NORTH-HOLLAND

Quaternionic Line-Sets and Quaternionic Kerdock Codes

William M. Kantor*
Department of Mathematics
University of Oregon
Eugene, Oregon 97403-1222

For Jaap Seidel on the occasion of his seventy-fifth birthday.

Submitted by Alan J. Hoffman

ABSTRACT

When n is even, orthogonal spreads in an orthogonal vector space of type $O^{-}(2n-2,2)$ are used to construct line-sets of size $(2^{n-1}+1)2^{n-2}$ in $\mathbb{H}^{2^{n-2}}$ all of whose angles are 90° or $\cos^{-1}(2^{-(n-2)/2})$. These line-sets are then used to obtain quaternionic Kerdock codes. These constructions are based on ideas used by Calderbank, Cameron, Kantor, and Seidel in real and complex spaces.

1. INTRODUCTION

In [1], Calderbank, Cameron, Kantor, and Seidel studied real and complex two-angle line-sets and associated codes over $\mathbb{Z}_2$ or $\mathbb{Z}_4$, obtained from binary vector spaces by using extraspecial 2-groups. In particular, for each even integer $n \geqslant 4$ they constructed line-sets of size $(2^{n-1}+1)2^{n}$ in $\mathbb{R}^{2^n}$ all of whose angles are 90° or $\cos^{-1}(2^{-n/2})$, and line-sets of size $(2^{n-1}+1)2^{n-1}$ in $\mathbb{C}^{2^{n-1}}$ all of whose angles are 90° or $\cos^{-1}(2^{-(n-1)/2})$. One of the results of this paper is the quaternionic analogue of these:

* This research was supported in part by an NSF grant.

655 Avenue of the Americas, New York, NY 10010

0024-3795/95/$9.50
SSDI 0024-3795(95)00549-7

THEOREM 1.1. *For each even $n \geqslant 4$ there are line-sets of size $(2^{n-1}+1)2^{n-2}$ in $\mathbb{H}^{2^{n-2}}$ all of whose angles are* $90°$ *or* $\cos^{-1}(2^{-(n-2)/2})$.

In the real, complex, and quaternionic cases, the size of the line-set is maximal subject to having just the stated two angles in the stated dimensions. This is discussed at length in [1] for real and complex spaces. For quaternionic spaces the fact that $(2^{n-1}+1)2^{n-2}$ is the maximal possible number of lines is in [3] (based on results in [7]), and also in [6].

This paper is a sequel to [1]. In particular, the construction of the line-sets in the theorem parallels analogous ones there for real and complex spaces. As in [1], we will construct many inequivalent line-sets. Continuing our emulation of that paper, we will use the line-sets to construct *quaternionic Kerdock codes*, which are certain subsets of Q_8^{2n-2}, and then to obtain their distance distribution relative to a suitable metric (Theorem 8.1). We will also describe the transition from these codes to the associated binary Kerdock codes (Section 7). In view of [1], none of the results are surprising, nor is the fact that all calculations here are more complicated than those in that reference.

This paper, as well as [1], wouldn't exist if it weren't for Jaap Seidel. He posed the question of relating binary and real orthogonal geometries, which was discussed at length in [1]. He prodded, implored, and coaxed in his well-known friendly, energetic, forceful, and inquisitive manner. He felt strongly that quaternionic versions of results in [1] absolutely had to be found and studied. This paper is intended as experimentation in the direction he hoped for.

2. ISOMETRIES OF AN $O^-(2k+2,2)$-SPACE

The next two sections present elementary calculations concerning finite orthogonal geometries.

Consider a $2k+2$-dimensional binary vector space with basis $x_1,\dots,x_k,t_1,t_2,y_1,\dots,y_k$, equipped with the quadratic form $Q^-(\sum_i a_ix_i + \sum_\mu b_\mu t_\mu + \sum_i c_iy_i) := \sum_i a_ic_i + b_1 + b_2 + b_1b_2$. Thus, we are dealing with an $O^-(2k+2,2)$-space: its maximal totally singular subspaces have dimension k (an example of such a subspace is $\langle x_1,\dots,x_k\rangle$).

In this section we will determine the group R of all isometries that induce the identity on both $\langle x_1,\dots,x_k\rangle$ and $\langle x_1,\dots,x_k\rangle^\perp/\langle x_1,\dots,x_k\rangle$, using matrices with respect to the basis $x_1,\dots,x_k,t_1,t_2,y_1,\dots,y_k$. If P is any square matrix, let $d(P)$ denote the row vector whose entries are those on the diagonal of P in their natural order.

LEMMA 2.1. *R consists of all transformations whose matrices have the form*

$$\begin{pmatrix} I & d_2^T & d_1^T & C \\ O & 1 & 0 & d_1 \\ O & 0 & 1 & d_2 \\ O & O & O & I \end{pmatrix},$$

where $d_1, d_2 \in \mathbb{Z}_2^k$ and $C + d_1^T d_2$ is a symmetric matrix such that $d(C + d_1^T d_2) = d_1 + d_2$.

Proof. The matrix of any element r of R has the form

$$\begin{pmatrix} I & B & C \\ O & I & D \\ O & O & I \end{pmatrix},$$

where $B = (b_{i\mu})$, $C = (c_{ij})$, and $D = (d_{\mu j})$ are binary $k \times 2$, $k \times k$, and $2 \times k$ matrices, respectively. In other words, we have

$$x_i r = x_i + \sum_{\mu} b_{i\mu} t_\mu + \sum_j c_{ij} y_j$$

$$t_\mu r = t_\mu + \sum_j d_{\mu j} y_j$$

$$y_i r = y_i.$$

These equations determine an isometry if and only if the following hold (for all appropriate i, j, μ):

$$0 = Q(x_i) = c_{ii} + b_{i1} + b_{i2} + b_{i1} b_{i2}$$

$$0 = (x_i, x_j) = c_{ij} + c_{ji} + b_{i1} b_{j2} + b_{i2} b_{j1}$$

$$0 = (x_i, t_\mu) = b_{i,2-\mu} + d_{\mu i}.$$

Then $c_{ii} = d_{1i} + d_{2i} + d_{1i} d_{2i}$ and $c_{ij} + c_{ji} = d_{1i} d_{2j} + d_{2i} d_{1j}$ for all i, j. ■

Alternatively, start with a skew-symmetric $k \times k$ matrix S, and with $d_1, d_2 \in \mathbb{Z}_2^k$; let $\Delta(d_i)$ be the diagonal matrix whose entries are those of d_i in their natural order. Write

$$[d_2, d_1, S] := \begin{pmatrix} I & d_2^T & d_1^T & S + \Delta(d_1) + \Delta(d_2) + d_1^T d_2 \\ O & 1 & 0 & d_1 \\ O & 0 & 1 & d_2 \\ O & O & O & I \end{pmatrix}.$$

By Lemma 2.1,

Lemma 2.2. *$R = \{[d_2, d_1, S] \mid S$ is a $k \times k$ skew-symmetric matrix and $d_1, d_2 \in \mathbb{Z}_2^k\}$.*

Multiplication in R is given by

$$[d_2, d_1, S][d_2', d_1', S'] = \left[d_2 + d_2', d_1 + d_1', S + S' + d_2^T d_1' + d_1'^T d_2\right]. \tag{2.3}$$

Then $Z(R) = \{[0, 0, S] \mid S$ *is skew-symmetric*$\}$, and this is isomorphic to the space of $k \times k$ skew-symmetric binary matrices. Moreover, $|R| = 2^{2k + k(k-1)/2}$ and $R/Z(R) \cong \mathbb{Z}_2^{2k}$.

Lemma 2.4. *If $[d_2, d_1, S]$, $[d_2', d_1', S'] \in R$, then $\langle x_1, \dots, x_k \rangle [d_2, d_1, S] \cap \langle x_1, \dots, x_k \rangle [d_2', d_1', S'] = 0$ if and only if the $k \times (k+2)$ matrix $(d_2^T - d_2'^T \;\; d_1^T - d_1'^T \;\; C - C')$ has rank k, where $C = S + \Delta(d_1) + \Delta(d_2) + d_1^T d_2$ and $C' = S' + \Delta(d_i') + \Delta(d_2') + d_1'^T d_2'$.*

Proof. A vector in $\langle x_1, \dots, x_k \rangle [d_2, d_1, S] \cap \langle x_1, \dots, x_k \rangle [d_2', d_1', S']$ must have the form $(v, vd_2^T, vd_1^T, vC) = (v, vd_2'^T, vd_1'^T, vC')$ with $v \in \mathbb{Z}_2^k$. ■

Later we will be interested in maximal-sized sets of subspaces behaving as in the preceding lemma (cf. Section 6).

3. FROM $n \times n$ SKEW-SYMMETRIC MATRICES TO THE MATRICES IN SECTION 2

Now consider a $2n$-dimensional binary vector space with basis $x_1, \dots, x_n, y_1, \dots, y_n$, equipped with the quadratic form $Q(\Sigma_i a_i x_i + \Sigma_i c_i y_i) := \Sigma_i a_i c_i$. Thus, we are dealing with an $O^+(2n, 2)$-space. The n-dimensional subspaces $X := \langle x_1, \dots, x_n \rangle$ and $Y := \langle y_1, \dots, y_n \rangle$ are totally singular. Let

$$\begin{aligned} t_1 &= x_{n-1} + y_{n-1} + y_n \\ t_2 &= x_n + y_n \\ u_1 &= x_{n-1} + y_{n-1} \\ u_2 &= x_n + y_{n-1} + y_n. \end{aligned}$$

Note that

$$\begin{aligned} x_{n-1} &= t_2 + u_1 + u_2 \\ x_n &= t_1 + t_2 + u_1 \\ y_{n-1} &= t_2 + u_2 \\ y_n &= t_1 + u_1. \end{aligned}$$

Both $\langle t_1, t_2 \rangle$ and $\langle u_1, u_2 \rangle$ are anisotropic: they have no nonzero singular vectors. Using the basis $x_1, \dots, x_{n-2}, t_1, t_2, y_1, \dots, y_{n-2}$ of $\langle u_1, u_2 \rangle^\perp$, we see that space is an $O^-(2n-2, 2)$-space. Hence, we are back in the situation of Section 2, with $2k + 2 = 2n - 2$.

Any totally singular n-space U such that $U \cap Y = 0$ has the form

$$X(V)\begin{pmatrix} I & M \\ O & I \end{pmatrix}$$

for an $n \times n$ skew-symmetric matrix M. On the other hand, $U \cap \langle u_1, u_2 \rangle^\perp$ is a totally singular subspace of $\langle u_1, u_2 \rangle^\perp$ having dimension at least $n - 2$, so that it must have dimension $n - 2$ and have the same appearance as in

Lemma 2.1. Let C, d_1, and d_2 be as in that lemma. In order to determine them from M, write

$$M = (m_{\alpha\beta}) = \begin{pmatrix} M'' & M_{n-1}^T & M_n^T \\ M_{n-1} & 0 & l \\ M_n & l & 0 \end{pmatrix} \tag{3.1}$$

for an $(n-2) \times (n-2)$ matrix M'', where $M_{n-1}, M_n \in \mathbb{Z}_2^{n-2}$ and $l \in \mathbb{Z}_2$.

