$\mathbb{Z}_4$-KERDOCK CODES, ORTHOGONAL SPREADS, AND EXTREMAL EUCLIDEAN LINE-SETS

A. R. CALDERBANK, P. J. CAMERON,
W. M. KANTOR, *and* J. J. SEIDEL

[Received 27 November 1995—Revised 25 July 1996]

1. *Introduction*

Kerdock and Preparata codes are non-linear binary codes that contain more codewords than any comparable linear codes presently known; see [**6**, **20**, **29**, **28**]. These codes have excellent error-correcting capabilities and have the remarkable property of being 'formal duals', in the sense that although these codes are non-linear, the distance distribution of either is the MacWilliams transform of the distance distribution of the other (see MacWilliams and Sloane [**28**, Chapter 15]). Kerdock and Preparata codes exist for all lengths $2^{m+1} \geqslant 16$, where throughout this introduction m will denote an odd integer greater than or equal to 3. If $2^{m+1} > 16$, these codes are not unique in the sense that several codes exist with the same weight distributions [**3**, **16**, **17**, **18**, **26**].

Recently, Hammons, Kumar, Calderbank, Sloane and Solé [**14**] showed that the Kerdock and Preparata codes can be very simply constructed as binary images under a certain natural map, called the *Gray map*, of linear codes over $\mathbb{Z}_4$ (although this requires a slight modification of the notion of 'Preparata' codes: the new ones and the classical ones have the same weight distribution but they are not isomorphic if $2^{m+1} > 16$). The Gray map will be defined and studied later in § 8. For now we note its main property: *it is an isometry* ($\mathbb{Z}_4^N$, Lee metric) $\to$ ($\mathbb{Z}_2^{2N}$, Hamming metric), where the Lee metric is a standard metric defined in § 8.

One of the main results of the present paper is an explanation of the Gray map in terms of suitable finite groups and geometries (Theorem 8.3). *En route* to this, we will see connections between the geometry of binary orthogonal and symplectic vector spaces on the one hand, and extremal real and complex line-sets having only two angles on the other. Extraspecial groups will be the source of these connections.

This research can be viewed as beginning in a paper by Cameron and Seidel [**9**]. That paper used quadratic forms on $\mathbb{Z}_2^{m+1}$ in order to construct a family of $\frac{1}{2}N^2$ lines through the origin of $\mathbb{R}^N$, where $N = 2^{m+1}$, such that any two are either perpendicular or at an angle θ, where $\cos\theta = 1/\sqrt{N}$. In fact, their line-sets were unions of $\frac{1}{2}N$ frames (that is, N pairwise orthogonal 1-spaces); these sets appear in the right-hand portion of Corollary 3.5 (but in notation quite different from that of [**9**]). Recently, König [**22**] observed that this line-set is not extremal (also see Levenštein [**25**]). While constructing the isometric embedding $\ell_2^N \to \ell_4^{N(N+1)/2}$ (cf.

Research of W. M. Kantor was supported in part by NSF and NSA grants.

1991 *Mathematics Subject Classification*: primary 94B60; secondary 51M15, 20C99.

Lyubich and Vaserstein [**27**]) he augmented the set of $\frac{1}{2}N^2$ lines from [**9**] by the standard coordinate frame. This did not increase the set of prescribed angles (this observation also is tucked into Corollary 3.5). The augmented system of lines meets an upper bound obtained by Delsarte, Goethals and Seidel [**11**]. Whereas their proof used Jacobi polynomials, we will give a proof of this upper bound in § 2 using elementary tensor algebra; we will also discuss the graph-theoretic structure of any system of lines meeting the upper bound.

The construction in [**9**] used binary Kerdock codes. Therefore, it was natural to imitate that construction by using the $\mathbb{Z}_4$-linear Kerdock code of length $N' = 2^m$ discovered by Hammons *et al.* [**14**]. This results in a set of N'^2 lines in $\mathbb{C}^{N'}$ that are either perpendicular or at an angle θ', where $\cos\theta' = 1/\sqrt{N'}$. Once again, this set is a union of pairwise disjoint frames (this set appears later in the right-hand portion of Corollary 5.7). Adding the coordinate frame extends this to a line-set in $\mathbb{C}^{N'}$ of size $N'^2 + N'$ which has these angles but meets another upper bound; this result is due to Delsarte, Goethals and Seidel [**11**].

The extremal real and complex line-sets in the preceding two paragraphs were constructed by adding the standard coordinate frame to a line-set arising from a version of a Kerdock code. This construction seemed to us too 'inhomogeneous', in the sense that the line-set was a union of frames, but one frame was somehow distinguished. This raised the question of whether there might be a more uniform description of all of the frames, a description that did not involve singling out any one frame. This question also suggested a direction in which to look for an answer: a similar situation had been encountered in other research concerning binary Kerdock codes.

Kantor [**16**, I] investigated connections between orthogonal spreads and Kerdock sets. When the vector space $\mathbb{Z}_2^{2m+2}$ is equipped with the quadratic form $x_1x_{m+2} + x_2x_{m+3} + \ldots + x_{m+1}x_{2m+2}$, there are $(2^{m+1} - 1)(2^m + 1)$ singular points (that is, 1-spaces on which the form vanishes), comprising a hyperbolic quadric in the corresponding projective space. An *orthogonal spread* is a partition of this set of points into $2^m + 1$ totally singular $(m + 1)$-spaces. In [**16**, I], orthogonal spreads are used to construct Kerdock codes and vice versa. We will review this correspondence in § 3. As in the preceding paragraph, the construction *also* distinguishes one (arbitrary) member of the spread as part of the relationship with Kerdock codes (see the remark following Corollary 3.5 below). This was too much of a coincidence, suggesting that there had to be some way to pass between the binary world of orthogonal spreads and the real or complex world of frames and line-sets.

Most of this paper is concerned with the bridge between these differently-flavoured geometries: extraspecial 2-groups. Section 2 describes the groups we require, as well as their unique faithful irreducible real representations. There is nothing new here from a group-theoretic point of view. Each such group E has order 2^{1+2k} for some integer k, and arises as a group of isometries of the Euclidean space $\mathbb{R}^{2^k}$. On the other hand, $E/Z(E)$ naturally inherits a quadratic form, producing the desired binary geometry. Section 3 describes how these two geometries associated with E produce extremal real line-sets when $k = m + 1$ and m is odd as before.

In §§ 4 and 5 we change groups slightly in order to connect symplectic spreads, $\mathbb{Z}_4$-Kerdock codes and extremal complex line-sets. In § 6 we describe how to

pass from extremal line-sets in $\mathbb{R}^{2^{m+1}}$ derived from orthogonal spreads to extremal line-sets in $\mathbb{C}^{2^m}$ derived from symplectic spreads.

Section 7 gives a simple geometric construction of an orthogonal spread in $E/Z(E)$ starting with a symplectic spread (taken from Kantor [**16**, I]). A geometric correspondence between symplectic and orthogonal spreads is also expressed in computational terms as a correspondence between binary symmetric $m \times m$ matrices and binary skew-symmetric $(m+1) \times (m+1)$ matrices.

Symplectic spreads in a binary vector space determine $\mathbb{Z}_4$-Kerdock codes, while orthogonal spreads determine binary Kerdock codes. In Theorem 8.3 we show that the geometric/group-theoretic map from symplectic spreads to orthogonal spreads induces the Gray map from a corresponding Kerdock code over $\mathbb{Z}_4$ to its binary image.

Examples of Kerdock and Preparata codes are given in § 9. Code equivalence is discussed at length in § 10. Large numbers of inequivalent $\mathbb{Z}_4$-Kerdock codes are constructed (using results of Kantor [**18**]). We will see that the construction of new $\mathbb{Z}_4$-linear Preparata codes amounts to the construction of certain types of affine translation planes and certain types of division algebras (Proposition 8.9 and Corollary 8.11). Using this we will obtain $\mathbb{Z}_4$-linear Preparata codes not equivalent to those constructed by Hammons *et al.* [**14**].

Finally, in § 11 we consider the analogue of the binary case using extraspecial p-groups for odd primes p, in order to relate symplectic spreads and extremal line-sets in $\mathbb{C}^{p^m}$. However, the behaviour of extraspecial groups when p is odd is known to be quite different from that when $p = 2$. In particular, orthogonal geometry does not enter at all, nor does any analogue of Kerdock codes.

For the convenience of the reader we have included a 'road map' of the paper in Table 1. Numbers in parentheses indicate Sections.

2. *Extraspecial 2-groups*

Let k be a fixed positive integer and let $N = 2^k$. In later sections we will take $k = m+1$ when considering orthogonal spreads and $k = m$ when considering symplectic spreads.

For a prime p, a p-group P is said to be *extraspecial* if the centre $Z(P)$ has order p and if $P/Z(P)$ is elementary abelian (and hence a vector space over $\mathrm{GF}(p)$).

We begin with a description of an extraspecial 2-group $E = E_k$ of order 2^{1+2k} as an irreducible group of orthogonal $N \times N$ matrices with real entries. Since E has 2^{2k} distinct linear characters and $2^{1+2k} = 2^{2k} \cdot 1^2 + (2^k)^2$, this will be the unique faithful irreducible representation of E. We also construct explicitly a group L of real orthogonal transformations containing E as a normal subgroup. Elements of L act on E by conjugation, fixing the centre $Z(E)$ of order 2. Hence there is a well-defined action on the elementary abelian group $\overline{E} = E/Z(E)$ of order 2^{2k}. We will see that this action on $\overline{E}$ preserves an explicit non-singular quadratic form Q, providing a bridge between binary orthogonal and real orthogonal geometry.

Let V denote the vector space $\mathbb{Z}_2^k$. For $x, y \in V$, let $x \cdot y$ denote the usual dot product.

Equip $\mathbb{R}^N$ with the usual inner product, and let $O(\mathbb{R}^N)$ denote the corresponding group of orthogonal linear transformations. We will tend to identify orthogonal matrices with the corresponding orthogonal transformations.

TABLE 1. *A map of* §§ 2–10

Discrete $\mathbb{Z}_2$*-world* (3)		*Real world* (2)
		$O(\mathbb{R}^{2^{m+1}})$
		$\vert$ $L \leqslant N_{O(\mathbb{R}^{2^{m+1}})}(E)$
$\overline{E} = E/Z(E)$ elementary abelian of order $2^{2(m+1)}$		L $L/E \cong O^+(2m+2,2)$
		$\vert$
		E extraspecial 2-group of order $2^{1+2(m+1)}$
induced action on $\overline{E}$ preserving the quadratic form $Q(\bar{e}) = e^2$	(2), (3) $\longleftrightarrow$	L acts on E by conjugation
orthogonal spread Σ: partition of the $(2^{m+1}-1)(2^m+1)$ singular points by 2^m+1 totally singular $(m+1)$-spaces	(3) $\longrightarrow$	collection $\mathcal{F}(\Sigma)$ of 2^m+1 orthogonal frames each containing 2^{m+1} 1-spaces
(6) $\downarrow$ $\downarrow$ (7)		$\downarrow$ Gray Map (8), (9), (10)
symplectic spread Σ': partition of the $(2^m-1)(2^m+1)$ points by 2^m+1 totally isotropic m-spaces	(5) $\longrightarrow$	collection $\mathcal{F}(\Sigma')$ of 2^m+1 unitary frames each containing 2^m complex 1-spaces
induced action on $\overline{F}$ preserving the alternating form $(\overline{f}_1, \overline{f}_2) = [f_1, f_2]$	(4), (5) $\longleftrightarrow$	$L^\natural$ acts on F by conjugation
		$U(\mathbb{C}^{2^m})$
		$\vert$ $L^\natural \leqslant N_{U(\mathbb{C}^{2^m})}(F)$
$\overline{F} = F/Z(F)$ elementary abelian of order 2^{2m}		$L^\natural$ $L^\natural/F \cong \mathrm{Sp}(2m,2)$
		$\vert$
		$F = E^\natural\langle iI\rangle$ 2-group of order 2^{2+2m}
Discrete $\mathbb{Z}_4$*-world* (5)		*Complex world* (4)

Label the standard basis of $\mathbb{R}^N$ as e_v, with $v \in V$. For $b \in V$, define the permutation matrix $X(b)$ and diagonal matrix $Y(b)$ as follows:

$$X(b)\colon\ e_v \to e_{v+b} \quad \text{and} \quad Y(b) := \mathrm{diag}[(-1)^{b\cdot v}].$$

The groups $X(V) := \{X(b) \mid b \in V\}$ and $Y(V) := \{Y(b) \mid b \in V\}$ are contained in $O(\mathbb{R}^N)$ and are isomorphic to the additive group V. Let $E := \langle X(V), Y(V)\rangle$;

this is an irreducible subgroup of $O(\mathbb{R}^N)$. We will spend most of this paper examining E, in spite of the fact that this group, and this representation, have been thoroughly investigated within group-theoretic contexts [**15**, pp. 355–357; **1**, p. 109; **32**, pp. 97–98; **21**, pp. 148–155].

LEMMA 2.1. *The group* $E = \langle X(V), Y(V)\rangle$ *is extraspecial of order* 2^{1+2k}, *and* $Z(E) = \langle -I\rangle$. *Moreover,* $E = X(V)Y(V)\langle -I\rangle$, *and every element of* E *can be written uniquely in the form* $X(a)Y(b)(-I)^\gamma$ *for some* $a, b \in V$ *and* $\gamma \in \mathbb{Z}_2$.

Proof. For all $a, b \in V$,

$$X(a)^{-1}Y(b)^{-1}X(a)Y(b) = (-1)^{a\cdot b}I \tag{2.2}$$

since

$$\begin{aligned} e_v(X(a)^{-1}Y(b)^{-1}X(a)Y(b)) &= [(-1)^{b\cdot(v+a)}e_{v+a}](X(a)Y(b)) \\ &= (-1)^{b\cdot(v+a)}(-1)^{b\cdot v}e_v. \end{aligned}$$

It follows that multiplication in E is given by the formula

$$\begin{aligned} (X(a)Y(b)(-I)^\gamma)(X(a')Y(b')(-I)^{\gamma'}) &= X(a)(Y(b)X(a'))Y(b')(-I)^{\gamma+\gamma'} \\ &= X(a+a')Y(b+b')(-I)^{\gamma+\gamma'+a'\cdot b} \end{aligned} \tag{2.3}$$

for all $a, b, a', b' \in V$ and $\gamma, \gamma' \in \mathbb{Z}_2$. Hence $E = X(V)Y(V)\langle -I\rangle$, $Z(E) = \langle -I\rangle$, and $E/Z(E) \cong V \oplus V$. The uniqueness assertion is clear.

The natural map from E to $\overline{E} = E/Z(E)$ will be used very frequently; an overbar will signify an image under this map (for example, the image of $X(a)$ will be denoted $\overline{X}(a)$).

We identify the centre $Z(E)$ of E with $\mathbb{Z}_2$ and consider the map $Q\colon \overline{E} \to \mathbb{Z}_2$ defined by $Q(\overline{e}) = e^2$ for any $\overline{e} \in \overline{E}$ and any preimage e of $\overline{e}$ in E. Then Q is a non-singular quadratic form on $\overline{E}$. The associated alternating bilinear form on $\overline{E}$ is given by $(\overline{e}_1, \overline{e}_2)_{\overline{E}} = [e_1, e_2]$, where $[x, y] = x^{-1}y^{-1}xy$ denotes the commutator of x and y; we will generally drop the subscript '$\overline{E}$' when there is no possibility of confusion with the inner product on $\mathbb{R}^N$. From (2.3) and (2.2) we have

$$Q(\overline{X}(a)\overline{Y}(b)) = a \cdot b, \tag{2.4}$$

$$(\overline{X}(a)\overline{Y}(b),\ \overline{X}(a')\overline{Y}(b')) = a \cdot b' - a' \cdot b. \tag{2.5}$$

Note that the k-spaces $\overline{X}(V)$ and $\overline{Y}(V)$ are *totally singular*: the quadratic form Q vanishes on each of them. Also, $\overline{X}(V) \cap \overline{Y}(V) = 0$. Hence, $\overline{E}$ is an $\Omega^+(2k, 2)$-space: it has maximal Witt index (or, equivalently, the associated quadric is hyperbolic). For more information about extraspecial groups and quadratic forms we refer the reader to various texts [**15**, pp. 355–357; **1**, p. 109; **32**, pp. 97–98; **33**].

We will require isometries of $\mathbb{R}^N$ that normalize E. These isometries normalize the centre $Z(E)$, act on $\overline{E}$ by conjugation, and induce isometries of $\overline{E}$. Of particular interest is the matrix

$$H = \frac{1}{\sqrt{N}}[(-1)^{u\cdot v}]_{u,v\in V}. \tag{2.6}$$

Here $\sqrt{N}H$ is the k-fold Kronecker product of the 2×2 Hadamard matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ (so that $H^2 = I$) and is also the character table of V (the equation $H^2 = I$ expresses orthogonality of characters). We have

$$\begin{aligned} e_a HX(b)H &= \left(\frac{1}{\sqrt{N}} \sum_v (-1)^{a\cdot v} e_{v+b}\right) H \\ &= \frac{1}{N} \sum_{v,w} (-1)^{a\cdot v + (v+b)\cdot w} e_w \\ &= \frac{1}{N} \sum_w (-1)^{a\cdot b} \left(\sum_v (-1)^{(a+w)\cdot(v+b)} \right) e_w \\ &= (-1)^{a\cdot b} e_a, \end{aligned}$$

from which it follows that

$$H^{-1}X(b)H = HX(b)H = Y(b). \tag{2.7}$$

Define the unit vector

$$e_b^* := \frac{1}{\sqrt{N}} \sum_v (-1)^{b\cdot v} e_v \tag{2.8}$$

to be the 'bth' row of H.

In addition to the standard basis of $\mathbb{R}^N$ we will need to choose a basis of $\overline{E}$. Let $v_1, \ldots, v_k$ denote the standard basis of $V = \mathbb{Z}_2^k$. This determines bases $x_1, \ldots, x_k$ of $\overline{X}(V)$ and $y_1, \ldots, y_k$ of $\overline{Y}(V)$, namely $x_j = \overline{X}(v_j)$ and $y_j = \overline{Y}(v_j)$. These are essentially 'dual' bases of $\overline{X}(V)$ and $\overline{Y}(V)$ with respect to $(\ ,\ )_{\overline{E}}$: $(x_i, y_j) = \delta_{ij}$ for all i, j. We will always write matrices of linear transformations on $\overline{E}$ with respect to the ordered basis $x_1, \ldots, x_k, y_1, \ldots, y_k$. By (2.7), H induces the map $x_j \leftrightarrow y_j$ on $\overline{E}$.

Every matrix A in the general linear group $\mathrm{GL}(V)$ induces an orthogonal transformation $\tilde{A}$ of $\mathbb{R}^N$ by permuting coordinates: $e_v \mapsto e_{vA}$. We will identify $\mathrm{GL}(V)$ with $\{\tilde{A} \mid A \in \mathrm{GL}(V)\}$.

LEMMA 2.9. (i) *The orthogonal transformation $\tilde{A}$ normalizes E and induces $\left(\begin{smallmatrix} A & O \\ O & A^{-T} \end{smallmatrix}\right)$ on $\overline{E}$ by conjugation:*

$$\tilde{A}^{-1}\overline{X}(a)\overline{Y}(b)\tilde{A} = \overline{X}(aA)\overline{Y}(bA^{-T}) = \overline{X}(a)\overline{Y}(b) \begin{pmatrix} A & O \\ O & A^{-T} \end{pmatrix}.$$

(ii) *The group* $\mathrm{GL}(V)$ *acts transitively by conjugation on both*

$$\{\overline{X}(a)\overline{Y}(b) \mid a \cdot b = 0,\ a, b \neq 0\} \quad \textit{and} \quad \{\overline{X}(a)\overline{Y}(b) \mid a \cdot b = 1\}.$$

Proof. (i) For all $b, v \in V$ we have

$$e_v(\tilde{A}^{-1}X(b)\tilde{A}) = e_{vA^{-1}+b}\tilde{A} = e_{v+bA} = e_v X(bA),$$

so that $\tilde{A}^{-1}X(b)\tilde{A} = X(bA)$. Furthermore,

$$e_v(\tilde{A}^{-1}Y(b)\tilde{A}) = e_{vA^{-1}}(-1)^{vA^{-1}\cdot b}\tilde{A} = (-1)^{v\cdot bA^{-T}} e_v = e_v Y(bA^{-T}),$$

so that $\tilde{A}^{-1}Y(b)\tilde{A} = Y(bA^{-T})$. This implies (i).

(ii) The group $\mathrm{GL}(V)$ acts transitively on the set of incident point-hyperplane pairs from V as well as on the set of non-incident point-hyperplane pairs from V.

Later we will need still more isometries of both $\overline{E}$ and $\mathbb{R}^N$. It is straightforward to check that the isometries of $\overline{E}$ that induce the identity on $\overline{Y}(V)$ are precisely those described by matrices $\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$, where M is a skew-symmetric $k \times k$ matrix (recall that a skew-symmetric matrix has zero diagonal, by definition). We require an isometry d_M of $\mathbb{R}^N$ that induces $\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$ on $\overline{E}$ by conjugation.

To this end let Q_M be any quadratic form on V for which the associated bilinear form is uMv^T, so that $Q_M(u+v) = Q_M(u) + Q_M(v) + uMv^T$ for all $u, v \in V$. Let

$$d_M := \operatorname{diag}[(-1)^{Q_M(v)}]. \tag{2.10}$$

Then

$$\begin{aligned} e_v d_M^{-1} X(a) d_M X(a) &= (-1)^{Q_M(v)} e_{v+a} d_M X(a) \\ &= (-1)^{Q_M(v)+Q_M(v+a)} e_v \\ &= (-1)^{Q_M(a)} (-1)^{(aM)\cdot v} e_v, \end{aligned}$$

so that $d_M^{-1} X(a) d_M X(a) = (-1)^{Q_M(a)} Y(aM)$. Hence,

$$d_M^{-1}(\overline{X}(a)\overline{Y}(b)) d_M = \overline{X}(a)\overline{Y}(aM)\overline{Y}(b) = \overline{X}(a)\overline{Y}(b) \begin{pmatrix} I & M \\ O & I \end{pmatrix}. \tag{2.11}$$

Note that the diagonal matrix d_M depends on the choice of the quadratic form Q_M, but that the effect of conjugation by d_M is independent of this choice.

This proves part of the next lemma. The remainder of the lemma further relates totally singular k-spaces of $\overline{E}$ to the corresponding skew-symmetric matrices; the proof is straightforward (see Kantor [**16**, I, § 5]).

