Generalized Hamming Schemes

Chris Godsil
Combinatorics & Optimization
University of Waterloo

November 5, 2010

Abstract

We introduce a class of association schemes that generalizes the Hamming scheme. We derive generating functions for their eigenvalues, and use these to obtain a version of MacWilliams theorem.

1 Association Schemes

An association scheme is a collection of graphs that fit together nicely. It is easiest to offer a precise definition in terms of adjacency matrices. So an *association scheme* $\mathcal{A}$ on v vertices is a set of $v \times v$ 01-matrices $A_1, \ldots, A_d$ such that:

(1) $A_0 = I$.

(2) $\sum_{i=0}^{d} A_i = J$.

(3) If $A_i \in \mathcal{A}$ then $A_i^T \in \mathcal{A}$.

(4) There are constants $p_{i,j}(k)$ such that

$$A_i A_j = \sum_{r=0}^{d} p_{i,j}(r) A_r.$$

(5) For all i and j we have $A_i A_j = A_j A_i$.

By virtue of (4), the complex span of the matrices A_i forms an algebra, known as the *Bose-Mesner algebra* of the scheme and denoted by $\mathbb{C}[\mathcal{A}]$. Given (5), this algebra is commutative. Note that the constants $p_{i,j}(k)$ must be integers; they are the *intersection numbers* of the scheme.

An association scheme is *symmetric* if each matrix A_i is symmetric. If we restrict ourselves to symmetric schemes the last axiom is redundant. Some workers prefer to drop the last axiom but since there are as yet no really convincing combinatorial applications making use of this generality, we will work with the axioms just stated. The schemes we work with in this paper will be symmetric.

We view the matrices $A_1, \dots, A_d$ as the adjacency matrices of directed graphs $X_1, \dots, X_d$ and we will often view a scheme as a set of graphs. We refer to these graphs as the *color classes* of the scheme. Since J lies in the Bose-Mesner algebra (by (2)) and since the Bose-Mesner algebra is commutative, we have $A_iJ = JA_i$ for each i. Hence each of the color classes is regular.

For more background on association schemes see [5, 3].

The *Hamming scheme* $H(n,q)$ is a useful and relevant example of an association scheme. Its vertices are the n-tuples of elements of a set Q with size q. Two tuples α and β are adjacent in the graph X_i if they differ in exactly i positions—equivalently if they are at Hamming distance i. In this context we often call the vertices *words*. It is easy to see that the matrices A_i satisfy the first three axioms and that they are symmetric. We leave the verification of the final two axioms as an exercise and note that $H(n,q)$ is a symmetric scheme. The Hamming scheme is of fundamental importance in coding theory.

We introduce a generalization of the Hamming scheme. Let $\mathcal{A}$ be a fixed association scheme with d classes and vertex set V. If v and w are elements of V^n, let $h(v,w)$ be the vector of length $d+1$ with rth-entry equal to the number of coordinates j such that v_j and w_j are r-related in $\mathcal{A}$. For any n-tuples v and w the vector $h(v,w)$ has non-negative integer entries, and these entries sum to n. Conversely, any such vector can be written as $h(v,w)$ for some v and w. If x is an integer vector of length $d+1$ with entries summing to n, let A_x be the 01-matrix with rows and columns indexed by V^n, and with $A_{v,w}$ equal to 1 if and only if $h(v,w) = x$. Denote this set of matrices by $H(n,\mathcal{A})$.

