A Family of Optimal Packings in Grassmannian Manifolds

P. W. Shor and N. J. A. Sloane
Information Sciences Research
AT&T Research
Murray Hill, NJ 07974

Revised December 13, 1996

ABSTRACT

A remarkable coincidence has led to the discovery of a family of packings of $m^2 + m - 2$ $m/2$-dimensional subspaces of $m$-dimensional space, whenever $m$ is a power of 2. These packings meet the “orthoplex bound” and are therefore optimal.

Keywords: Grassmannian manifolds, packings, separating subspaces, Barnes-Wall lattices, quantum coding theory, Clifford groups
1. Introduction

Let \( G(m,n) \) denote the Grassmannian space of all \( n \)-dimensional subspaces of real Euclidean \( m \)-dimensional space \( \mathbb{R}^m \). The principal angles \( \theta_1, \ldots, \theta_n \in [0, \pi/2] \) between two subspaces \( P, Q \in G(m,n) \) are defined by

\[
\cos \theta_i = \max_{u \in P} \max_{v \in Q} u \cdot v = u_i \cdot v_i ,
\]

for \( i = 1, \ldots, n \), subject to \( u \cdot u = v \cdot v = 1 \), \( u \cdot u_j = 0 \), \( v \cdot v_j = 0 \) (\( 1 \leq j \leq i - 1 \)). We define the distance\(^1\) between \( P \) and \( Q \) to be

\[
d(P,Q) = \sqrt{\sin^2 \theta_1 + \cdots + \sin^2 \theta_n} .
\]

In [11] we discussed the problem of finding good packings in \( G(m,n) \), that is, for given \( N = 1, 2, \ldots \), of choosing \( P_1, \ldots, P_N \in G(m,n) \) so that \( \min \limits_{i \neq j} d(P_i, P_j) \) is maximized. It was shown that for \( N > m(m + 1)/2 \) the highest achievable distance, \( d_N(m,n) \), satisfies

\[
d_N^2(m,n) \leq \frac{n(m-n)}{m} . \tag{1}
\]

A necessary condition for equality to hold in (1) is that \( N \leq (m-1)(m+2) \). An especially interesting case occurs when \( m \) is even, \( n = m/2 \), and \( N = (m-1)(m+2) \), where we found optimal packings for \( m = 2, 4 \) and \( 8 \); that is, packings of 4 lines in \( \mathbb{R}^2 \), 18 2-spaces in \( \mathbb{R}^4 \) and 70 4-spaces in \( \mathbb{R}^8 \). The first is the familiar configuration seen on the British flag (the Union Jack), the second is the “double-nine”, a classic configuration from nineteenth-century geometry (see the references in [11] and also (3) below), but the third was discovered only after a very considerable computer-assisted search. At the time [11] was written we believed that there would be no further examples in this series.

It came as a considerable surprise therefore when we discovered that such packings exist whenever \( m \) is a power of 2.

These packings were discovered by a remarkable coincidence. One of us (P.W.S.) had discovered a family of groups in connection with quantum coding theory [10], and asked the other (N.J.A.S.) for the best way to determine their orders. N.J.A.S. explained to P.W.S. that the Magma computer system [6], [7], [8] was ideal for this, and gave as an example the symmetry group of above-mentioned set of 70 4-spaces in \( \mathbb{R}^8 \), an 8-dimensional group of order

\[^1\text{It is shown in [11] that this is a metric, and in fact is essentially the } L_2 \text{ distance between the matrices that describe the orthogonal projections onto } P \text{ and } Q.\]

2^7 8! = 5160960. To our astonishment, the first of his groups that P.W.S. tested turned out to be (almost) exactly the same group.

The version of the group that arises from quantum coding in fact has the coordinates in a slightly nicer order, and produces the 70 planes as the orbit of the plane spanned by the first four coordinate vectors. With the help of our colleague R. H. Hardin we verified that the next three groups in the series produced packings meeting the bound in 16, 32 and 64 dimensions. Further investigation then produced the general construction given in Section 3. The groups are described in Section 2.