LEMMA 2.12. (i) *Every totally singular k-space W of $\overline{E}$ such that $\overline{Y}(V) \cap W = 0$ has the form*

$$W = d_M^{-1} \overline{X}(V) d_M = \overline{X}(V) \begin{pmatrix} I & M \\ O & I \end{pmatrix} = \{\overline{X}(a)\overline{Y}(aM) \mid a \in V\}$$

for a unique binary skew-symmetric $k \times k$ matrix M. The linear transformation of $\overline{E}$ produced by $\left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$ preserves the quadratic form Q.

(ii) *Let M_1 and M_2 be binary skew-symmetric $k \times k$ matrices for which the corresponding totally singular k-spaces W_1 and W_2 satisfy $\overline{Y}(V) \cap W_1 = \overline{Y}(V) \cap W_2 = 0$. Then $W_1 \cap W_2 = 0$ if and only if $M_1 - M_2$ is non-singular.*

We need one further element of $O(\mathbb{R}^N)$ that normalizes E: one that induces a transvection on $\overline{E}$. First note that

$$E = E_k = X(\langle v_1 \rangle) Y(\langle v_1 \rangle) \langle -I \rangle \cdot X(\langle v_2, \ldots, v_k \rangle) Y(\langle v_2, \ldots, v_k \rangle) \langle -I \rangle$$

can be viewed as $E_1 \otimes E_{k-1}$, the tensor (or Kronecker) product of groups of 2×2 and $2^{k-1} \times 2^{k-1}$ matrices. Let $H_2 = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ and $\tilde{H}_2 = H_2 \otimes I$. Then H_2 normalizes the dihedral group $\langle X(v_1), Y(v_1) \rangle = X(\langle v_1 \rangle) Y(\langle v_1 \rangle) \langle -I \rangle$ of order 8, interchanging $X(v_1)$ and $Y(v_1)$ and fixing $\langle X(v_1) Y(v_1) \rangle$. (All of this is the special case $k = 1$ of (2.7).) It follows that $\tilde{H}_2$ normalizes E while centralizing $X(\langle v_2 \ldots, v_k \rangle) Y(\langle v_2 \ldots, v_k \rangle) \langle -I \rangle$. Thus, *$\tilde{H}_2$ induces a transvection on $\overline{E}$.*

We now have enough isometries of $\overline{E}$ to generate the orthogonal group $O^+(2k, 2)$ using conjugation by isometries in $O(\mathbb{R}^N)$ that normalize E (this is

not the group $\Omega^+(2k, 2)$, which has index 2 in $O^+(2k, 2)$ and is simple if $k \geqslant 3$). Namely, if

$$L := \langle E,\ \mathrm{GL}(V),\ d_M,\ H,\ \tilde{H}_2 \mid M \text{ is skew-symmetric} \rangle, \tag{2.13}$$

then L contains E as a normal subgroup and L/E acts on $\overline{E}$ by conjugation. Note that L contains all isometries of $\overline{E}$ that fix $\overline{Y}(V)$, and hence all that fix $H^{-1}\overline{Y}(V)H = \overline{X}(V)$; these two groups of isometries generate $\Omega^+(2k, 2)$ [**1**, (43.7)]. Since $\tilde{H}_2$ induces a transvection on $\overline{E}$, it follows that

LEMMA 2.14. *The group L induces $O^+(2k, 2)$ on $\overline{E}$.*

3. *Binary Kerdock codes, orthogonal spreads, and real line-sets with prescribed angles*

Fix an *odd* integer m, and let $k = m + 1$ in the preceding section. Now $E = E_{m+1}$ is an extraspecial 2-group of order $2^{1+2(m+1)}$, and $\overline{E}$ is an $\Omega^+(2m + 2, 2)$-space.

DEFINITION. An *orthogonal spread* of $\overline{E}$ is a family Σ of $2^m + 1$ totally singular $(m + 1)$-spaces such that every singular point of $\overline{E}$ belongs to exactly one member of Σ. (Note that $\overline{E}$ contains $(2^{m+1} - 1)(2^m + 1)$ singular points, that is, singular 1-spaces, of which $2^{m+1} - 1$ are in any given totally singular $(m + 1)$-space.)

The construction of orthogonal spreads will be discussed in §§ 7 and 9. In this section we will describe their relationship to Kerdock codes.

By Lemma 2.14, L acts transitively on the ordered pairs of disjoint (except for 0) totally singular $(m+1)$-spaces of $\overline{E}$. After replacing Σ by $\Sigma\ell$ for some $\ell \in L$ we may assume that $\overline{X}(V), \overline{Y}(V) \in \Sigma$. By Lemma 2.12(i), any $\overline{A} \in \Sigma \setminus \{\overline{Y}(V)\}$ can be written in the form $\overline{X}(V)\left(\begin{smallmatrix} I & M_A \\ O & I \end{smallmatrix}\right)$ for a unique skew-symmetric $(m + 1) \times (m + 1)$ matrix M_A. The matrix $\left(\begin{smallmatrix} I & M_A \\ O & I \end{smallmatrix}\right)$ (or, to be more precise, the linear transformation it induces) preserves the quadratic form Q defined on $\overline{E}$ (cf. (2.4)).

Consider a set of binary skew-symmetric $(m + 1) \times (m + 1)$ matrices such that the difference of any two is non-singular. Since the first rows of matrices in this set must be distinct, such a set has size at most 2^m. The important case is when this bound is achieved.

DEFINITION. A *Kerdock set* is a set of 2^m binary skew-symmetric $(m + 1) \times (m + 1)$ matrices such that the difference of any two is non-singular.

By Lemma 2.12(ii), $\{M_A \mid \overline{A} \in \Sigma \setminus \{\overline{Y}(V)\}\}$ *is a Kerdock set for any orthogonal spread* Σ *containing* $\overline{Y}(V)$. The corresponding *Kerdock code* $\mathcal{K}(\Sigma)$ is a binary code of length 2^{m+1}; its 2^{m+1} coordinate positions are labelled by vectors in $V = \mathbb{Z}_2^{m+1}$, and

$$\mathcal{K}(\Sigma) := \{(Q_{M_A}(v) + s \cdot v + \varepsilon)_{v \in V} \mid \overline{A} \in \Sigma \setminus \{\overline{Y}(V)\},\ s \in V,\ \varepsilon \in \mathbb{Z}_2\}, \tag{3.1}$$

where, for each $\overline{A} \in \Sigma \setminus \{\overline{Y}(V)\}$, Q_{M_A} denotes any quadratic form associated with the alternating bilinear form uM_Av^T. Thus, $|\mathcal{K}(\Sigma)| = 2^m \cdot 2^{m+1} \cdot 2 = 2^{2m+2}$.

REMARK. It is important to observe that this notation is very ambiguous. The Kerdock set depends on the choice of a pair of members of Σ to play the roles of $\overline{X}(V)$ and $\overline{Y}(V)$, and on the choice of dual bases in $\overline{X}(V)$ and $\overline{Y}(V)$. However, up to equivalence of codes, the Kerdock code $\mathcal{K}(\Sigma)$ *depends only on* Σ *and on the distinguished member* $\overline{Y}(V)$ of Σ that was discarded in the construction of the Kerdock set. In choosing the notation $\mathcal{K}(\Sigma)$ rather than, say, $\mathcal{K}(\Sigma, \overline{Y}(V))$, we have suppressed this dependence. This is just the sort of inhomogeneity alluded to in § 1. See Kantor [**16**] for more information about this construction and the unavoidability of this dependence. Expositions of this relationship between orthogonal spreads and Kerdock codes are given in [**26**] and [**8**, pp. 143–148]. (*Note.* On p. 147 of [**8**] there is an incorrect assertion that there is a one-to-one correspondence between Kerdock sets and orthogonal spreads.)

Next we consider the Euclidean geometry of the extraspecial 2-group E.

LEMMA 3.2. *If* e_b^* *is as in* (2.8), *then*

(i) $\{\langle e_v\rangle \mid v \in V\}$ *is the set of irreducible submodules for* $Y(V)$*;*

(ii) $\{\langle e_b^*\rangle \mid b \in V\}$ *is the set of irreducible submodules for* $X(V)$.

Proof. (i) Since $Y(V)$ is a group of diagonal matrices it certainly leaves invariant each of the 1-spaces $\langle e_v\rangle$. If $u, v \in V$ are distinct, then there exists $b \in V$ with $b \cdot u \neq b \cdot v$, and then $Y(b)$ acts differently on $\langle e_u\rangle$ and $\langle e_v\rangle$. Thus, we have 2^{m+1} inequivalent 1-dimensional submodules of an 2^{m+1}-dimensional module, so these comprise all irreducible submodules.

(ii) By (2.7), the 1-spaces $\langle e_b H\rangle = \langle e_b^*\rangle$ are the irreducible submodules of $H^{-1}Y(V)H = X(V)$.

LEMMA 3.3. *Let* A *and* B *be subgroups of* E *such that* $\overline{A}$ *and* $\overline{B}$ *are totally singular* $(m+1)$*-spaces of* $\overline{E}$.

(i) *The set* $\mathcal{F}(A)$ *of* A*-irreducible subspaces of* $\mathbb{R}^{2^{m+1}}$ *is an orthogonal frame: a set of* 2^{m+1} *pairwise orthogonal lines through the origin.*

(ii) *Assume that* $\overline{A} \cap \overline{B} = 0$, *and let* u_1 *and* u_2 *be unit vectors in different members of* $\mathcal{F}(A) \cup \mathcal{F}(B)$. *If* u_1 *and* u_2 *are both in different members of* $\mathcal{F}(A)$, *or both are in different members of* $\mathcal{F}(B)$, *then* $(u_1, u_2) = 0$*; otherwise,* $|(u_1, u_2)| = 2^{-(m+1)/2}$.

(iii) *The set* $\mathcal{F}(A)$ *is left invariant by* E.

Proof. In view of the transitivity of L on the ordered pairs $\overline{A}$, $\overline{B}$ in (ii), we may assume that $A = X(V)$ and $B = Y(V)$. Part (i) now follows directly from Lemma 3.2(i). Also by Lemma 3.2 and (2.8), $(e_a, e_b^*) = 2^{-(m+1)/2}(-1)^{a\cdot b}$ for all $a, b \in V$; since $(u_1, u_2) = 0$ whenever $\langle u_1\rangle$ and $\langle u_2\rangle$ belong to the same orthogonal frame, this proves (ii). To prove part (iii) we observe that $\langle A, -I\rangle$ is a normal subgroup of E, so that E leaves invariant the set $\mathcal{F}(A)$ of irreducible submodules for $\langle A, -I\rangle$.

REMARK. The issue of whether or not a subgroup A of E that projects onto $\overline{A}$ contains $-I$ is immaterial in the above lemma, and will be immaterial in the sequel.

THEOREM 3.4. *Let Σ be an orthogonal spread of the $\Omega^+(2m+2,2)$-space $\overline{E}$, and let*

$$\mathcal{F}(\Sigma) := \bigcup_{\overline{A}\in\Sigma} \mathcal{F}(A).$$

Then $\mathcal{F}(\Sigma)$ consists of $2^{m+1}(2^m+1)$ lines of $\mathbb{R}^{2^{m+1}}$ such that, if u_1 and u_2 are unit vectors in different members of $\mathcal{F}(\Sigma)$, then $|(u_1,u_2)| = 0$ or $2^{-(m+1)/2}$.

Proof. This follows immediately from Lemma 3.3.

The Kerdock code $\mathcal{K}(\Sigma)$ introduced in (3.1) can be recovered very simply from $\mathcal{F}(\Sigma)$:

COROLLARY 3.5. $\mathcal{K}(\Sigma) = \{(c_v)_v \in \mathbb{Z}_2^{2^{m+1}} \mid \langle((-1)^{c_v})_v\rangle \in \mathcal{F}(\Sigma)\}$.

Proof. By (2.8) and (2.10), $\mathcal{F}(\Sigma)\backslash\{\mathcal{F}(Y(V))\}$ consists of 1-spaces each of which contains exactly two vectors of length $2^{(m+1)/2}$, namely $\pm 2^{(m+1)/2} e_b^* d_M = \pm\sum_v (-1)^{b\cdot v}(-1)^{Q_M(v)} e_v$ with $M = M_A$ for $\overline{A} \in \Sigma\backslash\{\overline{Y}(V)\}$. Now use (3.1).

REMARK. The sets $\mathcal{F}(\Sigma)$ are essentially not new: they arose in work of Cameron and Seidel [**9**], König [**22**] and Levenštein [**25**]. Namely, while investigating combinatorial properties of the sets of quadratic and alternating bilinear forms on an even-dimensional binary vector space, Cameron and Seidel constructed what, in the present notation, amounts to the line-sets $\mathcal{F}(\Sigma)\backslash\{\mathcal{F}(Y(V))\}$. Later, König and Levenštein independently observed that one could add the frame determined by the standard basis vectors and maintain the same inner products.

Bounds for line-sets in $\mathbb{R}^N$ with prescribed angles

The line-sets $\mathcal{F}(\Sigma)$ in Theorem 3.4 are extremal in the sense that $|\mathcal{F}(\Sigma)|$ meets an upper bound obtained by Delsarte, Goethals and Seidel [**11**] for line-sets in $\mathbb{R}^N$ with prescribed angles (cf. [**4**]). We now derive this upper bound using elementary tensor algebra, and we describe the graph-theoretic structure of extremal line-sets that meet the bound.

Fix any positive integer N, let $e_1,\ldots,e_N$ be the standard basis of $\mathbb{R}^N$ and let S denote the unit sphere in $\mathbb{R}^N$. *Consider a spanning set Ω of n points of S such that $|(a,b)| \in \{0,\alpha\}$ for all $a \neq b$ in Ω, where $0 < \alpha < 1$* (so, in particular, $\Omega \cap (-\Omega) = \emptyset$). Write the Gram matrix of Ω as

$$\mathrm{Gram}(\Omega) = I + \alpha C,$$

where C is an $n \times n$ symmetric matrix with diagonal entries 0 and all other entries $0, \pm 1$. Since Ω spans $\mathbb{R}^N$, $\mathrm{Gram}(\Omega)$ has nullity $n-N$ and the spectrum of C has the form $\{(-1/\alpha)^{n-N}, \lambda_1, \ldots, \lambda_N\}$ for some real numbers λ_i (none of which is $-1/\alpha$).

Let $S^3(\mathbb{R}^N)$ denote the space of symmetric 3-tensors of $\mathbb{R}^N$, of dimension $\binom{N+2}{3}$; for proofs of this and other elementary facts about tensor algebra see [**31**]. For each $a \in \Omega$, $S^3(\mathbb{R}^N)$ contains the tensors $v_a := a \otimes a \otimes a$ and

$$h_a := \tfrac{1}{3} \sum_{i=1}^{N} (a \otimes e_i \otimes e_i + e_i \otimes a \otimes e_i + e_i \otimes e_i \otimes a).$$

We begin by showing that

$$\begin{aligned} \mathrm{Gram}(v_a ; h_a) &:= \mathrm{Gram}(\{v_a, h_a \mid \ a \in \Omega\}) \\ &= \begin{pmatrix} I + \alpha^3 C & I + \alpha C \\ I + \alpha C & \frac{1}{3}(N+2)(I + \alpha C) \end{pmatrix}. \end{aligned} \tag{3.6}$$

Namely, for all $a, b \in \Omega$,

$$(v_a, v_b) = (a, b)^3,$$

$$(v_b, h_a) = 3 \times \tfrac{1}{3}(a, b) \sum_{i=1}^{N} (b, e_i)^2 = (a, b),$$

$$(h_a, h_b) = \tfrac{3}{9} \textstyle\sum_{i=1}^{N} (a, b)(e_i, e_i)^2 + \tfrac{6}{9} \sum_{i=1}^{N} (a, e_i)(b, e_i)(e_i, e_i) = \tfrac{1}{3}(N+2)(a, b),$$

which proves (3.6).

The $n \times n$ matrix $I + \alpha^3 C$ is the sum of a positive definite matrix $(1 - \alpha^2) I$ and a positive semidefinite matrix $\alpha^2 \,\mathrm{Gram}(\Omega) = \alpha^2 (I + \alpha C)$, and hence is non-singular and positive definite. As seen above, it is also the Gram matrix of n vectors v_a in $\binom{N+2}{3}$-space. This proves that

$$n \leqslant \binom{N+2}{3}. \tag{3.7}$$

This inequality is the *absolute bound* obtained by Delsarte, Goethals and Seidel: it is independent of the exact angles of the line-set.

In order to go further, simultaneously apply elementary row and column operations to (3.6) in order to see that the matrix

$$\begin{pmatrix} I + \alpha^3 C - \frac{3}{N+2}(I + \alpha C) & O \\ O & \frac{N+2}{3}(I + \alpha C) \end{pmatrix}$$

is also positive semidefinite. Then so is

$$(N+2)(I + \alpha^3 C) - 3(I + \alpha C) = (N+2)(1 - \alpha^2) I - [3 - \alpha^2 (N+2)](I + \alpha C).$$

This implies that, for $i = 1, \ldots, N$,

$$0 \leqslant 1 + \alpha \lambda_i \leqslant \frac{(N+2)(1 - \alpha^2)}{3 - (N+2)\alpha^2} \tag{3.8}$$

assuming that the denominator is positive. Since $n = \mathrm{Tr}(I + \alpha C) = \sum_{i=1}^{N} (1 + \alpha \lambda_i)$, we deduce that

$$n \leqslant \frac{N(N+2)(1 - \alpha^2)}{3 - (N+2)\alpha^2}. \tag{3.9}$$

This is the *special bound* obtained by Delsarte, Goethals and Seidel.

If equality holds in (3.9), then all of the $1+\alpha\lambda_i$ are equal to their upper bound given in (3.8), and C has two eigenvalues: $-1/\alpha$ with multiplicity $n-N$, and

$$\beta := \left(\frac{(N+2)(1-\alpha^2)}{3-(N+2)\alpha^2} - 1\right)\Big/\alpha = \frac{n-N}{N\alpha} \tag{3.10}$$

with multiplicity N. Consequently,

$$\left(C + \frac{1}{\alpha}I\right)(C-\beta I) = 0. \tag{3.11}$$

However, more can be said in this case (see Cameron and van Lint [**8**] for the definition and basic theory of strongly regular graphs):

PROPOSITION 3.12. *If equality holds in* (3.9), *then 'perpendicularity' defines a strongly regular graph on* Ω. *In particular, if* $\alpha = 1/\sqrt{N}$ *then* Ω *is a union of* $\frac{1}{2}(N+2)$ *orthonormal bases, with points in different bases not perpendicular.*

Proof. Since $(a\otimes a, b\otimes b) = (a,b)^2$, we have $\mathrm{Gram}\{a\otimes a \mid a\in\Omega\} = ((a,b)^2) = I+\alpha^2 A$, where A is a symmetric $(0,1)$ matrix. Note that the row sums of A are all β/α. For, each such row sum is a diagonal entry of C^2, and these are all β/α by (3.11) since the diagonal entries of C are all 0.

Since $\dim S^2(\mathbb{R}^N) = \binom{N+1}{2}$, the matrix A has at least $n-\binom{N+1}{2}$ eigenvalues equal to $-1/\alpha^2$. Another eigenvalue is β/α, so there are $\binom{N+1}{2}-1$ unknown eigenvalues ρ_j, all of which are real. We have

$$0 = \mathrm{Tr}\, A = \beta/\alpha + \sum_j \rho_j + \left(n - \binom{N+1}{2}\right)(-1/\alpha^2), \tag{3.13}$$

$$n\beta/\alpha = \mathrm{Tr}\, A^2 = \beta^2/\alpha^2 + \sum_j \rho_j^2 + \left(n-\binom{N+1}{2}\right)(1/\alpha^4).$$

Using (3.10), we find that

$$\begin{aligned}
\sum 1 &= \tfrac{1}{2}(N+2)(N-1),\\
\sum \rho_j &= -(N+2)(N-1)(1-N\alpha^2)/2\alpha^2\Delta,\\
\sum \rho_j^2 &= (N+2)(N-1)(1-N\alpha^2)^2/2\alpha^4\Delta^2,
\end{aligned}$$

where $\Delta = 3-(N+2)\alpha^2$. Thus, by the Cauchy–Schwarz inequality,

$$\rho_j = -(1-N\alpha^2)/\alpha^2\Delta$$

for $j = 1, \ldots, \frac{1}{2}(N+2)(N-1)$, and hence the graph is strongly regular.

If $\alpha^2 = 1/N$ then $\rho_i = 0$, and the perpendicularity graph is the union of $\frac{1}{2}(N+2)$ disjoint N-cliques: Ω is the union of $\frac{1}{2}(N+2)$ orthonormal bases, with members of different bases not perpendicular.

The case $\alpha^2 = 1/N$ is the one appearing in Theorem 3.4. It is natural to ask whether or not all extremal line-sets in the 'Kerdock case' $\alpha^2 = 1/N$ are derived from orthogonal spreads, but this question appears to be difficult. Suppose that $\mathcal{F}$ is such an extremal line-set. By taking one of its frames as the (standard)

coordinate frame, we can describe $\mathcal{F}$ by $\frac{1}{2}N(N+2)$ unit vectors, one per line modulo switching. The Gram matrix of these vectors has rank N, and is partitioned into square blocks of size N: identity matrices on the diagonal and (normalized) Hadamard matrices elsewhere (cf. [**9**]). This leads to difficult open questions concerning the relationships between such extremal line-sets $\mathcal{F}$ and line-sets $\mathcal{F}(\Sigma)$ originating from orthogonal spreads Σ. We do not even know whether N must have the form 2^{m+1}. If it does, and if $\mathcal{F}$ is converted to a binary code C by changing 1 and -1 to 0 and 1, respectively, then C has the weight distribution of a Kerdock code. However, we do not know whether the code C must be equivalent to one arising from some orthogonal spread. Each Hadamard submatrix of the above Gram matrix produces a subcode of C having the same weight distribution as a first-order Reed–Muller code, but we cannot prove that this needs to be an actual Reed–Muller code, nor even that C must lie inside a second-order Reed–Muller code.

In order to understand this situation somewhat better, consider a set consisting of d orthonormal bases behaving as in Proposition 3.12. We may assume that one of the bases is the standard one. Then each of the other bases consists of the rows of an orthogonal matrix; by assumption, it is a normalized Hadamard matrix. For $d = 2$, any Hadamard matrix can occur. However, for $d > 2$, there are further restrictions, coming from the fact that *the transition matrices* $H_i^{-1}H_j$ *between these bases are themselves normalized Hadamard matrices.*

For instance, the case $d = 3$ is equivalent (with a change in notation) to the existence of three Hadamard matrices H_1, H_2, H_3 of order N satisfying $H_1H_2H_3 = N^{3/2}I$. Note that N must be a square. (This also follows from the fact that the eigenvalue $-1/\alpha$ of the Gram matrix is rational, since its multiplicity is greater than that of any other eigenvalue.)