Proposition 3.2. *$C = M'' + M_{n-1}^T M_{n-1} + M_n^T M_n + (1+l) M_{n-1}^T M_n + l M_n^T M_{n-1}$,*

$$d_1 = (1+l) M_{n-1} + M_n,$$

$$d_2 = M_{n-1} + l M_n,$$

and $S := C + d_1^T d_2 + \Delta(d_1 + d_2)$ is a skew-symmetric matrix.

Proof. The subspace U consists of all vectors of the following form (where (a_α) ranges through $\mathbb{Z}_2^n$):

$$\begin{aligned}
&\sum_1^n a_\alpha x_\alpha + \sum_1^n \sum_1^n a_\alpha m_{\alpha\beta} y_\beta \\
&= \sum_1^{n-2} a_\alpha x_\alpha + a_{n-1} x_{n-1} + a_n x_n + \sum_{\alpha=1}^{n} \sum_{\beta=1}^{n-2} a_\alpha m_{\alpha\beta} y_\beta \\
&\quad + \sum_1^n a_\alpha m_{\alpha\, n-1} y_{n-1} + \sum_1^n a_\alpha m_{\alpha n} y_n \\
&= \sum_1^{n-2} a_\alpha x_\alpha + a_{n-1}[t_2 + u_1 + u_2] + a_n[t_1 + t_2 + u_1] \\
&\quad + \sum_{\alpha=1}^{n} \sum_{\beta=1}^{n-2} a_\alpha m_{\alpha\beta} y_\beta + \sum_1^n a_\alpha m_{\alpha\, n-1}[t_2 + u_2] + \sum_1^n a_\alpha m_{\alpha n}[t_1 + u_1] \\
&= \sum_1^{n-2} a_\alpha x_\alpha + \sum_{\alpha=1}^{n} \sum_{\beta=1}^{n-2} a_\alpha m_{\alpha\beta} y_\beta \\
&\quad + \left(a_n + \sum_1^n a_\alpha m_{\alpha n} \right) t_1 + \left(a_{n-1} + a_n + \sum_1^n a_\alpha m_{\alpha\, n-1} \right) t_2 \\
&\quad + \left(a_{n-1} + a_n + \sum_1^n a_\alpha m_{\alpha n} \right) u_1 + \left(a_{n-1} + \sum_1^n a_\alpha m_{\alpha\, n-1} \right) u_2 .
\end{aligned}$$

Then $U \cap \langle u_1, u_2 \rangle^{\perp}$ consists of those vectors such that the coordinates of u_1 and u_2 vanish:

$$a_{n-1} + a_n = \sum_1^n a_\alpha m_{\alpha n}$$

$$a_{n-1} = \sum_1^n a_\alpha m_{\alpha\, n-1}.$$

Since $m_{n-1\, n-1} = m_{nn} = 0$ and $m_{n\, n-1} = m_{n-1 n} = l$ by skew-symmetry, this yields

$$(1 + l)a_{n-1} + a_n = \sum_1^{n-2} a_\alpha m_{\alpha n}$$

$$a_{n-1} + la_n = \sum_1^{n-2} a_\alpha m_{\alpha\, n-1}$$

and hence

$$a_{n-1} = \sum_1^{n-2} a_\alpha [m_{\alpha\, n-1} + lm_{\alpha n}]$$

$$a_n = \sum_1^{n-2} a_\alpha [(1 + l)m_{\alpha\, n-1} + m_{\alpha n}].$$

Now our t_1- and t_2-coordinates can be rewritten as follows:

$$a_n + \sum_1^n a_\alpha m_{\alpha n} = a_n + la_{n-1} + \sum_1^{n-2} a_\alpha m_{\alpha n}$$

$$= \sum_1^{n-2} a_\alpha \{[(1 + l)m_{\alpha\, n-1} + m_{\alpha n}] + l[m_{\alpha\, n-1} + lm_{\alpha n}] + m_{\alpha n}\}$$

$$= \sum_1^{n-2} a_\alpha \{m_{\alpha\, n-1} + lm_{\alpha n}\}$$

and

$$a_{n-1} + a_n + \sum_1^n a_\alpha m_{\alpha\, n-1}$$

$$= a_{n-1} + (1+l)a_n + \sum_1^{n-2} a_\alpha m_{\alpha\, n-1}$$

$$= \sum_1^{n-2} a_\alpha \{[m_{\alpha\, n-1} + lm_{\alpha n}] + (1+l)[(1+l)m_{\alpha\, n-1}$$

$$+ m_{\alpha n}] + m_{\alpha\, n-1}\}$$

$$= \sum_1^{n-2} a_\alpha \{(1+l)m_{\alpha\, n-1} + m_{\alpha n}\}.$$

Finally, if $1 \leqslant \beta \leqslant n-2$, then our y_β-coordinate is

$$\sum_{\alpha=1}^{n} a_\alpha m_{\alpha\beta} = \sum_{\alpha=1}^{n-2} a_\alpha m_{\alpha\beta} + a_{n-1} m_{n-1\,\beta} + a_n m_{n\beta}$$

$$= \sum_{\alpha=1}^{n-2} a_\alpha m_{\alpha\beta} + \sum_{\alpha=1}^{n-2} a_\alpha [m_{\alpha\, n-1} + lm_{\alpha n}] m_{n-1\,\beta}$$

$$+ \sum_{\alpha=1}^{n-2} a_\alpha [(1+l)m_{\alpha\, n-1} + m_{\alpha n}] m_{n\beta}$$

$$= \sum_{\alpha=1}^{n-2} a_\alpha \{m_{\alpha\beta} + m_{n-1\,\alpha} m_{n-1\,\beta} + lm_{n\alpha} m_{n-1\,\beta}$$

$$+ (1+l)m_{n-1\,\alpha} m_{n\beta} + m_{n\alpha} m_{n\beta}\}.$$

Consequently, a typical vector in $U \cap \langle u_1, u_2\rangle^{\perp}$ can be written

$$\begin{aligned}
&\sum_1^{n-2} a_\alpha x_\alpha + \sum_{\beta=1}^{n-2}\left(\sum_{\alpha=1}^{n} a_\alpha m_{\alpha\beta}\right) y_\beta + \left(a_n + \sum_1^n a_\alpha m_{\alpha n}\right) l_1 \\
&\quad + \left(a_{n-1} + a_n + \sum_1^n a_\alpha m_{\alpha\, n-1}\right) t_2 \\
&\quad = \sum_1^{n-2} a_\alpha x_\alpha + \sum_1^{n-2} a_\alpha \{m_{\alpha\, n-1} + l m_{\alpha n}\} t_1 \\
&\qquad + \sum_1^{n-2} a_\alpha \{(1+l) m_{\alpha\, n-1} + m_{\alpha n}\} t_2 \\
&\qquad + \sum_{\beta=1}^{n-2}\left(\sum_{\alpha=1}^{n-2} a_\alpha \{m_{\alpha\beta} + m_{n-1\,\alpha} m_{n-1\,\beta} + l m_{n\alpha} m_{n-1\,\beta}\right. \\
&\qquad\qquad \left. + (1+l) m_{n-1\,\alpha} m_{n\beta} + m_{n\alpha} m_{n\beta}\}\right) y_\beta .
\end{aligned}$$

In other words, if C and d_1, d_2 are the matrix and vectors stated in the proposition, then the coordinate vectors of the members of $U \cap \langle u_1, u_2\rangle^{\perp}$ with respect to the basis $x_1, \ldots, x_{n-2}, t_1, t_2, y_1, \ldots, y_{n-2}$ of $\langle u_1, u_2\rangle^{\perp}$ all have the form $(a_\alpha)(I\ d_2^T\ d_1^T\ C)$, where (a_α) ranges through $\mathbb{Z}_2^{n-2}$. Now Lemma 2.1 completes the proof of the proposition. ■

Of course, it is easy to check the last part of Proposition 3.2 directly:

$$\begin{aligned}
C + d_1^T d_2 + \Delta(d_1 + d_2) = M'' &+ (1+l)\left[M_{n-1}^T M_n + M_n^T M_{n-1}\right] \\
&+ (1+l)\left[M_n^T M_n + \Delta(M_n)\right] \\
&+ l\left[M_{n-1}^T M_{n-1} + \Delta(M_{n-1})\right].
\end{aligned}$$

Remark 1. The mapping $M \mapsto (C, d_1, d_2)$ is 2 to 1: l can be chosen to be 0 or 1. Namely, assume that the triple (C, d_1, d_2) behaves as in Section 2. Pick either possible value of l. Then d_1 and d_2 determine M_{n-1} and M_n, and hence together with C also determine the matrix M'', which is skew-symmetric (reverse the reasoning at the end of the above proof).

This observation will come back to haunt us in Section 7.

REMARK 2. The proposition should be compared with the version in an $O(2n-1,2)$-space (or an $Sp(2n-2,2)$-space) appearing in [1, Section 7]. There we also started with M, and obtained a symmetric matrix P such that

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

Thus, with reasonably self-evident notation, $P = M' + M_n^T M_n$.

REMARK 3. The proposition has an analogue over any field.

4. QUATERNIONIC SPACES AND EXTRASPECIAL 2-GROUPS

We briefly introduce some of the notation in [1]. Let n be even. Start with $\mathbb{R}^{2^n}$, equipped with the usual scalar product. The standard basis $\{e_v \mid v \in V\}$ is indexed by $V := \mathbb{Z}_2^n$. The extraspecial group E is the subgroup $\langle X(b), Y(b) \mid b \in V \rangle$ of the usual real orthogonal group $O(\mathbb{R}^{2^n})$, where $X(b)\colon e_v \mapsto e_{v+b}$ and $Y(b) = \mathrm{diag}[(-1)^{b \cdot v}]_{v \in V}$. Here $|E| = 2^{1+2n}$; the center $Z = Z(E) = \{\pm I\}$ has order 2, and will be identified with $\mathbb{Z}_2$. Let tilde denote the natural map $E \to E/Z$. (N.B. An overbar was used in [1]. Here we wish to avoid an awkwardness this caused in that paper: the inability to apply this map to the complex number i without suggesting complex conjugation.) The associated quadratic form on E/Z is defined (for all $e \in E$) by $Q(\tilde{e}) = e^2 \in Z \cong \mathbb{Z}_2$. The normalizer of E in $O(\mathbb{R}^{2^n})$ induces the full orthogonal group $O^+(2n,2)$ on $\tilde{E}$.

