Journal of Algebraic Combinatorics **9** (1999), 129–140

A Group-Theoretic Framework for the Construction of Packings in Grassmannian Spaces

A.R. CALDERBANK, R.H. HARDIN, E.M. RAINS, P.W. SHOR AND N.J.A. SLOANE
Information Sciences Research, AT&T Labs—Research, 6180 Park Avenue, Florham Park, NJ 07932-0971

Received February 14, 1997

Abstract. By using totally isotropic subspaces in an orthogonal space $\Omega^+(2i, 2)$, several infinite families of packings of 2^k-dimensional subspaces of real 2^i-dimensional space are constructed, some of which are shown to be optimal packings. A certain Clifford group underlies the construction and links this problem with Barnes-Wall lattices, Kerdock sets and quantum-error-correcting codes.

Keywords: Grassmannian packings, quantum computing, orthogonal geometry, Clifford group

1. Introduction

The central problem is to arrange N n-dimensional subspaces of $\mathbb{R}^m$ so they are as far apart as possible. Numerous constructions and bounds were given in [10, 20] (see also [21]). In the present paper we give an algebraic framework for constructing such arrangements that explains all the examples constructed or conjectured in [20].

The two main constructions obtained by these methods are stated in Theorems 1 and 2. Theorem 3 describes an unrelated construction which yields another infinite family of optimal packings. Table 1 summarizes the parameters of the packings obtained in dimensions up to 128.

$G(m, n)$ will denote the Grassmannian space of n-dimensional subspaces of $\mathbb{R}^m$. We shall refer to the elements of $G(m, n)$ as n-dimensional planes, or simply *planes*. For reasons discussed in [10], we define the *distance* between two n-dimensional planes P, Q in $\mathbb{R}^m$ by

$$d(P, Q) = \sqrt{\sin^2\theta_1 + \cdots + \sin^2\theta_n}\ , \tag{1}$$

where $\theta_1, \ldots, \theta_n$ are the principal angles[1] between P and Q. For given values of m, n, N we wish to find the best packings of N planes in $G(m, n)$, that is, subsets $\mathcal{P} = \{P_1, \ldots, P_N\} \subset G(m, n)$ such that $d(\mathcal{P}) = \min_{i \neq j} d(P_i, P_j)$ is maximized ($d(\mathcal{P})$ is called the *minimal distance* of the packing). We refer to [10] for applications and earlier references.

It was shown in [10] that $G(m, n)$ equipped with the metric (1) has an isometric embedding in $\mathbb{R}^D$, $D = (m-1)(m+2)/2$, obtained by representing each plane $P \in G(m, n)$ by the orthogonal projection from $\mathbb{R}^m$ to P. If A is an $n \times m$ generator matrix for P, whose rows are orthonormal vectors spanning P, then the projection is represented by the matrix

$\Pi_P = A^t A$, where t denotes transposition. Π_P is an $m \times m$ symmetric idempotent matrix with trace n, and so lies in $\mathbb{R}^D$. All such Π_P for $P \in G(m,n)$ lie on a sphere of radius $\sqrt{n(m-n)/m}$ in $\mathbb{R}^D$. Furthermore, if two planes $P, Q \in G(m,n)$ are represented by projection matrices Π_P, Π_Q then

$$d^2(P,Q) = n - \text{trace }\ (\Pi_P\ \Pi_Q) = \frac{1}{2}||\Pi_P - \Pi_Q||^2\ , \tag{2}$$

where[2] $||\ \ ||$ denotes the L_2 or Frobenius norm of a matrix ([10], Theorem 5.1).