Two things should become clear without too much effort: if $\mathcal{A} = H(1,q)$ then $H(n,\mathcal{A})$ is the Hamming scheme $H(n,q)$ and, in any case, these matrices in $H(n,\mathcal{A})$ satisfy the first three axioms for an association scheme. Generalized Hamming schemes were defined by Delsarte [5, Section 2.5], where they are referred to as *extensions* and a number of examples are given. One of the goals of this paper is prove that, for all choices of base scheme, $H(n, \mathcal{A})$ is an association scheme and to provide some of its applications. Delsarte's construction can be viewed as based on the symmetric group $\mathrm{Sym}(n)$, we will see that it can be generalized by replacing the symmetric group by any permutation group on n symbols. Some of our results have already been applied by Martin and Stinson in their work on (T, M, S)-nets [9] and by Chan and Munemasa in [4]. (They cite the research report CORR98-20, issued by the Department of Combinatorics and Optimization at the University of Waterloo.)

2 Idempotents and Eigenvalues

If M and N are $m \times n$ matrices, their *Schur product* is the $m \times n$ matrix $M \circ N$ given by

$$(M \circ N)_{i,j} := M_{i,j} N_{i,j}.$$

A matrix is idempotent with respect to the Schur product if and only if it is a 01-matrix. The $m \times n$ matrices over a field form a commutative algebra relative to the Schur product with multiplicative identity the all-ones matrix J. It is an easy exercise to see that that a vector space of matrices is an algebra relative to the Schur product if and only if it has a basis of 01-matrices. Consequently the Bose-Mesner algebra of an association scheme is Schur-closed. It is a crucially important property of an association scheme that the operations of matrix and Schur multiplication are dual to each other.

An idempotent in algebra is *minimal* if there is non non-trivial way of writing it as a sum of other idempotents. The matrices A_i are the minimal Schur idempotents in the Bose-Mesner algebra, viewed as an algebra under Schur multiplication. They form one basis of the Bose-Mesner algebra. We introduce a second important basis. An eigenspace of $\mathcal{A}$ is a subspace U of $\mathbb{R}^n$, maximal subject to the condition that each matrix in $\mathcal{A}$ acts on U as a scalar. As the Bose-Mesner algebra is closed under Hermitian transposes, it is semisimple. It follows that there are orthogonal projections $E_0, \ldots, E_d$ and real numbers $p_i(j)$ such that:

(a) $E_0 = \frac{1}{v} J$,

(b) $\sum_i E_i = I$,

(c) $E_i^2 = E_i$ and $E_i E_j = 0$ if $i \neq j$,

(d) $A_i = \sum_j p_i(j) E_j$.

We will call these matrices the *principal idempotents* of the scheme. (They are the minimal idempotents of the Bose-Mesner algebra, relative to the usual matrix multiplication.)

The scalars $p_i(j)$ are the *eigenvalues* of the association scheme and the matrix P given by

$$P_{i,j} = p_j(i)$$

is its *matrix of eigenvalues*. We have

$$A_i = \sum_j p_i(j) E_j.$$

Since the principal idempotents of $\mathcal{A}$ lie in its Bose-Mesner algebra, there are also scalars $q_i(j)$ such that

$$E_i = \frac{1}{v} \sum q_i(j) A_j.$$

If Q is the matrix with ij-entry $q_j(i)$ then $PQ = vI$.

Since the Bose-Mesner algebra of a scheme is closed under Schur multiplication, it follows that there must be scalars $q_{i,j}(k)$ such that

$$E_i \circ E_j = \frac{1}{v} \sum_{r=0}^{d} q_{i,j}(r) E_r.$$

These scalars are the *Krein parameters* of the scheme, they need not be integers, but must be non-negative.

3 Automorphisms and Subschemes

We call an association scheme $\mathcal{B}$ a *subscheme* of a scheme $\mathcal{A}$ if each matrix in $\mathcal{B}$ is a sum of elements of $\mathcal{A}$. (This is also called a fusion scheme.) It is immediate that $\mathcal{B}$ is a subscheme of $\mathcal{A}$ if and only the Bose-Mesner algebra of $\mathcal{B}$ is a subalgebra of the Bose-Mesner algebra of $\mathcal{A}$ that is closed under Hermitian transpose and the Schur product. We also point out here that a commutative algebra of real matrices is the Bose-Mesner algebra of an association scheme if and only if it is closed under transpose and Schur multiplication and contains J.