2. The group

The group \( \mathcal{G}_i \) that arises from quantum coding theory is a subgroup of the real orthogonal group \( O(V, \mathbb{R}) \), where \( V \) denotes \( \mathbb{R}^m \), \( m = 2^i \), \( i \geq 1 \), with coordinates indexed by binary \( i \)-tuples \( x = (x_1, \ldots, x_i) \in \mathbb{F}_i \), and \( \mathbb{F} \) is the field of order 2. \( \mathcal{G}_i \) is generated by the following \( 2^i \times 2^i \) orthogonal matrices:

(i) all permutation matrices \( \pi_{A,b} \) corresponding to affine transformations \( x \mapsto Ax + b \) of \( \mathbb{F}_i \), where \( A \) is any invertible \( i \times i \) matrix over \( \mathbb{F} \) and \( b \in \mathbb{F}_i \), and

(ii) the matrix \( H = \text{diag}\{H_2, H_2, \ldots, H_2\} \), where \( H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix} \) (and + denotes +1, − denotes −1).

By multiplying these generators it is easy to see that, for \( i \geq 2 \), \( \mathcal{G}_i \) contains the matrix \( H' = \text{diag}\{H_4, H_4, \ldots, H_4\} \), where

\[
H_4 = \frac{1}{2} \begin{pmatrix} + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & &
It turns out that $\mathcal{H}_i$ and $\mathcal{G}_i$ are well-known groups. $\mathcal{H}_i$ is the Clifford group $CT_i^+(2^i)$ studied in [4], [5], [14], which in recent years has been used in the classification of finite simple groups (see the references in [9]). $\mathcal{H}_i$ is relevant for the present work because of its connection with the Barnes-Wall lattices.

Although the original paper of Barnes and Wall [3] describes a family of lattices in each dimension $m = 2^i$ ($i \geq 1$), the most interesting lattices are the pair with the highest number of minimal vectors (this number is given by the formula displayed in (4)). We denote this pair of $2^i$-dimensional lattices by $BW_i$ and $BW'_i$. A construction of these lattices using Reed-Muller codes is given in [2] and in [12], p. 234, example (f) (see also [13]).

$BW_i$ and $BW'_i$ are geometrically similar lattices, differing only by a rotation and change of scale. When $i = 1$, for example, we can take $BW_1$ to be the square lattice $Z^2$ (Fig. 1, solid circles), and $BW'_1$ to be its sublattice of index 2 (Fig. 1, double circles). In this case the matrix $D = \sqrt{2}H_2$ acts as an endomorphism sending $BW_1$ to $BW'_1$. In exactly the same way, the matrix $\sqrt{2}H$ sends $BW_i$ to $BW'_i$, a geometrically similar sublattice of index $2^{m/2}$ (cf. [12], pp. 240–241). Applying $\sqrt{2}H$ twice sends $BW_i$ to $2.BW_i$.

- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -

Figure 1: The first pair of Barnes-Wall lattices, $BW_1$ (small circles) and $BW'_1$ (large circles).

Wall [14] showed that for $i \neq 3$, $\mathcal{H}_i$ is the full automorphism group of the lattices $BW_i$ and $BW'_i$. (The case $i = 3$ is special, since $BW_3$ and $BW'_3$ are copies of the root lattice $E_8$.) The group $\mathcal{H}_i$ has a normal subgroup $E$ which is an extra-special 2-group of order $2^{1+2i}$, and $\mathcal{H}_i/E$ is isomorphic to the orthogonal group $O_{2i}^+(2) \cong D_i(2)$. The order of $\mathcal{H}_i$ is

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

By adjoining the irrational matrix $H$ we obtain the full group $\mathcal{G}_i$, twice the size of $\mathcal{H}_i$. The
group $G_i$ also appears in an apparently totally different context in \[9\] (see the group $L$ defined in Eq. (2.13)).

The way the group $G_i$ arises in quantum coding theory is as follows. The quantum state space of $i$ 2-state quantum systems is the complex space $\mathbb{C}^m$, $m = 2^i$. Quantum computation involves making unitary transformations in this space (see \[10\], \[1\]). Some transformations may be much easier to realize than others, and it is therefore important to know which sets of transformations are sufficient for quantum computation, that is, which sets generate a group dense in $SU(2^i)$. An interesting set of transformations which generate a finite group are the linear Boolean functions on quantum bits (the permutation matrices in our group $G_i$), and certain rotations of quantum bits by $\pi/2$. To obtain the corresponding subgroup of the orthogonal group $SO(2^i)$, only one rotation is required, which can be taken to be the matrix $H$.

3. The construction

We specify a subspace $P \in G(m,n)$ by giving a generator matrix, that is, an $n \times m$ matrix whose rows span $P$. We will use the same symbol for the subspace and the generator matrix, and $P^\perp$ will denote the subspace orthogonal to $P$ (or a generator matrix thereof). $I$ denotes an identity matrix.