It follows from this embedding that if $\mathcal{P}$ is a packing of N planes in $G(m,n)$ then

$$d(\mathcal{P})^2 \le \frac{n(m-n)}{m}\ \frac{N}{N-1} \tag{3}$$

(the "simplex bound"). Equality requires $N \le D + 1 = \binom{m+1}{2}$, and occurs if and only if the N points in $\mathbb{R}^D$ corresponding to the planes form a regular equatorial simplex ([10], Corollary 5.2). Also, for $N > D+1$,

$$d(\mathcal{P})^2 \le \frac{n(m-n)}{m} \tag{4}$$

(the "orthoplex bound"). Equality requires $N \le 2D = (m-1)(m+2)$, and occurs if the N points form a subset of the $2D$ vertices of a regular orthoplex (generalized octahedron). If $N = 2D$ this condition is also necessary ([10], Corollary 5.3).

2. The algebraic framework

The following machinery was used in [7] to construct Kerdock sets, among other things, and in [8, 9] to construct quantum error-correcting codes. The starting point is the standard method of associating a finite orthogonal space to an extraspecial 2-group, as described for example in [2], Theorem 23.10, or [15], Theorem 13.8.

The end result will be the construction of various packings of n-spaces in a parent space $V = \mathbb{R}^m$, where $m = 2^i$. As basis vectors for V we use e_u, $u \in U = \mathbb{F}_2^i$. The constructions will involve certain subgroups of the real orthogonal group $\mathcal{O} = O(V, \mathbb{R})$.

For $a, b \in U$ we define transformations $X(a) \in \mathcal{O}$, $Y(b) \in \mathcal{O}$ by

$$X(a) : e_u \to e_{u+a}, \quad Y(b) : e_u \to (-1)^{b \cdot u} e_u, \quad u \in U,$$

where the dot indicates the usual inner product in U. Then $X = \langle X(a) : a \in U \rangle$, $Y = \langle Y(b) : b \in U \rangle$ are elementary Abelian subgroups of $\mathcal{O}$ of order 2^i, and $E = \langle X, Y \rangle \subset \mathcal{O}$ is an extraspecial 2-group[3] of order 2^{2i+1} ([7], Lemma 2.1). The elements of E have the form $\pm X(a)Y(b)$, $a, b \in U$, and satisfy

$$Y(b)X(a) = (-1)^{a \cdot b} X(a)Y(b),$$

$$(-1)^s X(a)Y(b)(-1)^{s'} X(a')Y(b') = (-1)^{a' \cdot b + s + s'} X(a+a')Y(b+b').$$

The center $\Xi(E)$ of E is $\{\pm I\}$, and $\bar{E} = E/\Xi(E)$ is an elementary Abelian group of order 2^{2i} whose elements can be denoted by $\bar{X}(a)\bar{Y}(b)$, $a, b \in U$, where we are using the bar $\bar{}$ for images under the homomorphism from E to $\bar{E}$. As in [2], Theorem 23.10, we define a quadratic form $Q : \bar{E} \to \mathbb{F}_2$ by

$$Q(\bar{g}) = \begin{cases} 0 & \text{if } g^2 = +I \\ 1 & \text{if } g^2 = -I \end{cases}$$

for $\bar{g} \in \bar{E}$, where $g \in E$ is any preimage of $\bar{g}$, and so $Q(\bar{X}(a)\bar{Y}(b)) = a \cdot b$.

The associated alternating bilinear form $B : \bar{E} \times \bar{E} \to \mathbb{F}_2$ is given by

$$B(\bar{g}_1, \bar{g}_2) = Q(\bar{g}_1 + \bar{g}_2) + Q(\bar{g}_1) + Q(\bar{g}_2),$$

for $\bar{g}_1, \bar{g}_2 \in \bar{E}$, and so

$$B(\bar{X}(a)\bar{Y}(b),\ \bar{X}(a')\bar{Y}(b')) = a \cdot b' + a' \cdot b. \tag{5}$$

Then $(\bar{E}, Q)$ is an orthogonal vector space of type $\Omega^+(2i, 2)$ and maximal Witt index (cf. [12]).