Examples can be constructed as follows. Let $N = 16s^2$, and suppose that there exists a net of order $4s$ and index r. (See Cameron and van Lint [**8**, Chapter 7] for the definition of a net.) If $r \geqslant 2s$, let P_1 be a set of $2s$ parallel classes, and let A_1 be the adjacency matrix of the point graph of the resulting sub-net of order $2s$. Then $H_1 = 2A_1 - J$ is a symmetric Hadamard matrix. If P_2 is another $2s$-set of parallel classes such that $|P_1 \cap P_2| = s$ (this requires that $r \geqslant 3s$), we find that $H_1H_2 = -4sH_3$, where H_3 corresponds to $P_3 = P_1 \triangle P_2$. So, if there exists a family of $d-1$ $2s$-subsets of an r-set, any two intersecting in s points, then we obtain $d-1$ Hadamard matrices with the corresponding properties, and hence d orthonormal bases having the properties of Proposition 3.12. Note that this construction produces far fewer than the potential maximum number $\frac{1}{2}(N+2)$ of bases. It also shows that sets of bases can be obtained in which inequivalent Hadamard matrices occur—unlike the case of Lemma 3.3, in which all of the Hadamard matrices are equivalent to the one produced in Lemma 3.2 (Hadamard matrices of 'Sylvester type').

Much more general results can be found in a paper by Delsarte, Goethals and Seidel [**11**]. They obtained very general bounds for finite subsets Ω of S having prescribed angles, as well as combinatorial consequences when equality holds.

The geometry of the line-sets $\mathcal{F}(\Sigma)$

LEMMA 3.14. *Let G be the group of all elements of $O(\mathbb{R}^{2^{m+1}})$ that send each of the frames $\mathcal{F}(X(V))$ and $\mathcal{F}(Y(V))$ to itself. Then G normalizes E.*

Proof. Let $g \in G$. Since $X(V)$ is transitive on the standard basis vectors e_v, with $v \in V$, we may replace g by its product with an element of $X(V)$, and assume that g fixes $\langle e_0 \rangle \in \mathcal{F}(Y(V))$. In fact we may now replace g by a scalar multiple of itself and assume that g fixes e_0.

Similarly $Y(V)$ is transitive on $\mathcal{F}(X(V))$, while inducing the identity on $\mathcal{F}(Y(V))$. Arguing as above we may also assume that g fixes $\langle e_0^* \rangle \in \mathcal{F}(X(V))$.

We will prove that g is in the general linear group $\mathrm{GL}(V)$ occurring in Lemma 2.9. This will suffice, since by that lemma the group $\mathrm{GL}(V)$ normalizes E while permuting the members of both $\mathcal{F}(X(V))$ and $\mathcal{F}(Y(V))$.

For each $v \in V$, there is some $\alpha_v = \pm 1 \in \mathbb{R}$ and some $\tilde{v} \in V$ such that $e_v g = \alpha_v e_{\tilde{v}}$. Also for each $a \in V$, there is some $\beta_a = \pm 1 \in \mathbb{R}$ and some $\tilde{a} \in V$ such that $e_a^* g = \beta_a e_{\tilde{a}}^*$. By linearity,

$$\begin{aligned}\sum_v \alpha_v (-1)^{a \cdot v} e_{\tilde{v}} &= \left(\sum_v (-1)^{a \cdot v} e_v \right) g \\ &= 2^{(m+1)/2} e_a^* g \\ &= 2^{(m+1)/2} \beta_a e_{\tilde{a}}^* \\ &= \beta_a \sum_v (-1)^{\tilde{a} \cdot v} e_v,\end{aligned}$$

so that $\alpha_v (-1)^{a \cdot v} = \beta_a (-1)^{\tilde{a} \cdot \tilde{v}}$ for all $a, v \in V$.

If $v = 0$, then $\tilde{v} = 0$ and $\alpha_v = 1$, so that $\beta_a = 1$ for all $a \in V$. Similarly $\alpha_v = 1$ for all $v \in V$, and hence $a \cdot v = \tilde{a} \cdot \tilde{v}$ for all $a, v \in V$. If $v, w \in V$, then for all $a \in V$,

$$\tilde{a} \cdot v \tilde{-} w = a \cdot (v - w) = \tilde{a} \cdot (\tilde{v} - \tilde{w})$$

so that $v \tilde{-} w = \tilde{v} - \tilde{w}$. It follows that the permutation $v \to \tilde{v}$ is linear! Let A be a matrix such that $\tilde{v} = vA$ for all v. Then $\tilde{a} \cdot vA = a \cdot v$ for all $v \in V$, and this equation uniquely determines $\tilde{a}$ in terms of a and A. (In fact $\tilde{a} = aA^{-T}$.)

We digress with an observation concerning orthogonal spreads. While we continue to assume that our field has order 2, the following result and its proof hold for any finite field $\mathrm{GF}(q)$.

LEMMA 3.15. *Let Σ be a spread in an $O^+(2m+2, 2)$-space V, where $m > 1$. If $h \in O^+(2m+2, 2)$ induces the identity on Σ, then $h = 1$.*

Proof. Otherwise, we may assume that $|h| = p$ is prime. Consider three different subspaces $E, F, F' \in \Sigma$. Since the bilinear form on V induces an isomorphism from F' to the dual space of E, the representations of h on E and F' are contragredient. So are those on F and F'. Thus, the representations on E and F are isomorphic.

Let W be the sum of an isomorphism class of h-isomorphic submodules of E. Then W is isomorphic to a submodule W' of F. If U is any irreducible submodule of V isomorphic to a submodule of W, then $U \subseteq W + W'$: each $u \in U$ can be written $u = e + f$ with $e \in E$, $f \in F$, and $u \mapsto e$ defines an isomorphism from U into E and hence into W. Similarly, $f \in W'$.

Thus, if $\dim W = k$ then the $2k$-space $W + W'$ meets each member of Σ in a k-space. Since these intersections pairwise meet at 0, we have $2^{2k} - 1 \geqslant (2^k - 1)|\Sigma|$, so that $2^k + 1 \geqslant 2^m + 1$ and hence $k \geqslant m$.

If $p = 2$ then we can choose W to be the space of fixed vectors within E. Then $C_V(h)$ has dimension $2 \dim W = 2m$, so that $[V, h] = C_V(h)^\perp$ has dimension 2. If $e \neq eh \in E$ then $e - eh \in [V, h]$. Thus, the 2-space $[V, h]$ meets the $2^m + 1$ members of Σ in different points, which is impossible since $m > 1$.

Thus, h is semisimple. However, $2m > m + 1$, so there cannot be two different choices for W in E, and hence h is irreducible on E. Then $p \mid (2^{(m+1)/2} + 1)$.

Moreover, a Sylow p-subgroup of $O^+(2m + 2, 2)$ is cyclic. An element of order p can be obtained as follows. We may assume that $V = \mathrm{GF}(2^{m+1}) \oplus \mathrm{GF}(2^{m+1})$, equipped with the quadratic form $\varphi(x, y) := T(xy)$, where T: $\mathrm{GF}(2^{m+1}) \to \mathrm{GF}(2)$ is the trace map. We may also assume that h: $(x, y) \mapsto (\alpha x, \alpha^{-1} y)$ with $\alpha \in \mathrm{GF}(2^{m+1})$ of order p. Since $\alpha^{-1} = \alpha^{2^{(m+1)/2}}$, the following n-spaces are fixed by h: $\mathrm{GF}(2^{m+1}) \times 0$ and $\{(x, ax^{2^{(m+1)/2}}) \mid x \in \mathrm{GF}(2^{m+1})\}$ for each $a \in \mathrm{GF}(2^{m+1})$. Since they cover all of V, these are all of the $(m + 1)$-spaces fixed by h. We need to determine how many of them are totally singular. Let $a \in \mathrm{GF}(2^{m+1})$. Then $T(axx^{2^{(m+1)/2}}) = 0$ for all $x \in \mathrm{GF}(2^{m+1})$ if and only if $T(a\,\mathrm{GF}(2^{(m+1)/2})) = 0$, and this occurs for only $2^{(m+1)/2}$ choices of a. Thus, h fixes only $2^{(m+1)/2} + 1$ totally singular $(m + 1)$-spaces. Since $2^{(m+1)/2} + 1 < |\Sigma|$, we have the desired contradiction.

PROPOSITION 3.16. *Let Σ_1 and Σ_2 be orthogonal spreads of $\overline{E}$.*

(i) *Any isometry of $\overline{E}$ sending Σ_1 to Σ_2 is induced by an element of $O(\mathbb{R}^{2^{m+1}})$ sending $\mathcal{F}(\Sigma_1)$ to $\mathcal{F}(\Sigma_2)$ (in fact by many such elements). In particular, the set-stabilizer of Σ_1 in $\Omega^+(2m + 2, 2)$ is induced by a subgroup of $O(\mathbb{R}^{2^{m+1}})$ preserving the set $\mathcal{F}(\Sigma_1)$.*

(ii) *The subgroup E is the pointwise stabilizer of $\mathcal{F}(\Sigma_1)$ in $O(\mathbb{R}^{2^{m+1}})$.*

(iii) *Any element of $O(\mathbb{R}^{2^{m+1}})$ sending $\mathcal{F}(\Sigma_1)$ to $\mathcal{F}(\Sigma_2)$ normalizes E and induces an orthogonal transformation of $\overline{E}$ sending Σ_1 to Σ_2.*

Proof. (i) This follows immediately from the definition of $\mathcal{F}(\Sigma_1)$ in Theorem 3.4.

(ii) By Lemma 3.14, the pointwise stabilizer of $\mathcal{F}(\Sigma_1)$ normalizes E and hence induces a group of orthogonal transformations on $\overline{E}$. By Lemma 3.15, the pointwise stabilizer of Σ_1 in $O^+(2m + 2, 2)$ is 1.

(iii) The sets $\mathcal{F}(A)$, with $A \in \Sigma_1$, are the maximal families of pairwise perpendicular members of $\mathcal{F}(\Sigma_1)$ (this reflects the graph structure of $\mathcal{F}(\Sigma_1)$). Part (ii) implies that, if $g \in O(\mathbb{R}^{2^{m+1}})$ sends $\mathcal{F}(\Sigma_1)$ to $\mathcal{F}(\Sigma_2)$, then g normalizes E. Thus, g induces an automorphism on $\overline{E}$.

In view of Corollary 10.9 below, it follows that, *if m is odd and composite, then there are more than $2^{\sqrt{m}/2}$ extremal line-sets $\mathcal{F}(\Sigma)$ that are inequivalent under the action of $O(\mathbb{R}^{2^{m+1}})$.*

4. *Extraspecial 2-groups continued*

Let $k = m$ in §2, and let E_m be the extraspecial 2-group of order 2^{1+2m} introduced there. No parity assumption is made concerning m. We are now going to extend E_m slightly, at the same time switching from real to complex space.

In this section we will view e_v, with $v \in V$, as the standard basis of $\mathbb{C}^N$, where $N = 2^m$. We equip $\mathbb{C}^N$ with the usual hermitian inner product, and denote the full isometry group by $U(\mathbb{C}^N)$. This inner product restricts to the usual one on the real 'subspace' $\langle e_v \mid v \in V\rangle_{\mathbb{R}}$, so that $O(\mathbb{R}^N) \leqslant U(\mathbb{C}^N)$. Moreover, $E_m < U(\mathbb{C}^N)$.

Let $i = \sqrt{-1}$ and $F := E_m\langle iI\rangle$ (this is the *central product* of E_m and $\langle iI\rangle$: these two groups commute, and they intersect in the centre $\langle -I\rangle$ of E_m; cf. Aschbacher [**1**, p. 32]). Then $|F| = 2^{2+2m}$, $Z(F) = \langle iI\rangle$, and $\overline{F} := F/Z(F)$ is elementary abelian of order 2^{2m}. As before we will use an overbar to denote the natural map $F \to F/Z(F)$. Once again we identify $\langle -I\rangle$ with $\mathbb{Z}_2$ in order to obtain a non-singular alternating binary form on $\overline{F}$ defined by $(\overline{f}_1, \overline{f}_2)_F = [f_1, f_2] \in \langle -I\rangle$ for $f_1, f_2 \in F$. As in (2.5), $(\overline{X}(a)\overline{Y}(b), \overline{X}(a')\overline{Y}(b'))_F = a \cdot b' - a' \cdot b$ for all $a, b, a', b' \in V$. This time the m-spaces $\overline{X}(V)$ and $\overline{Y}(V)$ are *totally isotropic*: each is perpendicular to itself. Moreover, $\overline{X}(V) \cap \overline{Y}(V) = 0$.

Once again we will require many isometries of $\mathbb{C}^{2^m}$ that normalize F, as well as the isometries they induce on $\overline{F}$ by conjugation. Again let $v_1, \ldots, v_m$ denote the standard basis of $V = \mathbb{Z}_2^m$, and let $x_j = \overline{X}(v_j)$ and $y_j = \overline{Y}(v_j)$. Then $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ are dual bases of $\overline{X}$ and $\overline{Y}$, and $x_1, \ldots, x_m, y_1, \ldots, y_m$ is a basis of $\overline{F}$. The group L introduced in (2.13) lies in $U(\mathbb{C}^N)$ since it lies in $O(\mathbb{R}^N)$, and it normalizes F since it normalizes E_m and $\langle iI\rangle$.

In order to obtain additional isometries we now turn to the counterparts of the diagonal transformations d_M defined in (2.10), thereby finally introducing $\mathbb{Z}_4$ into these considerations. This time it is straightforward to check that the isometries of $\overline{F}$ which induce the identity on $\overline{Y}(V)$ are precisely those described by matrices $\left(\begin{smallmatrix} I & P \\ O & I \end{smallmatrix}\right)$, where P is a binary symmetric $m \times m$ matrix (compare Lemmas 2.12 and 4.7). For a given P we require an isometry d_P of $\mathbb{C}^{2^m}$ that normalizes F and induces $\left(\begin{smallmatrix} I & P \\ O & I \end{smallmatrix}\right)$ on $\overline{F}$, by analogy with (2.11).

In place of the quadratic form $Q_M\colon V \to \mathbb{Z}_2$ that occurs in (2.10), we will use a map $T_P\colon V \to \mathbb{Z}_4$ which is called a *$\mathbb{Z}_4$-valued quadratic form on V* by Brown [**7**] (cf. [**35**]). This is obtained as follows. Since $P = (P_{jk})$ is a $(0, 1)$-matrix, we may view its entries $0, 1$ as elements of $\mathbb{Z}_4$. Start with $\widehat{V} = \mathbb{Z}_4^m$ and with the quadratic form $\widehat{v}P\widehat{v}^T$ for $\widehat{v} \in \widehat{V}$; we emphasize that the entries of P are to be viewed as $0, 1 \in \mathbb{Z}_4$.

We say that $\widehat{v} = (\alpha_1, \ldots, \alpha_m) \in \widehat{V}$ is a *lift of* $v \in V$ if $\widehat{v} \equiv v \pmod 2$. Define

$$T_P(v) := \sum_j P_{jj}\alpha_j^2 + 2\sum_{j<k} P_{jk}\alpha_j\alpha_k\,, \tag{4.1}$$

where $\widehat{v} = (\alpha_1, \ldots, \alpha_m)$ is some lift of v; note that (4.1) is independent of the choice of lift. It is immediate that, for any $u, v \in V$,

$$T_P(u + v) = T_P(u) + T_P(v) + 2\widehat{u}P\widehat{v}^T\,, \tag{4.2}$$

where $\widehat{u}$ and $\widehat{v}$ are lifts of u and v, respectively.

Recall that two binary quadratic forms are associated with the same alternating bilinear form if and only if their difference is a linear functional. An analogous result holds here.

LEMMA 4.3. *A map* T'_P: $V \to \mathbb{Z}_4$ *satisfies the condition in* (4.2) *if and only if* $T'_P(v) = T_P(v) + 2\widehat{v}D\widehat{v}^T$ *for a unique* $m \times m$ *diagonal* $(0,1)$*-matrix* D.

Proof. Since $T_P - T'_P$ satisfies

$$(T_P - T'_P)(u+v) = (T_P - T'_P)(u) + (T_P - T'_P)(v)$$

for all $u, v \in V$, it is an additive map $V \to \mathbb{Z}_4$ and thus maps into $2\mathbb{Z}_4$. When $2\mathbb{Z}_4$ is identified with $\mathbb{Z}_2$ we see that $T_P - T'_P$ is a linear functional on V. Any such linear functional into $2\mathbb{Z}_4$ can be written as $v \mapsto 2\widehat{v}D\widehat{v}^T$ for a unique $m \times m$ diagonal $(0,1)$-matrix D.

By analogy with (2.10), let

$$d_P := \operatorname{diag}[i^{T_P(v)}]. \tag{4.4}$$

Then

$$\begin{aligned} e_v d_P^{-1} X(a) d_P X(a) &= i^{-T_P(v)} e_{v+a} d_P X(a) \\ &= i^{-T_P(v)} i^{T_P(v+a)} e_v \\ &= i^{T_P(a)} i^{2aPv^T} e_v \\ &= i^{T_P(a)} (-1)^{aP\cdot v} e_v, \end{aligned}$$

so that $d_P^{-1} X(a) d_P X(a) = i^{T_P(a)} Y(aP)$. Since d_P commutes with $Y(b)$ (both are diagonal matrices), we have

$$d_P^{-1}(\overline{X}(a)\overline{Y}(b))d_P = \overline{X}(a)\overline{Y}(aP)\overline{Y}(b) = \overline{X}(a)\overline{Y}(b)\begin{pmatrix} I & P \\ O & I \end{pmatrix}. \tag{4.5}$$

We now have enough isometries of $\overline{F}$ to generate the symplectic group $\mathrm{Sp}(2m,2)$ using conjugation by elements of $U(\mathbb{C}^{2^m})$ that normalize F. Namely, if

$$L^\natural := \langle F, \mathrm{GL}(V), H, d_P \mid P \text{ is a binary symmetric } m \times m \text{ matrix} \rangle, \tag{4.6}$$

then $L^\natural$ contains F as a normal subgroup, and $L^\natural/F$ acts on $\overline{F}$ by conjugation, inducing $\mathrm{Sp}(2m,2)$ on $\overline{F}$ (cf. [**33**, p. 72]). The analogue of Lemma 2.12 is the following lemma.

LEMMA 4.7. (i) *Every totally isotropic* m*-space* W *of* $\overline{F}$ *such that* $\overline{Y}(V) \cap W = 0$ *has the form*

$$W = d_P^{-1}\overline{X}(V)d_P = \overline{X}(V)\begin{pmatrix} I & P \\ O & I \end{pmatrix} = \{\overline{X}(a)\overline{Y}(aP) \mid a \in V\}$$

for a unique binary symmetric $m \times m$ *matrix* P. *The linear transformation of* $\overline{E}$ *produced by* $\left(\begin{smallmatrix} I & P \\ O & I \end{smallmatrix}\right)$ *preserves the form* $(\ ,\ )$.

(ii) *Let* P_1 *and* P_2 *be binary symmetric* $m \times m$ *matrices for which the corresponding totally isotropic* m*-spaces* W_1 *and* W_2 *satisfy* $\overline{Y}(V) \cap W_1 = \overline{Y}(V) \cap W_2 = 0$. *Then* $W_1 \cap W_2 = 0$ *if and only if* $P_1 - P_2$ *is non-singular.*

5. $\mathbb{Z}_4$-*Kerdock codes, symplectic spreads and complex line-sets with prescribed angles*

We continue with the notation introduced in § 4.

DEFINITION. A *symplectic spread* of $\overline{F}$ is a family Σ' of 2^m+1 totally isotropic m-spaces such that every point in $\overline{F}$ lies in a unique member of Σ'. (Note that there are exactly $(2^m+1)(2^m-1)$ points, 2^m-1 of which are in any given m-space.)

A symplectic spread is a spread in the conventional sense (see Dembowski [**12**, p. 219]): a family Σ' of $\sqrt{|W|}+1$ subspaces of size $\sqrt{|W|}$ of a finite vector space W such that every non-zero vector lies in exactly one member of Σ'. A spread Σ' determines an *affine plane* $\mathbf{A}(\Sigma')$ *of order* $\sqrt{|W|}$ as follows: points are vectors, and lines are the cosets $A+w$, where $A\in\Sigma'$ and $w\in W$. This accounts for the importance of spreads in finite geometry.

After replacing Σ' by Σ'^{ℓ} for some $\ell\in L^{\natural}$ we may assume $\overline{X}(V)$, $\overline{Y}(V)\in\Sigma'$. By Lemma 4.7, any totally isotropic m-space $\overline{A}\in\Sigma'$, with $\overline{A}\neq\overline{Y}(V)$, can be written in the form $\overline{X}(V)\left(\begin{smallmatrix} I & P_A \\ O & I\end{smallmatrix}\right)=\{\overline{X}(a)\overline{Y}(aP_A)\mid a\in V\}$ for a unique binary symmetric $m\times m$ matrix P_A; here, $\left(\begin{smallmatrix} I & P_A \\ O & I\end{smallmatrix}\right)$ induces an isometry of $\overline{F}$. In terms of the affine plane $\mathbf{A}(\Sigma')$, the subspace $\{\overline{X}(a)\overline{Y}(aP_A)\mid a\in V\}$ can be thought of as the line '$y=xP_A$'.

Part (ii) of Lemma 4.7 implies that

$$\mathcal{S}(\Sigma'):=\{P_A\mid \overline{A}\in\Sigma'\setminus\{\overline{Y}(V)\}\} \tag{5.1}$$

is a set of 2^m symmetric $m\times m$ matrices such that the difference of any two is non-singular. If the word 'symmetric' is deleted here, the preceding condition on $m\times m$ matrices is essentially the definition of a *spread set* in [**12**, p. 220]; the corresponding affine plane $\mathbf{A}(\mathcal{S}(\Sigma'))$ can be viewed as having $V\oplus V$ as its set of points, while the lines are the sets of points $(x,y)\in V\oplus V$ having the familiar appearance

$$x=b \quad\text{or}\quad y=xP_A+b \quad\text{with } b\in V \text{ and } \overline{A}\in\Sigma'\setminus\{\overline{Y}(V)\}. \tag{5.2}$$

On the other hand, the corresponding $\mathbb{Z}_4$*-code* $\mathcal{H}_4(\Sigma')$ comprises 2^{2m+2} vectors in $\mathbb{Z}_4^{2^m}$; the 2^m coordinate positions are labelled by vectors v in $V=\mathbb{Z}_2^m$. Much of the rest of this paper is concerned with the following subset of $\mathbb{Z}_4^{2^m}$:

$$\mathcal{H}_4(\Sigma'):=\{(T_{P_A}(v)+2\widehat{s}\cdot\widehat{v}+\varepsilon)_v\mid \overline{A}\in\Sigma',\ \widehat{s}\in\widehat{V},\ \varepsilon\in\mathbb{Z}_4\},$$

where T_{P_A} is the $\mathbb{Z}_4$-valued quadratic form introduced in (4.1) with $P=P_A$, and $\widehat{v}\in\mathbb{Z}_4^m$ is congruent to $v\in V$ modulo 2 (again see §4). Alternatively, we can write

$$\mathcal{H}_4(\Sigma'):=\{(T_{P_A}(v)+2\widehat{s}\cdot\widehat{v}+\varepsilon)_v\mid \overline{A}\in\Sigma',\ s\in V,\ \varepsilon\in\mathbb{Z}_4\}. \tag{5.3}$$

If m is odd, $\mathcal{H}_4(\Sigma')$ will be called a $\mathbb{Z}_4$*-Kerdock code.*

REMARK. It is again important to observe that this notation is ambiguous. The set $\{P_A\mid \overline{A}\in\Sigma'\setminus\{\overline{Y}(V)\}\}$ depends on the choice of a pair of members of Σ' to play the role of $\overline{X}(V)$, $\overline{Y}(V)$, and on the choice of dual bases in $\overline{X}(V)$ and $\overline{Y}(V)$. Thus, the notation $\mathcal{S}(\Sigma')$ for the preceding set of matrices is ambiguous. Up to equivalence of codes, $\mathcal{H}_4(\Sigma')$ *depends only on* Σ' *and on the distinguished member* $\overline{Y}(V)$ of Σ' that was discarded in the construction of the set $\mathcal{S}(\Sigma')$.