Let $\mathcal{A}$ be an association scheme with d classes. Let M^* denote the conjugate-transpose of the complex matrix M. We call a map $M \mapsto M^\psi$ on the Bose-Mesner algebra of $\mathcal{A}$ an *algebra automorphism* if

$$\begin{aligned}(M^*)^\psi &= (M^\psi)^*,\\ (MN)^\psi &= M^\psi N^\psi,\\ (M \circ N)^\psi &= M^\psi \circ N^\psi.\end{aligned}$$

An algebra automorphism must permute the matrices A_i among themselves and fix I. Similarly it must permute the principal idempotents E_j and fix J.

If $\mathcal{A}$ be an association scheme that is not symmetric, then the transpose map is an algebra automorphism. More important, for us, is the next example. Consider the product scheme $\mathcal{A}^{\otimes n}$ and let Γ be any permutation group on the set $\{1, 2, \dots, n\}$. If $g \in \Gamma$ define

$$(A_{i_1} \otimes \cdots \otimes A_{i_n})^g = A_{i_{1g}} \otimes \cdots \otimes A_{i_{ng}}.$$

It is immediate that g is an algebra automorphism of $\mathcal{A}^{\otimes n}$.

3.1 Theorem. *Let $\mathcal{A}$ be an association scheme on d classes and let Γ be a group of algebra automorphisms of $\mathcal{A}$. Then the matrices in $\mathbb{C}[\mathcal{A}]$ fixed by each element of Γ form the Bose-Mesner algebra of a subscheme of $\mathcal{A}$.*

Proof. The subspace of the Bose-Mesner algebra of $\mathcal{A}$ consisting of the matrices fixed by the elements of Γ is closed under transposes, multiplication and Schur multiplication. Hence it is the Bose-Mesner algebra of an association scheme, necessarily a subscheme of $\mathcal{A}$. □

3.2 Corollary. *$H(n, \mathcal{A})$ is an association scheme.*

Proof. Let Γ be the symmetric group on n letters. Then Γ acts as a group of algebra automorphisms on the Bose-Mesner algebra of $\mathcal{A}^{\otimes n}$. The subspace of fixed matrices is the Bose-Mesner algebra of $H(n, \mathcal{A})$. □

The Bose-Mesner algebra of a scheme $\mathcal{A}$ is a vector space. Hence we may view $\mathcal{A}^{\otimes n}$ as the n-th graded piece of the tensor algebra. Given this, $H(n, \mathcal{A})$ is the n-th graded piece of the symmetric algebra. Thus we have shown that the graded pieces of the symmetric algebra are Schur-closed. We note one useful consequence of this.

3.3 Lemma. *For any association scheme $\mathcal{A}$ we have*

$$H(m, H(n, \mathcal{A})) \cong H(mn, \mathcal{A}). \qquad \square$$

We consider one example. Let $\mathcal{C}_4$ denote the two-class association scheme formed by the cycle of length four and its complement. $\mathcal{C}_4 = H(n, 2)$ and $H(n, \mathcal{C}_4) = H(2n, 2)$. This observation plays a small role in the construction of the Kerdock codes as linear codes over $\mathbb{Z}_4$. We discuss this in Section 6.

4 Generating Functions

We start by deriving a generating function for the eigenvalues of $H(n, \mathcal{A})$.

Let $\mathcal{A}$ be an association scheme with d classes, formed by the matrices $A_0, \ldots, A_d$. If α is a vector of length $d+1$ with non-negative integer entries summing to n, let A_α denote the matrix in $H(n, \mathcal{A})$ with vw-entry 1 if and only if $h(v, w) = \alpha$. Note that A_α is the sum of all products

$$A_{i_1} \otimes \cdots \otimes A_{i_r}$$

where A_r occurs exactly $\alpha(r)$ times, for $r = 0, 1, \ldots, d$. If $E_0, \ldots, E_d$ are the principal idempotents of $\mathcal{A}$, we similarly define E_β to be the sum of all products

$$E_{i_1} \otimes \cdots \otimes E_{i_r}$$

where E_r occurs exactly $\beta(r)$ times, for $r = 0, 1, \ldots, d$.