The normalizer of E in $\mathcal{O}$ is a certain Clifford group L, of order

$$2^{i^2+i+2}(2^i - 1)\prod_{j=1}^{i-1}(4^j - 1)$$

(cf. [7], Section 2). L is generated by E, all permutation matrices $G(A, a) \in \mathcal{O} : e_u \to e_{Au+a}$, $u \in U$, where A is an invertible $i \times i$ matrix over $\mathbb{F}_2$ and $a \in U$, and the further matrix $H = (H_{u,v})$, $H_{u,v} = 2^{-i/2}(-1)^{u \cdot v}$, $u, v \in U$.

The group L acts on E by conjugation, fixing the center, and so also acts on $\bar{E}$. In fact L acts on $\bar{E}$ as the orthogonal group $O^+(2i, 2)$ ([7], Lemma 2.14).

This Clifford group L has arisen in several different contexts, providing a link between the present problem, the Barnes-Wall lattices (see [4, 5, 20, 22]), the construction of orthogonal spreads and Kerdock sets [7], and the construction of quantum error-correcting codes [3, 9]. It also occurs in several purely group-theoretic contexts—see [7] for references.

The connection with quantum computing arises because if certain conditions are satisfied the invariant subspaces mentioned in Theorem 1 form good quantum-error-correcting codes [8, 9].

3. The construction from totally singular subspaces

A subspace $\bar{S} \subseteq \bar{E}$ is *totally singular* if $Q(\bar{g}) = 0$ for all $\bar{g} \in \bar{S}$. Then $\dim \bar{S} \leq i$, and if $\dim \bar{S} = i$ then $\bar{S}$ is *maximally totally singular*. It follows from (5) that the preimage

$T \subseteq E$ of a maximally totally singular space $\bar{T}$ is an Abelian subgroup of E, of order 2^{i+1}. T contains $-I$, and has 2^{i+1} linear characters, associated with 2^i mutually perpendicular one-dimensional invariant subspaces forming a coordinate frame $\mathcal{F}(T) \subset V$ ([7], Lemma 3.3).

Since L acts as $O^+(2i, 2)$ on $\bar{E}$, L takes any ordered pair of maximally totally singular subspaces that meet in $\{0\}$ to X and Y, respectively. The corresponding coordinate frames in V are

$$\mathcal{F}(X) = \left\{ e_v^* = \frac{1}{2^{i/2}} \sum_{u \in U} (-1)^{u \cdot v} e_u : v \in U \right\} \tag{6}$$

and

$$\mathcal{F}(Y) = \{e_u : u \in U\}, \tag{7}$$

respectively.

If $\bar{S} \subseteq \bar{T}$ has dimension k, its preimage $S \subseteq E$ has 2^{k+1} linear characters, and 2^k distinct invariant subspaces, each of which is spanned by 2^{i-k} of the vectors in $\mathcal{F}(T)$.

We can now state our first main construction for Grassmannian packings.

Theorem 1 *Given k, with $0 \leq k \leq i-1$, the set of all invariant subspaces of the preimages S of all $(i-k)$-dimensional totally singular subspaces $\bar{S}$ of $\bar{E}$ is a packing of N planes in $G(2^i, 2^k)$ with minimal distance $d = 2^{(k-1)/2}$, where*

$$N = 2^{i-k} \begin{bmatrix} i \\ k \end{bmatrix} \prod_{j=k}^{i-1} (2^j + 1),$$

and

$$\begin{bmatrix} i \\ k \end{bmatrix} = \frac{(2^i - 1) \cdots (2^{i-k+1} - 1)}{(2^k - 1) \cdots (2 - 1)}$$

is a Gaussian binomial coefficient.

Proof: There are

$$\begin{bmatrix} i \\ k \end{bmatrix} \prod_{j=k}^{i-1} (2^j + 1)$$

choices for $\bar{S}$ ([6], Lemma 9.4.1) and each $\bar{S}$ yields 2^{i-k} planes.