Next we consider the unitary geometry of the 2-group F. The next two lemmas are the counterparts of Lemmas 3.2 and 3.3.

LEMMA 5.4. (i) *The set* $\{\langle e_v\rangle \mid v \in V\}$ *is the set of irreducible submodules for* $Y(V)$.

(ii) *The set* $\{\langle e_b^*\rangle \mid b \in V\}$ *is the set of irreducible submodules for* $X(V)$.

In fact, this is immediate by Lemma 3.2, since $Y(V)$ and $X(V)$ are real matrix groups. However, when these are moved to other subgroups of F using $L^\natural$, complex numbers enter.

LEMMA 5.5. *Let* A *and* B *be subgroups of* F *such that* $\overline{A}$ *and* $\overline{B}$ *are totally isotropic* m*-dimensional subspaces of the symplectic space* $\overline{F}$.

(i) *The set* $\mathcal{F}(A)$ *of* A*-irreducible subspaces of* $\mathbb{C}^{2^m}$ *is an orthogonal frame.*

(ii) *Assume that* $\overline{A} \cap \overline{B} = 0$, *and let* u_1 *and* u_2 *be unit vectors in different members of* $\mathcal{F}(A) \cup \mathcal{F}(B)$. *If* u_1 *and* u_2 *are both in* $\mathcal{F}(A)$, *or are both in* $\mathcal{F}(B)$, *then* $(u_1, u_2) = 0$; *otherwise,* $|(u_1, u_2)| = 2^{-m/2}$.

(iii) *The set* $\mathcal{F}(A)$ *is left invariant by* F.

(iv) *If* $B = Y(V)$, *and if* u_1 *and* u_2 *are unit vectors such that* u_1 *lies in a member of* $\mathcal{F}(A)$ *and* u_2 *lies in a member of* $\mathcal{F}(B)$, *then* $(u_1, u_2) \in \{1, -1, i, -i\}2^{-m/2}$.

Proof. For parts (i)–(iii), by using the group $L^\natural$ we may assume that $A = X(V)$ and $B = Y(V)$. Parts (i) and (ii) follow directly from Lemma 5.4 as in the proof of Lemma 3.3. Part (iii) follows from the fact that $\langle A, iI\rangle$ is normal in F.

(iv) By Lemma 5.4(ii) and (4.4), each member of $\mathcal{F}(A) = \mathcal{F}(\overline{X}(V))d_P$ is spanned by a unit vector all of whose coordinates are 1, -1, i, or $-i$.

THEOREM 5.6. *Let* Σ' *be any symplectic spread of the symplectic space* $\overline{F}$. *Then*

$$\mathcal{F}(\Sigma') := \bigcup_{\overline{A} \in \Sigma'} \mathcal{F}(A)$$

consists of $2^m(2^m + 1)$ 1*-spaces in* $\mathbb{C}^{2^m}$ *such that, if* u_1 *and* u_2 *are unit vectors in different members of* $\mathcal{F}(\Sigma')$, *then* $|(u_1, u_2)| = 0$ *or* $2^{-m/2}$.

This follows immediately from the preceding lemma. As in Corollary 3.5, the $\mathbb{Z}_4$-code $\mathcal{H}_4(\Sigma')$ introduced in (5.3) can be recovered very simply from $\mathcal{F}(\Sigma')$.

COROLLARY 5.7. $\mathcal{H}_4(\Sigma') = \{(c_v)_v \in \mathbb{Z}_4^{2^m} \mid \langle (i^{c_v})_v\rangle \in \mathcal{F}(\Sigma')\}$.

Proof. Use (2.8), (4.4) and (5.3) as in the proof of Corollary 3.5.

Bounds for lines-sets in $\mathbb{C}^N$ *with prescribed angles*

Once again the line-set $\mathcal{F}(\Sigma')$ is extremal in the sense that $|\mathcal{F}(\Sigma')|$ meets another upper bound obtained by Delsarte, Goethals and Seidel [**11**], this time for line-sets in $\mathbb{C}^N$ with prescribed angles. The proofs are very similar to those in § 3.

For any N let $e_1, \ldots, e_N$ be the standard basis of $\mathbb{C}^N$. Once again equip $\mathbb{C}^N$ with the usual hermitian inner product, and let S denote the unit sphere. Let a^* denote the complex conjugate of $a \in \mathbb{C}^N$. *Consider a spanning set* Ω *of* n *points of* S *such that* $|(a, b)| \in \{0, \alpha\}$ *for all* $a \neq b$ *in* Ω, *where* $0 < \alpha < 1$. Then $\mathrm{Gram}(\Omega) = I + \alpha C$, where C is a matrix with diagonal entries 0 and all other

non-zero entries u satisfying $|u| = 1$. Once again the spectrum of C has the form $\{(-1/\alpha)^{n-N}, \lambda_1, \ldots, \lambda_N\}$. Since $\mathrm{Gram}(\Omega)$ is a hermitian matrix, its eigenvalues $\lambda_1, \ldots, \lambda_N$ are real.

The vector space $S^2(\mathbb{C}^N) \otimes \mathbb{C}^N$ has dimension $N\binom{N+1}{2}$. For each $a \in \Omega$ this space contains the tensors $v_a := a \otimes a \otimes a^*$ and $h_a := \frac{1}{2}\sum_i (a \otimes e_i + e_i \otimes a) \otimes e_i$. As before,

$$\mathrm{Gram}(v_a\,; h_a \mid\ a \in \Omega) = \begin{pmatrix} I + \alpha^3 C & I + \alpha C \\ I + \alpha C & \frac{1}{2}(N+1)(I + \alpha C) \end{pmatrix},$$

and $I + \alpha^3 C$ is positive definite, from which we deduce the *absolute bound*

$$n \leqslant N\binom{N+1}{2}.$$

Using row and column transformations as in § 3, we find that

$$0 \leqslant 1 + \alpha\lambda_i \leqslant \frac{(N+1)(1-\alpha^2)}{2 - (N+1)\alpha^2} \tag{5.8}$$

assuming that the denominator is positive, and hence

$$n = \mathrm{Tr}(I + \alpha C) = \sum_{i=1}^{N} (1 + \alpha\lambda_i) \leqslant \frac{N(N+1)(1-\alpha^2)}{2 - (N+1)\alpha^2}, \tag{5.9}$$

which is the *special bound* obtained by Delsarte, Goethals and Seidel.

When equality holds in the special bound, the matrix C has two eigenvalues: $-1/\alpha$ with multiplicity $n - N$ and $\beta := (n - N)/N\alpha$. In this case we consider the Gram matrix $\mathrm{Gram}(a \otimes a^*)$ of the tensors $a \otimes a^* \in \mathbb{C}^N \otimes \mathbb{C}^N$ for $a \in \Omega$. This time $\mathrm{Gram}(a \otimes a^*) = I + \alpha^2 A$, where A is a $(0,1)$-matrix whose row sums are all β/α (the diagonal entries of CC^*). As in § 3 we find that the eigenvalues of A are β/α with multiplicity 1, $-1/\alpha^2$ with multiplicity $n - N^2$, and $(N\alpha^2 - 1)/(2\alpha^2 - (N+1)\alpha^4)$ with multiplicity $N^2 - 1$. It follows that A is the adjacency matrix of a strongly regular graph. In the special 'Kerdock case' $\alpha^2 = 1/N$, the graph is the union of $N + 1$ disjoint N-cliques: Ω is the union of $N + 1$ orthonormal bases, with members of different bases not perpendicular.

REMARKS. (1) In the special 'Kerdock case', the graph-theoretic structure of any extremal line-set meeting the special bound coincides with that of any set $\mathcal{F}(\Sigma')$ derived from a symplectic spread Σ', just as we saw in Proposition 3.5 for the real case. However, the difficult open questions posed in the remarks following that proposition are even more difficult for the present type of extremal line-set. Namely, once again an extremal line-set produces a Gram matrix whose off-diagonal blocks are Hadamard matrices, but this time these are *complex* Hadamard matrices. Their entries may involve complex numbers other than $\{1, -1, i, -i\}$, since it is permitted to multiply any row by a complex number of modulus 1 and the corresponding column by its complex conjugate. However, it is not clear whether we can make all entries lie in $\{1, -1, i, -i\}$ by appropriate row and column multiplications of this form, as holds for $\mathcal{F}(\Sigma)$. Moreover, we do not even have a characterization of the sets $F(\Sigma)$ in terms of their $\mathbb{Z}_4$-codes, as we did in the binary case (see the remarks following Proposition 3.12).

(2) Delsarte, Goethals, and Seidel obtained their bounds on the cardinality of systems of lines with prescribed angles using Jacobi polynomials: absolute bounds that depend only on the number of possible angles, and special bounds that depend on the angles themselves. Theorem 7.5 of their paper asserts that, if equality holds in the special bound, then the extremal line-sets form an association scheme. In the special case of two possible angles α, β, the extremal line-sets form a strongly regular graph, where two lines are adjacent if the angle between them is β. Our derivation of a special case of this result uses only elementary tensor algebra, and in the special 'Kerdock case' it reveals the simple structure of the strongly regular graph. For connections to homogeneous and harmonic polynomials on the sphere we refer the reader to Koornwinder [**23**, **24**].

(3) Is it possible to say something about the Molien series of the groups L and $L^\natural$, such as the minimal degree of an invariant? We would then have information regarding properties of $\mathcal{F}(\Sigma)$ and $\mathcal{F}(\Sigma')$ as spherical designs (see Seidel [**30**] for background).

The geometry of the line-sets $\mathcal{F}(\Sigma')$

The counterparts of Lemma 3.14 and Proposition 3.16 are as follows.

LEMMA 5.10. *The group of all elements of* $U(\mathbb{C}^{2^m})$ *sending each of the frames* $\mathcal{F}(X(V))$ *and* $\mathcal{F}(Y(V))$ *to itself normalizes* F.

PROPOSITION 5.11. *Let* Σ'_1 *and* Σ'_2 *be symplectic spreads of* $\overline{F}$.

(i) *Any symplectic transformation sending* Σ'_1 *to* Σ'_2 *is induced by an element of* $U(\mathbb{C}^{2^m})$ *sending* $\mathcal{F}(\Sigma'_1)$ *to* $\mathcal{F}(\Sigma'_2)$ (*in fact by many such elements*). *In particular, the set-stabilizer of* Σ'_1 *in* $\mathrm{Sp}(2m, 2)$ *is induced by a subgroup of* $U(\mathbb{C}^{2^m})$ *preserving* $\mathcal{F}(\Sigma'_1)$.

(ii) *The pointwise stabilizer of* $\mathcal{F}(\Sigma'_1)$ *in* $U(\mathbb{C}^{2^m})$ *is* $\langle F, CI\rangle$, *where* $C \subseteq \mathbb{C}^*$ *is the unit circle; moreover,* F *is the set of all elements in this pointwise stabilizer of order dividing* 4.

(iii) *Any element of* $U(\mathbb{C}^{2^m})$ *sending* $\mathcal{F}(\Sigma'_1)$ *to* $\mathcal{F}(\Sigma'_2)$ *normalizes* F *and induces a symplectic transformation of* $\overline{F}$ *sending* Σ'_1 *to* Σ'_2.

Proof. (i) This follows from Theorem 5.6.

(ii) By Proposition 5.10, the pointwise stabilizer of $\mathcal{F}(\Sigma'_1)$ in $U(\mathbb{C}^{2^m})$ normalizes F and hence induces a group of symplectic transformations on $\overline{F}$. As in the proof of Proposition 3.16, the pointwise stabilizer of Σ'_1 in $\mathrm{Sp}(2m, 2)$ is 1.

The unit circle enters as the scalars lying in the unitary group. The last part of (ii) follows from the fact that the product of an element of F with a scalar of order not dividing 4 also has order not dividing 4.

(iii) The sets $\mathcal{F}(A)$, with $A \in \Sigma_1$, are the maximal families of pairwise perpendicular members of $\mathcal{F}(\Sigma'_1)$. Part (ii) implies that, if $g \in U(\mathbb{C}^{2^m})$ sends $\mathcal{F}(\Sigma'_1)$ to $\mathcal{F}(\Sigma'_2)$, then g normalizes $\langle F, \mathbb{C}I\rangle$. Thus, g induces a symplectic transformation of $\langle F, \mathbb{C}I\rangle / Z(\langle F, \mathbb{C}I\rangle) \cong \overline{F}$.

In view of Corollary 10.9 below, it follows that, *if* m *is odd and composite, then there are more than* $2^{\sqrt{m}/2}$ *extremal line-sets* $\mathcal{F}(\Sigma')$ *that are inequivalent under the action of* $U(\mathbb{C}^{2^m})$.

6. *From the real space* $\mathbb{R}^{2^{m+1}}$ *to the complex space* $\mathbb{C}^{2^m}$

Let m be an odd integer and let $V = \mathbb{Z}_2^{m+1}$ and $E = E_{m+1}$ be as in § 3. Recall that $v_1, \ldots, v_{m+1}$ is the standard basis of V.

Fix an element $\omega \in E$ of order 4, so that $\overline{\omega}$ is a non-singular vector in $\overline{E}$. Writing $\omega = X(a)Y(b)(-I)^\gamma$ as in Lemma 2.1, we see from (2.3) that its centralizer is

$$C_E(\omega) = \{X(a')Y(b')(-I)^{\gamma'} \mid a', b' \in V,\ \gamma' \in \mathbb{Z}_2, \text{ and } a \cdot b' = a' \cdot b\},$$

so that $C_E(\omega)$ projects onto $\overline{\omega}^\perp$ by (2.5).

Since $\omega^2 = -I$, the eigenvalues of ω are $\pm i$, so ω fixes no 1-space of $\mathbb{R}^{2^{m+1}}$. In fact, for every vector u we have $(u, u\omega) = 0$ (since $(u, u\omega) = (u\omega, u\omega^2) = -(u, u\omega)$). Choose ω so that $\omega = X(a)Y(b)$ (cf. Lemma 2.1). Then $a \cdot b = 1$ by (2.4). Let V' be any hyperplane of V not containing a. By the definition of $X(a)$ and $Y(b)$ (cf. § 2), for any $v' \in V'$ we have $e_{v'}\omega = \pm e_{v'+a}$, where $v' + a \notin V'$. It follows that $\{e_{v'}, e_{v'}\omega \mid v' \in V'\}$ is an orthonormal basis of $\mathbb{R}^{2^{m+1}}$.

Also since $\omega^2 = -I$, we may identify the ring $\mathbb{R} + \omega\mathbb{R}$ with $\mathbb{C}$. In view of the conjugacy of elements of order 4 in E as expressed in Lemma 2.9(ii), for simplicity we may assume that $\omega = X(v_{m+1})Y(v_{m+1})$. However, it is important to note that *there are many different choices for fields isomorphic to* $\mathbb{C}$ *obtained in this manner*. For, we will have a specific orthogonal spread Σ of $\overline{E}$, so that we cannot freely change to a different copy of $\mathbb{C}$ while preserving Σ. (*Note.* Overbars will continue to have the same meaning as before; they will never be used to denote complex conjugation.)

Again for simplicity we choose $V' := \langle v_1, \ldots, v_m\rangle$. If we let $X(V') = \{X(b) \mid b \in V'\}$ and define $Y(V')$ similarly, then $E_m := X(V')Y(V')\langle -I\rangle$ is an extraspecial group of order 2^{1+2m}, and $F := C_E(\omega)$ is just $E_m\langle\omega\rangle$, as in § 5.

Now we can view $\mathbb{R}^{2^{m+1}}$ as $\mathbb{C}^{2^m}$. Then we have seen that $\{e_{v'} \mid v' \in V'\}$ is a basis over $\mathbb{C}$. Use this as an orthonormal basis over $\mathbb{C}$ in order to define a hermitian inner product. In an attempt to decrease the likelihood of confusion, throughout the remainder of this section we will use the notation $(\ ,\ )_\mathbb{R}$ and $(\ ,\ )_\mathbb{C}$ for the real and hermitian inner products on our vector space. Then $(u, u)_\mathbb{R} = (u, u)_\mathbb{C}$ for all vectors u, perpendicularity with respect to $(\ ,\ )_\mathbb{C}$ implies perpendicularity with respect to $(\ ,\ )_\mathbb{R}$ (but not vice versa), and F preserves $(\ ,\ )_\mathbb{C}$.

If $\overline{A}$ is a totally singular $(m+1)$-space of the orthogonal space $\overline{E}$, then the frame $\mathcal{F}(A)$ produces a set

$$\mathcal{F}_\omega(A) := \{\mathbb{C}u \mid \mathbb{R}u \in \mathcal{F}(A)\}$$

of 1-spaces of $\mathbb{C}^{2^m}$. Lemma 3.3(iii) implies that ω permutes the members of $\mathcal{F}(A)$. Since ω cannot fix any member of $\mathcal{F}(A)$, it must map each member to another one perpendicular to the first; together these two span a 1-space over $\mathbb{C}$. Any two complex 1-spaces obtained in this manner are perpendicular: $\mathcal{F}_\omega(A)$ *is a frame of* $\mathbb{C}^{2^m}$.

PROPOSITION 6.1. *Let* Σ *be an orthogonal spread of* $\overline{E}$, *and let* $\mathcal{F}(\Sigma)$ *be the corresponding set of lines in* $\mathbb{R}^{2^{m+1}}$. *Then*

$$\mathcal{F}_\omega(\Sigma) := \bigcup_{\overline{A} \in \Sigma} \mathcal{F}_\omega(A)$$

is a set of $2^m(2^m+1)$ *lines in* $\mathbb{C}^{2^m}$. *If* u *and* v *are unit vectors in different members of* $\mathcal{F}_\omega(\Sigma)$, *then* $|(u,v)_{\mathbb{C}}| = 0$ *or* $2^{-m/2}$.

Proof. We may assume that u and v are in members of $\mathcal{F}_\omega(A)$ and $\mathcal{F}_\omega(B)$ respectively, where $\overline{A}$ and $\overline{B}$ are distinct members of Σ. Let u_i, with $1 \leqslant i \leqslant 2^m$, be unit vectors in different members of $\mathcal{F}_\omega(A)$. Then $u_1, \ldots, u_{2^m}, u_1\omega, \ldots, u_{2^m}\omega$ is a *real* orthonormal basis (since $(\mathbb{C}u_i, \mathbb{C}u_j)_{\mathbb{C}} = 0$ for $i \neq j$, and we know that $(u_i, u_i\omega)_{\mathbb{R}} = 0$). Write

$$v = \sum_{j=1}^{2^m} u_j(a_j + b_j\omega) = \sum_{j=1}^{2^m} (a_j u_j + b_j(u_j\omega))$$

for some $a_j, b_j \in \mathbb{R}$. By Theorem 3.4, $a_j = (v, u_j)_{\mathbb{R}}$ and $b_j = (v, u_j\omega)_{\mathbb{R}}$ are $\pm 2^{-(m+1)/2}$. It follows that $|(v,u_j)_{\mathbb{C}}| = (a_j^2 + b_j^2)^{1/2} = 2^{-m/2}$. Since $u = \alpha u_j$ for some j and some scalar α of norm 1, we have $|(v,u)_{\mathbb{C}}| = 2^{-m/2}$.

7. *From orthogonal spreads to symplectic spreads and back*

We have yet to see how the line-set $\mathcal{F}_\omega(\Sigma)$ introduced in § 6 relates to symplectic spreads. Recall that $\omega = X(v_{m+1})Y(v_{m+1})$ has order 4.

Note that, if $\overline{A} \in \Sigma$, then $\overline{A} \not\subseteq \omega^\perp$; for otherwise $\overline{\omega} \in \overline{A}^\perp = \overline{A}$, which contradicts the non-singularity of the $\overline{\omega}$. Hence $\dim(\overline{A} \cap \overline{\omega}^\perp) = m$. Every singular vector in $\overline{\omega}^\perp$ is in a unique member of $\{\overline{A} \cap \overline{\omega}^\perp \mid \overline{A} \in \Sigma\}$. Now project into the symplectic $2m$-space $\overline{F} = \overline{\omega}^\perp / \langle\overline{\omega}\rangle$ in order to obtain the set

$$\Sigma_{\overline{\omega}} := \{\langle \overline{A} \cap \overline{\omega}^\perp, \overline{\omega}\rangle / \langle\overline{\omega}\rangle \mid \overline{A} \in \Sigma\}. \tag{7.1}$$

This is a family of $2^m + 1$ totally isotropic m-spaces covering all of $\overline{F}$: it is a symplectic spread.

Kantor [**16**] described a simple construction reversing this process. Start with a symplectic spread Σ' of $\overline{F} = \overline{\omega}^\perp / \langle\overline{\omega}\rangle$. This lifts to a set of totally singular m-spaces of $\overline{\omega}^\perp$, namely

$$\Sigma'' = \{W \mid W \text{ is a totally singular subspace of } \overline{\omega}^\perp \text{ that projects onto a member of } \Sigma'\}.$$

We may assume that one member of Σ'' is contained in $\overline{Y}(V)$. Every other member of Σ'' is contained in exactly two totally singular $(m+1)$-spaces of $\overline{E}$; exactly one of those meets $\overline{Y}(V)$ only in 0, and we choose this one. Let Σ be the set of all of the totally singular $(m+1)$-spaces of $\overline{E}$ arising in this way (including $\overline{Y}(V)$):

$$\Sigma := \{\overline{Y}(V)\} \cup \{X \mid X \text{ is a totally singular subspace of } \overline{E} \text{ that contains some member of } \Sigma'' \text{ and has only 0 in common with } \overline{Y}(V)\}. \tag{7.2}$$

Then Σ is an orthogonal spread of $\overline{E}$. Moreover, $\Sigma_{\overline{\omega}} = \Sigma'$ in the notation of the previous paragraph. We emphasize that this spread $\Sigma_{\overline{\omega}}$ depends on the choice of $\overline{\omega}$. Given Σ, different choices of $\overline{\omega}$ can produce inequivalent symplectic spreads

and inequivalent Kerdock codes. This is studied at length in [**17**]. Even when Σ' produces a desarguesian plane, after constructing Σ one can then make different choices of non-singular points $\overline{\omega}$ in order to obtain new planes and codes (this is crucial for Theorem 10.3 below).

