Association schemes related to Kasami codes and Kerdock sets

van Dam, E.R.; de Caen, D.

Published in:
Designs Codes and Cryptography

Publication date:
1999


Designs, Codes and Cryptography, 18, 89–102 (1999)

Association Schemes Related to Kasami Codes and Kerdock Sets

D. DE CAEN decaen@mast.queensu.ca
Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, Canada

E. R. VAN DAM edwin.vandam@kub.nl
Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, Canada

Dedicated to the memory of E. F. Assmus

Received May 5, 1998; Revised May 5, 1998; Accepted August 14, 1998

Abstract. Two new infinite series of imprimitive 5-class association schemes are constructed. The first series of schemes arises from forming, in a special manner, two edge-disjoint copies of the coset graph of a binary Kasami code (double error-correcting BCH code). The second series of schemes is formally dual to the first. The construction applies vector space duality to obtain a fission scheme of a subscheme of the Cameron-Seidel 3-class scheme of linked symmetric designs derived from Kerdock sets and quadratic forms over $GF(2)$.

Keywords: association scheme, binary code, quadratic form

1. Codes and Schemes

In what follows we will freely use standard terminology and results from algebraic combinatorics, especially coding theory and association schemes. Among the many good texts available, we mention [10] for coding and [1] for schemes. Chapter 11 of [1] is an extensive presentation of the "coset graph" construction of distance-regular graphs. Given a linear q-ary code C of length n, i.e. a subspace of $V = GF(q)^n$, one defines the *coset graph* $\Gamma(C)$ by taking as vertices the cosets of C in V, and joining two cosets when they have representatives at Hamming distance one. Under certain restrictive assumptions on C (cf. Thms. 11.1.6 and 11.1.13 in [1]), the coset graph $\Gamma(C)$ is distance-regular.

One particular series of linear binary codes is pertinent to this paper. For a positive integer t, the *Kasami code* K_t consists of all subsets S of $GF(2^{2t+1})\backslash\{0\}$ such that $\sum_{r\in S} r = \sum_{r\in S} r^3 = 0$. These are also known as double error-correcting BCH codes. Note that, by identifying each subset S with its characteristic vector, one may think of K_t as a binary code of length $2^{2t+1}-1$. The coset graph $\Gamma(K_t)$ (let's call it a Kasami graph) is distance-regular of diameter three ([1], Thm. 11.2.1). In slightly different language, we have a metric 3-class association scheme with relations Γ_1, Γ_2 and Γ_3, where Γ_i has the same vertex set as $\Gamma(K_t)$ and two vertices are adjacent in Γ_i if and only if they have distance i in the Kasami graph.

PROPOSITION 1 *The Kasami graph $\Gamma(K_t)$ has the following equivalent description. The vertices are all ordered pairs of elements in $GF(2^{2t+1})$. Two distinct ordered pairs (a, x) and (b, y) are adjacent if and only if $a + b = (x + y)^3$.*

Proof. The vertices of $\Gamma(K_t)$ are the distinct cosets $S + K_t$ of K_t (viewed as a subspace of a binary vector space of dimension $2^{2t+1} - 1$), where S ranges over all subsets of $GF(2^{2t+1})\backslash\{0\}$. To each coset $S + K_t$, assign the ordered pair $\left(\sum_{r\in S} r^3, \sum_{r\in S} r\right)$ of field elements. The definition of K_t implies that this map is well defined. The verification that this map is a graph isomorphism (between $\Gamma(K_t)$ and the other description) is routine and left to the reader. ∎

Let us change notation and write $G_1 = \Gamma(K_t)$; so t is fixed and in the background. Define another graph G_2 as follows. It has the same vertex set as G_1, namely all ordered pairs of elements of $GF(2^{2t+1})$. Two distinct ordered pairs (a, x) and (b, y) are adjacent in G_2 if and only if $a + b = xy(x + y)$. Note that since $(x + y)^3 = xy(x + y) + x^3 + y^3$, the involution $(a, x) \mapsto (a + x^3, x)$ is an isomorphism between G_1 and G_2. Furthermore, since cubing is a bijection on $GF(2^{2t+1})$, it follows easily that G_1 and G_2 have no edges in common. Indeed, what we have here is a remarkably nice edge-disjoint placement of two copies of the Kasami graph: their adjacency matrices commute, and they are two of the relations in a 5-class association scheme. The precise result is the following. Recall that $Tr(z) = z + z^2 + \ldots + z^{2^{2t}}$ is the trace map from $GF(2^{2t+1})$ onto $GF(2)$.

THEOREM 2 *Define five relations on the set of ordered pairs of elements of $GF(2^{2t+1})$ as follows. For distinct pairs (a, x) and (b, y), the possible relations are*

$$
\begin{aligned}
&G_1 \ : \ x \neq y \ \text{ and } \ a + b = (x + y)^3;\\
&G_2 \ : \ x \neq y \ \text{ and } \ a + b = xy(x + y);\\
&G_3 \ : \ x \neq y, a + b \neq (x + y)^3 \ \text{ and } \ Tr\left(\frac{a+b}{(x+y)^3}\right) = 1;\\
&G_4 \ : \ x \neq y, a + b \neq xy(x + y) \ \text{ and } \ Tr\left(\frac{a+b}{(x+y)^3}\right) = 0;\\
&G_5 \ : \ x = y \ \text{ and } \ a \neq b.
\end{aligned}
$$

Then the relations G_i, together with the identity relation G_0, form an association scheme.

Theorem 2 will be proved in several steps. Before doing so, we remark that there is a more general version of the binary Kasami code (cf. [1], p. 358); namely, one may replace the cubing map by $x \mapsto x^{s+1}$, where $s = 2^f$ and $GCD(f, 2t+1) = 1$. The above construction of a 5-class scheme extends to this more general case, where now G_1 and G_2 are defined by the equations $a + b = (x + y)^{s+1}$ and $a + b = xy(x^{s-1} + y^{s-1})$, etc.. But no new "scheme parameters" are obtained in this way; and we felt it would be better, both for ease of presentation and readability, to confine ourselves to the case $s = 2$.