We compute the distance between two planes from (2). Suppose P_j is a 2^k-dimensional invariant subspace of V corresponding to the character χ_j of the subgroup $S_j \subseteq E$, for

$j = 1, 2$. We may assume $-I \in S_1 \cap S_2$ and $\chi_1(-I) = \chi_2(-I) = -1$. Then

$$\Pi_j = \frac{1}{|S_j|} \sum_{g \in S_j} \chi_j(g) g \in \mathcal{O}$$

is the orthogonal projection onto P_j. Also

$$\begin{aligned}
\operatorname{trace}(\Pi_1\ \Pi_2) &= \frac{1}{|S_1||S_2|} \sum_{g_1 \in S_1} \sum_{g_2 \in S_2} \chi_1(g_1)\chi_2(g_2) \operatorname{trace}(g_1 g_2) \\
&= \frac{1}{|S_1||S_2|} \sum_{g_1 \in S_1 \cap S_2} \sum_{g_2 = \pm g_1^{-1}} \chi_1(g_1)\chi_2(g_2) \operatorname{trace}(g_1 g_2) \\
&= \frac{2}{|S_1||S_2|} \sum_{g_1 \in S_1 \cap S_2} \chi_1(g_1)\chi_2\big(g_1^{-1}\big) \operatorname{trace}(I) \\
&= \begin{cases} \dfrac{2|S_1 \cap S_2| 2^i}{|S_1||S_2|} & \text{if } \chi_1 = \chi_2 \text{ on } S_1 \cap S_2 \\ 0 & \text{otherwise.} \end{cases}
\end{aligned} \tag{8}$$

This implies from (2) that

$$d^2(P_1,\ P_2) = \begin{cases} 2^k - \dfrac{|\overline{S_1 \cap S_2}|}{|\bar{S}_1||\bar{S}_2|} 2^i & \text{if } \chi_1 = \chi_2 \text{ on } S_1 \cap S_2 \\ 2^k & \text{otherwise.} \end{cases} \tag{9}$$

So if $S_1 = S_2$ and $\chi_1 \neq \chi_2$ the planes are orthogonal and at distance $2^{k/2}$; otherwise $S_1 \neq S_2$, $|\overline{S_1 \cap S_2}| \leq 2^{i-k-1}$, and their distance satisfies

$$d^2 \geq 2^k - 2^{k-1} = 2^{k-1},$$

as claimed. □

The principal angles $\theta_1, \ldots, \theta_{2^k}$ between any two planes in the packing may be found by a similar calculation, using the fact that the singular values of $\Pi_1 \Pi_2$ are $\cos^2 \theta_1, \ldots, \cos^2 \theta_{2^k}$ together with $2^i - 2^k$ zeros. It turns out that the principal angles are either all equal to $\pi/2$, or else N_1 of them are equal to $\arccos 2^{-r/4}$ and $2^k - N_1$ are equal to $\pi/2$, where r is the rank of Q on $\bar{S}_1 \cup \bar{S}_2$ and

$$N_1 = 2^{2k-i+r/2} |\bar{S}_1 \cap \bar{S}_2| \,.$$

Examples Taking $k = 0$ in the theorem we obtain a packing of

$$(2+2)(2^2+2) \cdots (2^i+2)$$

lines in $G(2^i, 1)$ with minimal angle $\pi/4$ (as in [20]). These are the lines defined by the minimal vectors in the 2^i-dimensional Barnes-Wall lattice together with their images under H (cf. [11], p. 151).[4]

With $i = 2,\ k = 1$ and $i = 3,\ k = 2$ we obtain two important special cases: 18 planes in $G(4, 2)$ and 70 planes in $G(8, 4)$ (cf. [10, 20]). More generally, when $k = i - 1$ we obtain the packing of

$$f(i) = 2(2^i - 1)(2^{i-1} + 1)$$

planes in $G(2^i, 2^{i-1})$ with $d^2 = 2^{i-2}$ that is the main result of [20]. These packings meet the orthoplex bound of (4) and are therefore optimal. (We do not know if any of the other examples are optimal. Even if not optimal as Grassmannian packings, they may be optimal subject to constraints on the spectrum of distances between planes—cf. [7], Proposition 3.12.) An explicit recursive construction for the special case $k = i-1$ is given in [20].