Let $s_0, \ldots, s_d$ be a set of $d+1$ independent commuting variables and let s denote the column vector with i-th entry equal to s_i for each i. If α is a vector of length $d+1$ with non-negative integer entries, let s^α be the monomial given by

$$s^\alpha := \prod_{i=1}^{n} s_i^{\alpha(i)}.$$

It follows immediately that

$$(s_0 A_0 + \cdots + s_d A_d)^{\otimes n} = \sum_\alpha s^\alpha A_\alpha, \tag{4.1}$$

where α ranges over all $\binom{d+n}{n}$ vectors of length $d+1$ with non-negative integer entries summing to n. Similarly, if $t_0, \ldots, t_d$ are independent commuting variables then

$$(t_0 E_0 + \cdots + t_d E_d)^{\otimes n} = \sum_\beta t^\beta E_\beta. \tag{4.2}$$

4.1 Lemma. *We have*

$$\sum_\alpha A_\alpha s^\alpha = \sum_\beta (Ps)^\beta E_\beta$$

and

$$\sum_\alpha (P^{-1}t)^\alpha A_\alpha = \sum_\beta t^\beta E_\beta.$$

Proof. If

$$t_j := \sum_i s_i p_i(j)$$

then

$$\sum_j t_j E_j = \sum_{i,j} s_i p_i(j) E_j = \sum_i s_i A_i.$$

Hence our claims follow from (4.1) and (4.2). □

Suppose $\mathcal{A}$ is an association scheme on v vertices with matrix of eigenvalues P. An association scheme $\mathcal{B}$ is *formally dual* to $\mathcal{A}$ if the matrix of eigenvalues of $\mathcal{B}$ is vP^{-1}. Hence Lemma 4.1 has the following consequence.

4.2 Corollary. *If $\mathcal{A}$ and $\mathcal{B}$ are formally dual association schemes then $H(n,\mathcal{A})$ and $H(n,\mathcal{B})$ are formally dual. If $\mathcal{A}$ is formally self-dual then $H(n,\mathcal{A})$ is too.* □

Denote the eigenvalue of A_α associated to the idempotent E_β by $p_\alpha(\beta)$. Then multiplying both sides of the first identity in Lemma 4.1 by E_γ yields

$$\sum_\alpha s^\alpha p_\alpha(\gamma) = (Ps)^\gamma, \tag{4.3}$$

which provides a generating function for the eigenvalues of $H(n,\mathcal{A})$.

5 MacWilliams Theorem

Let $\mathcal{A}$ be an association scheme of order v with Schur idempotents $A_0,\dots,A_d$. If C is a subset of the vertices of $\mathcal{A}$ with characteristic vector x then the vector

$$\frac{1}{|C|}(x^T A_0 x, x^T A_1 x, \dots, x^T A_d x)$$

is called the *inner distribution* of C. The central problem of coding theory is to find the subsets of the vertices of $H(n,q)$ of maximal size, subject to given constraints on the inner distribution. One of the main contributions of the theory of association schemes is that it allows us to define what is essentially a Fourier transform of the inner distribution vector.

Let $E_0,\dots,E_d$ be the principal idempotents of $\mathcal{A}$. The vector

$$\frac{v}{|C|^2}(x^TE_0x, x^TE_1x,\dots,x^TE_dx)$$

is the *dual inner distribution*.