We will also need a different and more computational way of viewing this process, in terms of the matrices appearing in Lemmas 2.12 and 4.7.

Consider a totally isotropic m-space W' of the symplectic space $\overline{F}$ such that $W' \cap \overline{Y}(V') = 0$. Let P be the binary symmetric $m \times m$ matrix such that $W' = \overline{X}(V') \left(\begin{smallmatrix} I & P \\ O & I \end{smallmatrix}\right)$ (cf. Lemma 4.7).

LEMMA 7.3. *There is a unique totally singular $(m+1)$-space $W = \overline{X}(V) \left(\begin{smallmatrix} I & M \\ O & I \end{smallmatrix}\right)$ of $\overline{E}$ such that $W \cap \overline{Y}(V) = 0$ and $\langle W \cap \overline{\omega}^{\perp}, \overline{\omega}\rangle / \langle \overline{\omega} \rangle = W'$. Here M is the binary skew-symmetric $(m+1) \times (m+1)$ matrix given by*

$$M = \begin{pmatrix} P + d(P)^T d(P) & d(P)^T \\ d(P) & 0 \end{pmatrix}, \tag{7.4}$$

where $d(P)$ is the vector in V' whose coordinates are the diagonal entries of P in the natural order.

REMARK. Equation (7.4) defines a bijection $P \mapsto M$ from symmetric $m \times m$ matrices P to skew-symmetric $(m+1) \times (m+1)$ matrices M. Indeed, given a skew-symmetric $(m+1) \times (m+1)$ matrix M, let the last row be $(d\ 0)$ and find P from the principal minor indicated in (7.4). Conversely, given a symmetric $m \times m$ matrix P, observe that the matrix M in (7.4) is, indeed, skew-symmetric. However, note that this bijection is not linear.

Proof of Lemma 7.3. Write vectors of $V = \mathbb{Z}_2^{m+1}$ in the form (v, α) with $v \in V' = \mathbb{Z}_2^m$ and $\alpha \in \mathbb{Z}_2$. Then the vectors of $\overline{E}$ can be written (v, α, z, β) with $v, z \in V'$ and $\alpha, \beta \in \mathbb{Z}_2$. Note that $\overline{Y}(V')$ consists of all vectors having $v = 0$ and $\alpha = 0$. By (2.4), the quadratic form Q is given by $Q(v, \alpha, z, \beta) = v \cdot z + \alpha\beta$.

We are given the subspace $W' = \{(v, vP) \mid v \in V'\}$ of $\overline{F} = \overline{X}(V')\overline{Y}(V')$. Since $\omega = X(v_{m+1})Y(v_{m+1})$, we have $\overline{\omega} = (0, 1, 0, 1)$ and hence $\overline{\omega}^{\perp} = \{(v, \alpha, y, \alpha) \mid v, y \in V', \alpha \in \mathbb{Z}_2\}$. Pulling W' back to $\overline{\omega}^{\perp}$ yields a unique totally singular m-space

$$\{(v, v \cdot d(P), vP, v \cdot d(P)) \mid v \in V'\}.$$

(For, this is an m-space, and is totally singular since $v \cdot vP = v \cdot d(P) = (v \cdot d(P))^2$ for all $v \in V'$.) Any totally singular $(m+1)$-space W properly containing this m-space must contain a vector of the form $(0, \alpha, y, \beta)$; this vector is singular if and only if α or β is 0. Since we want to have $W \cap \overline{Y}(V) = 0$, we must have $\alpha = 1$ and $\beta = 0$.

Since $(0, 1, y, 0)$ and $(v, v \cdot d(P), vP, v \cdot d(P))$ need to be perpendicular for all $v \in V'$, it follows that $y \cdot v = v \cdot d(P)$ and hence $y = d(P)$. Thus, W is uniquely determined (as we already observed above):

$$\begin{aligned} W &= \{(v, v \cdot d(P) + \alpha, vP + \alpha d(P), v \cdot d(P)) \mid v \in V', \alpha \in \mathbb{Z}_2\} \\ &= \{(v, \gamma, vP + vd(P)^T d(P) + \gamma d(P), v \cdot d(P)) \mid v \in V', \gamma \in \mathbb{Z}_2\} \end{aligned}$$

since $[v \cdot d(P)]d(P) = vd(P)^T d(P)$.

Note that the parity of m did not enter into the lemma. Also, there is a simple counterpart of this lemma for any perfect field of characteristic 2: just let the entries of $d(P)$ be the square roots of the diagonal entries of P in the natural order.

Now consider a symplectic spread Σ' of $\overline{F}$ containing $\overline{X}(V')$ and $\overline{Y}(V')$. Let $\Sigma' \setminus \{\overline{Y}(V)\}$ consist of the subspaces $\overline{A} = \overline{X}(V)\left(\begin{smallmatrix} I & P_A \\ O & I \end{smallmatrix}\right)$ for symmetric $m \times m$ matrices P_A. Then Lemma 7.3 lifts Σ' to the following orthogonal spread:

$$\Sigma = \{\overline{Y}(V)\} \cup \left\{ \overline{X}(V) \begin{pmatrix} I & M_{P_A} \\ O & I \end{pmatrix} \;\middle|\; \overline{A} \in \Sigma' \setminus \{\overline{Y}(V')\} \right\} \tag{7.5}$$

where

$$M_A = \begin{pmatrix} P_A + d(P_A)^T d(P_A) & d(P_A)^T \\ d(P_A) & 0 \end{pmatrix}. \tag{7.6}$$

Finally, we return to the complex line-set $\mathcal{F}_w(\Sigma)$ defined in Proposition 6.1.

PROPOSITION 7.7. *Let Σ be an orthogonal spread in $\overline{E}$, and let $\omega \in E$ have order* 4. *Then $\mathcal{F}_\omega(\Sigma) = \mathcal{F}(\Sigma_{\overline{\omega}})$.*

Proof. Let $\overline{A} \in \Sigma$. Let $A_{\overline{\omega}}$ denote the preimage in F of the member $\overline{A} \cap \overline{\omega}^\perp$ of the symplectic spread $\Sigma_{\overline{\omega}}$. It suffices to show that $\mathcal{F}_\omega(A) = \mathcal{F}(A_{\overline{\omega}})$, where the latter frame is calculated using $\Sigma_{\overline{\omega}}$.

Note that $A_{\overline{\omega}} = C_A(\omega)\langle \omega I \rangle$. Since A fixes each member of $\mathcal{F}(A)$, so does $C_A(\omega)$. Also, ω merges pairs of members of $\mathcal{F}(A)$ into 1-spaces over $\mathbb{C}$, and these pairs must be $C_A(\omega)$-invariant. Hence $A_{\overline{\omega}}$ fixes each 1-space in $\mathcal{F}_\omega(A)$. By Lemma 5.5(ii), there are exactly 2^m 1-spaces of $\mathbb{C}^{2^m}$ fixed by $A_{\overline{\omega}}$; we have found them all.

REMARKS. (1) By (7.2) and Lemmas 2.12(ii) and 4.7(ii), the correspondence (7.4) between binary symmetric $m \times m$ matrices P and binary skew-symmetric $(m+1) \times (m+1)$ matrices M commutes with the action of the general linear group $\mathrm{GL}(V')$. This is easy to verify directly, as shown below, and is to be expected since the matrix P depends on the choice of dual basis for $\overline{X}(V')$, $\overline{Y}(V')$, and $\mathrm{GL}(V')$ is transitive on such dual bases:

$$\begin{array}{ccc} P & \xrightarrow{(7.4)} & M = \begin{pmatrix} P + d(P)^T d(P) & d(P)^T \\ d(P) & 0 \end{pmatrix} \\ \Big\downarrow P \mapsto APA^T & & \Big\downarrow M \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} M \begin{pmatrix} A^T & 0 \\ 0 & 1 \end{pmatrix} \\ APA^T & \xrightarrow{(7.4)} & \begin{pmatrix} APA^T + Ad(P)^T d(P) A & Ad(P)^T \\ d(P)A^T & 0 \end{pmatrix} \end{array}$$

Hence (7.4) determines a many-to-one correspondence between congruence classes of symmetric $m \times m$ matrices under $\mathrm{GL}(V')$ and congruence classes of skew-symmetric $(m+1) \times (m+1)$ matrices under $\mathrm{GL}(V)$.

Any skew-symmetric matrix is congruent to a block diagonal matrix M_k with k diagonal blocks $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and all other entries 0. Thus, two skew-symmetric $(m+1) \times (m+1)$ matrices are congruent if and only if they have the same rank.

Any symmetric matrix is congruent to a block diagonal matrix $P_{\ell,j}$ with j diagonal blocks $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\ell - 2j$ diagonal blocks (1) and all other entries 0. The correspondence (7.4) maps the congruence classes containing $P_{2k,j}$ or $P_{2k-1,j}$ for some j to the congruence class containing M_k.

(2) Let M_1 and M_2 be the binary skew-symmetric $(m+1) \times (m+1)$ matrices obtained from the symmetric $m \times m$ matrices P_1, P_2 respectively under the correspondence (7.4). We claim that $\mathrm{Rank}(P_1 - P_2) = 1$ *or* 2 *if and only if* $\mathrm{Rank}(M_1 - M_2) = 2$. This provides a realization of the 'alternating forms graph' [**5**, pp. 281–284, 287] in terms of symmetric matrices.

First suppose that $\mathrm{Rank}(P_1 - P_2) = 1$ or 2. Then there exist $v, z \in V'$ such that

$$P_2 = P_1 + \varepsilon_1 v^T v + \varepsilon_2 z^T z + \varepsilon_3 (v^T z + z^T v)$$

for some $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathbb{Z}_2$. Note that $\varepsilon_3 = \varepsilon_2 \varepsilon_1$ if and only if $\mathrm{Rank}(P_2 - P_1) = 1$ and $P_2 = P_1 + (\varepsilon_1 v + \varepsilon_2 z)^T (\varepsilon_1 v + \varepsilon_2 z)$. For brevity, let $d_1 = d(P_1) \in V'$ be the vector whose entries are the diagonal elements of P_1 in the natural order. Then

$$M_1 = \begin{pmatrix} P_1 + d_1^T d_1 & d_1^T \\ d_1 & 0 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} P_2 + (d_1 + \varepsilon_1 v + \varepsilon_2 z)^T (d_1 + \varepsilon_1 v + \varepsilon_2 z) & (d_1 + \varepsilon_1 v + \varepsilon_2 z)^T \\ d_1 + \varepsilon_1 v + \varepsilon_2 z & 0 \end{pmatrix},$$

and

$$M_2 + M_1 = \begin{pmatrix} (\varepsilon_3 + \varepsilon_2 \varepsilon_1)(v^T z + z^T v) + d_1^T (\varepsilon_1 v + \varepsilon_2 z) & (\varepsilon_1 v + \varepsilon_2 z)^T \\ \quad + (\varepsilon_1 v^T + \varepsilon_2 z^T) d_1 & \\ \varepsilon_1 v + \varepsilon_2 z & 0 \end{pmatrix}.$$

If $\varepsilon_3 = \varepsilon_2 \varepsilon_1$ then

$$M_2 + M_1 = \begin{pmatrix} d_1^T \\ 1 \end{pmatrix} (\varepsilon_1 v + \varepsilon_2 z, 0) + \begin{pmatrix} (\varepsilon_1 v + \varepsilon_2 z)^T \\ 0 \end{pmatrix} (d_1, 1),$$

and if $\varepsilon_3 \neq \varepsilon_2 \varepsilon_1$ then $M_2 + M_1$ is similar to the matrix

$$\begin{pmatrix} z^T \\ \varepsilon_1 \end{pmatrix} (v, \varepsilon_2) + \begin{pmatrix} v^T \\ \varepsilon_2 \end{pmatrix} (z, \varepsilon_1).$$

In either case $\mathrm{Rank}(M_2 - M_1) = 2$. It is not hard to show that this argument reverses.

8. *From $\mathbb{Z}_4$-Kerdock codes to $\mathbb{Z}_2$-Kerdock codes*

In this section we show that the geometric map in § 7 from symplectic to orthogonal spreads induces the Gray map from the corresponding $\mathbb{Z}_4$-Kerdock code to its binary image.

The Gray map

First we need to recall the definition of the Gray map used by Hammons *et al.* in [**14**]. Figure 1 shows the Gray encoding of quaternary symbols $0, 1, 2, 3$ in $\mathbb{Z}_4$ as pairs of binary digits.

FIG. 1. The Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$

The 2-adic expansion of $c \in \mathbb{Z}_4$ is

$$c = \alpha(c) + 2\beta(c); \tag{8.1}$$

write $\gamma(c) = \alpha(c) + \beta(c)$ for all $c \in \mathbb{Z}_4$. We now have three maps $\mathbb{Z}_4 \to \mathbb{Z}_2$, as follows:

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

They extend in an obvious way to maps from $\mathbb{Z}_4^N$ to $\mathbb{Z}_2^N$ for any positive integer N. We construct binary codes from quaternary codes using the *Gray map* ϕ: $\mathbb{Z}_4^N \to \mathbb{Z}_2^{2N}$ given by

$$\phi(v) = (\beta(v), \gamma(v)), \quad \text{where } v \in \mathbb{Z}_4^N. \tag{8.2}$$

Figure 1 is the case $N = 1$ of this.

The *Lee weights* of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$ respectively, and the Lee weight $\mathrm{wt}_L(a)$ of $a \in \mathbb{Z}_4^N$ is the rational sum of the Lee weights of its components. This weight function defines a distance $d_L(\ ,\ )$ on $\mathbb{Z}_4^N$ called the *Lee metric.* The fundamental property of the Gray map [**14**] is that it is an *isometry* ($\mathbb{Z}_4^N$, Lee metric) $\to$ ($\mathbb{Z}_2^{2N}$, Hamming metric).

REMARKS. (1) The Gray map ϕ distinguishes the partition $\pi = \{\{i, i+N\} \mid i = 1, \ldots, N\}$ of the N coordinate positions. If we follow ϕ by an arbitrary permutation h (which is, of course, an isometry of ($\mathbb{Z}_2^{2N}$, Hamming metric)) then we obtain an isometry ($\mathbb{Z}_4^N$, Lee metric) $\to$ ($\mathbb{Z}_2^{2N}$, Hamming metric) that distinguishes the partition π^h. All isometries between these two metric spaces that send 0 to 0 arise in this manner.

(2) Equivalences of codes over $\mathbb{Z}_4$ use the group of monomial transformations, which preserves the Lee metric.

The Gray map and extraspecial 2-groups

We are now ready to relate spreads and extraspecial 2-groups to the Gray map. First we need to collect the notation scattered throughout earlier sections.

Let $m > 1$ be an odd integer, and let $E = E_{m+1}$ be the extraspecial 2-group of order $2^{1+2(m+1)}$ studied in §§2, 3 and 7. Let V' be the hyperplane $\langle v_1, \ldots, v_m \rangle$ of $V = \mathbb{Z}_2^{m+1}$ spanned by the first m standard basis vectors. Fix $\omega = X(v_{m+1})Y(v_{m+1}) \in E$ of order 4, as in §§6 and 7. Then $E_m := X(V')Y(V')\langle -I \rangle$ is an extraspecial group of order 2^{1+2m}, and we consider the slightly larger group $F = E_m\langle \omega I \rangle$. Overbars will denote the natural map $F \to F/Z(F)$, *not the natural map* $E \to E/Z(E)$. (Some care is needed with notation: $E/Z(E)$ and $F/Z(F)$ have dimension $2m+2$ and $2m$, respectively.)

Start with a symplectic spread Σ' of $\overline{F}$. By (5.3) this determines the $\mathbb{Z}_4$-code

$$\mathcal{K}_4(\Sigma') = \{(T_{P_{A'}}(v') + 2\widehat{s'} \cdot \widehat{v'} + \varepsilon')_{v' \in V'} \mid \overline{A}' \in \Sigma', s' \in V', \varepsilon' \in \mathbb{Z}_4\},$$

where $P_{A'}$ is the binary symmetric $m \times m$ matrix corresponding to the totally isotropic m-space $\overline{A}' \in \Sigma' \backslash \{\overline{Y}(V')\}$ via Lemma 4.7(i). (Note that the vector space called 'V'$= \mathbb{Z}_2^m$ in § 5 is now called 'V''.) By (7.2), the symplectic spread Σ' lifts to an orthogonal spread Σ of $E/Z(E)$; let $\widehat{A}$ denote the lift of $\overline{A}' \in \Sigma' \backslash \{\overline{Y}(V')\}$. (See the remark at the end of the last paragraph concerning the need for care with notation: we cannot write '$\overline{A}$' here.) In view of (3.1), Σ determines the $\mathbb{Z}_2$-code

$$\mathcal{H}(\Sigma) = \{(Q_{M_{\widehat{A}}}(v) + s \cdot v + \varepsilon)_{v \in V} \mid AZ/Z \in \Sigma,\ s \in V,\ \varepsilon \in \mathbb{Z}_2\},$$

where $M_{\widehat{A}}$ is the binary skew-symmetric $(m+1) \times (m+1)$ matrix corresponding via Lemma 2.12(i) to the totally singular $(m+1)$-space $\widehat{A} \in \Sigma$.

We view $V = V' \oplus \mathbb{Z}_2$ as listed so that the first 2^m coordinate positions are $(v'\ 0)$ and the rest are $(v'\ 1)$. This order of coordinates determines our Gray map.

THEOREM 8.3. *The Gray map sends* $\mathcal{K}_4(\Sigma')$ *to* $\mathcal{H}(\Sigma)$.

Proof. Consider the element $(T_{P_{A'}}(v') + 2s' \cdot v' + \varepsilon')_{v' \in V'}$ of $\mathcal{K}_4(\Sigma')$, where $\overline{A}' \in \Sigma'$, $s' \in V'$, $\varepsilon' \in \mathbb{Z}_4$. In order to simplify notation write $P = P_{A'}$ and $M = M_{\widehat{A}}$. Recall from (4.1) that

$$T_P(v') + 2\widehat{s}' \cdot \widehat{v}' + \varepsilon' = \sum_{j=1}^{m} P_{jj}\alpha_j^2 + 2\sum_{j<k} P_{jk}\alpha_j\alpha_k + 2\widehat{s}' \cdot \widehat{v}' + \varepsilon', \tag{8.4}$$

where $\widehat{v}' = (\alpha_1, \ldots, \alpha_m)$ is any lift of $v' = (v'_1, \ldots, v'_m)$ into $\mathbb{Z}_4^m$. We need the 2-adic expansion of (8.4), so first we need to determine $a, b \in \mathbb{Z}_2$ such that

$$\sum_j P_{jj}\alpha_j^2 = a + 2b. \tag{8.5}$$

Passing modulo 2 gives $d(P) \cdot v' = a$ since $\alpha_j^2 \equiv \alpha_j \pmod 2$. (Of course, here $d(P) \cdot v'$ is calculated in $\mathbb{Z}_2$.) Squaring (8.5) gives

$$\sum_j P_{jj}^2\alpha_j^4 + 2\sum_{j<k} P_{jj}P_{kk}\alpha_j^2\alpha_k^2 = a^2 = a\,,$$

so that

$$2b = \sum_j P_{jj}\alpha_j^2 - \sum_j P_{jj}^2\alpha_j^4 - 2\sum_{j<k} P_{jj}P_{kk}\alpha_j^2\alpha_k^2$$

and hence

$$b = \sum_{j<k} P_{jj}P_{kk}v'_jv'_k \quad \text{(calculated in } \mathbb{Z}_2\text{)},$$

since $\alpha_j^4 = \alpha_j^2$ for any $\alpha_j \in \mathbb{Z}_4$. This produces the required 2-adic expansion

$$\begin{aligned} &T_P(v') + 2\widehat{s}' \cdot \widehat{v}' + \varepsilon' \qquad (8.6)\\ &= (d(P)\cdot v' \oplus \lambda) + 2\left(\sum_{j<k}(P_{jk} + P_{jj}P_{kk})\alpha_j\alpha_k + \widehat{s}'\cdot\widehat{v}' + \lambda d(P)\cdot\widehat{v}' + \mu\right); \end{aligned}$$

here $\oplus$ denotes binary addition (so that $x + y = x \oplus y + 2xy$ for $x, y \in \{0, 1\} \subset \mathbb{Z}_4$), $\varepsilon' = \lambda + 2\mu$ is the 2-adic expansion of ε', and $d(P)$ is identified with its lift. Let U_P be the 'upper triangular portion' of $P + d(P)^T d(P)$, obtained by changing to 0 all entries of the latter matrix below the main diagonal; this is a 0,1 matrix, with entries viewed over $\mathbb{Z}_2$ or $\mathbb{Z}_4$, depending upon the context. Then $P + d(P)^T d(P) = U_P + U_P^T$, and we can rewrite (8.6) as

$$\begin{aligned} &T_P(v') + 2\widehat{s}' \cdot \widehat{v}' + \varepsilon'\\ &\quad = (d(P)\cdot\widehat{v}' \oplus \lambda) + 2(\widehat{v}'U_P\widehat{v}'^T + \widehat{s}'\cdot\widehat{v}' + \lambda d(P)\cdot\widehat{v}') + \mu\,. \qquad (8.7) \end{aligned}$$

By Lemma 7.3, the binary skew-symmetric $(m+1)\times(m+1)$ matrix M corresponding to P is given by

$$M = \begin{pmatrix} P + d(P)^T d(P) & d(P)^T \\ d(P) & 0 \end{pmatrix} = \begin{pmatrix} U_P & d(P)^T \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} U_P & d(P)^T \\ 0 & 0 \end{pmatrix}^T.$$

We are viewing V as the set of pairs $(v'\ \varepsilon)$ with $v' \in V'$ and $\varepsilon \in \mathbb{Z}_2$. Then one of the quadratic forms on V associated with M is given by

$$\begin{aligned} Q_M(v) &= (v'\ \varepsilon)\begin{pmatrix} U_P & d(P)^T \\ 0 & 0 \end{pmatrix}(v'\ \varepsilon)^T + (s'\ \lambda)\cdot(v'\ \varepsilon) + (\lambda d(P)\quad 0)\cdot(v'\ \varepsilon)\\ &= (\widehat{v}'U_Pv'^T + s'\cdot v' + \lambda d(P)\cdot v') + \varepsilon(v'd(P)^T + \lambda). \qquad (8.8) \end{aligned}$$

It remains to compare (8.7) and (8.8). Each $v' \in V'$ determines one coordinate position for $\mathbb{Z}_4^m$, with coordinate given by the left-hand side of (8.7). But v' also determines two coordinate positions for $V = \mathbb{Z}_2^{m+1}$, namely positions $(v'\ 0)$ and $(v'\ 1)$. By (8.7) and (8.8),

in position $v' \in \mathbb{Z}_4^m$ *there is a coordinate* $T_P(v') + 2\widehat{s}'\cdot\widehat{v}' + \varepsilon' \in \mathbb{Z}_4$;

this determines the following coordinates of a vector in $\mathbb{Z}_2^{m+1}$:

in position $(v'\ 0)$: $v'U_Pv'^T + s'\cdot v' + \lambda d(P)\cdot v' + \mu$;

in position $(v'\ 1)$: $v'U_Pv'^T + d(P)\cdot v' + s'\cdot v' + \lambda d(P)\cdot v' + \mu + \lambda$.