For $k = 1$ and $k = i - 2$ we obtain two further sequences of packings whose existence was conjectured in [20].

The construction given in the theorem can be restated in an equivalent but more explicit way as follows. Let P_0 be the 2^k-dimensional plane spanned by the coordinate vectors e_u, where $u \in U$ is of the form $00\ldots0 * \ldots *$, with $i - k$ initial zeros. Then the packing consists of all the images of P_0 under the group L.

The parameters of all the packings obtained from the theorem in dimensions up to 128 can be seen in Table 1.

Many other packings can be obtained from the images under L of other starting planes, and still more by replacing L by smaller groups. We mention just one such family. With the $m = 2^i$ coordinate vectors $e_u \in V$ arranged in lexicographic order, let $\mathcal{L}(m, n)$ denote the packing in $G(m, n)$ obtained from the images under L of the plane spanned by the first n coordinate vectors. The $\mathcal{L}(2^i, 2^k)$ are the packings described in Theorem 1. In particular, $\mathcal{L}(2^i, 2^{i-2})$ contains $(1/3)\, f(i)\, f(i-1)$ planes and has $d^2 = 2^{i-3}$. The numerical evidence (see the entries marked "(1a)" in Table 1) suggests that $\mathcal{L}(2^i, 3 \cdot 2^{i-3})$ contains $(1/3)\, f(i)\, f(i-1)\, f(i-2)$ planes and has $d^2 = 2^{i-4}$, and that $\mathcal{L}(2^i, 5 \cdot 2^{i-4})$ contains $(1/3)\, f(i)\, f(i-1)\, f(i-2)\, f(i-3)$ planes and has $d^2 = 2^{i-5}$.

4. Spreads and clique-finding

The packings constructed in Section 3 contains very large numbers of planes. Smaller packings can be obtained by using only some of the totally singular spaces.

Theorem 2 *Suppose a set of M totally singular $(i - k)$-subspaces $\bar{S}$ of $\bar{E}$ can be found such that any pair intersect in a space of dimension at most l. Then the set of invariant subspaces of all the preimages $S \subseteq E$ is a packing of $2^{i-k}M$ planes in $G(2^i,\ 2^k)$ with minimal distance satisfying*

$$d^2 \geq 2^k - 2^{2k+l-i}\ . \tag{10}$$

Table 1. Parameters of Grassmannian packings constructed in this paper.

m	n	N	d^2	Source
3	1	6	4/5	(3)
4	1	12	3/4	(2a)
4	1	24	1/2	(1)
4	1	24	0.5182...	[10]
4	2	6	1	(2d)
4	2	6	6/5	[10]
4	2	18	1	(1)
7	3	28	16/9	(3)
8	1	240	1/2	(1)
8	2	20	3/2	(2d)
8	2	20	1.5789...	[10]
8	2	40	3/2	(2c)
8	2	44	3/2	[10]
8	2	420	1	(1)
8	3	1680	1/2	(1a)
8	4	70	2	(1)
16	1	144	15/16	(2a)
16	1	4320	1/2	(1)
16	2	72	7/4	(2d)
16	2	136	7/4	(2c)
16	2	1040	3/2	(2c)
16	2	16200	1	(1)
16	3	151200	1/2	(1a)
16	4	72	15/4	(2e)
16	4	180	3	(2b)
16	4	6300	2	(1)
16	5	453600	1/2	(1a)
16	6	113400	1	(1a)
16	7	64800	1/2	(1a)
16	8	270	4	(1)
23	11	276	144/25	(3)
31	15	496	256/33	(3)
32	1	146880	1/2	(1)
32	2	272	15/8	(2d)

(*Continued on next page.*)