Now suppose that C is a subset of the vertices of $H(n,\mathcal{A})$, with characteristic vector x. Define the *weight enumerator* of C to be the polynomial

$$W_C(s)=\frac{1}{|C|}\sum_\alpha x^TA_\alpha x\, s^\alpha$$

and the *dual weight enumerator* to be

$$W_C^\perp(t)=\frac{v^n}{|C|^2}\sum_\beta x^TE_\beta x\, t^\beta.$$

Either of these polynomials determines the other:

5.1 Theorem. *Let $\mathcal{A}$ be an association scheme of order v and let P be its matrix of eigenvalues. Let C be a subset of the vertices of $H(n,\mathcal{A})$. Then*

$$W_C^\perp(t)=\frac{v^n}{|C|}W_C(P^{-1}t).$$

Proof. We have

$$\sum_\alpha A_\alpha(P^{-1}t)^\alpha=\sum_\alpha E_\alpha t^\alpha,$$

from which the result follows directly. □

If we restrict ourselves to translation schemes, we can say more. An *automorphism* of an association scheme is a permutation of its vertices that is an automorphism of each colour class in the scheme. (There is essentially no relation between automorphisms and Bose-Mesner automorphisms.) An association scheme is a *translation scheme* if there is an abelian group, Γ say, of automorphisms acting transitively on its vertices. If $\mathcal{A}$ is a translation scheme relative to the abelian group Γ, then $H(n,\mathcal{A})$ is a translation scheme relative to the abelian group Γ^n. If $\mathcal{A}$ is a translation scheme relative to Γ then, since we may assume without loss that Γ acts faithfully and therefore regularly, we may identify the vertex set of $\mathcal{A}$ with Γ: associate some fixed vertex of $\mathcal{A}$ to the identity, and associate the image of this vertex under an element γ of Γ with γ. A subset of the vertices of a translation scheme is *additive* if its image in Γ is a subgroup. A scheme may be a translation scheme relative to more than one group; for example, $H(n,2)$ is a translation scheme relative to the group $\mathbb{Z}_4^a \times \mathbb{Z}_2^b$ for any non-negative integers a and b such that $2a+b=n$.

Let $\Gamma^\perp$ denote the character group of Γ. The *dual* to a subset C of Γ is the set

$$C^\perp := \{\chi \in \Gamma^* : \chi(x) = 1,\ \forall x \in C\}.$$

Note that $C^\perp$ is a subgroup of $\Gamma^\perp$ and, if C is a subgroup of Γ then $C^{\perp\perp} = C$. As $\Gamma^\perp$ and Γ are isomorphic, we may view $\Gamma^\perp$ as an abelian group of automorphisms of $\mathcal{A}$, and hence identify $C^\perp$ with a subset of the vertices of $\mathcal{A}$. With all this established [3, Theorem 2.10.12] yields:

5.2 Theorem. *If $\mathcal{A}$ is a translation scheme and C is an additive subset of $H(n,\mathcal{A})$, then $W_{C^\perp}(t) = W_C^\perp(t)$.* □

This brings us to one of the main results of this paper.

5.3 Corollary. *Let $\mathcal{A}$ be a translation scheme and let P be its matrix of eigenvalues. If C is an additive subset of the vertices of $\mathcal{A}$, then*

$$W_{C^\perp}(t) = \frac{v^n}{|C|} W_C(P^{-1}t).$$ □

We consider the simplest case, when $\mathcal{A}$ is the scheme with one class on q vertices. Then $H(n,\mathcal{A}) = H(n,q)$. A linear code of length n over $GF(q)$ is an additive subset of $H(n,q)$ and $C^\perp$ is the usual dual code. The matrix of eigenvalues for $\mathcal{A}$ is

$$P = \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$$

and its inverse is $q^{-1}P$. So Theorem 5.1 and Theorem 5.2 imply that, if C is a linear code in $H(n,q)$, then

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

This is the standard form of MacWilliams theorem (see, for example, [8, Theorem 5.13]).