Fix a basis $v_1, \dots, v_n$ of V. Then $\tilde{X}(v_1), \dots, \tilde{X}(v_n)$ and $\tilde{Y}(v_1), \dots, \tilde{Y}(v_n)$ are dual bases of $\tilde{X}(V)$ and $\tilde{Y}(V)$. Write

$$\begin{aligned} i &= X(v_n)Y(v_{n-1}+v_n), & j &= X(v_{n-1})Y(v_{n-1}), \\ t_1 &= X(v_{n-1})Y(v_{n-1}+v_n), & t_2 &= X(v_n)Y(v_n). \end{aligned} \tag{4.1}$$

Then $Q_8 := \langle i, j\rangle$ and $\langle t_1, t_2\rangle$ are commuting quaternion groups of order 8. We match this notation with that of Section 3 by writing $x_\alpha = \bar{X}(v_\alpha)$ and $y_\alpha = \tilde{Y}(v_\alpha)$ for $1 \leqslant \alpha \leqslant n$; the present t_1 and t_2 project modulo Z onto those in Section 3, while i and j project onto u_2 and u_1, respectively.

Let V'' denote the subspace of V spanned by $v_1, \dots, v_{n-2}$, and write

$$E^- := \langle t_1, t_2, X(V''), Y(V'')\rangle.$$

(N.B. The notation "V''" is intended to parallel notation used in [1]; cf. (6.6) below. It has nothing to do with commutator subgroups.) E is the central product of the extraspecial group E^- of order $2^{2(n-1)+1}$ with Q_8, and E^- is the central product of the extraspecial group $\langle X(V''), Y(V'')\rangle$ of order $2^{2(n-2)+1}$ with $\langle t_1, t_2\rangle$.

Let $\mathbb{H}$ denote the quaternion algebra $\mathbb{R}Q_8 = \mathbb{R}\langle i, j\rangle$. This acts on $\mathbb{R}^{2^n}$: real scalars originally acted on the left, but we can also view them as acting on the right; elements of $\langle i, j\rangle$ act on the right. (Care is needed here, since we are dealing with a noncommutative division algebra.) Then $\{e_v \mid v \in V''\}$ is an $\mathbb{H}$-basis of $\mathbb{R}^{2^n}$. We will view $\mathbb{R}^{2^n}$ as $\mathbb{H}^{2^{n-2}}$ by writing $(a_v)_{v \in V''} := \Sigma_{v \in V''} e_v a_v$ for $a_v \in \mathbb{H}$.

Since t_1 and t_2 commute with i and j, they are $\mathbb{H}$-linear. Their action is as follows (for all $v \in V''$, so that $v \cdot v_{n-1} = 0 = v \cdot v_n$):

$$\begin{aligned} e_v t_1 &= e_v X(v_{n-1}) Y(v_{n-1}) Y(v_n) &&= e_v Y(v_n) j &&= e_v j, \\ e_v t_2 &= e_v X(v_n) Y(v_{n-1} + v_n) Y(v_{n-1}) &&= e_v Y(v_{n-1}) i &&= e_v i. \end{aligned} \tag{4.2}$$

Thus, $(a_v)_{v \in V''} t_1 = (\Sigma_{v \in V''} e_v a_v) t_1 = \Sigma_{v \in V''} (e_v t_1) a_v = (j a_v)_{v \in V''}$ for any $a_v \in \mathbb{H}$, whereas the scalar j acts via $(a_v)_{v \in V''} j = (a_v j)_{v \in V''}$. The actions of t_1 and t_2 are those of diagonal matrices. In general, if $\delta_v \in \mathbb{H}$ for each $v \in V''$, then the diagonal matrix $D = \operatorname{diag}[\delta_v]_{v \in V''}$ acts via $(a_v)_{v \in V''} D = (\delta_v a_v)_{v \in V''}$.

We equip $\mathbb{H}^{2^{n-2}}$ with the usual hermitian inner product, so that our $\mathbb{H}$-basis becomes an orthonormal basis. Then E lies in the resulting unitary group $\mathrm{U}(\mathbb{H}^{2^{n-2}})$: if $v \in V''$ and $b \in V$, then $e_v Y(b) = \pm e_v$ and $e_v X(b) \in e_w Q_8$ for some $w \in V''$ (e.g., $e_v X(v_n) = e_v Y(v_{n-1} + v_n) X(v_n) = -e_v i$). Similarly, each element A of $\mathrm{GL}(V'')$ can be viewed as lying in $\mathrm{U}(\mathbb{H}^{2^{n-2}})$, inducing a permutation $e_v \mapsto e_{vA}$ of our basis of $\mathbb{H}^{2^{n-2}}$ and normalizing both E^- and $Y(V'')$ (cf. [1, Section 2]). Yet another unitary transformation is induced by the matrix $H \in \mathrm{O}(\mathbb{R}^{2^{n-2}}) < \mathrm{U}(\mathbb{H}^{2^{n-2}})$ whose rows are the vectors $e_b^* := 2^{-(n-2)/2} \Sigma_{v \in V''} (-1)^{b \cdot v} e_v$ for $b \in V''$. This normalizes E and interchanges $X(V'')$ and $Y(V'')$ (cf. [1, Section 2]). In the next section we will obtain unitary transformations normalizing E^- and inducing on $\tilde{E}^-$ the group R appearing in Lemmas 2.1 and 2.2. Assuming this, we see that *we have produced enough unitary transformations normalizing E^- to generate a* *group inducing* $\Omega^-(2n-2,2)$ on $\tilde{E}^-$ (the group $\Omega^-(2n-2,2)$ is the derived subgroup of $O^-(2n-2,2)$ if $n \geqslant 6$).

PROPOSITION 4.3. *Let U_1 and U_2 be any subgroups of E^- such that $\tilde{U}_1$ and $\tilde{U}_2$ are totally singular $(n-2)$-spaces and $\tilde{U}_1 \cap \tilde{U}_2 = 0$. Then*

(i) *the set $\mathcal{F}(U_1)$ of U_1-irreducible subspaces of $\mathbb{H}^{2^{n-2}}$ is an orthonormal frame; and*

(ii) *the angle between any member of $\mathcal{F}(U_1)$ and any member of $\mathcal{F}(U_2)$ is* $\cos^{-1}(2^{-(n-2)/2})$.

Proof. We may assume that $Z < U_1, U_2$. Using the normalizer of E^-, we can move our pair U_1, U_2 to the pair $Y(V'')Z$, $X(V'')Z$. Thus, it suffices to check (i) and (ii) in this concrete case.

Since $e_vY(b) = (-1)^{b \cdot v}e_v$ for all $b, v \in V''$, the 1-space spanned by e_v is invariant under $Y(V'')$, and we obtain $|V''|$ pairwise inequivalent $Y(V'')$-modules. This proves (i), and (ii) follows from the fact that $(e^*_b, e_v) = 2^{-(n-2)/2}$ for $b, v \in V''$. ■

5. QUATERNIONIC DIAGONAL MATRICES

In this section we will show that there are enough diagonal transformations of $\mathbb{H}^{2^{n-2}}$ normalizing E^- in order to induce on $\tilde{E}^- = E^-/\langle -I \rangle$ all the elements of R, the group of isometries discussed in Lemmas 2.1 and 2.2. Let x_α, y_α, t_1, and t_2 be as in Section 4. As in Section 2, we will use the basis $\tilde{x}_1, \ldots, \tilde{x}_{n-2}, \tilde{t}_1, \tilde{t}_2, \tilde{y}_1, \ldots, \tilde{y}_{n-2}$ in order to write linear transformations of $\tilde{E}^-$.

Fix an $(n-2) \times (n-2)$ symmetric binary matrix P, and view its entries as elements of $\mathbb{Z}_4$. For each $v \in V''$ let $\hat{v}$ denote a member of $\mathbb{Z}_4^{n-2}$ projecting onto v mod 2 (cf. [1, Section 4]). Define $f(v) := \hat{v}P\hat{v}^T$ for $v \in V''$, and $D := \text{diag}[i^{f(v)}]_{v \in V''}$, so that $(a_v)_{v \in V''}D = (i^{f(v)}a_v)_{v \in V''}$ for any $(a_v)_{v \in V''} \in \mathbb{H}^{2^{n-2}}$.

LEMMA 5.1.

(i) *D normalizes E^-.*

(ii) *The matrix induced by D on $\tilde{E}^-$ is*

$$\begin{pmatrix} I & O & d(P)^T & P \\ O & 1 & 0 & d(P) \\ O & 0 & 1 & O \\ O & O & O & I \end{pmatrix}.$$

Proof. First note that, for each $v \in V''$, $f(v) := \hat{v}P\hat{v}^T$ is a well-defined element of $\mathbb{Z}_4$, independent of the choice of $\hat{v}$ (cf. [1, Section 4]). Next, calculate that, for all $v, w \in V''$,

$$\begin{aligned} f(v+w) &= f(v) + f(w) + 2\hat{v}P\hat{w}^T, \\ f(w) &\equiv \hat{w}d(l')^T \pmod 2. \end{aligned} \tag{5.2}$$

Let $v, w \in V''$. Then D centralizes $Y(w)$, and by (4.2)

$$\begin{aligned} e_v D^{-1} X(w) D &= e_v i^{-f(v)} X(w) D = e_v X(w) D i^{-f(v)} \\ &= e_{v+w} D i^{-f(v)} = e_{v+w} i^{f(v+w)} i^{-f(v)} \\ &= e_{v+w} i^{f(w) + 2\hat{v}P\hat{w}^T} = e_v X(w) t_2^{f(w)} (-1)^{v(wP)^T} \\ &= e_v Y(wP) X(w) t_2^{f(w)}. \end{aligned}$$

Thus, $D^{-1}X(w)D = Y(wP)X(w)t_2^{f(w)} = \pm Y(wP)X(w)t_2^{\hat{w}d(P)^T}$ by (5.2).