LEMMA 3 *Given $d \neq 0$ and e in a finite field of characteristic two, then the equation $z^2 + dz + e = 0$ has (two) roots if and only if $Tr(ed^{-2}) = 0$.*

Lemma 3 is a standard result, and so its proof is omitted.

LEMMA 4

(i) G_3 equals $\Gamma_2(K_t)$, i.e. it is the distance-two graph of the Kasami graph G_1.

(ii) Similarly, G_4 is the distance-two graph of G_2.

Proof. The arguments for (i) and (ii) are essentially the same, so we only prove (i). Let (a, x) and (b, y) be two distinct vertices, and suppose that they have a common neighbour (c, z) in G_1. This means that the two equations $a+c = (x+z)^3$ and $b+c = (y+z)^3$ hold. Adding these equations and rearranging yields $(x+y)z^2+(x+y)^2z+a+b+x^3+y^3 = 0$. If $x = y$ then this forces $a = b$ and so $(a, x) = (b, y)$, contrary to our assumption; so $x + y \neq 0$. By Lemma 3 the above quadratic in z has (two) solutions if and only if

$$0 = Tr\left[\frac{a+b+x^3+y^3}{(x+y)^3}\right] = Tr\left[\frac{a+b}{(x+y)^3}\right] + Tr(1) + Tr\left[\frac{xy}{x^2+y^2}\right].$$

Note that $Tr(1) = 1$, since $GF(2^{2t+1})$ is an extension of $GF(2)$ of odd degree; also $Tr\left[\frac{xy}{x^2+y^2}\right] = Tr\left[\frac{xy+y^2+y^2}{x^2+y^2}\right] = Tr\left[\frac{y}{x+y}\right]+Tr\left[\left(\frac{y}{x+y}\right)^2\right] = 0$, since $Tr(w^2) = Tr(w)^2 = Tr(w)$ in general and so $Tr(w)+Tr(w^2) = 0$. Thus the quadratic $(x+y)z^2+(x+y)^2z+a+b+x^3+y^3 = 0$ has two roots z if and only if $x \neq y$ and $Tr\left[\frac{a+b}{(x+y)^3}\right] = 1$. Observe that if $a+b = (x+y)^3$, then the quadratic has the two roots $z = x$ and $z = y$ (and conversely); but these do not correspond to true common neighbours of (a, x) and (b, y), since loops are not allowed in G_1. We may thus conclude that the distinct vertices (a, x) and (b, y) have (two) common neighbours in G_1 if and only if $x \neq y$, $a+b \neq (x+y)^3$ and $Tr\left[\frac{a+b}{(x+y)^3}\right]$ equals 1. This is precisely the relation G_3. ∎

Let A_i be the adjacency matrix of the graph G_i. The assertion that the G_i's form an association scheme is equivalent to saying that the real linear span of the A_i's forms an algebra, i.e. each product A_iA_j equals $\sum_{k=0}^{5} p_{ij}^k A_k$ for suitable non-negative integers p_{ij}^k, called the intersection parameters. Thus to establish Theorem 2 we need to compute these products, or at least prove somehow that the p_{ij}^k's exist. Lemma 4 is a step in this direction: it easily implies that $A_1^2 = (2^{2t+1}-1)I + 2A_3$ and $A_2^2 = (2^{2t+1}-1)I + 2A_4$. Also, since G_1 and G_3 are relations in the three-class association scheme of a Kasami graph, it follows that A_1A_3 and A_3^2 are linear combinations of A_k's, and similarly so are A_2A_4 and A_4^2.

LEMMA 5 $A_1A_2 = A_2A_1 = A_3 + A_4 + A_5$.

Proof. Writing ax instead of (a, x) etc. for simplicity, we have

$$\begin{aligned}(A_1A_2)_{ax,by} &= \sum_{cz}(A_1)_{ax,cz}(A_2)_{cz,by} \\ &= \#\{(c, z) : a + c = (x + z)^3 \text{ and } b + c = yz(y + z)\}.\end{aligned}$$

Adding these two equations and rearranging leads to $a+b = (z+x+y)^3+(x+y)^3+x^3$. Since cubing is a bijection, we see that given (a, x) and (b, y) there exists a unique z

satisfying the previous equation. This means that A_1A_2 is a $(0,1)$-matrix and the off-diagonal zero entries of A_1A_2 correspond to those pairs (a,x) and (b,y) where $z=x$ or $z=y$ is the solution to the cubic. Now it easily follows that $A_1A_2 = J - I - A_1 - A_2 = A_3 + A_4 + A_5$. The argument for A_2A_1 is the same. ∎

LEMMA 6 *For all i, A_iA_5 is a linear combination of A_k's, i.e. the intersection parameters p^k_{i5} exist.*

Proof. Since G_5 has such a simple structure (it is a disjoint union of cliques of equal size), this is quite easy to check and so we omit the details. ∎

There is now enough information to complete the proof of Theorem 2. For example, why is A_1A_4 a linear combination of A_k's? We saw just before Lemma 5 that $A_2^2 = (2^{2t+1}-1)I + 2A_4$ or $A_4 = \frac{1}{2}(A_2^2 - (q-1)I)$ where $q := 2^{2t+1}$. Hence $A_1A_4 = \frac{1}{2}(A_1A_2^2 - (q-1)A_1) = \frac{1}{2}((J - I - A_1 - A_2)A_2 - (q-1)A_1)$ by Lemma 5. Applying Lemmas 4 and 5 once again yields the desired result. The remaining products go similarly, which proves Theorem 2.