5.4 Corollary. *Let $\mathcal{A}$ be an association scheme with d classes and let P be its matrix of eigenvalues. Let $\widehat{P}$ be the matrix representing the action of P on homogeneous polynomials of degree n in $s_0, \dots, s_d$. Then $\widehat{P}$ is the matrix of eigenvalues of $H(n, \mathcal{A})$.* □

Taking the Schur product of each side of the second identity in Lemma 4.1 with A_γ yields

$$\sum_\beta t^\beta q_\beta(\gamma) = (vP^{-1}t)^\gamma,$$

a generating function for the dual eigenvalues.

We illustrate some of these results by applying them to the Hamming scheme. The matrix of eigenvalues for $H(1, q)$ is

$$P = \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix},$$

with inverse $q^{-1}P$. We use Lemma 4.1, obtaining

$$\sum_{i=0}^{n} s_0^{n-i} s_1^i A_{n-i,i} = \sum_{j=0}^{n} (s_0 + (q-1)s_1)^{n-j}(s_0 - s_1)^j E_{n-j,j};$$

similarly

$$q^{-n} \sum_{i=0}^{n} (t_0 + (q-1)t_1)^{n-i}(t_0 - t_1)^i A_{n-i,i} = \sum_{j=0}^{n} t_0^{n-j} t_1^j E_{n-j,j}.$$

The generating function for the eigenvalues unfolds as:

$$\sum_i p_{n-i,i}(n-j, j) s_0^{n-i} s_1^i = (s_0 + (q-1)s_1)^{n-j}(s_0 - s_1)^j.$$

To decode these, note that $A_{n-i,i}$ is the i-th minimal Schur idempotent of $H(n, q)$ and $E_{n-j,j}$ is the j-th principal idempotent. Hence $p_{n-i,i}(n-j, j)$ represents $p_i(j)$.

6 Codes

We make some remarks on codes over $\mathbb{Z}_4$. Our aim is to show that a number of standard results follow easily from the theory we have described.

By a code C of length n over $\mathbb{Z}_4$, we mean simply a subset of $\mathbb{Z}_4^n$. The relevant association scheme depends on our choice of 'distance function'. Suppose first that, if x and y are words in C then $h_4(x,y)$ is the vector of length four, giving the number of coordinates i such that $x_i - y_i$ is 0, 1, 2 or 3 modulo 4. Let $\mathcal{D}_4$ denote the three-class scheme formed by the elements of $\mathbb{Z}_4$, viewed as 4×4 permutation matrices. The relations on $\mathbb{Z}_4^n$ determined by $h_4(x,y)$ form the scheme $H(n,\mathcal{D}_4)$. The matrix of eigenvalues for $\mathcal{D}_4$is

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix},$$

which satisfies $P^2 = 4I$. This scheme is linear and so Theorem 5.1 yields

$$W_C^{\perp}(s,t,u,v) = \frac{1}{|C|} W_C(s+t+u+v, s+it-u-iv, s-t+u-v, s-it-u+iv).$$

In coding theory terms, this is MacWilliams theorem for the *complete weight enumerator* of a code in $\mathbb{Z}_4^n$. Note that $\mathcal{D}_4$ is a translation scheme, so $W_C^{\perp} = W_{C^{\perp}}$ when C is an additive code.

Let $\mathcal{C}_4$ denote the two-class association scheme belonging to the undirected cycle on four vertices. This is the symmetric subscheme of $\mathcal{D}_4$ and has matrix of eigenvalues

$$P = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{pmatrix}.$$

Now $H(n,\mathcal{C}_4)$ is the scheme determined by $h_3(x,y)$, where $h_3(x,y)$ is a triple with entries counting the number of coordinates i such that $x_i - y_i$ is 0, 1 or 3, or 2 modulo 4. If $C \subseteq \mathbb{Z}_4^n$ then

$$W_C^{\perp}(s,t,u) = \frac{1}{|C|} W_C(s+2t+u, s-u, s-2t+u).$$

This is MacWilliams theorem for the *symmetrized weight enumerator*. As before, $W_C^{\perp} = W_{C^{\perp}}$ when C is additive. Of course this identity is a special of case of the previous one, which is probably best ascribed to Klemm. (See Satz 1.5 in [7, Satz 1.5].)