Also by (4.2) (together with the remark following it), we have

$$e_v t_1^{-1} D^{-1} t_1 D = e_v i^{f(v)} j i^{-f(v)} j^{-1} = e_v i^{2f(v)} = e_v(-1)^{vd(P)^T} = e_v Y(d(P)).$$

Similarly, $e_v t_2^{-1} D^{-1} t_2 D = e_v$. Thus,

$$\begin{aligned} X(w)^D &= \pm Y(wP) X(w) t_2^{wd(P)^T}, \\ t_1^D &= t_1 Y(d(P)), \\ t_2^D &= t_2, \\ Y(w)^D &= Y(w), \end{aligned}$$

which proves both (i) and (ii). ■

In the notation of Lemma 2.2, the matrix in (ii) is $[0, d(P), P + \Delta(d(P))]$. Now interchange the roles of i and j, as well as those of t_1 and t_2: starting with another $(n-2) \times (n-2)$ symmetric matrix P' in place of P, obtain another diagonal matrix $D' := \operatorname{diag}[j^{\hat{v}P'\hat{v}^T}]_{v \in V''}$ normalizing E^- such that the transformation induced by D' on $\tilde{E}^-$ has the matrix $[d(P'), 0, P' + \Delta(d(P'))]$. Then the transformation induced by DD' has the matrix

$$[0, d(P), P + \Delta(d(P))][d(P'), 0, P' + \Delta(d(P'))]$$

$$= [d(P'), d(P), P + P' + \Delta(d(P)) + \Delta(d(P'))]$$

by (2.3). We can now prove

PROPOSITION 5.3. *Each isometry $[d_2, d_1, S]$ of $\tilde{E}$ inducing the identity on $\langle \tilde{i}, \tilde{j} \rangle$, $\tilde{Y}(V'')$, and $\tilde{Y}(V'')^{\perp}/\tilde{Y}(V'')$ is induced by conjugation by an isometry of $\mathbb{H}^{2^{n-2}}$ normalizing E and E^-, namely* $\mathrm{diag}[i^{\hat{v}''(S+\Delta(d_1))\hat{v}''^T} j^{\hat{v}''\Delta(d_2)\hat{v}''^T}]_{v'' \in V''}$.

Proof. Let $P = S + \Delta(d_1)$ and $P' = \Delta(d_2)$ in the above discussion in order to see that the indicated diagonal matrix behaves as desired. ■

For a more explicit and symmetrical version of the above diagonal matrix, see Lemma 7.2 (or Theorem 7.4).

COROLLARY 5.4. *If U'' is any subgroup of E^- such that $\tilde{U}''$ is a totally singular $n-2$-space and $\tilde{U}'' \cap \tilde{Y}(V'') = 0$, then each member of $\mathscr{F}(U'')$ is spanned by a vector $2^{(n-2)/2} e_b^* D$ all of whose coordinates are in Q_8, where D is a diagonal matrix as in the preceding proposition.*

Proof. $\mathscr{F}(X(V''))$ consists of the 1-spaces spanned by the vectors e_b^*. Any other choice of $\tilde{U}''$ is the image of $\tilde{X}(V'')$ under one of the transformations in Proposition 5.3, in view of Lemma 2.2. ■

6. QUATERNIONIC LINE-SETS AND KERDOCK CODES

An *orthogonal spread* of $\tilde{E} = E/\langle -I \rangle$ is a family of $2^{n-1} + 1$ totally singular n-spaces such that every nonzero singular vector is in exactly one of its members. There are large numbers of orthogonal spreads not equivalent under the group $O^+(2n, 2)$ of isometries of $\tilde{E}$ [4, 5]. An *orthogonal spread* of $\tilde{E}^-$ is a family of $2^{n-1} + 1$ totally singular $n - 2$-spaces such that every nonzero singular vector is in exactly one of its members. Every orthogonal spread Σ of $\tilde{E}$ determines an orthogonal spread Σ^- of $\tilde{E}^-$:

$$\Sigma^- := \{U \cap \tilde{E}^- \mid U \in \Sigma\}.$$

Namely, dim $U \cap \tilde{E}^- \geqslant n-2$ and $U \cap \tilde{E}^-$ is totally singular, so that dim $U \cap \tilde{E}^- = n-2$; moreover, every nonzero vector in $\tilde{E}^-$ is in exactly one such U and hence in $U \cap \tilde{E}^-$. Of course, Σ^- heavily depends on the anisotropic 2-space $\langle i, j\rangle / \langle -I\rangle$ chosen in $\tilde{E}$.

We can now prove a more precise version of Theorem 1.1.

THEOREM 6.1. *$\mathscr{F}(\Sigma^-) := \bigcup\{\mathscr{F}(U'') \mid \tilde{U}'' \in \Sigma^-\}$ is a set of $(2^{n-1}+1)2^{n-2}$ lines in $\mathbb{H}^{2^{n-2}}$ all of whose angles are $90°$ or $\cos^{-1}(2^{-(n-2)/2})$.*

Proof. This is an immediate consequence of Proposition 4.3. ∎

Note that $(2^{n-1}+1)2^{n-2}$ is the maximal number of lines in $\mathbb{H}^{2^{n-2}}$ having the stated angles ([3], [7], and [6]). Also note that the preceding proof did not require any of the calculations in Sections 2 and 3. Those are needed to see that the lines all may be assumed to be spanned by vectors whose coordinates are all in $Q_8 \cup \{0\}$.

From now on we will assume that $\tilde{X}(V'')$, $\tilde{Y}(V'') \in \Sigma^-$. Then Σ^- consists of $\tilde{Y}(V'')$ and certain subspaces $\tilde{X}(V'')[d_2, d_1, S]$, in the notation of Lemma 2.2, and $\mathscr{F}(\Sigma^-)$ is the union of frames $\mathscr{F}(U'')$, $\tilde{U}'' \in \Sigma^-$; each line in $\mathscr{F}(\Sigma^-)$ is spanned either by a standard basis vector or by a vector all of whose coordinates are in Q_8 (by Corollary 5.4). This leads us to the *quaternionic Kerdock code*

$$\mathscr{K}_8(\Sigma^-) := \left\{(q_{v''})_{v'' \in V''} \in Q_8^{2^{n-2}} \mid \langle (q_{v''})_{v'' \in V''}\rangle \in \mathscr{F}(\Sigma^-)\right\}. \quad (6.2)$$

As in [1], this code depends heavily on choices other than Σ^-: the members $\tilde{X}(V'')$ and $\tilde{Y}(V'')$ of Σ^-, and the basis $v_1, \ldots, v_{n-2}$ of V''.

In order to be more explicit, recall that each $U \in \Sigma \setminus \{\tilde{Y}(V)\}$ has the form

$$X(V)\begin{pmatrix} I & M \\ O & I \end{pmatrix}$$

for a unique $n \times n$ skew-symmetric matrix M; let $\mathbf{M}(\Sigma)$ be the *Kerdock set* of all such matrices M. (N.B. Once again this notation is misleading: this set of matrices depends on Σ together with the choice of members $\tilde{X}(V)$, $\tilde{Y}(V)$ of Σ, as well as on the basis chosen for V.) Each $M \in \mathbf{M}(\Sigma)$ determines an element $[d_{2M}, d_{1M}, S_M] \in \mathrm{O}^-(2n-2, 2)$ as in Proposition 3.2, and hence also an isometry $\underline{D}_{[d_{2M}, d_{1M}, S_M]} \in \mathrm{U}(\mathbb{H}^{2^{n-2}})$ by Proposition 5.3, where $D_{[d_{2M}, d_{1M}, S_M]}$ sends $\bar{X}(V'')$ to $U \cap \tilde{E}^-$ by conjugation. Since

$$2^{(n-2)/2} e_b^* D_{[d_{2M}, d_{1M}, S_M]}$$
$$= \left((-1)^{b\cdot v''}\right)_{v'' \in V''} \operatorname{diag}\left[i^{\hat{v}''(S + \Delta(d_{1M}))\hat{v}''^T} j^{\hat{v}\Delta(d_{2M})\hat{v}''^T} \right]_{v'' \in V''},$$

it follows from Corollary 5.4 that

$$\mathscr{K}_8(\Sigma^-) = \left\{ \left((-1)^{b\cdot v''} i^{\hat{v}''(S_M + \Delta_{1M})\hat{v}''^T} j^{\hat{v}''\Delta_{2M}\hat{v}''^T} q \right)_{v'' \in V''} \;\middle|\; b \in V'',\ M \in \mathbf{M}(\Sigma),\ q \in Q_8 \right\}. \tag{6.3}$$

We will need to compare this quaternionic code with the related binary and $\mathbb{Z}_4$-codes. For this purpose we recall additional notation from [1].

Let $V = \mathbb{Z}_2^n$ and $V' = \mathbb{Z}_2^{n-1}$. Associated with each $M \in \mathbf{M}(\Sigma)$ there are

- skew-symmetric matrices M' and M'', and vectors $d \in V'$ and M_{n-1}, $M_n \in V''$, such that

$$M = \begin{pmatrix} M' & d^T \\ d & 0 \end{pmatrix} = \begin{pmatrix} M'' & M_{n-1}^T & M_n^T \\ M_{n-1} & 0 & l \\ M_n & l & 0 \end{pmatrix}; \tag{6.4}$$

- a quadratic form $Q_M : V \to \mathbb{Z}_2$ whose corresponding bilinear form is vMv^T (one form suffices here for each M);
- a symmetric $(n-1) \times (n-1)$ matrix $P_M = M' + d^T d$; and
- a set Σ' consisting of the following subspaces of $V' \oplus V'$: $x' = 0$, and $y' = x'P_M$ for $M \in \mathbf{M}(\Sigma)$ (where $(x', y') \in V' \oplus V'$).

Then the binary and $\mathbb{Z}_4$-Kerdock codes are as follows:

$$\mathscr{K}(\Sigma) = \left\{ \pm\left((-1)^{b\cdot v}(-1)^{Q_M(v)}\right)_{v \in V} \;\middle|\; b \in V,\ M \in \mathbf{M}(\Sigma) \right\}$$
$$\subseteq \langle -1 \rangle^{2^n} \equiv \mathbb{Z}_2^{2^n} \tag{6.5}$$

$$\mathscr{K}_4(\Sigma') = \left\{ i^{\epsilon}\left((-1)^{b'\cdot v'} i^{\hat{v}' P_M \hat{v}'^T}\right)_{v' \in V'} \;\middle|\; b' \in V',\ M \in \mathbf{M}(\Sigma),\ \epsilon \in \mathbb{Z}_4 \right\}$$
$$\subseteq \langle i \rangle^{2^{n-1}} \equiv \mathbb{Z}_4^{2^{n-1}}. \tag{6.6}$$

(These are not quite the definitions in [1]: here we have opted to use codewords whose entries are in mutiplicative versions of $\mathbb{Z}_2$ or $\mathbb{Z}_4$.) The corresponding real or complex line-sets consist of the standard orthonormal frame of $\mathbb{R}^{2^n}$ or $\mathbb{C}^{2^{n-1}}$ together with the 1-spaces spanned by the members of $\mathscr{K}(\Sigma)$ or $\mathscr{K}_4(\Sigma')$, respectively.

7. IN SEARCH OF A GRAY MAP

In this section we will follow the methodology in [1] a bit further, taking into account the remarks at the end of [1]: the transition between $\mathbb{Z}_4$- and binary Kerdock codes "could" have led to the Gray map studied in [2]. That is, we will describe transitions from our quaternionic Kerdock code $\mathscr{K}_8(\Sigma^-)$ to the binary and $\mathbb{Z}_4$-Kerdock codes exhibited in (6.5) and (6.6). A summary of the results of this section might be: simplifications occur and the transition is pretty, but the transition does not appear to arise from an actual map. This negative result is presented both for completeness and on the offchance that some reader will see a pattern overlooked here.