Table 1. (*Continued.*)

m	n	N	d^2	Source
32	2	1138320	1	(1)
32	4	948600	2	(1)
32	8	94860	4	(1)
32	16	1054	8	(1)
47	23	1128	576/49	(3)
64	1	2112	63/64	(2a)
64	1	9694080	1/2	(1)
64	2	1056	31/16	(2d)
64	2	152681760	1	(1)
64	4	1056	63/16	(2e)
64	4	262951920	2	(1)
64	8	2376	7	(2b)
64	8	56346840	4	(1)
64	16	2772	12	(2b)
64	16	1460844	8	(1)
64	32	4158	16	(1)
71	35	2556	1296/73	(3)
79	39	3160	1600/81	(3)
103	51	5356	2704/105	(3)
127	63	8128	4096/129	(3)
128	1	1260230400	1/2	(1)
128	2	4160	63/32	(2d)
128	2	40012315200	1	(1)
128	4	140043103200	2	(1)
128	8	62019088560	4	(1)
128	16	3445504920	8	(1)
128	32	22882860	16	(1)
128	64	16510	32	(1)

Proof: The bound on the minimal distance follows from (9). Equality holds in (10) if and only if some pair of the subspaces intersect in a subspace of dimension exactly l. □

Examples

(a) An *orthogonal spread* [7, 16, 18] is a partition of the nonzero totally singular points of $\bar{E}$ into $2^{i-1}+1$ totally singular i-spaces. Such a partition exists if and only if i is even (the construction is closely related to Kerdock codes), and then Theorem 2 applies with $M = 2^{i-1}+1$, $k = l = 0$, producing $2^i(2^{i-1}+1)$ lines in $G(2^i,\ 1)$ with minimal angle $\arccos 2^{-i/2}$.

(b) More generally, a *spread* ([14], Theorem 4.1.1) in a projective space $PG(s, q)$ is a partition of the points into copies of $PG(r, q)$, and exists if and only if $r + 1$ divides $s + 1$. Suppose now i is even and j divides i. If we take every totally singular i-space in an orthogonal spread and partition the nonzero points into copies of a $PG(j - 1, 2)$, using a spread, we obtain $M = (2^i - 1)/(2^j - 1)$ totally singular j-spaces in $\bar{E}$ which meet only in the zero vector. This produces a packings of $2^j(2^{i-1}+1)(2^i-1)/(2^j-1)$ planes in $G(2^i, 2^{i-j})$ with $d^2 = 2^{i-j} - 2^{i-2j}$.

In particular, because i is even we can always take $j = 2$, obtaining $4(2^{i-1} + 1)(2^i - 1)/3$ planes in $G(2^i,\ 2^{i-2})$ with $d^2 = 3 \cdot 2^{i-4}$. These packings meet the orthoplex bound of (4).

(c) When the general constructions in (a) and (b) are not applicable, or do not give the desired parameters, we may always resort to clique-finding. We form a graph whose nodes represent all totally singular $(i - k)$-spaces $\bar{S} \subseteq \bar{E}$, with an edge joining two nodes if the corresponding spaces intersect in a space of dimension at most l, and search for a maximal clique. Theorem 2 gives the parameters of the resulting packing.

For example, when $i = 3, k = 1, l = 0$, the graph on 2-spaces has 105 nodes and contains maximal cliques of size 10, producing packings of 40 planes in $G(8, 2)$ with $d^2 = 1.5$. These are suboptimal however, since packings of 44 planes in $G(8, 2)$ with $d^2 = 1.5$ were obtained in [10].

For $i = 4, k = 1, l = 0$, the graph on 3-spaces has 2025 nodes and contains cliques of size 17 (which is probably maximal), leading to packings of 136 planes in $G(16, 2)$ with $d^2 = 1.75$. For $l = 1$ the graph contains cliques of size at least 130, giving 1040 planes in $G(16, 2)$ with $d^2 = 1.5$. We do not know if these are optimal.

Instead of orthogonal spreads in real space, we can also make use of their analogues in complex or quaternionic space. Since the packings obtained do not seem especially good we give only a summary.