The sum of the entries of $h_3(x,y)$ is the *Lee distance* between x and y and

$$W_C(s^2, st, t^2)$$

is a form of the *Lee weight enumerator*.

There is one surprise here. The scheme $\mathcal{C}_4$ is equal to $H(2,2)$ and so, by Lemma 3.3, we have $H(n, \mathcal{C}_4) \cong H(2n, 2)$. The Lee weight enumerator for a code C, viewed as a subset of the vertices of $H(n, \mathcal{C}_4)$, is the usual weight enumerator for C, viewed as a subset of the vertices of $H(2n, 2)$, i.e., as a binary code. However it is possible that C is an additive code in $H(n, \mathcal{C}_4)$, but not in $H(2n, 2)$. In this case the binary weight enumerators for C and $C^\perp$ will satisfy

$$W_{C^\perp}(s^2, st, t^2) = \frac{1}{|C|} W_C((s+t)^2, s^2 - t^2, (s-t)^2,$$

even though C and $C^\perp$ are not linear as binary codes (and $C^\perp$ will not be the dual of C in the usual sense).

For further discussion of these weight enumerators, we refer the reader to [6, Section 2.2].

7 Modular Invariance

Let $\mathcal{A}$ be an association scheme with d classes and let P be its matrix of eigenvalues. Following Bannai, Bannai and Jaeger [2]] we say that $\mathcal{A}$ satisfies the *modular invariance property* if there is a diagonal matrix T and a constant c such that

$$(PT)^3 = cI.$$

This may seem an unlikely condition, but it does hold for the Hamming scheme and there is an interesting connection with the theory of spin models.

The following result generalizes Theorem 1 of Bannai and Bannai [1].

7.1 Lemma. *If the association scheme $\mathcal{A}$ satisfies the modular invariance property, so does $H(n, \mathcal{A})$.*

Proof. Assume that $\mathcal{A}$ has d classes and let P be its matrix of eigenvalues. If M is a $(d+1) \times (d+1)$ matrix, let $\widehat{M}$ denote the matrix representing the induced action of M on polynomials of degree n. If T is diagonal then so is $\widehat{T}$. If $(PT)^3 = cI$ then $(\widehat{P}\widehat{T})^3 = cI$. □

For those whom it helps, we remark that if $\mathcal{A}$ contains a matrix $W(+)$ that determines a spin model then $W(+)^{\otimes n}$ determines a spin model and lies in $H(n, \mathcal{A})$ (not just in $\mathcal{A}^{\otimes n}$).

Acknowledgement

I thank Bill Martin for a number of useful conversations on the topics in this paper. The reader should thank him for identifying a number of mistakes in an earlier version.

References

[1] Eiichi Bannai and Etsuko Bannai. Modular invariance of the character table of the Hamming association scheme H(d,q). *J. Number Theory*, 47(1):79–92, 1994.

[2] Eiichi Bannai, Etsuko Bannai, and François Jaeger. On spin models, modular invariance, and duality. *J. Algebraic Combin.*, 6(3):203–228, 1997.

[3] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.

[4] A. Chan and A. Munemasa. Hamming Graph in Nomura Algebra. *ArXiv e-prints*, October 2010.

[5] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[6] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé. The Z4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, 40(2):301–319, 1994.

[7] Michael Klemm. Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4. *Arch. Math. (Basel)*, 53(2):201–207, 1989.

[8] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[9] W. J. Martin and D. R. Stinson. Association schemes for ordered orthogonal arrays and (T,M,S)-nets. *Canad. J. Math.*, 51(2):326–346, 1999.