In view of the 2-adic expansion (8.7),

$$(d(P)\cdot v' \oplus \lambda) + 2(\widehat{v}'U_P\widehat{v}'^T + \widehat{s}'\cdot\widehat{v}' + \lambda d(P)\cdot\widehat{v}' + \mu)$$

produces

$$v'U_Pv'^T + s'\cdot v' + \lambda d(P)\cdot v' + \mu$$

and

$$v'U_P v'^T + s' \cdot v' + \lambda d(P) \cdot v' + d(P) \cdot v' + \mu + \lambda,$$

which is exactly the behaviour of the Gray map (8.2).

In view of Corollaries 3.5 and 5.7, this theorem can also be regarded as providing a transition from real to complex line-sets, as in Table 1.

This suggests another way to (try to) view the preceding theorem. Suppose that the relationship between real and complex line-sets via extraspecial groups had been noticed a few years ago. This would have suggested the definition of $\mathcal{K}_4(\Sigma')$, by analogy with $\mathcal{K}(\Sigma)$. The desire to see a relationship between $\mathcal{K}_4(\Sigma')$ and $\mathcal{K}(\Sigma)$ would then have led directly to the Gray map. This would *not*, however, have made evident the many remarkable properties of this map discovered by Hammons *et al.* [**14**].

In [**14**], a 'Preparata' code is constructed as follows: start with the classical Kerdock code but in its $\mathbb{Z}_4$-linear incarnation, form the dual code over $\mathbb{Z}_4$, and then pass back into the binary world. Therefore, it is important to understand the meaning of $\mathbb{Z}_4$-linearity of a $\mathbb{Z}_4$-Kerdock code. This is dealt with in the following proposition.

PROPOSITION 8.9. *The code $\mathcal{K}_4(\Sigma')$ is $\mathbb{Z}_4$-linear if and only if $\mathcal{S}(\Sigma') = \{P_{A'} \mid \overline{A}' \in \Sigma'\}$ is closed under binary addition.*

Proof. Let $\mathcal{Q}'$ be the additive group of all of the maps $T + \varepsilon\colon V' \to \mathbb{Z}_4$ such that T is a $\mathbb{Z}_4$-valued quadratic form and $\varepsilon \in \mathbb{Z}_4$ is a constant. This means that $T(u' + v') = T(u') + T(v') + 2\widehat{u}' P \widehat{v}'^T$ for all $u', v' \in V'$, where P is some binary symmetric $m \times m$ matrix. Note that $\mathcal{Q}'$ has a subgroup $\mathcal{L}'$ consisting of those maps $T + \varepsilon$ for which T is an additive map $V' \to \mathbb{Z}_4$. (Thus, the term 'quadratic' has to be viewed loosely.) Each P is associated with at least one form $T = T_P$, by (4.1); each T determines a unique P (recall that P is a binary matrix); and, by Lemma 4.3, the set of all T determining a given P is just the set of elements of the coset $T_P + \mathcal{L}'$ that send 0 to 0.

Consider the quotient group $\mathcal{Q}'/\mathcal{L}'$ (compare Cameron and Seidel [**9**]). Each of its elements can be written as $T_P + \mathcal{L}'$. If P and R are binary symmetric $m \times m$ matrices, we claim that

$$(T_P + \mathcal{L}') + (T_R + \mathcal{L}') = T_{P \oplus R} + \mathcal{L}', \tag{8.10}$$

where $\oplus$ again denotes binary addition. Namely, if $a, b \in \{0, 1\} \subset \mathbb{Z}_4$ then it is easy to check that $a + b = a \oplus b + 2ab$. By (4.1), if $v' \in V'$ and if $\widehat{v}' = (\alpha_1, \ldots, \alpha_m)$ is any lift of v', then

$$\begin{aligned} T_P(v') + T_R(v') &= \sum_j (P_{jj} + R_{jj})\alpha_j^2 + 2\sum_{j<k} (P_{jk} + R_{jk})\alpha_j \alpha_k \\ &= \sum_j (P \oplus R)_{jj}\alpha_j^2 + 2\sum_j P_{jj} R_{jj} \alpha_j^2 \ + 2\sum_{j<k} (P \oplus R)_{jk} \alpha_j \alpha_k, \end{aligned}$$

where $\widehat{v}' \mapsto 2\sum_j P_{jj} R_{jj} \alpha_j^2$ lies in $\mathcal{L}'$. Now (4.1) implies (8.10).

The $\mathbb{Z}_4$-Kerdock code $\mathcal{K}_4(\Sigma')$ can be viewed as the set of functions in the union of cosets $T_{P_{A'}} + \mathcal{L}'$: this code is the set of $|V'|$-tuples of values of these

functions. Hence, $\mathcal{K}_4(\Sigma')$ is $\mathbb{Z}_4$-linear if and only if these cosets form a subgroup; by (8.10), this occurs if and only if the set of symmetric matrices $P_{A'}$ is closed under binary addition.

In view of Dembowski [**12**, pp. 220, 237], it follows that

COROLLARY 8.11. *If $\mathcal{K}_4(\Sigma')$ is $\mathbb{Z}_4$-linear then the affine plane $\mathbf{A}(\Sigma')$ can be coordinatized by a (possibly non-associative) division algebra.*

The preceding proposition also suggests that we define

$$\mathcal{P}_4(\Sigma') := \mathcal{K}_4(\Sigma')^{\perp} \quad \text{if } \mathcal{K}_4(\Sigma') \text{ is linear,} \tag{8.12}$$

and call $\mathcal{P}_4(\Sigma')$ a $\mathbb{Z}_4$-*linear Preparata code*: it has the same Lee weight distribution as the $\mathbb{Z}_4$-linear Preparata code constructed in [**14**]. Moreover, again as in [**14**], $\phi(\mathcal{P}_4(\Sigma'))$ is a binary 'Preparata' code: it has the same (Hamming) weight distribution as one of the original Preparata codes. We will study these codes in detail in § 10.

9. *Examples*

EXAMPLE 9.1. The spread Σ' that produces the desarguesian affine plane $\mathbf{A}(\Sigma) = \mathrm{AG}(2, 2^m)$ consists of the 1-spaces of $\mathrm{GF}(2^m)^2$: the line $x = 0$, and the lines $y = ax$ for $a \in \mathrm{GF}(2^m)$ (compare (5.2)). This spread is symplectic with respect to any non-singular alternating bilinear form $(\ ,\ )$ on $W = \mathrm{GF}(2^m)^2$. If $\mathrm{Tr}\colon \mathrm{GF}(2^m) \to \mathrm{GF}(2)$ is the trace map, then $\mathrm{Tr}(\ ,\ )$ is a non-singular alternating bilinear form on the $\mathrm{GF}(2)$-space W. Since the members of Σ' were totally isotropic over $\mathrm{GF}(2^m)$, they remain totally isotropic over $\mathrm{GF}(2)$. Hence, Σ' is a symplectic spread when W is viewed either as a $\mathrm{GF}(2^m)$-space or as a $\mathrm{GF}(2)$-space. By Theorem 5.6, we obtain a family of $2^m(2^m + 1)$ lines in $\mathbb{C}^{2^m}$.

EXAMPLE 9.2. Assume that m is odd. The (desarguesian) symplectic spread described above determines an orthogonal spread Σ of an $\Omega^+(2m + 2, 2)$-space via the geometric correspondence (7.2). The Kerdock set $\{M_A \mid \overline{A} \in \Sigma \setminus \{\overline{Y}(V)\}\}$ in § 3 can be described as follows. Let $m > 1$ be odd, let $L = \mathrm{GF}(2^{rm})$, let $K = \mathrm{GF}(2^r)$, and let $\mathrm{Tr}\colon L \to K$ be the trace map. For $a \in L$ let M_a be the K-linear map $L \oplus K \to L \oplus K$ given by

$$(x, \alpha)M_a = (a^2x + a\,\mathrm{Tr}(ax) + \alpha a, \mathrm{Tr}(\alpha x))\,.$$

Then $\{M_a \mid a \in L\}$ is a Kerdock set: if $L \oplus K$ is equipped with the bilinear form $(x, \alpha) \cdot (y, \beta) := \mathrm{Tr}(xy) + \alpha\beta$, then $(x, \alpha)M_a \cdot (x, \alpha) = 0$ for all a, x, α, and $M_a + M_b$ is non-singular for any $a \neq b$ in L. This is the 'standard' Kerdock set when $K = \mathrm{GF}(2)$, producing the original Kerdock code $\mathcal{K}(\Sigma)$ (Dillon [**13**], Kantor [**16**]). (Here we have switched to linear transformations $L \to L$ in place of the $mr \times mr$ matrices appearing in the definition of Kerdock sets.)

On the other hand, in this case the $\mathbb{Z}_4$-Kerdock code $\mathcal{K}_4(\Sigma')$ constructed in § 5 is the $\mathbb{Z}_4$-linear code that appears in a paper by Hammons *et al.* [**14**, § 4.3]. The construction of the $\mathbb{Z}_4$-linear Kerdock and 'Preparata' codes by Hammons *et al.* [**14**] requires the Galois ring $\mathrm{GR}(4^m)$, an extension of $\mathbb{Z}_4$ of degree m, containing a $(2^m - 1)$th root of unity. To begin, let $h_2(x) \in \mathbb{Z}_2[X]$ be a primitive irreducible

polynomial of degree m. Then there is a unique monic polynomial $h(X) \in \mathbb{Z}_4[X]$ of degree m such that $h(X) \equiv h_2(X) \pmod 2$, and $h(X)$ divides $X^{2^m-1} - 1 \pmod 4$. Let ξ be a root of $h(X)$, so that $\xi^{2^m-1} = 1$. The *Galois ring* $\mathrm{GR}(4^m)$ is defined to be $\mathbb{Z}_4[\xi]$. Every element $c \in \mathrm{GR}(4^m)$ has a unique 2-adic representation $c = a + 2b$, where a and b are taken from the set $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{2^m-2}\}$. The *Frobenius map* f from $\mathrm{GR}(4^m)$ to itself is the ring automorphism that takes any element $c = a + 2b \in \mathrm{GR}(4^m)$ to $c^f = a^2 + 2b^2$. This map f generates the Galois group of $\mathrm{GR}(4^m)$ over $\mathbb{Z}_4$, and $f^m = 1$. The *relative trace* from $\mathrm{GR}(4^m)$ to $\mathbb{Z}_4$ is defined by

$$T(c) = c + c^f + \ldots + c^{f^{m-1}}, \quad \text{where } c \in \mathrm{GR}(4^m).$$

The $\mathbb{Z}_4$-linear Kerdock code $\mathcal{K}$ and 'Preparata' code $\mathcal{P}$ constructed by Hammons *et al.* [**14**] are

$$\mathcal{K} = \{(T(\lambda x) + \varepsilon)_{x \in \mathcal{T}} \mid \lambda \in \mathrm{GR}(4^m), \ \varepsilon \in \mathbb{Z}_4\}$$

and its dual code $\mathcal{P} = \mathcal{K}^\perp$. Thus, $\mathcal{P}$ is the $\mathbb{Z}_4$-linear code consisting of the vectors $(c_x)_{x \in \mathcal{T}}$, with $c_x \in \mathbb{Z}_4$, such that

$$\sum_{x \in \mathcal{T}} c_x = 0 \quad \text{and} \quad \sum_{x \in \mathcal{T}} c_x x = 0.$$

In order to connect the Kerdock code $\mathcal{K}$ with (5.3), write

$$\mathcal{K} = \{(T(\lambda_1 x) + 2T(\lambda_2 x) + \varepsilon)_{x \in \mathcal{T}} \mid \lambda_1, \lambda_2 \in \mathcal{T}, \ \varepsilon \in \mathbb{Z}_4\}.$$

Let ψ denote reduction modulo 2. Then ψ maps the Galois ring $\mathrm{GR}(4^m)$ to the finite field $\mathrm{GF}(2^m)$. We will view V' as $\mathrm{GF}(2^m)$, and also as $\mathcal{T}$: for each $v \in V'$ let $\psi^{-1}(v)$ denote the preimage of v lying in $\mathcal{T}$ (this is our old $\widehat{v}$). The map $v \mapsto 2T[\lambda_1 \psi^{-1}(v)]$ is a linear functional on $\mathrm{GF}(2^m)$. We claim that $v \mapsto T[\lambda_1 \psi^{-1}(v)]$ *defines a* $\mathbb{Z}_4$*-valued quadratic form on* $\mathrm{GF}(2^m)$:

$$T[\lambda_1 \psi^{-1}(v + w)] = T[\lambda_1 \psi^{-1}(v)] + T[\lambda_1 \psi^{-1}(w)] + 2B(v, w)$$

for some symmetric bilinear form $B(\ ,\ )$ on V'. In order to see this, write $\psi^{-1}(v) + \psi^{-1}(w) = a + 2b$ with $a, b \in \mathcal{T}$, so that $a = \psi^{-1}(v + w)$. Then

$$\begin{aligned} a = (a + 2b)^{2^m} &= (\psi^{-1}(v) + \psi^{-1}(w))^{2^m} \\ &= \psi^{-1}(v) + \psi^{-1}(w) + 2[\psi^{-1}(v)\psi^{-1}(w)]^{1/2}, \end{aligned}$$

so that

$$T[\lambda_1 \psi^{-1}(v + w)] - T[\lambda_1 \psi^{-1}(v)] - T[\lambda_1 \psi^{-1}(w)] = 2T[\lambda_1^2 \psi^{-1}(v)\psi^{-1}(w)],$$

as required. Consequently, $\mathcal{K}$ can, indeed, be written as in (5.3).

EXAMPLE 9.3. When m is odd and composite, Kantor [**17**] constructed exponential numbers of inequivalent orthogonal spreads of $\Omega^+(2m + 2, 2)$-space ('inequivalent' means that these are in different $O^+(2m + 2, 2)$-orbits). These spreads produce Kerdock sets and Kerdock codes over both $\mathbb{Z}_2$ and $\mathbb{Z}_4$. However, by Proposition 8.9 and Corollary 8.11 the $\mathbb{Z}_4$-codes are linear if and only if the associated set of symmetric matrices is closed under addition, in which case the associated translation plane $\mathbf{A}(\Sigma')$ is coordinatized by a non-associative division algebra. Very few examples of such spreads are known; they can all be described as follows [**16**].

Let $n > 1$ be odd, let $L = \mathrm{GF}(2^{rn})$, let $K = \mathrm{GF}(2^r)$, and let $\mathrm{Tr}: L \to K$ be the trace map. For $a \in L$ let P_a be the K-linear map $L \to L$ given by

$$xP_a = a^2x + a\,\mathrm{Tr}(x) + \mathrm{Tr}(ax).$$

Then $a \mapsto P_a$ is additive, and, if $a \neq 0$, then P_a is non-singular (Kantor [**16**, II, (5.4)]). (*Proof.* If $xP_a = 0$, write $z = ax$. Then $z^2 + z\,\mathrm{Tr}(x) + x\,\mathrm{Tr}(z) = 0$. Apply Tr and obtain $\mathrm{Tr}(z)^2 + \mathrm{Tr}(z)\,\mathrm{Tr}(x) + \mathrm{Tr}(x)\,\mathrm{Tr}(z) = 0$. Then $\mathrm{Tr}(z) = 0$ and hence $z^2 + z\,\mathrm{Tr}(x) = 0$. If $z \neq 0$ then $z = \mathrm{Tr}(x) \in K$; but then $\mathrm{Tr}(z) = z$ since n is odd, which produces the contradiction $z = 0$ since $\mathrm{Tr}(z) = 0$.)

Now equip L with the non-singular symmetric bilinear form $\mathrm{Tr}(xy)$, for $x, y \in L$. Then a straightforward calculation shows that

$$\mathrm{Tr}((xP_a)y) = \mathrm{Tr}(x(yP_a)) \quad \text{for all } a, x, y \in L\,,$$

so that P_a is symmetric (with respect to an orthonormal basis of L). Passing to GF(2) by using the trace map $K \to \mathrm{GF}(2)$ as in Example 9.1, we obtain a non-singular symmetric bilinear form on the GF(2)-space L with respect to which each P_a is symmetric.

When $m = rn$ is odd, let $\Sigma'(r, n)$ denote the symplectic spread of $\overline{F}$ obtained using this GF(2)-space of symmetric matrices, and let $\Sigma(r, n)$ denote the corresponding orthogonal spread of $\overline{E}$ obtained by means of (7.2). The following proposition summarizes information contained in a paper by Kantor [**16**].

PROPOSITION 9.4. (i) *The spreads* $\Sigma'(r_1, n_1)$ *and* $\Sigma'(r_2, n_2)$ *are inequivalent if* $(r_1, n_1) \neq (r_2, n_2)$.

(ii) *The spread* $\Sigma(1, m)$ *is equivalent to the orthogonal spread in Example* 9.2, *but* $\Sigma'(1, m)$ *is not equivalent to the desarguesian spread in Example* 9.1 *if* $m > 3$.

(iii) *If* Σ' *is a symplectic spread of* $\overline{F}$ *that behaves as in Proposition* 8.9 *and whose associated orthogonal spread* (*cf.* (7.2)) *is equivalent to the one in Example* 9.2, *then* Σ' *is equivalent to either the desarguesian spread or* $\Sigma'(1, m)$.

(iv) *The spread* $\Sigma(r, n)$ *is not equivalent to* $\Sigma(1, rn)$ *if* $r > 1$.

Proof. (i) [**16**, II, (5.5),(7.1)].
(ii) [**16**, I, (4.1) and II, § 5].
(iii) [**16**, I, (4.1)].
(iv) This follows from (iii).

In general, $\Sigma(r_1, n_1)$ and $\Sigma(r_2, n_2)$ are inequivalent if $(r_1, n_1) \neq (r_2, n_2)$. This and related questions have been addressed by Michael Williams in his thesis [**34**].

10. *Inequivalence*

We now return to the general framework of § 5, with the goal of discussing the problem of equivalence among the Gray images of the $\mathbb{Z}_4$-linear Preparata codes described above and those binary Preparata codes known previously. We begin by writing a generator matrix $G_4(\Sigma')$ for the $\mathbb{Z}_4$-linear Kerdock code $\mathcal{K}_4(\Sigma')$ given by (5.3). As in § 8, the 2^m coordinate positions are labelled by the

vectors v in $V' = \mathbb{Z}_2^m$. Let $P_1, \ldots, P_m$ be a basis for the space $\langle P_A \mid \bar{A} \in \Sigma' \rangle$, so that the $\mathbb{Z}_4$-valued quadratic forms $T_i = T_{P_i}$, for $1 \leqslant i \leqslant m$, span the $\mathbb{Z}_4$-module $\langle T_{P_A} \mid \bar{A} \in \Sigma' \rangle$. Then

$$G_4(\Sigma') = \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ & \cdots & T_1(v) & \cdots & \\ & & \vdots & & \\ & \cdots & T_m(v) & \cdots & \end{pmatrix}.$$

The Kerdock code $\mathcal{K}$ constructed by Hammons *et al.* [**14**] is generated by the matrix

$$\begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ & \cdots & T(x) & \cdots & \\ & \cdots & T(\zeta x) & \cdots & \\ & & \vdots & & \\ & \cdots & T(\zeta^{m-1}x) & \cdots & \end{pmatrix},$$

where the 2^m coordinate positions are indexed by $\mathcal{T} = \{0, 1, \zeta, \ldots, \zeta^{2^m-2}\}$ and $\mathcal{T}$ has been identified with V' as in Example 9.2. Recall that $T(\zeta^i x)$ defines a $\mathbb{Z}_4$-valued quadratic from, as observed above in Example 9.2.

Note that $\langle 2T_{P_A} \mid \bar{A} \in \Sigma' \rangle$ is the binary vector space of all linear functionals $v \mapsto 2\widehat{s} \cdot \widehat{v}$, where $s \in V'$. (Hence, $T_1, \ldots, T_m$ is a $\mathbb{Z}_4$-basis of the $\mathbb{Z}_4$-module $\langle T_{P_A} \mid \bar{A} \in \Sigma' \rangle$.) Write $s_i = d(P_i)$ (cf. (4.1) and Lemma 7.3), so that $s_1, \ldots, s_m$ is a basis of V', and the matrix

$$G_4 = \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ & \cdots & 2\widehat{s_1} \cdot \widehat{v} & \cdots & \\ & & \vdots & & \\ & \cdots & 2\widehat{s_m} \cdot \widehat{v} & \cdots & \end{pmatrix}$$

generates a $\mathbb{Z}_4$-linear code $\mathrm{RM}(1, m)_4$ that is common to all of the Kerdock codes $\mathcal{K}_4(\Sigma')$ given by (5.3). (This notation $\mathrm{RM}(1, m)_4$ arises from the fact [**14**, Theorem 7] that its Gray image $\phi(\mathrm{RM}(1, m)_4)$ is the usual $\mathbb{Z}_2$-linear first-order Reed–Muller code $\mathrm{RM}(1, m+1)$ of length 2^{m+1}.)

The matrix $G_4(\Sigma')$ is a parity check matrix for the $\mathbb{Z}_4$-linear Preparata code $\mathcal{P}_4(\Sigma')$ defined in (8.12). Also, G_4 is a parity check matrix for a $\mathbb{Z}_4$-linear code $H_4 = \mathrm{RM}(1, m)_4^{\perp}$. We note in passing that the Lee weight distribution of H_4 is the MacWilliams transform of that of $\mathrm{RM}(1, m)_4$, and hence the weight distribution of the binary code $\phi(H_4)$ is the MacWilliams transform of that of $\mathrm{RM}(1, m+1)$: the weight distribution of $\phi(H_4)$ is the same as that of the $\mathbb{Z}_2$-linear extended Hamming code of length 2^{m+1}. What is important for us is the fact that, when $m \geqslant 5$, the binary code $\phi(H_4)$ is non-linear [**14**, Theorem 8]. (When $m = 3$, $\phi(H_4)$ is the Hamming code [**14**, Theorem 18].)