7.1. *Another View of $\mathscr{K}_8(\Sigma^-)$*

Fix $M \in \mathbf{M}(\Sigma)$, and let M'', M_n, M_{n-1}, l be as in (3.1). Also, let U''_M denote any $(n-2) \times (n-2)$ matrix such that

$$M'' = U''_M + U''^T_M \tag{7.1}$$

(the simplest example being the "upper triangular portion" of the skew-symmetric matrix M''), so that Lemma 2.2 associates with M an isometry of $\tilde{E}^-$ with matrix $[d_2, d_1, S] := [d_{2M}, d_{1M}, S_M]$. Here, S is given in Proposition 3.2, while $M_{n-1} = ld_1 + d_2$ and $M_n = d_1 + (1+l)d_2$.

Write $\Delta_\mu = \Delta(d_\mu)$ for $\mu = 1, 2$. We need to simplify the matrix $\mathrm{diag}[i^{\hat{v}''(S+\Delta_1)\hat{v}''^T} j^{\hat{v}''\Delta_2\hat{v}''^T}]_{v'' \in V''}$ appearing in Proposition 5.3.

LEMMA 7.2. *$i^{\hat{v}''(S+\Delta_1)\hat{v}''^T} j^{\hat{v}''\Delta_2\hat{v}''^T} = i^x j^y (-1)^z$ with*

$$x = d_1 \cdot v'', \qquad y = d_2 \cdot v''$$

and

$$z = v'' U''_M v''^T + (1+l)x + ly + (M_{n-1} * M_n) \cdot v'',$$

where in each case the indicated dot product is the binary one, and $M_{n-1} * M_n$ denotes the pointwise product of the indicated vectors.

Proof. As in [1, Section 7], if $v'' = (a_\alpha) \in V''$, then the 2-adic expansion of $\hat{v}''(S + \Delta_1)\hat{v}''^T$ is

$$d_1 \cdot v'' + 2 \sum_{\alpha<\beta} \left[S_{\alpha\beta} + \Delta_{1\alpha}\Delta_{1\beta}\right] a_\alpha a_\beta = d_1 \cdot v'' + 2 \sum_{\alpha<\beta} \left[S_{\alpha\beta} + d_{1\alpha}d_{1\beta}\right] a_\alpha a_\beta \tag{7.3}$$

(where $d_{1\alpha}$ is viewed as an element of $\mathbb{Z}_4$). Similarly, $\hat{v}''\Delta_2\hat{v}''^T = d_2 \cdot v'' + 2\Sigma_{\alpha<\beta}\, d_{2\alpha}d_{2\beta}a_\alpha a_\beta$. Thus,

$$\begin{aligned} i^{\hat{v}''(S+\Delta_1)\hat{v}''^T} j^{\hat{v}''\Delta_2\hat{v}''^T} &= i^{d_1\cdot v'' + 2\Sigma_{\alpha<\beta}[S_{\alpha\beta} + d_{1\alpha}d_{1\beta}]a_\alpha a_\beta}\, j^{d_2\cdot v'' + 2\Sigma_{\alpha<\beta}\, d_{2\alpha}d_{2\beta}a_\alpha a_\beta} \\ &= i^{d_1\cdot v''} j^{d_2\cdot v''}(-1)^{\Sigma_{\alpha<\beta}[S_{\alpha\beta} + d_{1\alpha}d_{1\beta} + d_{2\alpha}d_{2\beta}]a_\alpha a_\beta}. \end{aligned}$$

Here, $S_{\alpha\beta} + d_{1\alpha}d_{1\beta} + d_{2\alpha}d_{2\beta}$ is the α, β entry of

$$\begin{aligned} S &+ d_1^T d_1 + d_2^T d_2 \\ &= M'' + M_{n-1}^T M_{n-1} + M_n^T M_n + (1 + l) M_{n-1}^T M_n + l M_n^T M_{n-1} \\ &\quad + d_1^T d_2 + \Delta_1 + \Delta_2 + d_1^T d_1 + d_2^T d_2 \\ &= M'' + \Delta_1 + \Delta_2 + M_{n-1}^T M_{n-1} + M_n^T M_n \\ &\quad + (1 + l) M_{n-1}^T M_n + l M_n^T M_{n-1} \\ &\quad + [(1 + l) M_{n-1} + M_n]^T [l M_{n-1} + (1 + l) M_n] \\ &\quad + [M_{n-1} + l M_n]^T [M_{n-1} + l M_n] \\ &= M'' + l M_{n-1}^T M_n + l M_n^T M_{n-1} + \Delta_1 + \Delta_2. \end{aligned}$$

Let N denote the upper triangular portion of the skew-symmetric matrix $M_{n-1}^T M_n + M_n^T M_{n-1}$, so that $l M_{n-1}^T M_n + l M_n^T M_{n-1} = l(N + N^T)$. Then

$$i^{\hat{v}''(S+\Delta_1)\hat{v}''^T} j^{\hat{v}''\Delta_2\hat{v}''^T} = i^{d_1\cdot v''} j^{d_2\cdot v''}(-1)^{v''(U_M'' + lN)v''^T + (d_1 + d_2)\cdot v''}.$$

Here, $N_{\alpha\beta}$ is 0 if $\alpha \geqslant \beta$ and is $d_{1\alpha}d_{2\beta} + d_{1\beta}d_{2\alpha} = M_{n-1\,\alpha}M_{n\beta} + M_{n\alpha}M_{n-1\,\beta}$ otherwise. Thus,

$$\begin{aligned} v''Nv''^{T} &= \sum_{\alpha<\beta} a_\alpha\left[M_{n-1\,\alpha}M_{n\beta} + M_{n\alpha}M_{n-1\,\beta}\right]a_\beta \\ &= \sum_{\alpha\neq\beta} a_\alpha\left[M_{n-1\,\alpha}\,M_{n\beta}\right]a_\beta \\ &= (M_{n-1}\cdot v'')(M_n\cdot v'') + (M_{n-1} * M_n)\cdot v'' \\ &= ([ld_1 + d_2]\cdot v'')([d_1 + (1+l)d_2]\cdot v'') + (M_{n-1} * M_n)\cdot v'' \\ &= ld_1\cdot v'' + (1+l)d_2\cdot v'' + (d_1\cdot v'')(d_2\cdot v'') + (M_{n-1} * M_n)\cdot v'', \end{aligned}$$

so that $v''(U''_M + lN)v''^{T} + (d_1 + d_2)\cdot v''$ is the quantity z stated in the lemma. ■

THEOREM 7.4.

$$K_S(\Sigma^-) = \left\{\left(i^{d_{1M}\cdot v''}j^{d_{2M}\cdot v''}(-1)^{v''U''_M v''^{T} + b\cdot v''}q\right)_{v''\in V''}\right| \\ b \in V'',\, M \in \mathbf{M}(\Sigma),\, q \in Q_8\Big\},$$

where the indicated dot products are the binary ones.

Proof. For any given $b \in V''$ and $M \in \mathbf{M}(\Sigma)$,

$$(-1)^{b\cdot v''}(-1)^{v''U''_M v''^{T} + (1+l)x + ly + (M_{n-1} * M_n)\cdot v''} = (-1)^{v''U''_M v''^{T} + c\cdot v''}$$

where $c = b + (1+l)d_1 + ld_2 + M_{n-1} * M_n$. The theorem now follows from (6.3) and the preceding lemma. ■

REMARK 7.5. l disappeared in the above calculation, and hence in the simplified view of $\mathscr{K}_8(\Sigma)$ given in Theorem 7.4

7.2. *From Quaternions to* $\mathbb{Z}_2^4$

In order to relate Theorem 7.4 to the codeword $((-1)^{\delta}(-1)^{b\cdot v}(-1)^{Q_M(v)})_{v\in V}$ appearing in (6.5), where $\delta \in \mathbb{Z}_2$, again fix M, let $v = (v'', \nu_{n-1}, \nu_n) \in V$ with $v'' \in V''$, and write $a = v''U_M''v''^T$. Then

$$\begin{aligned} Q_M(v) &= (v'', \nu_{n-1}, \nu_n)\begin{pmatrix} U_M'' & M_{n-1}^T & M_n^T \\ 0 & 0 & l \\ 0 & 0 & 0 \end{pmatrix}(v'', \nu_{n-1}, \nu_n)^T \\ &= v''U_M''v''^T + \nu_{n-1}M_{n-1}\cdot v'' + \nu_n M_n \cdot v'' + \nu_{n-1}\nu_n l \\ &= a + \nu_{n-1}[ld_1\cdot v'' + d_2 \cdot v''] \\ &\qquad + \nu_n[d_1 \cdot v'' + (1+l)d_2 \cdot v''] + \nu_{n-1}\nu_n l \\ &= a + \nu_{n-1}[lx + y] + \nu_n[x + (1+l)y] + \nu_{n-1}\nu_n l. \end{aligned}$$

Also, if $b = (b'', \beta_{n-1}, \beta_n)$ with $\beta_{n-1}, \beta_n \in \mathbb{Z}_2$, then $b\cdot v = b''\cdot v'' + \beta_{n-1}\nu_{n-1} + \beta_n\nu_n$, so that the exponent of -1 of the vth entry in our codeword is

$$\begin{aligned} Q_M(v) &+ b\cdot v + \delta \\ &= a + \nu_{n-1}[lx + y] + \nu_n[x + (1+l)y] + \nu_{n-1}\nu_n l \\ &\qquad + b''\cdot v'' + \beta_{n-1}\nu_{n-1} + \beta_n\nu_n + \delta. \end{aligned}$$

On the other hand, by Theorem 7.4 a typical codeword of $\mathscr{K}_8(\Sigma^-)$ has the form

$$\left(i^{d_1M\cdot v''}j^{d_2M\cdot v''}(-1)^{v''U_M''v''^T + b''\cdot v''}q\right)_{v''\in V''} = \left(i^x j^y(-1)^{a+b''\cdot v''}q\right)_{v''\in V''}.$$

There are various choices we could make in order to proceed. We choose not to introduce additional terms in the exponents here, which would appear if we collected together all powers of i (and j). Instead, we will consider the entire codeword instead of just one coordinate at a time. Thus, we write each word in $\mathscr{K}_8(\Sigma^-)$ first as $(q_v'')_{v''\in V''}$, and then as

$$(q_v'')_{v''\in V''} = \left(i^{x(v'')}j^{y(v'')}(-1)^{a(v'')+b''\cdot v''}q_0\right)_{v''\in V''}$$

with $x(v'')$, $y(v'')$, $a(v'') \in \mathbb{Z}_2$, thereby making the vector 0 in V'' somehow "special." This leads to the following transition, where $q_0 = i^{\beta_n} j^{\beta_{n-1}}(-1)^{\delta}$, $\tilde{a}(v'') := a(v'') + b'' \cdot v'' + \delta$, and (as above) we abbreviate $x = x(v'')$, $y = y(v'')$, $\tilde{a} = \tilde{a}(v'')$:

$$\begin{aligned}(q_{v''})_{v'' \in V''} &= \left(i^x j^y (-1)^{\tilde{a}} \cdot i^{\beta_n} j^{\beta_{n-1}}\right)_{v'' \in V''} \\ &\to \big(\tilde{a}, \tilde{a} + lx + y + \beta_{n-1}, \tilde{a} + x + (1+l)y + \beta_n, \qquad (7.6) \\ &\qquad \tilde{a} + (1+l)x + ly + l + \beta_{n-1} + \beta_n\big)_{v'' \in V''}\end{aligned}$$

(using $(\nu_{n-1}, \nu_n) = (0,0), (1,0), (0,1), (1,1)$ for the four coordinates on the right side). However, (7.6) is not an actual map, since l is not visible on the left side. Note that this was already foreshadowed in Remark 7.5 (and at the end of Section 3).