(d) A *symplectic spread* is the complex analogue of an orthogonal spread, and leads to a family of $2^{i-1}(2^{i-1} + 1)$ vectors in $\mathbb{C}^{2^{i-1}}$ whose angles are $\pi/2$ or $\arccos 2^{-(i-1)/2}$, for $i \geq 2$ ([7], Theorem 5.6). This produces packings of $2^{i-1}(2^{i-1} + 1)$ planes in $G(2^i, 2)$ with $d^2 = 2 - 2^{-(i-2)}$.

(e) In a similar way, Kantor [17] constructs a family of $2^{i-2}(2^{i-1}+1)$ lines in quaternionic space of dimension 2^{i-2} whose angles are $\pi/2$ or $\arccos 2^{-(i-2)/2}$, for all even $i \geq 4$. This produces packings of $2^{i-2}(2^{i-1} + 1)$ planes in $G(2^i, 4)$ with $d^2 = 4 - 2^{-(i-2)}l$.

5. An infinite family of packings meeting the simplex bound

A packing of 28 planes in $G(7, 3)$ meeting the simplex bound of (3) was given in [10]. This may be generalized as follows.

Let p be a prime which is either 3 or congruent to -1 modulo 8, so that a Hadamard matrix H of order $(p + 1)/2$ exists. Let $Q = \{q_1, \ldots, q_{(p-1)/2}\}$ denote the nonzero quadratic residues modulo p, and $R = \{r_1, \ldots, r_{(p-1)/2}\}$ the nonresidues. The entries of H will be denoted by $H_{s,t}$, for $0 \leq s, t \leq (p-1)/2$, where we assume $H_{s,0} = H_{0,t} = 1$ for all s, t. We will construct a packing in $G(p,\ \frac{p-1}{2})$. Let $e_s (0 \leq s \leq p - 1)$ be coordinate vectors in $\mathbb{R}^p$, let $C = (1 + \sqrt{p+2})/\sqrt{p+1}$, and fix an element $k \in R$. Let $P_t (0 \leq t \leq (p-1)/2)$

be the $(p-1)/2$-dimensional plane spanned by the vectors

$$e_{q_s} + H_{st} C e_{kq_s}, \quad 1 \le s \le \frac{p-1}{2}.$$

For each P_t we obtain $p-1$ further planes by applying the cyclic permutation of coordinates $e_i \rightarrow e_{i+1 (\text{mod } p)}$, for a total of $p(p+1)/2$ planes.

Theorem 3 *The above construction produces a packing of $p(p+1)/2$ planes in $G(p, \frac{p-1}{2})$ in which the distance between every pair of planes satisfies*

$$d^2 = \frac{(p+1)^2}{4(p+2)}.$$

This packing meets the simplex bound of (3) *and is therefore optimal.*

Proof: The principal angles between two planes in the same orbit under the cyclic shift, for example P_0 and P_1, are 0 ($\frac{p-3}{4}$ times) and arcsin $2C/(1+C^2)$ ($\frac{p+1}{4}$ times), and so

$$d^2(P_0, P_1) = \frac{p+1}{4} \frac{4C^2}{(1+C^2)^2} = \frac{(p+1)^2}{4(p+2)}. \tag{11}$$

If the two planes are in different orbits, it is best to compute the corresponding projection matrices and then use (2) to compute the distance, making use of Perron's theorem [19] on quadratic residues. Again the distance is given by (11). We omit the details of this calculation. □

For example, when $p = 7$ and $C = \sqrt{2}$, taking $k = 3$ we find that the planes $P_0, \ldots, P_3$ are generated by

$$\begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & \pm C & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \pm C \\ 0 & 0 & 0 & 0 & 1 & \pm C & 0 \end{bmatrix}, \end{array}$$

where the product of the signs is $+1$ (as given in [10]). The full set of 28 planes is obtained by cycling the seven coordinates. Changing k to 6 we obtain a packing with the same distances but in which some of the principal angles have changed, showing that the packings of Theorem 3 are not unique.

Packings obtained from Theorem 3 are labeled “(3)” in Table 1.