2. The Eigenmatrices and Lattice of Fusion Schemes

The eigenmatrix of the 5-class scheme described in Theorem 2 is

$$P = \begin{bmatrix} 1 & 2^{2t+1}-1 & 2^{2t+1}-1 & (2^{2t}-1)(2^{2t+1}-1) & (2^{2t}-1)(2^{2t+1}-1) & 2^{2t+1}-1 \\ 1 & -2^{t+1}-1 & -1 & (2^t+1)^2 & -2^{2t}+1 & -1 \\ 1 & -1 & -2^{t+1}-1 & -2^{2t}+1 & (2^t+1)^2 & -1 \\ 1 & 2^{t+1}-1 & -1 & (2^t-1)^2 & -2^{2t}+1 & -1 \\ 1 & -1 & 2^{t+1}-1 & -2^{2t}+1 & (2^t-1)^2 & -1 \\ 1 & -1 & -1 & -2^{2t}+1 & -2^{2t}+1 & 2^{2t+1}-1 \end{bmatrix}$$

and the dual eigenmatrix Q is

$$\begin{bmatrix} 1 & 2^{t-1}(2^t-1)(2^{2t+1}-1) & 2^{t-1}(2^t-1)(2^{2t+1}-1) & 2^{t-1}(2^t+1)(2^{2t+1}-1) & 2^{t-1}(2^t+1)(2^{2t+1}-1) & 2^{2t+1}-1 \\ 1 & -2^{t-1}(2^t-1)(2^{t+1}+1) & -2^{t-1}(2^t-1) & 2^{t-1}(2^t+1)(2^{t+1}-1) & -2^{t-1}(2^t+1) & -1 \\ 1 & -2^{t-1}(2^t-1) & -2^{t-1}(2^t-1)(2^{t+1}+1) & -2^{t-1}(2^t+1) & 2^{t-1}(2^t+1)(2^{t+1}-1) & -1 \\ 1 & 2^{t-1}(2^t+1) & -2^{t-1}(2^t-1) & 2^{t-1}(2^t-1) & -2^{t-1}(2^t+1) & -1 \\ 1 & -2^{t-1}(2^t-1) & 2^{t-1}(2^t+1) & -2^{t-1}(2^t+1) & 2^{t-1}(2^t-1) & -1 \\ 1 & -2^{t-1}(2^t-1) & -2^{t-1}(2^t-1) & -2^{t-1}(2^t+1) & -2^{t-1}(2^t+1) & 2^{2t+1}-1 \end{bmatrix}$$

The derivation of these eigenmatrices is not difficult, given the following information. The two sets of graphs $\{G_0, G_1, G_3, G_2 \cup G_4 \cup G_5\}$ and $\{G_0, G_2, G_4, G_1 \cup G_3 \cup G_5\}$ are 3-class fusion schemes of our 5-class scheme; indeed they are the schemes of the Kasami graphs G_1 and G_2, respectively. The eigenmatrices of these 3-class schemes are known, cf. [3]; in conjunction with some elementary computations this yields the eigenmatrices P and Q above.

There are other fusion schemes of our 5-class scheme besides the two given above. The complete list of fusion schemes is given in Figure 1, which is presented as a sublattice of

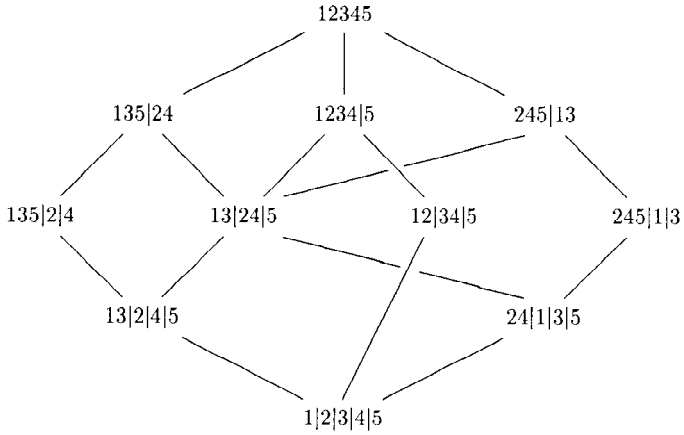

Figure 1. The lattice of fusion schemes.

the lattice of partitions of a 5-element set. For example "13|24|5" corresponds to the fusion scheme $\{G_0, G_1 \cup G_3, G_2 \cup G_4, G_5\}$. Recall ([6], p. 184) that fusion schemes of a given scheme correspond to certain row-equitable partitions of the eigenmatrix P; specifically, these are partitions of P into blocks such that each block has constant row sums (and the first row and first column of P each appear as singleton cells in the row and column partitions corresponding to the block partition). Thus one can find all fusion schemes by a careful inspection of P.

We shall not comment on all of the schemes in Figure 1, but one of them, namely 12|34|5, is particularly noteworthy.

PROPOSITION 7

(i) The scheme $\{G_0, G_1 \cup G_2, G_3 \cup G_4, G_5\}$ is a quotient of the underlying scheme of the distance-regular graph constructed in [2].

(ii) Conversely, given any 5-class association scheme having the same parameters as those of Theorem 2, then, letting A_1 and A_2 denote the adjacency matrices of the two connected relations of valency $2^{2t+1} - 1$, the matrix

$$M = \begin{bmatrix} A_1 & I + A_2 \\ I + A_2 & A_1 \end{bmatrix}$$

is the adjacency matrix of an antipodal distance-regular graph having the same parameters as those of [2].

Proof.

(i) Omitted; this is quite easy given the explicit description of the graphs in [2]. Incidentally, we recommend [7] for a deep study of quotient schemes.

(ii) Omitted; we should stress that this is simply a matter of the intersection parameters being what they should be, and so is independent of any explicit construction such as that of this paper. □