Since $\mathrm{RM}(1, m)_4 \subseteq \mathcal{K}_4(\Sigma')$, we have $\mathcal{P}_4(\Sigma') = \mathcal{K}_4(\Sigma')^{\perp} \subseteq \mathrm{RM}(1, m)_4^{\perp} = H_4$. Let $\widetilde{H}_4$ denote the $\mathbb{Z}_4$-linear code whose parity check matrix is

$$2G_4(\Sigma') = \begin{pmatrix} 2 & \cdots & 2 & \cdots & 2 \\ & \cdots & 2T_1(v) & \cdots & \\ & & \vdots & & \\ & \cdots & 2T_m(v) & \cdots & \end{pmatrix} = \begin{pmatrix} 2 & \cdots & 2 & \cdots & 2 \\ & \cdots & 2\widehat{s_1} \cdot \widehat{v} & \cdots & \\ & & \vdots & & \\ & \cdots & 2\widehat{s_m} \cdot \widehat{v} & \cdots & \end{pmatrix}.$$

Then $H_4 \subseteq \widetilde{H}_4$, and $\phi(\widetilde{H}_4)$ is $\mathbb{Z}_2$-linear.

LEMMA 10.1. *For $m \geqslant 5$, $\phi(\widetilde{H}_4)$ is the binary span of $\phi(H_4)$. The codewords of weight 2 in $\phi(H_4)$ are the vectors $v_i + v_{2^m+i}$, with $i = 1, \ldots, 2^m$, where $v_1, \ldots, v_{2^{m+1}}$ is the standard basis of $V = \mathbb{Z}_2^{2^{m+1}}$.*

Proof. Since $H_4 \subseteq \widetilde{H}_4$ and $\phi(\widetilde{H}_4)$ is linear, $\langle \phi(H_4) \rangle \subseteq \phi(\widetilde{H}_4)$. Moreover, since $\phi(H_4)$ is non-linear,

$$2^{2^m-m-2} = |\phi(H_4)| < |\langle \phi(H_4) \rangle| \leqslant |\phi(\widetilde{H}_4)| = 2^{2^m-m-1},$$

and it follows that $\langle \phi(H_4) \rangle = \phi(\widetilde{H}_4)$.

Thus, we must determine the words of weight 2 in $\phi(H_4)$. The words of Lee weight 2 in $\mathbb{Z}_4$ are those whose coordinates consist either of a single 2 and all others 0, or of two ± 1's and all others 0. The first type of word annihilates G_4, and its Gray image is exactly a vector $v_i + v_{2^m+i}$ for some i. No word of the second type can lie in H_4 since linear functionals separate points.

Zaitzev, Zinoviev and Semakov [**36**] proved that any binary code P of length 2^{m+1} with the same Hamming distance distribution as the original Preparata code [**29**] is contained in a uniquely determined binary code H with the same Hamming distance distribution as the extended Hamming code of length 2^{m+1}. Moreover, H is the union of P together with all binary vectors at Hamming distance 4 from P (or equivalently, $H = \bigcup \{P + w \mid w \text{ has weight } 4\}$). Note that the Gray map can be used to translate this theorem into the metric space ($\mathbb{Z}_4^{2^m}$, Lee metric); this was done explicitly by Hammons *et al.* [**14**, § 5.4] in the case of the Preparata code $\mathcal{P}_4(\Sigma')$, where Σ' is the desarguesian spread. In the case of the 'standard binary Preparata codes', the above partition was studied by Preparata [**29**], Baker *et al.* [**3**] and Kantor [**18**].

LEMMA 10.2. *For $m \geqslant 5$, no standard binary Preparata code is equivalent to the Gray image $\phi(\mathcal{P}_4(\Sigma'))$ of a $\mathbb{Z}_4$-linear Preparata code $\mathcal{P}_4(\Sigma')$.*

Proof. Any equivalence would be a linear transformation of the underlying vector space $\mathbb{Z}_2^{2^{m+1}}$, and hence send subspaces to subspaces. The binary span of any standard Preparata code is the usual extended Hamming code. However, we have already observed that $\phi(\mathcal{P}_4(\Sigma'))$ spans a larger code (by Lemma 10.1, it has words of weight 2).

THEOREM 10.3. *Let $m \geqslant 5$, and let $\mathcal{H}_4$ and $\mathcal{H}_4^\sharp$ be two $\mathbb{Z}_4$-linear Kerdock codes arising as in* (5.3). *Let $\mathcal{P}_4 = \mathcal{H}_4^\perp$ and $\mathcal{P}_4^\sharp = \mathcal{H}_4^{\sharp\perp}$ be the corresponding $\mathbb{Z}_4$-linear Preparata codes. Then the following are equivalent:*

(i) *$\mathcal{H}_4$ and $\mathcal{H}_4^\sharp$ are equivalent linear codes in $\mathbb{Z}_4^{2^m}$;*

(ii) *$\mathcal{P}_4$ and $\mathcal{P}_4^\sharp$ are equivalent linear codes in $\mathbb{Z}_4^{2^m}$;*

(iii) *$\phi(\mathcal{H}_4)$ and $\phi(\mathcal{H}_4^\sharp)$ are equivalent codes in $\mathbb{Z}_2^{2^{m+1}}$; and*

(iv) *$\phi(\mathcal{P}_4)$ and $\phi(\mathcal{P}_4^\sharp)$ are equivalent codes in $\mathbb{Z}_2^{2^{m+1}}$.*

Proof. Since monomial transformations of $\mathbb{Z}_4^{2^m}$ preserve the inner product, (i) and (ii) are equivalent. Before discussing (iv) we need to discuss the monomial transformations of $\mathbb{Z}_2^{2^{m+1}}$ induced from those of $\mathbb{Z}_4^{2^m}$. If g is any monomial transformation of $\mathbb{Z}_4^{2^m}$, then an isometry h of $\mathbb{Z}_2^{2^{m+1}}$ is determined by the following diagram:

$$\begin{array}{ccc} \mathbb{Z}_4^{2^m} & \xrightarrow{\ g\ } & \mathbb{Z}_4^{2^m} \\ {\scriptstyle \phi^{-1}}\uparrow & & \downarrow{\scriptstyle \phi} \\ \mathbb{Z}_2^{2^{m+1}} & \xrightarrow{\ h\ } & \mathbb{Z}_2^{2^{m+1}} \end{array}$$

Then h is a permutation of coordinates. This already shows that (i) implies (iii) and (ii) implies (iv), but we will need to be more explicit. The following two diagrams show the effect of h on the entries in the ith and $(i+2^m)$th coordinate positions for $i = 1, \ldots, 2^m$; the position j depends upon the effect of the monomial transformation g, as does the effect on the entry $a+2b$ in position i:

$$\begin{array}{ccc} \overset{i\text{th}}{a+2b} & \xrightarrow{\ g\ } & \overset{j\text{th}}{a+2b} \\ {\scriptstyle \phi^{-1}}\uparrow & & \downarrow{\scriptstyle \phi} \\ \underset{i\text{th}}{(b \mid a+b)} & \xrightarrow{\ h\ } & \underset{j\text{th}}{(b \mid a+b)} \\ & \underset{(i+2^m)\text{th}}{} & \quad \underset{(j+2^m)\text{th}}{} \end{array} \qquad \begin{array}{ccc} \overset{i\text{th}}{a+2b} & \xrightarrow{\ g\ } & \overset{j\text{th}}{a+2(a+b)} \\ & & = -(a+2b) \\ {\scriptstyle \phi^{-1}}\uparrow & & \downarrow{\scriptstyle \phi} \\ \underset{i\text{th}}{(b \mid a+b)} & \xrightarrow{\ h\ } & \underset{j\text{th}}{(a+b \mid b)} \\ & \underset{(i+2^m)\text{th}}{} & \quad \underset{(j+2^m)\text{th}}{} \end{array}$$

In particular, it follows that the permutation h preserves the partition $\pi = \{\{i, i+2^m\} \mid i = 1, \ldots, 2^m\}$. Conversely, every permutation of the coordinates of $\mathbb{Z}_2^{m+1}$ that preserves π arises from some monomial transformation of $\mathbb{Z}_4^m$. This can be seen either from the above diagrams, or by observing that the group of monomial permutations of $\mathbb{Z}_4^m$, and the group of permutations of the coordinates of $\mathbb{Z}_2^{m+1}$ preserving π, both have order $2^{2^m} 2^m!$.

We are now ready to prove that (iv) implies (ii) in the theorem. As noted prior to the proof of Lemma 10.2, $\phi(H_4)$ is uniquely determined by $\phi(\mathcal{P}_4)$, and hence so is its linear span $\langle \phi(H_4) \rangle$ as well as the set of vectors of weight 2 in that span. Consequently, by Lemma 10.1 the partition π can be recovered from $\phi(\mathcal{P}_4)$, and hence so can both ϕ and $\mathcal{P}_4$. If h is a coordinate permutation of $\mathbb{Z}_2^{m+1}$ that sends $\phi(\mathcal{P}_4)$ to $\phi(\mathcal{P}_4^\sharp)$, it follows that h preserves π, and hence lifts to an equivalence $\mathcal{P}_4 \to \mathcal{P}_4^\sharp$.

In order to prove that (iii) implies (i), we will study combinatorial aspects of the binary Kerdock code $\mathcal{K} := \phi(\mathcal{K}_4)$ in a manner superficially similar to what we have just done in order to prove that (iv) implies (ii). There is an equivalence relation on $\mathcal{K}$ defined as follows: two words are equivalent if and only if they are at distance 0, 2^m or 2^{m+1}; the equivalence classes are precisely the cosets of $\mathrm{RM}(1, m+1)$ (cf. Proposition 3.12). We will use the description of $\mathcal{K}$ coming from the proof of Theorem 8.3: each coset looks like

$$J_A := (v' U_{P_A} v'^T \mid v' U_{P_A} v'^T + d(P_A) \cdot v') + \mathrm{RM}(1, m+1)$$

for some $\overline{A} \in \Sigma\backslash\{\overline{Y}(V)\}$; here, P_A is as in (5.1)–(5.3), and U_{P_A} is the 'upper triangular' portion of $P_A + d(P_A)^T d(P_A)$ as in (8.7), so that $P_A + d(P_A)^T d(P_A) = U_{P_A} + U_{P_A}^T$.

Let J denote the following subset of $\mathbb{Z}_2^V$:

$$J := \{a + b + c \mid a \in J_A,\ b \in J_B,\ c \in J_C,\ \text{with } \overline{A}, \overline{B}, \overline{C} \in \Sigma\backslash\{\overline{Y}(V)\} \text{ and } P_A + P_B + P_C = 0\} + \mathrm{RM}(1, m+1).$$

If $P_A + P_B + P_C = 0$ then $d(P_A) + d(P_B) + d(P_C) = 0$. Thus, each coset of $\mathrm{RM}(1, m+1)$ contained in J has a coset representative that looks like

$$(v'(U_{P_A} + U_{P_B} + U_{P_C})v'^T \mid v'(U_{P_A} + U_{P_B} + U_{P_C})v'^T).$$

By the definition of $U_{P_A}, U_{P_B}, U_{P_C}$,

$$\begin{aligned}(U_{P_A} + U_{P_B} + U_{P_C}) + (U_{P_A} + U_{P_B} + U_{P_C})^T &= d(P_A + P_B)^T d(P_A + P_B) + d(P_A)^T d(P_A) + d(P_B)^T d(P_B) \\ &= d(P_A)^T d(P_B) + d(P_B)^T d(P_A).\end{aligned}$$

Thus, $U_{P_A} + U_{P_B} + U_{P_C} + d(P_A)^T d(P_B)$ is symmetric.

It follows that

$$\begin{aligned}v'(U_{P_A} + U_{P_B} + U_{P_C})v'^T &= v'd(P_A)^T d(P_B)v'^T + v'd(d(P_A)^T d(P_B))v'^T \\ &= [d(P_A) \cdot v'][d(P_B) \cdot v'] + d(d(P_A)^T d(P_B)) \cdot v'.\end{aligned}$$

Then

$$J = \{([d(P_A) \cdot v'][d(P_B) \cdot v'] \mid [d(P_A) \cdot v'][d(P_B) \cdot v']) \mid \overline{A}, \overline{B} \in \Sigma\backslash\{\overline{Y}(V)\}\} + \mathrm{RM}(1, m+1).$$

Since $\{M_A \mid \overline{A} \in \Sigma\backslash\{\overline{Y}(V)\}\}$ is a Kerdock set, $d(P_A)$ can be any vector in V' (cf. (7.4)). Thus,

$$J = \{(\ell_1(v')\ell_2(v') + \mu \mid \ell_1(v')\ell_2(v') + \mu + \lambda) \mid \ell_1, \ell_2 \in V'^*,\ \mu, \lambda \in \mathbb{Z}_2\},$$

where V'^* denotes the dual space of V' (note that $\ell_1(v')\ell_1(v') = \ell_1(v')$).

We now turn to the subspace $J^\perp$ of $\mathbb{Z}_2^V$ (of course, J itself is not a subspace). For any distinct $u_1, u_2 \in V'$, let $w(u_1, u_2)$ denote the word in $\mathbb{Z}_2^V$ whose $(u_1\ 0), (u_1\ 1), (u_2\ 0)$ and $(u_2\ 1)$ coordinates are 1 while all others are 0. Then $w(u_1, u_2)$ is a word of weight 4 in $J^\perp$.

We claim that *these are the only words of weight* 4 *in* $J^\perp$. For, suppose that there is another word with this property. Then this must correspond to the following equation holding for all $\ell_1, \ell_2 \in V'^*$ and some distinct $u_1, u_2, u_3 \in V'$:

$$\sum_1^4 \ell_1(u_i)\ell_2(u_i) = \gamma, \qquad \text{a constant.}$$

It is easy to check that this is impossible. (Namely, we may assume that $u_1 \neq 0, u_4$. Choosing ℓ_1 and ℓ_2 to vanish at all u_i we see that $\gamma = 0$; choosing ℓ_1 and ℓ_2 so that $\ell_1(u_1) = \ell_2(u_1) = 1$ and $\ell_1(u_i)\ell_2(u_i) = 0$ for $i \neq 1$, we obtain the contradiction $\gamma = 1$.)

It is easy to check that these words $w(u_1, u_2)$ of weight 4 have the following property: two vectors $(v_1'\ \varepsilon_1), (v_2'\ \varepsilon_2) \in V$ appear in more than one word $w(u_1, u_2)$ if and only if $v_1' = v_2'$.

Now note that J and $J^\perp$ were obtained canonically from $\mathcal{K}$, and hence so is the partition π discussed earlier in this proof. This means that $\mathcal{K}_4$ *has been recovered from* $\mathcal{K}$. Moreover, as we saw earlier, it follows that any equivalence $\phi(\mathcal{K}_4) \to \phi(\mathcal{K}_4^\sharp)$ lifts to an equivalence $\mathcal{K}_4 \to \mathcal{K}_4^\sharp$, as required.

The above proof also showed the following.

PROPOSITION 10.4. *If $\mathcal{K}_4$ is a $\mathbb{Z}_4$-linear Kerdock code of length $m \geqslant 5$, then there is only one $\mathbb{Z}_4$-linear structure on $\phi(\mathcal{K}_4)$, and only one on $\phi(\mathcal{P}_4)$.*

We have seen that, in the $\mathbb{Z}_4$-linear case, each equivalence $\phi(\mathcal{K}_4) \to \phi(\mathcal{K}_4^\sharp)$ lifts to an equivalence $\mathcal{K}_4 \to \mathcal{K}_4^\sharp$. What does such a lifting look like in terms of orthogonal spreads? We will consider this question in detail, in one important case, without assuming $\mathbb{Z}_4$-linearity. In order to state our result precisely, we need to recall some notation from §§ 2 and 5. As in earlier sections, coordinate vectors and matrices will be written with respect to the basis $\overline{X}(v_1), \ldots, \overline{X}(v_{m+1}), \overline{Y}(v_1), \ldots, \overline{Y}(v_{m+1})$ of $\overline{E}$. For example, $\overline{X}(v_{m+1})$ is the vector with 1 in position $m+1$ and 0 elsewhere.

Given an orthogonal spread Σ of $\overline{E}$, as usual we will consider the symplectic spread $\Sigma' = \Sigma_{\bar{\omega}}$ of $\overline{F}$ obtained from it as (7.1) using $\bar{\omega} = \overline{X}(v_{m+1})\overline{Y}(v_{m+1})$. Corresponding to Σ' is a set $\mathcal{S}(\Sigma')$ of binary symmetric matrices obtained as in (5.1). Earlier, we were able to avoid cumbersome notation involving the dependence of all of these objects on choices made for our two members $\overline{X}(V)$ and $\overline{Y}(V)$ of Σ as well as on the non-singular point $\bar{\omega}$, but now we will have to be somewhat more careful. Therefore, we will write $\mathcal{S}(\Sigma') = \mathcal{S}(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$; but note that we are still suppressing the notation for the dual bases chosen for $\overline{X}(V)$ and $\overline{Y}(V)$. Similarly, we will write $\mathcal{K}_4(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ instead of $\mathcal{K}_4(\Sigma')$. Now we can state the following general result concerning the equivalence of $\mathbb{Z}_4$-Kerdock codes.

THEOREM 10.5. *Let Σ and $\Sigma^\sharp$ be orthogonal spreads of $\overline{E}$ containing $\overline{X}(V)$ and $\overline{Y}(V)$. Let $\bar{\omega}$ be as above. Then the following are equivalent:*

(i) *$\mathcal{K}_4(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ and $\mathcal{K}_4(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ are equivalent $\mathbb{Z}_4$-Kerdock codes;*

(ii) *there are an invertible $m \times m$ matrix R, and a vector $s' \in V'$, such that the map $P \mapsto R[P + d(P)^T s' + s'^T d(P)]R^T$ sends $\mathcal{S}(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ to $\mathcal{S}(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$; and*

(iii) *there is an orthogonal transformation of $\overline{E}$ that sends Σ to $\Sigma^\sharp$ while fixing $\overline{X}(V), \overline{Y}(V)$, and $\overline{X}(v_{m+1})$.*

Proof. Assume (i), and let g be a monomial transformation of $\mathbb{Z}_4^{2^m}$ that induces an equivalence $\mathcal{K}_4(\Sigma') \to \mathcal{K}_4(\Sigma'^\sharp)$. By (4.1) or (4.2) together with (5.2), the subcode $2\mathcal{K}_4(\Sigma')$ can be identified with the first-order Reed–Muller code (here, $\mathbb{Z}_2$ is identified with $\mathbb{Z}_4/2\mathbb{Z}_4$). Since $2\mathcal{K}_4(\Sigma')g = 2\mathcal{K}_4(\Sigma'^\sharp)$, the equivalence g permutes coordinates via an affine transformation $v' \mapsto v'R + w'$ for some non-singular $m \times m$ matrix R and some $w' \in V'$.

Since g is a monomial transformation, it sends the all-one word to a word in $\mathcal{K}_4(\Sigma'^\sharp)$ all of whose coordinates are ± 1. In the notation of (5.3), this means that,

for some A, $T_{P_A}(v') + \varepsilon = \pm 1$ for all $v' \in V'$. By (8.6), $d(P_M) \cdot \widehat{v}' + \varepsilon = \pm 1$ for all $v' \in V'$, and hence $0 + \varepsilon = \pm 1$ and $d(P_M) \cdot \widehat{v}' = 0$ for all $v' \in V'$. Consequently, g sends the all-one word to one of the form

$$\pm(2\widehat{s'} \cdot \widehat{v'} + 1)_{v'} = \pm((-1)^{s' \cdot v})_{v'} \tag{10.6}$$

with $s' \in V'$. (*Note.* This is a remarkable identity associated with the ring $\mathbb{Z}_4$: it converts between additive and multiplicative notation in an unexpectedly simple manner.) It follows that g is given by

$$(c_{v'})g = \left((-1)^{s' \cdot (v'R + w')} c_{v'R + w'}\right)$$

for some $s' \in V'$.

By (5.3), the translation $v' \mapsto v' + w'$ is an automorphism of $\mathcal{H}_4(\Sigma'^{\sharp})$. Hence, we may suppose that the equivalence g takes the form

$$(c_{v'})g = \left((-1)^{s' \cdot v'R} c_{v'R}\right).$$

Let $(T_P(v'))_{v'} \in \mathcal{H}_4(\Sigma')$ arise from the $\mathbb{Z}_4$-valued quadratic form T_P corresponding (as in (4.2)) to the binary symmetric matrix $P \in \mathcal{S}(\Sigma')$, and let $(T_P(v'))_{v'}g = (T^{\sharp}(v'))_{v'} \in \mathcal{H}_4(\Sigma'^{\sharp})$. We need to calculate $\Delta := T^{\sharp}(u' + v') - T^{\sharp}(u') - T^{\sharp}(v')$ in order to determine the binary symmetric matrix underlying the $\mathbb{Z}_4$-valued quadratic form $T^{\sharp}(v')$ as in (4.2):

$$\begin{aligned}
\Delta &= (-1)^{s' \cdot (u'R + v'R)} T_P(u'R + v'R) - (-1)^{s' \cdot (u'R)} T_P(u'R) \\
&\quad - (-1)^{s' \cdot (v'R)} T_P(v'R) \\
&= (-1)^{s' \cdot (u'R + v'R)} [T_P(u'R) + T_P(u'R) + 2\widehat{u'R} P \widehat{v'R}^T] \\
&\quad - (-1)^{s' \cdot (u'R)} T_P(u'R) - (-1)^{s' \cdot (v'R)} T_P(v'R) \\
&= T_P(u'R)[(-1)^{s' \cdot (u'R + v'R)} - (-1)^{s' \cdot (u'R)}] \\
&\quad + T_P(v'R)[(-1)^{s' \cdot (u'R + v'R)} - (-1)^{s' \cdot (v'R)}] + 2\widehat{u'R} P \widehat{v'R}^T \\
&= T_P(u'R) 2\widehat{s'} \cdot \widehat{v'R} + T_P(v'R) 2\widehat{s'} \cdot \widehat{u'R} + 2\widehat{u'R} P \widehat{v'R}^T,
\end{aligned}$$

using (10.6). By (4.1), $2T_P(v'R) = 2\widehat{d(P)} \cdot \widehat{u'R}$, while $2[\widehat{d(P)} \cdot \widehat{u'R}][\widehat{s'} \cdot \widehat{u'R}] = \widehat{u'R}\widehat{d(P)}^T \widehat{s'}\, \widehat{v'R}^T$ by straightforward matrix multiplication. Thus,

$$\begin{aligned}
\Delta &= 2\widehat{u'R}[P + \widehat{d(P)}^T \widehat{s'} + \widehat{s'}^T \widehat{d(P)}] \widehat{v'R}^T \\
&= 2\widehat{u'R}[P + d(P)^T \widehat{s'} + \widehat{s'}^T \widehat{d(P)}] R^T \widehat{v'}^T.
\end{aligned}$$

It follows from (4.2) that the binary symmetric matrix associated with $(T_P(v'))_{v'}g$ is $R[P + s'^T d(P) + d(P)^T s']R^T$. This is precisely the assertion in (ii).