When this non-map is restricted to $x = 0$, $\beta_{n-1} = \beta_n = 0$, we obtain

$$\left(j^y(-1)^{\tilde{a}}\right)_{v'' \in V''} \to \left(\tilde{a}, \tilde{a} + y, \tilde{a} + (1+l)y, \tilde{a} + ly + l\right)_{v'' \in V''},$$

which is just the Gray map on the first two coordinates. Restricting (7.6) to $y = 0$, $\beta_{n-1} = \beta_n = 0$, we obtain

$$\left(i^x(-1)^{\tilde{a}}\right)_{v'' \in V''} \to \left(\tilde{a}, \tilde{a} + lx, \tilde{a} + y, \tilde{a} + (1+l)x + l\right)_{v'' \in V''},$$

which is just the Gray map on the first and third coordinates.

7.3. *From Quaternions to $\mathbb{Z}_4^2$*

The $\mathbb{Z}_4$-version of (7.6) also is unsatisfactory, but again is included for completeness. As in (7.3), in view of (6.4) we have the following 2-adic expansion:

$$\begin{aligned}\hat{v}'' P_M \hat{v}'^T &= d(P_M) \cdot v' + 2v' \begin{pmatrix} U_M'' & M_{n-1}^T \\ O & O \end{pmatrix} v'^T \\ &= (M_n, l) \cdot (v'', \nu) + 2(v'', \nu) \begin{pmatrix} U_M'' & M_{n-1}^T \\ O & O \end{pmatrix} (v'', \nu)^T \\ &= [M_n \cdot v'' +_2 l\nu] + 2\left[v'' U_M'' v''^T + \nu M_{n-1} \cdot v''\right] \\ &= [x +_2 (1+l)y +_2 l\nu] + 2[a + \nu(lx + y)],\end{aligned}$$

where $+_2$ denotes binary addition and $v' = (v'', \nu)$ and $b' = (b'', \beta)$ with $\nu, \beta \in \mathbb{Z}_2$. Let $\varepsilon = \beta_n + 2\delta$ in (6.6) (this involves a possibly arbitary decision on matching up the quaternionic and $\mathbb{Z}_4$ situations.) Then

$$\begin{aligned}
&\hat{v}' P_M \hat{v}'^T + 2\hat{b}' \cdot \hat{v}' + (\beta_n + 2\delta) \\
&\qquad = \Big\{[x +_2 (1+l)y +_2 l\nu] + 2\big[\tilde{a} + \nu\{lx + y\} \\
&\qquad\qquad\qquad + \hat{b}'' \cdot \hat{v}'' + \beta\nu + \mu\big]\Big\} + \beta_n .
\end{aligned}$$

Hence, letting $\nu = 0, 1$, we obtain

$$\begin{aligned}
(q_{v''})_{v'' \in V''} &= \left(i^x j^y (-1)^{\tilde{a}} \cdot i^{\beta_n} j^{\beta_{n-1}}\right)_{v'' \in V''} \\
&\to \big([x +_2 (1+l)y] + 2\tilde{a}, [x +_2 (1+l)y +_2 l] \qquad (7.7) \\
&\qquad + 2[\tilde{a} + lx + y]\big)_{v'' \in V''} + (\beta_n)_{v'' \in V''},
\end{aligned}$$

where the right side of (7.7) is viewed as the codeword

$$i^{\beta_n}\left((-1)^{\tilde{a}} i^{x +_2 (1+l)y}, (-1)^{\tilde{a} + lx + y} i^{x +_2 (1+l)y +_2 l}\right)_{v'' \in V''}$$

in $\mathscr{K}_4(\Sigma')$. However, (7.7) seems even more opaque than (7.6).

8. ADDITIONAL REMARKS

8.1. *Distance Distribution*

By analogy with the binary and $\mathbb{Z}_4$-cases, a "natural" metric on $Q_8^{2^n - 2}$ is the *Hamiltonian metric* induced from that of $\mathbb{H}^{2^n - 2}$ as follows:

$$d_H(w_1, w_2) := \|w_1 - w_2\|^2 / 2.$$

When restricted to $\langle i \rangle^{2^n - 2} \cong \mathbb{Z}_4^{2^n - 2}$, this is just the Lee metric.

THEOREM 8.1. *Given $w_0 \in \mathscr{K}_8(\Sigma^-)$, the Hamiltonian distances and the number of codewords at each distance from w_0 are as follows:*

Distance	*Number of codewords at that distance from w_0*
0	1
$2^{n-2} - 2^{(n-2)/2}$	$(2^{n-1} - 1)2^{n-2}$
2^{n-2}	$3 \cdot 2^{2n-2} + 2^{n-1} - 2$
$2^{n-2} + 2^{(n-2)/2}$	$(2^{n-1} - 1)2^{n-2}$
2^{n-1}	1

The total number of codewords is 2^{2n}.

Proof. We are considering 2^{n-1} frames, each having 2^{n-2} lines, where each line $\langle w \rangle$ has eight members wq of $\mathscr{K}_8(\Sigma^-)$ for $q \in Q_8$. Note that $\|w_0\| = 2^{(n-2)/2}$.

If $\langle w \rangle = \langle w_0 \rangle$, then $w = w_0 q$, so that $\|qw_0 - w_0\|^2/2 = 2^{n-2}|q - 1|^2/2$ is 0 if $q = 1$, 2^{n-1} if $q = -1$, and 2^{n-2} for the remaining six scalars q.

If $\langle w \rangle$ is perpendicular to $\langle w_0 \rangle$, then $\|qw_0 - w_0\|^2/2 = 2 \cdot 2^{n-2}/2$. There are $2^{n-2} - 1$ such lines $\langle w \rangle$, and each has eight codewords.

In the remaining cases the angle between $\langle w \rangle$ and $\langle w_0 \rangle$ is $\cos^{-1} 2^{-(n-2)/2}$. There are $(2^{n-1} - 1)2^{n-2}$ such lines, and for each of them we may assume that w is chosen with $(w, w_0) = (2^{(n-2)/2})^2 2^{-(n-2)/2} = 2^{(n-2)/2}$. Then $\|qw - w_0\|^2/2 = [2 \cdot 2^{n-2} - 2^{(n-2)/2}(q + \bar{q})]/2$ is

$$\begin{array}{ll} 2^{n-2} - 2^{(n-2)/2} & \text{if } \ q = 1, \\ 2^{n-2} + 2^{(n-2)/2} & \text{if } \ q = -1, \text{ and} \\ 2^{n-2} & \text{if } \ q \neq \pm 1. \end{array}$$

In particular, the number of codewords at distance 2^{n-2} from w_0 is

$$(2^{n-1} - 1)2^{n-2} \cdot 6 + (2^{n-1} - 1) \cdot 8 + 6 = 3 \cdot 2^{2n-2} + 2^{n-1} - 2. \qquad \blacksquare$$

Thus, $\mathscr{K}_8(\Sigma^-)$ is *distance-invariant*. The corresponding table of distances for a binary Kerdock code of length 2^n is as follows:

Distance	Number of codewords at that distance from w_0
0	1
$2^{n-1} - 2^{(n-2)/2}$	$(2^{n-1} - 1)2^n$
2^{n-1}	$2^{n+1} - 2$
$2^{n-1} + 2^{(n-2)/2}$	$(2^{n-1} - 1)2^n$
2^n	1

The total number of codewords is 2^{2n}. Of course, this implies that there is no isometry from the binary to the quaternionic code (not even up to a constant multiple of distances), thereby "explaining" the failures occurring in the preceding section. However, only at this stage have we discussed a metric on $Q_8^{2^n-2}$, because it is conceivable that there is a "natural" metric, other than d_H, with respect to which the binary and quaternionic Kerdock codes are isometric.

Theorem 7.4 contains a somewhat explicit version of the codewords in $\mathscr{K}_8(\Sigma^-)$. It is not straightforward to use those formulas in order to prove the above theorem. Namely, there are too many cases to consider; for example, we might have $d_1 = d_2 = 0$ and $M \neq O$, or, alternatively, U might be singular but nonzero. On the other hand, it would be interesting to see if the theorem gave additional information concerning the various vectors d_1, d_2, and matrices U corresponding to the various members M of the Kerdock set.

8.2. *Relationships among Line-Sets*

There is a simple analogue of [1, Proposition 7.2], relating $\mathscr{F}(\Sigma^-)$ to a suitable set of real lines. Recall from [1, Section 3] that, whenever A is a subgroup of E such that $\tilde{A} \in \Sigma$, there is a set $\mathscr{F}(A)$ of exactly 2^n pairwise perpendicular lines of $\mathbb{R}^{2^n}$ left invariant by A; $\mathscr{F}(\Sigma)$ is defined to be the union of all of these sets $\mathscr{F}(A)$ as $\tilde{A}$ runs through Σ. Note that E normalizes AZ and hence leaves $\mathscr{F}(A)$ invariant.

PROPOSITION 8.2. $\mathscr{F}(\Sigma^-) = \{u\mathbb{H} \mid u\mathbb{R} \in \mathscr{F}(\Sigma)\}$.

Proof. Let $\tilde{A} \in \Sigma$. Let A^- denote the preimage in E^- of the member $\tilde{A} \cap U^-$ of the orthogonal spread Σ^- of $\bar{E}^-$. If $u\mathbb{R} \in \mathscr{F}(A)$, then A^- leaves invariant $u\mathbb{R}$ and hence also $u\mathbb{H}$. Since Q_8 permutes the lines in $\mathscr{F}(A)$ in orbits of size 4, this produces 2^{n-2} lines of $\mathbb{H}^{2^n-2}$ left invariant by A^-. However, by Proposition 4.3, that is exactly the number of quaternionic lines left invariant by A^-. ■

8.3. *Equivalences among Line-Sets*

Exactly as in [1, Corollaries 3.7 and 5.6], two line-sets of the form $\mathscr{F}(\Sigma^-)$ (obtained using the same group E^-) are equivalent under $\mathrm{U}(\mathbb{H}^{2^n-2})$ if and only if the corresponding orthogonal spreads Σ^- are equivalent under the orthogonal group $\mathrm{O}^-(2n-2, 2)$ of $\tilde{E}^-$. There are undoubtedly large numbers of inequivalent orthogonal spreads in $\tilde{E}^-$, in fact many more than there are in $\tilde{E}$, but this has yet to be proved. The methods used in [4] and [5] do not appear to apply in this situation.