If $\mathcal{B}$ is an association scheme with eigenmatrix P and dual eigenmatrix Q, then another scheme $\mathcal{B}^*$ is called *formally dual* to $\mathcal{B}$ if it has eigenmatrix Q (and dual eigenmatrix P). This notion is due to Delsarte [5], who showed that in the case of a translation scheme $\mathcal{B}$, there is an explicit duality transform between $\mathcal{B}$ and a dual scheme $\mathcal{B}^*$; indeed, this is the familiar duality between a finite abelian group and its character group. In general, it appears that a formally dual pair $\mathcal{B}$ and $\mathcal{B}^*$ need not be structurally related. Now if $\mathcal{B}$ is the 5-class scheme of our Theorem 2 (or any scheme with the same parameters), then the existence of a formally dual scheme $\mathcal{B}^*$ appears feasible. By this we mean that the dual intersection parameters q_{ij}^k of $\mathcal{B}$, which must be nonnegative reals according to the Krein conditions, are in fact nonnegative integers and so could be the intersection parameters of some scheme $\mathcal{B}^*$ (which must then be formally dual to $\mathcal{B}$). In the second half of the present paper we will construct such a scheme. Note that our earlier construction via Kasami graphs is not a translation scheme (this follows from Proposition 7 and the results in [2]), although it seems tantalizingly close to one (e.g., the fusions 1|3|245 and 2|4|135 are each translation schemes). Thus one needs another approach; our construction will make use of quadratic forms and Kerdock sets over $GF(2)$. To motivate this approach we make the following remark. The schemes constructed in [2] are formally dual to the Cameron-Seidel scheme [4] of linked symmetric designs derived from quadratic forms and Kerdock sets over $GF(2)$. Since, by Proposition 7 above, the fusion scheme 12|34|5 is a quotient of the scheme of [2], and since "quotient scheme" and "subscheme" are dual concepts, it seemed natural to us to try and construct a formal dual to the 12|34|5 fusion scheme by locating a suitable subscheme of the Cameron-Seidel scheme. This is precisely how our construction proceeds; furthermore, by a natural fissionning method (here "natural" is in reference to vector space duality) we obtain a 5-class formal dual to our original 5-class scheme.

3. Schemes and Kerdock Sets

We begin with a brisk review of some basic concepts; our primary source is Cameron and Seidel [4], but see also Chapter 26 of Van Lint and Wilson [11]. Let V be a (finite-dimensional) vector space over $GF(2)$. A *quadratic form* is a map $Q : V \to GF(2)$ such that $Q(0) = 0$ and

$$B(x, y) := Q(x + y) + Q(x) + Q(y)$$

is bilinear. Note that B must be alternating, i.e. $B(x, x) = 0$ for all x. In this situation we say that Q lies over B and sometimes write $Q : B$. An arbitrary symmetric bilinear form $B(x, y)$ is said to be non-singular if the only vector x for which $B(x, y) = 0$ for all y is $x = 0$. An alternating bilinear form cannot be non-singular unless V has even dimension; thus in what follows we will suppose that $\dim(V) = 2t + 2$ for a positive integer t. (Of course this notation is chosen so as to agree with the first part of this paper.)

A quadratic form is called non-singular if its associated bilinear form is non-singular. Such a quadratic form Q has a type $\chi(Q) = \pm 1$, where Q has precisely $2^{2t+1} + \chi(Q)2^t$ zeroes. The projective quadrics associated to non-singular quadratic forms with $\chi = +1$ are called hyperbolic, those with $\chi = -1$ elliptic.

Let S be a set of alternating bilinear forms on V. If the sum of any two distinct members of S is non-singular, then S is called a non-singular set. It is not hard to show that S can have at most 2^{2t+1} members; when equality holds S is called a *Kerdock set*. The first construction of such maximal sets was given (for all t) by Kerdock [9]; whence the nomenclature. Kantor [8] gives a recent survey of Kerdock sets and their relation to finite geometry. We now proceed to the construction of some 5-class association schemes.

THEOREM 8 *In a vector space V of dimension $2t+2$ over $GF(2)$, fix a vector v in V and a linear form L on V such that $L(v) = 1$. Let S be a Kerdock set of alternating forms on V. Define a system of relations as follows. The vertex set consists of all ordered pairs (B, Q), where $B \in S$, Q lies over B and $Q(v) = 0$. For distinct pairs (B, Q) and (B', Q'), the possible relations are*

$$
\begin{aligned}
R_1 &: B \neq B', \chi(Q+Q') = -1 \quad \text{and} \quad \chi(Q+Q'+L) = -1;\\
R_2 &: B \neq B', \chi(Q+Q') = -1 \quad \text{and} \quad \chi(Q+Q'+L) = +1;\\
R_3 &: B \neq B', \chi(Q+Q') = +1 \quad \text{and} \quad \chi(Q+Q'+L) = +1;\\
R_4 &: B \neq B', \chi(Q+Q') = +1 \quad \text{and} \quad \chi(Q+Q'+L) = -1;\\
R_5 &: B = B' \quad \text{and} \quad Q \neq Q'.
\end{aligned}
$$

Then the relations R_i, together with the identity relation R_0, form an association scheme. This scheme is formally dual to the association scheme of Theorem 2.

The proof of Theorem 8 is rather laborious; we will present in detail several of the harder computations and skip most of the easier ones. Following Cameron and Seidel [4], our work will be facilitated by the use of a certain Gram matrix indexed by all quadratic forms on V. Let $\mathcal{F}$ be the 2^{2t+2}-dimensional rational vector space consisting of all rational-valued functions on V. To each quadratic form Q on V associate the function $\overline{Q}$ in $\mathcal{F}$ defined by $\overline{Q}(x) = 2^{-t-1}(-1)^{Q(x)}$. The definition of χ presented earlier for non-singular quadratic forms extends to all quadratic forms (cf. [4], Prop. 2). Letting (a, b) denote the standard inner product on $\mathcal{F}$, we have that $(\overline{Q}, \overline{Q'}) = 2^{-t-1}\chi(Q+Q')$ for all quadratic forms Q and Q' (cf. [4], Prop. 3). This observation is a key tool in proving Theorem 8, since it suggests that the computation of intersection parameters for the relations R_i can be expressed as certain (colossal) sums of $(+1)$'s and (-1)'s; for example, the above equation of Cameron and Seidel may be written as

$$\chi(Q+Q') = 2^{-t-1}\sum_{x \in V}(-1)^{Q(x)+Q'(x)} \quad .$$

Let G be the Gram matrix for all quadratic forms on V; thus $G_{Q,Q'}$ equals $(\overline{Q}, \overline{Q'})$. For each alternating bilinear form B, there are 2^{2t+2} quadratic forms that lie over B; thus G has a natural block partition (G_{ij}), where G_{ij} is the $2^{2t+2} \times 2^{2t+2}$ submatrix of G whose rows correspond to the quadratic forms $Q : B_i$ and the columns correspond to the $Q : B_j$.