Conversely, starting with $\mathcal{S}(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$, $\mathcal{S}(\Sigma^{\sharp}, \overline{X}(V), \overline{Y}(V), \bar{\omega})$, R and s' as in (ii), reverse the preceding argument in order to obtain (i).

Next we show that (ii) implies (iii). Let $P \in \mathcal{S}(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$, and write $P^{\sharp} = R^T[P + s'^T d(P) + d(P)^T s']R$, so that $P^{\sharp} \in \mathcal{S}(\Sigma^{\sharp}, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ by hypothesis. Let M and $M^{\sharp}$ be the skew-symmetric matrices obtained, respectively, from P and $P^{\sharp}$ using (7.4). Then

$$M = \begin{pmatrix} M_1 & d(P)^T \\ d(P) & 0 \end{pmatrix} \quad \text{and} \quad M^{\sharp} = \begin{pmatrix} P^{\sharp} + d(P^{\sharp})^T d(P^{\sharp}) & d(P^{\sharp})^T \\ d(P^{\sharp}) & 0 \end{pmatrix},$$

where $M_1 = P + d(P)^T d(P)$. Let

$$B = \begin{pmatrix} R^{-T} & s^T \\ O & 1 \end{pmatrix} \quad \text{and} \quad \widetilde{B} = \begin{pmatrix} B & O \\ O & B^{-T} \end{pmatrix}. \tag{10.7}$$

Then $\widetilde{B}$ is the matrix of an element of $O^+(\overline{E})$ (cf. Lemma 2.9(i)), and

$$\widetilde{B}^{-1} \begin{pmatrix} I & M \\ O & I \end{pmatrix} \widetilde{B} = \begin{pmatrix} I & O & R[M_1 + s'^T d(P) + d(P)^T s']R^T & R^T d(P)^T \\ O & 1 & d(P)R & 0 \\ O & O & I & O \\ O & 0 & O & 1 \end{pmatrix}.$$

Here,

$$\begin{aligned} R^T[M_1 + s'^T d(P) + d(P)^T s']R \\ = R^T[P + s'^T d(P) + d(P)^T s']R + [d(P)R]^T[d(P)R], \end{aligned}$$

where $d(R^T PR) = d(P)R = d\big(P + s'^T d(P) + d(P)^T s'\big)R$ since

$$\begin{aligned} (R^T PR)_{ii} &= \sum_{kj} R_{ki} P_{kj} R_{ji} \\ &= \sum_{j<k} (R_{ki} P_{kj} R_{ji} + R_{ji} P_{jk} R_{ki}) + \sum_k R_{ki} P_{kk} R_{ki} \\ &= \sum_k P_{kk} R_{ki} \end{aligned}$$

(as $R_{ki} P_{kj} R_{ji} = R_{ji} P_{jk} R_{ki}$). Consequently,

$$\widetilde{B}^{-1} \begin{pmatrix} I & M \\ O & I \end{pmatrix} \widetilde{B} = \begin{pmatrix} I & M^\sharp \\ O & I \end{pmatrix},$$

and $\widetilde{B}$ sends Σ to $\Sigma^\sharp$ since it fixes Y and

$$X \begin{pmatrix} I & M \\ O & I \end{pmatrix} \widetilde{B} = X\widetilde{B}^{-1} \begin{pmatrix} I & M \\ O & I \end{pmatrix} \widetilde{B} = X \begin{pmatrix} I & M^\sharp \\ O & I \end{pmatrix}.$$

Thus, $\widetilde{B}$ behaves as in (iii).

Conversely, suppose that $\widetilde{B}$ is a matrix inducing an orthogonal transformation as in (iii). Then $\widetilde{B}$ can be written as in (10.7) for some invertible matrix R and some $s' \in V'$. Reversing the previous argument, we find that

$$R^T[P + s'^T d(P) + d(P)^T s']R \in \mathcal{S}(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$$

whenever $P \in \mathcal{S}(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$, and hence that (ii) holds.

COROLLARY 10.8. *If $\mathcal{K}_4(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ and $\mathcal{K}_4(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ are two equivalent $\mathbb{Z}_4$-Kerdock codes, then the binary Kerdock codes $\mathcal{K}(\Sigma)$ and $\mathcal{K}(\Sigma^\sharp)$ are also equivalent.*

COROLLARY 10.9. *For each odd composite integer m, there are more than $2^{\sqrt{m}/2}$ inequivalent $\mathbb{Z}_4$-Kerdock codes of length 2^{2^m}, and more than $2^{\sqrt{m}/2}$ inequivalent $\mathbb{Z}_2$-Kerdock codes of length $2^{2^{m+1}}$.*

Proof. By a result of Kantor [**18**], there are more than $2^{\sqrt{m}/2}$ inequivalent orthogonal spreads of $\overline{E}$.

The codes in the previous corollary are non-linear. The argument in the next consequence of Theorem 10.5 explains what condition (iii) means when dealing with the case $\Sigma = \Sigma^\sharp$.

COROLLARY 10.10. *The $\mathbb{Z}_4$-linear Kerdock codes arising from Examples* 9.2 *and* 9.3 *are equivalent.*

Proof. The desarguesian spread Σ' of $\overline{F}$ in Example 9.1 yields an orthogonal spread Σ of $\overline{E}$ as in Example 9.2, and $X(V), \overline{Y}(V) \in \Sigma$. Fix $s' \in V' \setminus \{0\}$, write $R = I$, let B and $\widetilde{B}$ be as in (10.7), and set $\Sigma^\sharp := \Sigma\widetilde{B}$. Then $\widetilde{B}$ induces an orthogonal transformation of $\overline{E}$ having order 2 and behaving as in Theorem 10.5. It remains to describe the $\mathbb{Z}_4$-Kerdock codes $\mathcal{H}_4(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ and $\mathcal{H}_4(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$.

The code $\mathcal{H}_4(\Sigma, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ is just the $\mathbb{Z}_4$-Kerdock code in Example 9.2: the one discovered by Hammons *et al.* [**14**].

The code $\mathcal{H}_4(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$, the set $\mathcal{S}(\Sigma^\sharp, \overline{X}(V), \overline{Y}(V), \bar{\omega})$ of symmetric matrices, and a certain symplectic spread determine one another as in (5.8) and (5.3). This symplectic spread is the one called $\Sigma^\sharp_{\bar{\omega}}$ in (7.1). It is equivalent to the symplectic spread $(\Sigma^\sharp\widetilde{B})_{\bar{\omega}\widetilde{B}} = \Sigma_{\bar{\omega}\widetilde{B}}$. Here, $\bar{\omega}\widetilde{B} = \overline{X}(v_{m+1})\overline{Y}(s' + v_{m+1})$. By Proposition 9.4(ii), if $s' \neq 0$ then $\Sigma_{\bar{\omega}\widetilde{B}}$ is equivalent to the symplectic spread in Example 9.3.

COROLLARY 10.11. *If m is odd and composite then there is a $\mathbb{Z}_4$-linear Kerdock code not equivalent to the one in Example* 9.2. *The corresponding $\mathbb{Z}_4$-linear Preparata code and binary Preparata code are also not equivalent to ones arising from Examples* 9.2 *and* 9.3.

Proof. By Proposition 9.4(iii), if $m = rn$ with $r, n > 1$, then the orthogonal spreads $\Sigma(r, n)$ and $\Sigma(1, m)$ are not equivalent. Hence, neither are the Kerdock codes $\mathcal{H}_4(\Sigma(r, n), \overline{X}(V), \overline{Y}(V), \bar{\omega})$ and $\mathcal{H}_4(\Sigma(1, m), \overline{X}(V), \overline{Y}(V), \bar{\omega})$, by Theorem 10.5. The case of Preparata codes follows from Theorem 10.3.

A census of binary Preparata codes

The following binary Preparata codes are presently known.

(i) The original Preparata codes (Preparata [**29**]).

(ii) The variants of (i) studied by Baker *et al.* [**3**] and Kantor [**18**].

(iii) The codes (other than the one of length 2^4 in (i)) constructed by Hammons *et al.* [**14**] as Gray images of $\mathbb{Z}_4$-linear codes.

(iv) The codes in Corollary 10.11.

The isomorphisms among the codes (i) and (ii) were completely determined in [**18**]. These codes span the usual extended Hamming code; the codes in (iii) and (iv) do not, by Lemma 10.1. Consequently, the codes in (iii) and (iv) are not equivalent to any in (i) or (ii), and they are not equivalent to one another by Proposition 9.4.

Additional $\mathbb{Z}_4$-linear Preparata codes can be constructed by using Example 9.3 together with (7.4). Very recently, large numbers of other binary and $\mathbb{Z}_4$-linear

Preparata codes have been obtained by a generalization of the constructions in Example 9.3 and the preceding corollaries [**34**].

11. *Extraspecial p-groups, symplectic spreads and complex line-sets with prescribed angles*

Let $q = p^m$ for any odd prime p and any integer $m \geqslant 1$. Let V be an m-dimensional vector space over GF(p), and label the standard basis of $\mathbb{C}^q$ as e_v, where $v \in V$. Equip $\mathbb{C}^q$ with the usual hermitian inner product; again let $U(\mathbb{C}^q)$ be the corresponding unitary group. Let ξ be a primitive pth root of unity in $\mathbb{C}$. For $b \in V$ define elements of $U(\mathbb{C}^q)$ by

$$X(b)\colon\ e_v \mapsto e_{v+b} \quad \text{and} \quad Y(b) := \operatorname{diag}[\xi^{b\cdot v}].$$

Let $X(V) := \{X(b) \mid b \in V\}$ and $Y(V) := \{Y(b) \mid b \in V\}$.

LEMMA 11.1. *The group $E := \langle X(V), Y(V)\rangle$ is extraspecial of order p^{1+2m}, and $Z(E) = \langle \xi I\rangle$. Moreover, $E = X(V)Y(V)\langle -I\rangle$, and every element E can be written uniquely in the form $X(a)Y(b)(\xi I)^\gamma$ for some $a, b \in V$ and $\gamma \in \mathrm{GF}(p)$.*

Again let $\overline{E} = E/Z(E)$, and for $b \in V$ write $e_b^* = p^{-m/2}\sum_v \xi^{b\cdot v} e_v$.

LEMMA 11.2. *The following hold:*

(i) $\{\langle e_v\rangle \mid v \in V\}$ *is the set of irreducible submodules for* $Y(V)$*;*

(ii) $\{\langle e_b^*\rangle \mid b \in V\}$ *is the set of irreducible submodules for* $X(V)$.

We identify $Z(E)$ with GF(p) in order to obtain a non-singular alternating bilinear form on $\overline{E}$ defined by $(\overline{e}_1, \overline{e}_2) = [e_1, e_2] \in Z(E)$. As in (2.5), $\big(\overline{X}(a)\overline{Y}(b), \overline{X}(a')\overline{Y}(b')\big) = a'\cdot b - a\cdot b'$. The m-spaces $\overline{X}(V)$ and $\overline{Y}(V)$ are totally isotropic and have only 0 in common.

There is a subgroup GL(V) of $U(\mathbb{C}^q)$ normalizing E and acting on $\overline{E}$ exactly as in Lemma 2.9(i).

LEMMA 11.3. *Let $\overline{A}$ and $\overline{B}$ be totally isotropic m-spaces of the symplectic space $\overline{E}$ over* GF(p).

(i) *The set $\mathcal{F}(A)$ of A-irreducible subspaces of $\mathbb{C}^q$ is an orthogonal frame.*

(ii) *If $\overline{A} \cap \overline{B} = 0$, and if u_1 and u_2 are unit vectors in different members of $\mathcal{F}(A) \cup \mathcal{F}(B)$, then $|(u_1, u_2)| = 0$ or $p^{-m/2}$.*

THEOREM 11.4. *Let Σ be any symplectic spread of the symplectic space $\overline{E}$. Then*

$$\mathcal{F}(\Sigma) := \bigcup_{\overline{A}\in\Sigma} \mathcal{F}(A)$$

consists of $q(q+1)$ lines with the following property: if u_1 and u_2 are unit vectors in different members of $\mathcal{F}(\Sigma)$ then $|(u_1, u_2)| = 0$ or $p^{-m/2}$.

The complex line-set $\mathcal{F}(\Sigma)$ is extremal in the sense described following (5.9). Some of these line-sets (those corresponding to desarguesian planes) appear in

papers by Levenštein [**25**, p. 529] and König [**22**, Theorem 2] stripped of our group-theoretic and geometric contexts.

LEMMA 11.5. *The group of all elements of $U(\mathbb{C}^q)$ sending each of the frames $\mathcal{F}(X(V))$, $\mathcal{F}(Y(V))$, to itself normalizes E.*

COROLLARY 11.6. *Let Σ_1 and Σ_2 be symplectic spreads of $\overline{E}$.*

(i) *Any symplectic transformation sending Σ_1 to Σ_2 is induced by an element of $U(\mathbb{C}^q)$ sending $\mathcal{F}(\Sigma_1)$ to $\mathcal{F}(\Sigma_2)$ (in fact by many such unitary transformations). In particular, the set-stabilizer of Σ_1 in $\mathrm{Sp}(2m, p)$ is induced by a subgroup of $U(\mathbb{C}^{p^m})$ preserving the frame $\mathcal{F}(\Sigma)$.*

(ii) *The pointwise stabilizer of $\mathcal{F}(\Sigma)$ in $U(\mathbb{C}^q)$ is $\langle E, CI\rangle$ where $C \subseteq \mathbb{C}^*$ is the unit circle.*

(iii) *Any element of $U(\mathbb{C}^q)$ sending $\mathcal{F}(\Sigma_1)$ to $\mathcal{F}(\Sigma_2)$ induces a projective symplectic transformation of $\overline{E}$ sending Σ_1 to Σ_2.*

Note that (4.5) and Lemma 4.7 hold without change with $d_M := \mathrm{diag}[\xi^{vMv^T/2}]$.

As in Example 1 of § 9, desarguesian planes produce examples of symplectic spreads and hence of extremal complex line-sets. However, there are relatively few examples known of non-desarguesian symplectic spreads in odd characteristic. These are surveyed in [**2**] and [**19**]. Once again, in spite of the small numbers known, there must be large numbers of inequivalent examples.

The odd behaviour of 4

It is natural to wonder, both in the context of Hammons *et al.* [**14**] and the present paper, whether there might be a theory of codes over rings other than $\mathbb{Z}_4$ paralleling these recent developments. While there is no way to 'prove' that no such analogues exist, our geometric and group-theoretic points of view provide some negative indications.

First of all, this section dealt with symplectic spaces, not orthogonal ones. There is no analogue in odd characteristic of the peculiar but wonderful relationships between orthogonal and symplectic spaces and groups. In characteristic 2, every quadratic form produces an alternating bilinear form (since $(v, v) = Q(v + v) - Q(v) - Q(v) = 0$). Nothing comparable occurs in odd characteristic, neither from a purely computational point of view nor within finite group theory or finite geometry.

Next, in § 4 we extended an extraspecial 2-group E_m to a slightly larger group F. This had the effect of increasing the numbers of elements of order 2 and 4 without introducing elements of larger orders. This is what produces an action of a full symplectic group, and helps to explain the occurrence of this slightly larger group F. Extending further, by further increasing the size of the centre, would also introduce elements of larger orders. Such extensions are of less interest, and do not arise in any natural group-theoretic context (compare [**1**, pp. 109–111]).

This proves nothing, it merely suggests that neither $\mathrm{GF}(p)$ with p odd, nor $\mathbb{Z}_8$, is likely to produce results close to what has been discovered using $\mathbb{Z}_4$. The natural progression on the right-hand side of our 'road map' in Table 1 is to the quaternion world. This suggests that the 'correct' generalization will involve

a non-abelian group in place of $\mathbb{Z}_4$; the quaternion case will be investigated elsewhere.

Acknowledgement. We are grateful to J. I. Hall and a referee for numerous helpful comments.

References

1. M. ASCHBACHER, *Finite group theory* (Cambridge University Press, 1986).
2. L. BADER, W. M. KANTOR, and G. LUNARDON, 'Symplectic spreads from twisted fields', *Boll. Un. Mat. Ital. A* (7) 8 (1994) 383–389.
3. R. D. BAKER, J. H. VAN LINT, and R. M. WILSON, 'On the Preparata and Goethals codes', *IEEE Trans. Inform. Theory* 29 (1983) 342–345.
4. A. A. BLOKHUIS and J. J. SEIDEL, 'Few-distance sets in $\mathbb{R}^{p,q}$', *Combinatorica. Convegno Roma 23–26 maggio 1983*, Symposia Mathematica 28 (Istitut Nazionale di Alta Matematica Francesco Severi, Rome; Academic Press, London, 1986), pp. 145–158.
5. A. E. BROUWER, A. M. COHEN, and A. NEUMAIER, *Distance-regular graphs* (Springer, New York, 1989).
6. A. E. BROUWER and L. M. G. M. TOLHUIZEN, 'A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters', *Des. Codes Cryptogr.* 3 (1993) 95–98.
7. E. H. BROWN, 'Generalizations of Kervaire's invariant', *Ann. of Math.* 95 (1972) 368–383.
8. P. J. CAMERON and J. H. VAN LINT, *Designs, graphs, codes and their links*, London Mathematical Society Student Texts 22 (Cambridge University Press, 1991).
9. P. J. CAMERON and J. J. SEIDEL, 'Quadratic forms over GF(2)', *Indag. Math.* 35 (1973) 1–8.
10. P. DELSARTE and J. M. GOETHALS, 'Alternating bilinear forms over GF(q)', *J. Combin. Theory Ser. A* 19 (1975) 26–50.
11. P. DELSARTE, J. M. GOETHALS, and J. J. SEIDEL, 'Bounds for systems of lines and Jacobi polynomials', *Philips Res. Repts.* 30 (1975) 91–105.
12. P. DEMBOWSKI, *Finite geometries* (Springer, Berlin, 1968).
13. J. F. DILLON, 'Elementary Hadamard difference sets', Ph.D. thesis, University of Maryland, 1974.
14. A. R. HAMMONS JR, P. V. KUMAR, A. R. CALDERBANK, N. J. A. SLOANE, and P. SOLÉ, 'The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes', *IEEE Trans. Inform. Theory* 40 (1994) 301–319.
15. B. HUPPERT, *Endliche Gruppen I* (Springer, New York, 1967).
16. W. M. KANTOR, 'Spreads, translation planes and Kerdock sets, I, II', *SIAM J. Alg. Discr. Math.* 3 (1982) 151–165, 308–318.
17. W. M. KANTOR, 'An exponential number of generalized Kerdock codes', *Inform. Control* 53 (1982) 74–80.
18. W. M. KANTOR, 'On the inequivalence of generalized Preparata codes', *IEEE Trans. Inform. Theory* 29 (1983) 345–348.
19. W. M. KANTOR, 'Note on Lie algebras, finite groups and finite geometries', *Groups, difference sets, and the monster* (eds K. T. Arasu *et al.*, de Gruyter, Berlin, 1996), pp. 73–81.
20. A. M. KERDOCK, 'A class of low-rate non-linear binary codes', *Inform. Control* 20 (1972) 182–187.
21. P. B. KLEIDMAN and M. W. LIEBECK, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series 129 (Cambridge University Press, 1990).
22. H. KÖNIG, 'Isometric embeddings of euclidean spaces into finite-dimensional ℓ_p-spaces', Banach Center Publications 34 (PWN, Warsaw, 1995), pp. 79–87.
23. T. KOORNWINDER, *The addition formula for Jacobi polynomials, II* (Math. Centrum Amsterdam Afd. Toegepaste Wisk. Rep. 133, 1972).
24. T. KOORNWINDER, 'The addition formula for Jacobi polynomials and spherical harmonics', *SIAM J. Appl. Math.* 25 (1973) 236–246.
25. V. I. LEVENŠTEIN, 'Bounds on the maximal cardinality of a code with bounded modulus of the inner product', *Soviet Math. Dokl.* 25 (1982) 526–531.
26. J. H. VAN LINT, 'Kerdock and Preparata codes', *Congr. Numer.* 39 (1983) 25–41.
27. Y. I. LYUBICH and L. N. VASERSTEIN, 'Isometric embeddings between classical Banach spaces, cubature formulas, and spherical designs', *Geom. Dedicata* 47 (1993) 327–362.
28. F. J. MACWILLIAMS and N. J. A. SLOANE, *The theory of error-correcting codes* (North-Holland, Amsterdam, 1977).
29. F. P. PREPARATA, 'A class of optimum non-linear double-error correcting codes', *Inform. Control* 13 (1968) 378–400.

30. J. J. SEIDEL, 'Harmonics and combinatorics', *Special functions: group theoretical aspects and applications* (eds R. A. Askey *et al.*, Reidel, Dordrecht, 1984), pp. 287–303.
31. R. SHAW, *Linear algebra and group representations*, vol. II (Academic Press, New York, 1982).
32. M. SUZUKI, *Group theory II* (Springer, New York, 1986).
33. D. E. TAYLOR, *The geometry of the classical groups* (Heldermann, Berlin, 1992).
34. M. E. WILLIAMS, 'Z_4-linear Kerdock codes, orthogonal geometries and non-associative division algebras', Ph.D. thesis, University of Oregon, 1995.
35. J. WOOD, 'Witt's extension theorem for mod four valued quadratic forms', *Trans. Amer. Math. Soc.* 336 (1993) 445–461.
36. G. V. ZAITZEV, V. A. ZINOVIEV, and N. V. SEMAKOV, 'Interrelation of Preparata and Hamming codes and extensions of Hamming codes to new double-error-correcting codes', *Second International Symposium on Information Theory*, Tsahkadzer, Armenia, 1971 (Akademiai Kiado-Budapest, 1973), pp. 253–263.

A. R. Calderbank
AT&T Bell Laboratories
Murray Hill
New Jersey 07974
U.S.A.

P. J. Cameron
School of Mathematical Sciences
Queen Mary and Westfield College
*London E*1 4*NS*

W. M. Kantor
Department of Mathematics
University of Oregon
Eugene
Oregon 97403
U.S.A.

J. J. Seidel
Faculty of Mathematics and Computing Science
Eindhoven University of Technology
5600 *MB Eindhoven*
The Netherlands