8.4. *Equivalences among Quaternionic Codes*

Our results on the equivalence of Q_8-Kerdock codes are incomplete. We will sketch the straightforward computations used thus far.

One "natural" definition of *equivalence* between codes in $Q_8^{2^{n-2}}$ is as follows: a map induced by a permutation of $Q_8^{2^{n-2}}$ of the form

$$(q''_v)_{v''\in V''} \mapsto \left((q_{v''\theta})^{\sigma(v'')}\right)_{v''\in V''}, \tag{8.3}$$

where θ is a permutation of coordinate positions and $\sigma(v'')$ is an automorphism or antiautomorphism of Q_8, one for each coordinate position. If, for example, all coordinates are powers of i, then this produces the monomial definition used in [1]. However, this definition also allows for the fact that one should be able to freely interchange i and j.

Suppose that Σ and $\Sigma^\#$ are orthogonal spreads of $\tilde{E}$, producing orthogonal spreads Σ^- and $\Sigma^{\#-}$ of $\tilde{E}^-$ as in Section 6. We assume that the latter spreads contain $\tilde{X}(V'')$ and $\tilde{Y}(V'')$. Let $\mathbf{M}(\Sigma)$ and $\mathbf{M}(\Sigma^\#)$ be the corresponding Kerdock sets of matrices (again as in Section 6), and let $\mathscr{K}_8(\Sigma^-)$ and $\mathscr{K}_8(\Sigma^{\#-})$ be the corresponding Q_8-Kerdock codes (cf. Theorem 7.4). For each $M \in \mathbf{M}(\Sigma)$ let $U'' = U''_M$, $d_1 = d_{1M}$, and $d_2 = d_{2M}$ be as before (cf. (7.1) and Lemma 7.2). Since $\mathbf{M}(\Sigma)$ is a Kerdock set, d_1, d_2, and $d_1 + d_2 = lM_{n-1} + M_n$ can be any vectors in V'' (for example, just choose $l = 0$ in the latter case). For notational convenience we will now let v (rather than v'') denote an arbitrary vector in V''; similarly, we will write U instead of U''.

EXAMPLE 8.4 *Some automorphisms of* $\mathscr{K}_8(\Sigma^-)$.

(i) *If* $w \in V''$, *then* $v \mapsto v + w$ *induces an automorphism* $(q_v) \mapsto (q_{v+w})$.

(ii) $(q_v) \mapsto (q_v^\sigma)$ *is an automorphism if* σ *is any automorphism or antiautomorphism of* Q_8.

Assume that the equivalence (8.3) sends $\mathscr{K}_8(\Sigma^-)$ to $\mathscr{K}_8(\Sigma^{\#-})$. Then it sends words all of whose coordinates are ± 1 to words of the same sort (these are just first-order Reed-Muller codes corresponding to the zero matrix of both $\mathbf{M}(\Sigma)$ and $\mathbf{M}(\Sigma^\#)$). Using Theorem 7.4, it follows that g induces a coordinate permutation θ that is an affine transformation of V'', namely, $v \mapsto vR + w$ for some $R \in GL(V'')$ and some (constant) vector w. By Example 8.4, we may assume that $w = 0$ and $\sigma(0) = 1$.

Our equivalence now has the form

$$(q_v)_{v \in V''} \mapsto \left((q_{vR})^{\sigma(v)}\right)_{v \in V''} \tag{8.5}$$

for automorphisms or antiautomorphisms $\sigma(v)$ of Q_8. For each $v \in V''$ there are $\alpha(v)$, $\beta(v)$, $\lambda(v)$, $\gamma(v)$, $\delta(v)$, $\mu(v) \in \mathbb{Z}_2$ such that

$$\begin{aligned} i^{\sigma(v)} &= i^{\alpha(v)} j^{\beta(v)} (-1)^{\lambda(v)} \\ j^{\sigma(v)} &= i^{\gamma(v)} j^{\delta(v)} (-1)^{\mu(v)} \\ \alpha(v)\delta(v) &- \beta(v)\gamma(v) = 1. \end{aligned} \tag{8.6}$$

Since $\sigma(0) = 1$, we have $\alpha(0) = \gamma(0) = 1$ and $\beta(0) = \delta(0) = \lambda(0) = \mu(0) = 0$.

Each $M \in \mathbf{M}(\Sigma)$ produces $U = U''_M$ and d_1, d_2 as before, and together with $q \in Q_8$ and $b \in V''$ yields a codeword in $\mathscr{K}_8(\Sigma^-)$. Under (8.5) this corresponds to a codeword in $\mathscr{K}_8(\Sigma^{\sharp -})$ arising from some $q^\sharp \in Q_8$, $b^\sharp \in V''$, and $M^\sharp \in \mathbf{M}(\Sigma^\sharp)$ with associated $U^\sharp = U''_{M^\sharp}$, $d_1^\sharp$, $d_2^\sharp$:

$$\left[i^{\alpha(v)} j^{\beta(v)} (-1)^{\lambda(v)}\right]^{d_1 \cdot vR} \left[i^{\gamma(v)} j^{\delta(v)} (-1)^{\mu(v)}\right]^{d_2 \cdot vR} (-1)^{vRU R^T v^T + b \cdot v} q^{\sigma(v)}$$
$$= i^{\alpha_1^\sharp \cdot v} j^{d_2^\sharp \cdot v} (-1)^{vU^\sharp v^T + b^\sharp \cdot v} q^\sharp$$

for all $v \in V''$. Here, $q^\sharp = q^{\sigma(0)} = q$, so that

$$\left[i^{\alpha(v)} j^{\beta(v)} (-1)^{\lambda(v)}\right]^{d_1 \cdot vR} \left[j^{\gamma(v)} i^{\delta(v)} (-1)^{\mu(v)}\right]^{d_2 \cdot vR} (-1)^{vRU R^T v^T + b \cdot v} q^{\sigma(v)}$$
$$= i^{d_1^\sharp \cdot v} j^{d_2^\sharp \cdot v} (-1)^{vU^\sharp v^T + b^\sharp \cdot v} \tag{8.7}$$

for all $v \in V''$. Write $q = i^{\varepsilon(i)} j^{\varepsilon(j)} (-1)^{\varepsilon(-1)}$ for some $\varepsilon(i)$, $\varepsilon(j)$, $\varepsilon(-1) \in \mathbb{Z}_2$.

Our first consequence of (8.7) is that $\alpha + \alpha(0)$, $\beta + \beta(0)$, $\gamma + \gamma(0)$, *and* $\delta + \delta(0)$ *are linear functionals on* V''. For, choose $b = 0$, $M = O$, and $q = i$ in order to see that there exist $d_1^\sharp$, $d_2^\sharp$, $b^\sharp$ such that $i^{\alpha(v)} j^{\beta(v)} \equiv i^{\sigma(v)} \equiv i^{d_1^\sharp \cdot v} j^{d_2^\sharp \cdot v} i \pmod{\langle -1 \rangle}$ for all $v \in V''$, which makes the stated linearity obvious.

Consequently, $\alpha(v) + 1 = u_\alpha \cdot v$, $\beta(v) = u_\beta \cdot v$, $\gamma(v) + 1 = u_\gamma \cdot v$, and $\delta(v) = u_\delta \cdot v$ for some $u_\alpha, u_\beta, u_\gamma, u_\delta \in V''$ and all $v \in V''$. Then

$$\begin{aligned} &\text{if} \quad u_\alpha \neq 0 \text{ and } u_\gamma \neq 0 \quad \text{then } u_\alpha = u_\gamma; \\ &\text{if} \quad u_\beta \neq 0 \text{ and } u_\delta \neq 0 \quad \text{then } u_\beta = u_\delta. \end{aligned} \tag{8.8}$$

For example, by (8.6), if $u_\alpha \neq 0$ and $u_\gamma \neq 0$ then $\alpha^{-1}(0) \subseteq \gamma^{-1}(1)$, where both of these sets have to be affine hyperplanes of V''.

Now we can show that $u_\alpha = u_\beta = u_\gamma = u_\delta = 0$. For, choose $q = 1$ and $b = 0$ in (8.7): for each M there exist $M^\sharp$, $b^\sharp$ such that (8.7) holds, so (by comparing exponents of i) $\alpha(v)d_1 \cdot vR + \gamma(v)d_2 \cdot vR = d_1^\sharp \cdot v$ for all $v \in V''$. Then $[\alpha(v)d_1R^T + \gamma(v)d_2R^T + d_1^\sharp] \cdot v = 0$ for all v. More precisely, in view of (8.8), one of the following holds:

$$\begin{aligned} u_\alpha &= 0, & \left[d_1R^T + \gamma(v)d_2R^T + d_1^\sharp\right] \cdot v &= 0 \quad \forall v \in V'', \\ u_\gamma &= 0, & \left[\alpha(v)d_1R^T + d_1^\sharp\right] \cdot v &= 0 \quad \forall v \in V'', \text{ or} \\ u_\alpha &= u_\gamma, & \left[\alpha(v)(d_1 + d_2)R^T + d_1^\sharp\right] \cdot v &= 0 \quad \forall v \in V''. \end{aligned}$$

Let perpendicularity refer to the dot product on V''. If $u_\alpha = 0 \neq u_\gamma$ we see that $\gamma^{-1}(0) \subseteq [d_1R^T + d_1^\sharp]^\perp$ and $\gamma^{-1}(1) \subseteq [d_1R^T + d_2R^T + d_1^\sharp]^\perp$, where $\gamma^{-1}(0)$ and $\gamma^{-1}(1)$ are the affine hyperplanes of V'' determined by $u_\gamma^\perp$. We may assume that $d_2R \neq 0$. It follows that one of the vectors $d_1R^T + d_1^\sharp$, $d_1R^T + d_2R^T + d_1^\sharp$ is 0 while the other is u_γ, so that $u_\gamma = d_2R^T$. Since d_2 can be any nonzero vector in V'', this is ridiculous. Similarly, $u_\alpha = 0 \neq u_\gamma$ is impossible, as is $u_\alpha = u_\gamma \neq 0$. Thus, $u_\alpha = u_\gamma = 0$; similarly, $u_\beta = u_\delta = 0$.