Further, each G_{ij} has the decomposition

$$G_{ij} = \begin{bmatrix} C_{ij} & D_{ij} \\ D_{ij} & C_{ij} \end{bmatrix}$$

where the row and column indices of the upper left block correspond to those quadratic forms (over B_i and B_j respectively) that vanish at v. (Recall that v is a distinguished nonzero vector used to define the vertex set in Theorem 8). Since $Q(v) = 0$ if and only if $(Q + L)(v) = 1$ (where L is the distinguished linear form in Theorem 8), it is notationally sound to list row and column indices for G_{ij} as follows: if $Q_1, Q_2, \ldots$ is some listing of the quadratic forms that vanish at v, then we should list the forms that don't vanish at v as $Q_1, Q_2, \ldots$ also, with the understanding that in this range Q_r corresponds to $Q_r + L$. This is probably the most coherent notation for discussing matrix products such as $C_{ij}D_{jk}$, as we shall do in the sequel. Note that in the above block decomposition for G_{ij}, it is indeed true that the upper-left and lower-right blocks are equal to each other; this corresponds to the identity

$$\begin{aligned} (\overline{Q+L}, \overline{Q'+L}) &= 2^{-2t-2} \sum_{x \in V} (-1)^{(Q+L)(x)+(Q'+L)(x)} \\ &= 2^{-2t-2} \sum_{x \in V} (-1)^{Q(x)+Q'(x)} \\ &= (\overline{Q}, \overline{Q'}). \end{aligned}$$

Similarly, it is clear that the upper-right and lower-left blocks of G_{ij} are equal to each other. This 2×2 block decomposition of each G_{ij} induces a corresponding 2×2 decomposition of all of G, which we write as

$$G = \begin{bmatrix} C & D \\ D & C \end{bmatrix}.$$

Let us write $E = C \circ D$, the entrywise product of C and D. A typical entry of E is thus

$$E_{Q,Q'} = C_{Q,Q'} D_{Q,Q'} = 2^{-4t-4} \sum_{x,y \in V} (-1)^{Q(x)+Q'(x)+Q(y)+Q'(y)+L(y)} .$$

We are now almost ready to embark on a series of calculations that will establish Theorem 8. First we need to clarify the precise connection between the Gram matrix G and the relations defined in the statement of Theorem 8. Since our construction only uses the alternating bilinear forms B_i, $i = 1$ to 2^{2t+1}, in some given Kerdock set S, we restrict G to the principal submatrix corresponding to all quadratic forms lying over just the B_i's in S; but we use the same symbols G, C, D and E for these submatrices.

PROPOSITION 9 *Let A_i be the adjacency matrix of relation R_i described in Theorem 8, $i = 0, \ldots, 5$. Then:*

$$\begin{aligned} A_1 &= \tfrac{1}{4}(J - I - A_5) - 2^{t-1}(C - I) - 2^{t-1}D + 2^{2t}E, \\ A_2 &= \tfrac{1}{4}(J - I - A_5) - 2^{t-1}(C - I) + 2^{t-1}D - 2^{2t}E, \\ A_3 &= \tfrac{1}{4}(J - I - A_5) + 2^{t-1}(C - I) + 2^{t-1}D + 2^{2t}E, \\ A_4 &= \tfrac{1}{4}(J - I - A_5) + 2^{t-1}(C - I) - 2^{t-1}D - 2^{2t}E. \end{aligned}$$

Proof. Recall that, by the fundamental identity of Cameron and Seidel ([4], Prop. 3), $(\overline{Q}, \overline{Q'}) = 2^{-t-1}\chi(Q+Q')$, and hence in our notation $C_{Q,Q'} = 2^{-t-1}\chi(Q+Q')$, $D_{Q,Q'} = 2^{-t-1}\chi(Q+Q'+L)$ and hence $E_{Q,Q'} = C_{Q,Q'}D_{Q,Q'} = 2^{-2t-2}\chi(Q+Q')\chi(Q+Q'+L)$. Given this and the definition of the R_i's, it is now straightforward to verify the above matrix identities; we leave this to the reader. ∎

PROPOSITION 10

(i) $(A_5+I)C = C(A_5+I) = J$; $(A_5+I)D = D(A_5+I) = (A_5+I)E = E(A_5+I) = O$;

(ii) $JC = CJ = 2^{2t+1}J$; $JD = DJ = JE = EJ = O$;

(iii) $C^2 = 2^{2t}C + \frac{1}{2}J$; $D^2 = 2^{2t}C - \frac{1}{2}J$; $CD = DC = 2^{2t}D$;

(iv) $CE = EC = \frac{1}{2}D$; $DE = ED = \frac{1}{2}C - 2^{-2t-2}J$;

(v) $E^2 = -2^{-2t-3}(A_5 + I) + \frac{1}{4}I$.

It is clear from Propositions 9 and 10 how to go about obtaining expressions for the products A_iA_j as linear combinations of the A_k's; we will not carry out the very tedious details. Also we will only prove some parts of Proposition 10; our sample will cover all of the types of cancellative arguments that arise in these computations. We start with an easy one, namely the first equations in Proposition 10(i) and (ii). For this it clearly suffices to show that each C_{ij} has row sums one. It's easy to show $C_{ii} = I$ for all i; when $i \neq j$, fix $Q' : B_i$ and observe that the sum of the entries of the Q'-row of C_{ij} equals

$$\begin{aligned}\sum_{Q:B_j}(\overline{Q'}, \overline{Q}) &= 2^{-2t-2}\sum_{Q:B_j}\sum_{x\in V}(-1)^{Q'(x)+Q(x)} \\ &= 2^{-2t-2}\sum_{x\in V}(-1)^{Q'(x)}\sum_{Q:B_j}(-1)^{Q(x)}.\end{aligned}$$

Now if $x = 0$ or v then $\sum_{Q:B_j}(-1)^{Q(x)} = 2^{2t+1}$; recall that we only sum over those Q that vanish at v. If x is not 0 or v then $\sum_{Q:B_j}(-1)^{Q(x)} = 0$, which can be seen by fixing a linear form ϕ such that $\phi(x) = 1$, $\phi(v) = 0$, and noting that the involution $Q \mapsto Q + \phi$ pairs the Q's that vanish at x with those that don't. Thus we have

$$\sum_{Q:B_j}(\overline{Q'}, \overline{Q}) = 2^{-2t-2}\cdot 2^{2t+1}[(-1)^{Q'(0)} + (-1)^{Q'(v)}] = 1,$$

as desired.