6. A table

Table 1 lists the parameters of the packings constructed in this paper in dimensions up to 128. When better packings with same parameters were given in [10], these are also mentioned. In the last column, “(1)” refers to Theorem 1, “(1a)” to the packings described at the end of Section 3, “(2a)”, . . . , “(2e)” to the examples following Theorem 2, and “(3)” to Theorem 3.

We must stress however that a very large number of other packings are known, especially in dimensions up to 16: see the constructions and tables in [10] and [21].

Notes

1. [13], p. 584.
2. [13], p. 56.
3. [15], p. 349.
4. The group of the Barnes-Wall lattice in dimension 2^i is a subgroup G of index 2 in L. This lattice can therefore be constructed by taking unit vectors along the coordinate frame $\mathcal{F}(Y)$, forming their images under G and then taking their integral closure.

References

1. D. Applegate and D.S. Johnson, personal communication, 1993. Their programs can be obtained from ftp://dimacs.rutgers.edu/pub/challenge/graph/solvers
2. M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, 1986.
3. C.H. Bennett, D. DiVincenzo, J.A. Smolin, and W.K. Wootters, “Mixed state entanglement and quantum error correction,” *Phys. Rev. A* **54** (1996) pp. 3824–3851; also LANL e-print quant-ph/9604024.
4. B. Bolt, T.G. Room, and G.E. Wall, “On Clifford collineation, transform and similarity groups I,” *J. Australian Math. Soc.* **2** (1961), 60–79.
5. B. Bolt, T.G. Room, and G.E. Wall, “On Clifford collineation, transform and similarity groups II,” *J. Australian Math. Soc.* **2** (1961), 80–96.
6. A.E. Brouwer, A.M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, *Ergebnisse der Mathematik 3.18*, Springer, Heidelberg, 1989.
7. 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,” *Proc. London Math. Soc.* **75**, pp. 436–480 (1997).
8. A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, “Quantum error correction and orthogonal geometry,” *Phys. Rev. Lett.* **78**, pp. 405–409 (1997); also LANL e-print quant-ph/9605005.
9. A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, “Quantum error correction via codes over $GF(4)$,” *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.
10. J.H. Conway, R.H. Hardin, and N.J.A. Sloane, “Packing lines, planes, etc.: Packings in Grassmannian space,” *Experimental Math.* **5** (1996), 139–159.
11. J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd edition, *Grundlehren der math. Wissenschaften 290*, Springer, New York, 1993.
12. J.A. Dieudonné, *La Géométrie des Groupes Classiques*, Springer-Verlag, Berlin, 1971.
13. G.H. Golub and C.F. Van Loan, *Matrix Computations*, 2nd edition, Johns Hopkins Univ. Press, 1989.
14. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Univ. Press, 1979.
15. B. Huppert, *Endliche Gruppen*, Springer-Verlag, Berlin, 1967.

16. W.M. Kantor, “Spreads, translation planes and Kerdock sets I,” *SIAM J. Alg. Discrete Methods* **3** (1982), 151–165.
17. W.M. Kantor, “Quanternionic line-sets and quaternionic Kerdock codes,” *Lin. Alg. Appl.* **226–228** (1995), 749–779.
18. W.M. Kantor, “Orthogonal spreads and translation planes,” in *Progress in Combinatorics*, E. Bannai and A. Munemasa (Eds.), *Advanced Studies in Pure Mathematics 24,* Math. Soc. Japan, 1996, pp. 227–242.
19. O. Perron, “Bemerkungen über die Verteilung der quadratischen Reste,” *Math. Zeit.* **56** (1952), 122–130.
20. P.W. Shor and N.J.A. Sloane, “A family of optimal packings in Grassmannian manifolds,” *J. Alg. Combin.*, **7** (1998), 157–163.
21. N.J.A. Sloane, *Grassmannian packings*, http://www.research.att.com/∼njas/grass.
22. G.E. Wall, “On Clifford collineation, transform and similarity groups IV,” *Nagoya Math. J.* **21** (1962), 199–222.