Consequently, $\alpha(v) = \delta(v) = 1$ and $\beta(v) = \gamma(v) = 0$ for all $v \in V''$. We note that this may seem slightly surprising: all of our automorphisms or antiautomorphisms $\sigma(v)$ have turned out to act in the same (trivial) manner on $Q_8/Z(Q_8)$.

Now (8.7) simplifies to

$$\begin{aligned} &\left[i(-1)^{\lambda(v)}\right]^{d_1 \cdot vR}\left[j(-1)^{\mu(v)}\right]^{d_2 \cdot vR}(-1)^{vRUR^Tv^T + b \cdot vR} \\ &\quad \times\left[i(-1)^{\lambda(v)}\right]^{\varepsilon(i)}\left[j(-1)^{\mu(v)}\right]^{\varepsilon(j)}(-1)^{\varepsilon(-1)} \\ &\quad = i^{d_1^\sharp \cdot v} j^{d_2^\sharp \cdot v}(-1)^{vU^\sharp v^T + b^\sharp \cdot v} i^{\varepsilon(i)} j^{\varepsilon(j)}(-1)^{\varepsilon(-1)} \end{aligned}$$

for all $v \in V''$. Comparing the exponents of i, j, and -1, we find that

$$d_1^\# = d_1 R^T, \qquad d_2^\# = d_2 R^T \tag{8.9}$$

and

$$vU^\# v^T + b^\# \cdot v = vRUR^T v^T + b \cdot vR + \lambda(v)(d_1 \cdot vR) + \mu(v)(d_2 \cdot vR)$$
$$+ \varepsilon(i)\lambda(v) + \varepsilon(j)\mu(v) + \varepsilon(i)(d_2 \cdot vR) \tag{8.10}$$

for all $v \in V''$. (The term $\varepsilon(i)(d_2 \cdot vR)$ arose when rearranging the product $j^{d_2 \cdot vR} i^{\varepsilon(i)}$.) Now we are ready to prove the following

Proposition 8.11. *$\mathscr{K}_8(\Sigma^-)$ and $\mathscr{K}_8(\Sigma^{\#-})$ are equivalent if, and only if, there exist $R \in \mathrm{GL}(V'')$ and s_1, $s_2 \in V''$ so that, for each $M \in \mathbf{M}(\Sigma)$ (with associated $U = U''_M$, d_1, d_2 as in Proposition 3.2 and (7.1)), there is some $M^\# \in \mathbf{M}(\Sigma^\#)$ (with associated $U^\# = U''_{M^\#}$, $d_1^\#$, $d_2^\#$) such that (8.9) holds and such that*

$$U^\# + RUR^T + s_1^T d_1 R^T + s_2^T d_2 R^T \tag{8.12}$$

is a symmetric matrix. In particular, if this condition holds, then

$$M^{\#''} = RM''R^T + s_1^T d_1 R^T + \left(s_1^T d_1 R^T\right)^T + s_2^T d_2 R^T + \left(s_2^T d_2 R^T\right)^T. \tag{8.13}$$

Proof. At this point we have $\lambda, \mu : V'' \to \mathbb{Z}_2$ such that, for any $M \in \mathbf{M}(\Sigma)$, $b \in V''$, $\varepsilon(i)$, $\varepsilon(j) \in \mathbb{Z}_2$, there are $M^\# \in \mathbf{M}(\Sigma^\#)$ and $b^\# \in V''$ for which (8.10) holds for all $v \in V''$. Here, *$\lambda(v)$ and $\mu(v)$ are linear functions.* For, we saw earlier that the codewords in $\mathscr{K}_8(\Sigma^-)$ arising from the matrix $M = O$ are sent to the codewords of $\mathscr{K}_8(\Sigma^{\#-})$ arising from $M^\# = O$. By (8.10) with $M = O$, we have $b^\# \cdot v = b \cdot v + \varepsilon(i)\lambda(v) + \varepsilon(j)\mu(v)$ for all $v \in V''$. Linearity follows if we choose $\{\varepsilon(i), \varepsilon(j)\} = \{0, 1\}$.

Write $\lambda(v) = s_1 \cdot v$ and $\mu(v) = s_2 \cdot v$ for some s_1, $s_2 \in V''$. Then (8.10) simplifies to

$$v\left[U^\# + RUR^T + s_1^T d_1 R^T + s_2^T d_2 R^T\right] v^T$$
$$= \left[b^\# + bR^T + \varepsilon(i)s_1 + \varepsilon(j)s_2 + \varepsilon(i)d_2 R^T\right] \cdot v$$

for all $v \in V''$. This is equivalent to the assertion that (8.12) is a symmetric matrix whose diagonal is

$$\Delta\left(b^{\#} + bR^T + \varepsilon(i)s_1 + \varepsilon(j)s_2 + \varepsilon(i)d_2R^T\right). \tag{8.14}$$

By (7.1), adding (8.12) to its transpose produces (8.13).

Conversely, given any $\varepsilon(i)$, $\varepsilon(j) \in \mathbb{Z}_2$, the requirement that (8.14) be the diagonal of (8.12) allows $b^{\#}$ to be determined from the other data. Consequently, we can reverse our entire argument in order to deduce the proposition. ■

Of course, we have also dealt with the automorphism group of $\mathscr{K}_8(\Sigma^-)$: it is generated by the automorphisms in Example 8.4 together with those arising as in the preceding proposition.

By analogy with [1, Theorem 10.4], it is natural to hope that any code equivalence will correspond to an equivalence between the orthogonal spreads Σ and $\Sigma^{\#}$. The obstacle appears to be the same as in Section 7: l does not appear at all in the proposition. In order to clarify this, we will indicate a "geometric" version of equivalence between some codes of the form $\mathscr{K}_8(\Sigma^-)$.

Consider *any* matrix

$$\begin{pmatrix} R & s_1^T & s_2^T & & & \\ O & 1 & 0 & & O & \\ O & 0 & 1 & & & \\ & & & R^T & O & O \\ & O & & s_1 & 1 & 0 \\ & & & s_2 & 0 & 1 \end{pmatrix}$$

with $R \in \mathrm{GL}(n-2, 2)$ and $s_1, s_2 \in V''$. This represents an orthogonal transformation of $\tilde{E}$ fixing $\tilde{X}(V)$, $\tilde{Y}(V)$, $\tilde{X}(v_{n-1})$, and $\tilde{X}(v_n)$. If $M \in \mathbf{M}(\Sigma)$ is as in (6.4), then the above matrix conjugates

$$\begin{pmatrix} I & M \\ O & I \end{pmatrix} \text{ to } \begin{pmatrix} I & M^{\#} \\ O & I \end{pmatrix},$$

where

$$M^\sharp = \begin{pmatrix} R & s_1^T & s_2^T \\ O & 1 & 0 \\ O & 0 & 1 \end{pmatrix} M \begin{pmatrix} R^T & O & O \\ s_1 & 1 & 0 \\ s_2 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} M^{\sharp\prime\prime} & RM_{n-1}^T + ls_1^T & RM_n^T + ls_2^T \\ M_{n-1}R^T + ls_2 & 0 & l \\ M_nR^T + ls_1 & l & 0 \end{pmatrix}$$

with

$$M^{\sharp\prime\prime} = RM''R^T + s_1^TM_{n-1}R^T + RM_{n-1}^Ts_1 + s_2^TM_nR^T + RM_n^Ts_2 + ls_1^Ts_2 + ls_2^Ts_1$$

Moreover, $d_1^\sharp = d_1R^T + ls_1$, $d_2^\sharp = d_2R^T + ls_2$ by Proposition 3.2, and we can let $U^\sharp = RUR^T + s_1^TM_{n-1}R^T + s_2^TM_nR^T + ls_1^Ts_2$. Now

$$i^{d_1^\sharp\cdot v}j^{d_2^\sharp\cdot v}(-1)^{vU^\sharp v^T + b^\sharp\cdot v}q^\sharp \tag{8.15}$$

$$= i^{d_1R^T +_2 ls_2\cdot v}j^{d_2R^T +_2 ls_1\cdot v}(-1)^{vRU\,R^Tv^T + v\,s_1^TM_{n-1}R^Tv^T + v\,s_2^TM_nR^Tv^T + l\,vs_1^Ts_2v^T + b^\sharp\cdot v}q^\sharp.$$

This suggests that there should be a map $\mathbb{H}^{2^{n-2}} \to \mathbb{H}^{2^{n-2}}$ sending each vector listed in Theorem 7.4 to the right side of (8.15). This runs up against the same type of problem encountered in Section 7. In particular, we do not have the situation occurring in Proposition 8.11. Nevertheless, (8.15) is tantalizingly close to the conditions in Proposition 8.11, especially when $l = 0$.

REMARK. We have defined code-equivalence using a family of automorphisms and antiautomorphisms. Another definition would involve only a single one of these: one could define two quaternionic codes to be equivalent if there is an isometry of the underlying complex space sending one to the other. This definition fits well with the metric used in Section 8.1. Of course, we have seen that, for the codes we are considering, these two definitions of equivalence are equivalent.

8.5. *Open Questions*

There should be interesting quaternionic codes other than those studied here. Is there any way to use (7.6) to get new coding-theoretic results in situations other than that of Kerdock codes? Is there any way to use (7.6) to convert nonlinear to linear codes, as was done in [2]? Here, "linearity" means "a subgroup of Q_8^N." Since $\mathscr{K}_8(\Sigma^-)$ appears to be nonlinear, this seems dubious.

Questions of equivalence that were raised in Section 8.4 need to be examined more carefully. Does there exist a broad generalization of all of this, replacing $\mathbb{Z}_2$, $\mathbb{Z}_4$, and Q_8 by extraspecial groups or central products of extraspecial groups with $\mathbb{Z}_4$? Admittedly, this is far-fetched. Note that the exponent of the group is kept at 4 (or 2 in the "degenerate" binary case), as suggested at the end of [1].

As in [1], there are natural but difficult questions concerning the existence of other types of extremal line-sets behaving as in Theorem 1.1. Of course, such questions are even harder in the present context.

REFERENCES

1 A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, submitted for publication.

2 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* 40:301–319 (1994).

3 S. G. Hoggar, *t*-designs in projective spaces. *European J. Combin.* 3:233–254 (1982).

4 W. M. Kantor, Spreads, translation planes and Kerdock sets. I, II, *SIAM J. Algebraic Discrete Methods* 3:151–165, 308–318 (1982).

5 W. M. Kantor, An exponential number of generalized Kerdock codes, *Inform. and Control* 5:74–80 (1982).

6 V. I. Levenštein, Bounds on the maximal cardinality of a code with bounded modulus of the inner product. *Soviet Math. Dokl.* 25:526–531 (1982).

7 A. Neumaier, Combinatorial configurations in terms of distances, Memo. 81-09, Dept. of Mathematics, Technical Univ. Eindhoven.

Accepted 11 October 1994