Next we tackle the first equation in Proposition 10(iii). For the block matrices we have $(C^2)_{ik} = \sum_j C_{ij}C_{jk}$, where this sum has 2^{2t+1} terms, one for each alternating form B_j in the Kerdock set S. If $Q' : B_i$ and $Q'' : B_k$ are given, we compute

$$\begin{aligned}(C_{ij}C_{jk})_{Q',Q''} &= \sum_{Q:B_j}(C_{ij})_{Q',Q}(C_{jk})_{Q,Q''} \\ &= 2^{-4t-4}\sum_{Q:B_j}\sum_{x\in V}(-1)^{Q'(x)+Q(x)}\sum_{y\in V}(-1)^{Q(y)+Q''(y)}\end{aligned}$$

$$= 2^{-4t-4}\sum_{x,y}(-1)^{Q'(x)+Q''(y)}\sum_{Q:B_j}(-1)^{Q(x)+Q(y)}$$
$$= 2^{-4t-4}\sum_{x,y}(-1)^{Q'(x)+Q''(y)+B_j(x,y)}\sum_{Q:B_j}(-1)^{Q(x+y)}.$$

Observe that if $x+y\neq 0$ and $x+y\neq v$, then there exists a linear form ϕ with $\phi(x+y)=1$ and $\phi(v)=0$, from which it follows as before that $\sum_{Q:B_j}(-1)^{Q(x+y)}=0$. Hence,

$$(C_{ij}C_{jk})_{Q',Q''} = 2^{-2t-3}\sum_{x\in V}\Big[(-1)^{Q'(x)+Q''(x)}+(-1)^{Q'(x)+Q''(x+v)+B_j(x,v)}\Big]$$
$$= \tfrac{1}{2}C_{Q',Q''}+2^{-2t-3}\sum_{x}(-1)^{Q'(x)+Q''(x+v)+B_j(x,v)}.$$

Summing this over all j we get

$$(C^2)_{Q',Q''} = 2^{2t}C_{Q',Q''}+2^{-2t-3}\sum_{x}(-1)^{Q'(x)+Q''(x+v)}\sum_{j}(-1)^{B_j(x,v)}.$$

LEMMA 11 *If $x\neq 0$ and $x\neq v$, then $B_j(x,v)$ equals 0 and 1 equally often, as B_j ranges over a Kerdock set.*

Proof. Each linear form $\phi_j(y):=B_j(y,v)$ is well defined on the quotient space $V/\{0,v\}$. Let $x_1=x,x_2,\ldots,x_{2t+1}$ be a basis of $V/\{0,v\}$. Observe that the $(2t+1)\times 2^{2t+1}$ array $M_{ij}:=B_j(x_i,v)$ consists of all distinct binary columns of height $2t+1$; for, if two columns, say the j^{th} and k^{th}, were identical that would imply that B_j+B_k is singular, a contradiction. But then it follows that each row of M has exactly 2^{2t} zeroes and 2^{2t} ones. ∎

Continuing our calculation of C^2, we infer from Lemma 11 that

$$(C^2)_{Q',Q''} = 2^{2t}C_{Q',Q''}+\tfrac{1}{4}\Big[(-1)^{Q'(0)+Q''(v)}+(-1)^{Q''(0)+Q'(v)}\Big]$$
$$= 2^{2t}C_{Q',Q''}+\tfrac{1}{2};$$

since Q' and Q'' are arbitrary quadratic forms vanishing at v we have obtained the sought-for equation $C^2=2^{2t}C+\frac{1}{2}J$. We note in passing that the second equation in Proposition 10(iii) does not have a typographical error: there is a certain asymmetry between C and D.

Two more parts of Proposition 10 will be proved in detail, namely the first equation of (iv) and then (v). As with C^2, we will calculate CE on each block: $(CE)_{ik}=\sum_j C_{ij}E_{jk}$. For each $Q':B_i$ and $Q'':B_k$ we have, since $E=C\circ D$,

$$(C_{ij}E_{jk})_{Q',Q''} = \sum_{Q:B_j}C_{Q',Q}C_{Q,Q''}D_{Q,Q''}$$
$$= 2^{-6t-6}\sum_{Q:B_j}\sum_{x\in V}(-1)^{Q'(x)+Q(x)}\sum_{y\in V}(-1)^{Q(y)+Q''(y)}\sum_{z\in V}(-1)^{Q(z)+Q''(z)+L(z)}$$
$$= 2^{-6t-6}\sum_{x,y,z}(-1)^{Q'(x)+Q''(y)+Q''(z)+L(z)}\sum_{Q:B_j}(-1)^{Q(x)+Q(y)+Q(z)}$$
$$= 2^{-6t-6}\sum_{x,y,z}(-1)^{Q'(x)+Q''(y)+Q''(z)+L(z)+B_j(x,y)+B_j(x+y,z)}\sum_{Q:B_j}(-1)^{Q(x+y+z)}.$$

Now if $x + y + z \neq 0$ and $x + y + z \neq v$, then (by an argument used twice already) it follows that the inner sum over $Q : B_j$ vanishes. Hence the above expression is equal to

$$2^{-4t-5} \sum_{x,y} (-1)^{Q'(x)+Q''(x)+L(x)+L(y)+B_{jk}(x,y)}[1 - (-1)^{B_{jk}(x+y,v)}]$$

where we have set $B_{jk} := B_j + B_k$ for convenience; and replacing y by $y + x$ yields the slightly simpler expression

$$2^{-4t-5} \sum_{x} (-1)^{Q'(x)+Q''(x)} \sum_{y} (-1)^{L(y)+B_{jk}(x,y)}[1 - (-1)^{B_{jk}(y,v)}].$$

We now analyze the inner summation over y (thinking of x as fixed). If $B_{jk}(y, v) = 0$ then $1 - (-1)^{B_{jk}(y,v)}$ equals zero, and so we need only consider the inner summation over those y's where $B_{jk}(y, v) = 1$, hence the summation becomes

$$2 \sum_{y:B_{jk}(y,v)=1} (-1)^{L(y)+B_{jk}(x,y)}.$$

But now observe that this sum usually vanishes: if the linear form $L(y) + B_{jk}(x, y)$, as a function of y, is not the zero form, and if the linear forms $L(y) + B_{jk}(x, y)$ and $B_{jk}(v, y)$ are not equal forms, then it is not hard to see that the above summation vanishes. For the two exceptional cases we need the following lemma.

