_A \Delta_S = \Delta_{T^{(-)}} (X_{A^{-T}} \Delta_{A^T \circ A^{(-)}} X_A) \Delta_S$$

If we define

$$\Xi := X_{A^{-T}} \Delta_{A^T \circ A^{(-)}} X_A$$

then

$$\Xi \Delta_S = \Delta_T \Xi. \tag{8.7.1}$$

We compute $\Xi(M)$, for any $v \times v$ matrix $M$. Note that

$$\Xi(M) = A^{-T}(A^T \circ A^{-1} \circ (AM))$$

Since $(A, A^{(-)})$ and $(A^T, A^{(-)T})$ are both one-sided Jones pairs, there is an invertible diagonal matrix $C$ such that $A^T = C^{-1}AC$. Therefore

$$A^T \circ A^{-1} = (C^{-1}AC) \circ A^{-1} = C^{-1}JC$$

and so

$$A^T \circ A^{-1} \circ (AM) = (C^{-1}JC) \circ (AM) = C^{-1}AMC = A^T C^{-1} MC$$

and consequently

$$\Xi(M) = A^{-T}(A^T \circ A^{-1} \circ (AM)) = C^{-1}MC.$$

Now apply each side of (8.7.1) to $M$; we get

$$T \circ (C^{-1}MC) = C^{-1}(S \circ M)C = S \circ) C^{-1}MC).$$

We conclude that $S = T$. □

# Index