LEMMA 12

(i) For each non-singular alternating form B, there exists a unique $x \in V$ such that $B(x, y) = L(y)$ for all y. When $B = B_{jk}$ with $j \neq k$ let us denote this unique x by x_{jk}.

(ii) For k fixed the set $\{x_{jk}\}$, as $j \neq k$ varies over the indices of a Kerdock set, equals the set of non- zero vectors in the kernel of L.

Proof.

(i) Left to the reader.

(ii) Clearly each x_{jk} is non-zero and lies in the kernel of L. On the other hand, for distinct j's (say j_1 and j_2) the corresponding x_{jk}'s are distinct, otherwise one would easily derive the contradiction that $B_{j_1} + B_{j_2}$ is singular. Since a Kerdock set has the same number of elements as ker$L$, we are done. □

We may now wrap up our computation of CE. Using Lemma 12(i) it is straightforward to check that everything reduces to

$$(C_{ij}E_{jk})_{Q',Q''} = 2^{-2t-3}[(-1)^{Q'(x_{jk})+Q''(x_{jk})} - (-1)^{Q'(x_{jk}+v)+Q''(x_{jk}+v)}]$$

when $j \neq k$; and when $j = k$ we have $C_{ij}E_{jj} = 0$, since E_{jj} itself is zero. Therefore

$$\begin{aligned}(CE)_{Q',Q''} &= 2^{-2t-3}\sum_{j:j\neq k}[(-1)^{Q'(x_{jk})+Q''(x_{jk})} - (-1)^{Q'(x_{jk}+v)+Q''(x_{jk}+v)}]\\ &= 2^{-2t-3}\sum_{0\neq y\in\ker L}[(-1)^{(Q'+Q'')(y)} - (-1)^{(Q'+Q'')(y+v)}]\\ &\quad \text{(by Lemma 12(ii))}\\ &= 2^{-2t-3}\sum_{0\neq y\in\ker L}[(-1)^{(Q'+Q''+L)(y)} + (-1)^{(Q'+Q''+L)(y+v)}]\\ &= 2^{-2t-3}\sum_{y\in V}(-1)^{(Q'+Q''+L)(y)} = \tfrac{1}{2}D_{Q',Q''}\ ;\end{aligned}$$

and so finally $CE = \frac{1}{2}D$. Because of symmetry we have $EC = CE = \frac{1}{2}D$ also.

Finally, we shall work out the last identity stated in Proposition 10. As before we have to compute block-matrix products $E_{ij}E_{jk}$. If $i = j$ or $j = k$ then this product is the zero matrix. So we may assume that $i \neq j$ and $j \neq k$; if $Q' : B_i$ and $Q'' : B_k$ then $2^{8t+8}(E_{ij}E_{jk})_{Q',Q''}$ equals

$$\begin{aligned}&\sum_{Q:B_j}\sum_{x,y,z,w}(-1)^{Q'(x)+Q(x)+Q'(y)+Q(y)+L(y)+Q(z)+Q''(z)+Q(w)+Q''(w)+L(w)}\\ &\qquad = \sum_{x,y,z,w}(-1)^{Q'(x)+Q'(y)+L(y)+Q''(z)+Q''(w)+L(w)}\sum_{Q:B_j}(-1)^{Q(x)+Q(y)+Q(z)+Q(w)}.\end{aligned}$$

Note that $Q(x)+Q(y)+Q(z)+Q(w) = Q(x+y+z+w)+B_j(x,y)+B_j(x+y,z)+B_j(x+y+z,w)$ for each $Q : B_j$; and, by a previous argument, if $x+y+z+w \neq 0$ and $x+y+z+w \neq v$ then the sum of minus one to the power $Q(x+y+z+w)$, summed over $Q : B_j$, vanishes. Thus we are left with only $w = x+y+z$ or $w = x+y+z+v$; after some elementary manipulations, and writing $B_{jk} = B_j + B_k$ as before, putting $Q^\dagger := Q' + Q''$ and replacing z by $z+x+y$ one is led to the following expression for $2^{6t+7}(E_{ij}E_{jk})_{Q',Q''}$:

$$\sum_{x,y}(-1)^{Q^\dagger(x)+Q^\dagger(y)+L(y)+B_{jk}(x,y)}\sum_{z}(-1)^{L(z)+B_{jk}(x+y,z)}[1-(-1)^{B_{jk}(z,v)}].$$

Similarly to the analysis for the product CE, one finds that, for given x and y, the inner sum over z vanishes unless the linear form L equals $B_{jk}(x+y,\cdot)$ or equals $B_{jk}(x+y+v,\cdot)$. Recalling the vector x_{jk} from Lemma 12, it is then routine to show that the previous expression for $(E_{ij}E_{jk})_{Q',Q''}$ boils down to

$$\begin{aligned}&2^{-4t-5}\sum_{x\in V}(-1)^{Q^\dagger(x)+Q^\dagger(x+x_{jk})}[1+(-1)^{B_{ik}(x+x_{jk},v)+B_{jk}(x,v)}]\\ &\qquad = 2^{-4t-5}(-1)^{Q^\dagger(x_{jk})}\sum_{x}(-1)^{B_{ik}(x,x_{jk})}[1+(-1)^{B_{ij}(x,v)+B_{ik}(x_{jk},v)}].\end{aligned}$$

We now claim that if $i \neq k$ then this last sum over x vanishes. Indeed, this sum clearly equals

$$2\sum_{x}(-1)^{B_{ik}(x,x_{jk})}$$

where x is restricted to the range where $B_{ij}(x, v) = B_{ik}(x_{jk}, v)$. Therefore, unless the (non-zero) linear forms $B_{ik}(\cdot, x_{jk})$ and $B_{ij}(\cdot, v)$ are equal, the sum must be zero. But indeed the forms in question are *not* equal, for if so we derive the contradiction $0 = B_{ij}(v, v) = B_{ik}(v, x_{jk}) = B_{ij}(v, x_{jk}) + B_{jk}(v, x_{jk}) = B_{ij}(v, x_{jk}) + L(v) = B_{ik}(x_{jk}, x_{jk}) + 1 = 1$.

Thus we have shown that $(E_{ij}E_{jk})_{Q',Q''} = 0$ if $i \neq k$. (Recall that $i \neq j$ and $j \neq k$ was assumed at the outset.) If $i = k$ then

$$\begin{aligned}(E_{ij}E_{ji})_{Q',Q''} &= 2^{-4t-5}(-1)^{Q^\dagger(x_{ji})}\sum_x [1 + (-1)^{B_{ij}(x,v)}] \\ &= 2^{-2t-3}(-1)^{Q^\dagger(x_{ji})}.\end{aligned}$$

Hence, if Q' and Q'' lie over the same alternating form B_i, then

$$\begin{aligned}(E^2)_{Q',Q''} &= \sum_j (E_{ij}E_{ji})_{Q',Q''} \\ &= 2^{-2t-3}\sum_j (-1)^{Q^\dagger(x_{ji})} \\ &= 2^{-2t-3}\sum_{0\neq y\in \ker L} (-1)^{Q^\dagger(y)} \quad \text{(by Lemma 12(ii))} \\ &= \begin{cases} -2^{-2t-3}, & \text{if } Q^\dagger \neq 0 \text{ (i.e. } Q' \neq Q'') \\ 2^{-2t-3}(2^{2t+1}-1), & \text{if } Q' = Q''. \end{cases}\end{aligned}$$

This easily yields $E^2 = -2^{-2t-3}(A_5 + I) + \frac{1}{4}I$, as desired.

The dual version of Proposition 7(ii) is the following.

PROPOSITION 13 *Given any 5-class association scheme having the same parameters as those of Theorem 8, then the matrix*

$$M = \begin{bmatrix} A_1 + A_2 & A_1 + A_4 \\ A_1 + A_4 & A_1 + A_2 \end{bmatrix}$$

is the incidence matrix of a system of $2^{2t+1}-1$ *linked symmetric* 2-$(2^{2t+2}, 2^{2t+1}-2^t, 2^{2t}-2^t)$ *designs (i.e., it is the adjacency matrix of one of the graphs in a 3-class association scheme with the same parameters as the Cameron-Seidel scheme).*

Proof. This is, like Proposition 7(ii), just a matter of parameters. ■

4. Concluding Remarks

When $t = 1$ the schemes described in Theorem 2 and Theorem 8 have the same parameters; in other words the eigenmatrices P and Q coincide and we have a formally self-dual situation. Presumably our two constructions yield isomorphic schemes in this case, but we have not checked it. (After seeing a first draft of this paper, Rudi Mathon informed us that, when $t = 1$, a scheme with these parameters has also been implicitly constructed by himself and Anne Penfold Street; see p. 102 of [12].) Note that when $t = 1$ the Kasami coset graph

is essentially unique; indeed the graph parameters are that of the folded 7-cube, which is uniquely determined by its intersection array ([1], Thm. 9.2.7). When $t \geq 2$ there are several distinct binary Kasami codes (as remarked after the statement of our Theorem 2); from the work in [2] and Proposition 7 it follows that the resulting 5-class schemes are not isomorphic. In the same vein, it is known that when $2t + 1$ is composite there are inequivalent Kerdock sets (cf. [8], §3.9). These may well yield non-isomorphic 5-class schemes, but we have not pursued the matter.

It is known that formally dual pairs of association schemes have the same lattice of fusion schemes (cf. [6], bottom of p. 185). Hence the schemes of our Theorem 8 have the fusion schemes sketched in Figure 1; we were careful to list the relations R_i in the correct order, i.e., note that 14|23|5 is *not* a fusion scheme, whereas 12|34|5 and 13|24|5 are so.

Acknowledgments

Financial support has been provided by a grant from NSERC of Canada. We thank David Gregory for his help.

References

1. A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-regular graphs*, Springer-Verlag (1989).
2. D. de Caen, R. Mathon and G. E. Moorhouse, A family of antipodal distance-regular graphs related to the classical Preparata codes, *Journal of Algebraic Combinatorics*, Vol. 4 (1995) pp. 317–327.
3. A. R. Calderbank and J.-M. Goethals, Three-weight codes and association schemes, *Philips Journal of Research*, Vol. 39 (1984) pp. 143–152.
4. P. J. Cameron and J. J. Seidel, Quadratic forms over $GF(2)$, *Proc. Koninkl. Nederl. Akademie van Wetenschappen, Series A*, Vol. 76 *Indag. Math.*, Vol. 35 (1973) pp. 1–8.
5. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Research Reports Suppl.*, Vol. 10 (1973) 97 pages.
6. C. D. Godsil, Equitable partitions, *Combinatorics, Paul Erdös is Eighty*, Volume 1, János Bolyai Math. Soc., Budapest (1993) pp. 173–192.
7. C. D. Godsil and W. J. Martin, Quotients of association schemes, *Journal of Combinatorial Theory A*, Vol. 69 (1995) pp. 185–199.
8. W. M. Kantor, Orthogonal spreads and translation planes, *Advanced Studies in Pure Mathematics*, Vol. 24, *Progress in Algebraic Combinatorics*, Math. Soc. Japan, Tokyo (1996) pp. 227-242.
9. A. M. Kerdock, A class of low-rate nonlinear binary codes, *Information and Control*, Vol. 20 (1972) pp. 182–187.
10. J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag (1982).
11. J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge Univ. Press (1992).
12. R. Mathon and A. Penfold Street, Overlarge sets and partial geometries, *Journal of Geometry*, Vol. 60 (1997) pp. 85–104.