The construction is recursive. We define a set $Q_i$ containing $2^{2i-1}$ monomial matrices of size $2^{i-1} \times 2^{i-1}$ by $Q_1 = \{(+),(-)\}$,

$$Q_i = \left\{ \begin{pmatrix} + & 0 \\ 0 & + \end{pmatrix} \otimes Q, \begin{pmatrix} + & 0 \\ 0 & - \end{pmatrix} \otimes Q, \begin{pmatrix} 0 & + \\ + & 0 \end{pmatrix} \otimes Q, \begin{pmatrix} 0 & + \\ - & 0 \end{pmatrix} \otimes Q; Q \in Q_{i-1} \right\},$$

for $i \geq 2$. Then $C_i$ is defined by

$$C_1 = \{(+0),(0+),(++),(+-)\},$$

$$C_i = \left\{ (I0), (0I), \begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix}, \begin{pmatrix} P & 0 \\ 0 & P^\perp \end{pmatrix}, (IQ); P \in C_{i-1}, Q \in Q_i \right\},$$
for $i \geq 2$. For example, $C_2$ consists of the 18 matrices
\[
\begin{cases}
(0+00, 00+), (00+0, 000+), (00+0, 0000), (0+00, 000+), (00+0, 0000), \\
(00+0, 0000), (0+00, 0000), (00+0, 0000), (00+0, 0000),
\end{cases}
\]
\[\text{(3)}\]

(The third set of matrices in (3) are the matrices $(IQ)$. ) These are generator matrices for 18 2-spaces in $\mathbb{R}^4$.

**Theorem.** Let $m = 2^i$, $i \geq 1$. The generator matrices $C_i$ define a set of $(m - 1)(m + 2) = 2^{2i} + 2^i - 2$ $\frac{1}{2}m$-dimensional subspaces of $\mathbb{R}^m$. The distance between any two subspaces is either $\sqrt{m/4}$ or $\sqrt{m/2}$.

**Proof.** The number of subspaces is, by induction,
\[
2 + 2(2^{2i-2} + 2^{i-1} - 2) + 2^{2i-1} = 2^{2i} + 2^i - 2,
\]
as claimed.

Since the recursive definition of the $C_i$ mentions the matrices $(I0)$ and $(0I)$, the coordinate positions of $C_i$ can be labeled from left to right with binary $i$-tuples in the natural order, and the group $G_i$ then acts by multiplication on the right. It is now easy to find matrices in $G_i$ that permute the subspaces transitively. We leave the details to the reader. Therefore, to determine the distances between the planes, we may assume that one of the planes has generator matrix
\[
A = \begin{bmatrix}
1 & 0 & & \\
1 & 1 & 0 & \\
& & \ldots & \\
& & & 1
\end{bmatrix}.
\]

We recall (cf. [11]) that if a second plane has generator matrix
\[
B = \begin{bmatrix}
c_1 & s_1 & & \\
c_2 & s_2 & & \\
c_3 & s_3 & & \\
& & \ldots & \\
c_n & s_n & &
\end{bmatrix},
\]

5
where \( c_1^2 + s_1^2 = \cdots = c_n^2 + s_n^2 = 1, \) \( n = 2^{i-1}, \) then the principal angles between \( A \) and \( B \) are \( \arccos c_1, \arccos c_2, \ldots, \arccos c_n. \)

The principal angles between \( A \) and \((0I)\) are \( \pi/2 \) \((n \text{ times})\). Between \( A \) and the subspaces

\[
\begin{pmatrix}
P & 0 \\
0 & P
\end{pmatrix}
\]

or

\[
\begin{pmatrix}
P & 0 \\
0 & P^\perp
\end{pmatrix}
\]

they are \( 0 \) \((n/2 \text{ times})\), \( \pi/2 \) \((n/2 \text{ times})\); and between \( A \) and \((IQ)\) they are \( \pi/4 \) \((n \text{ times})\). The distance from \( A \) to any other plane is therefore either \( \sqrt{n/2} \) or \( \sqrt{n}. \)

Since the bound \((\ref{eq:bound})\) is achieved, this is an optimal packing.

Together with R. H. Hardin, we are also investigating other families of subspaces that can be obtained from the same group. If the initial subspace is taken to be that spanned by the first coordinate vector, the orbit consists of the minimal vectors of the Barnes-Wall lattice \( BW_i \), together with their images under the transformation \( H \), giving a total of

\[
(2 + 2)(2^2 + 2) \cdots (2^i + 2)
\]

(4)

lines, with minimal angle \( \pi/4 \). Taking the plane spanned by the first two coordinates as the initial plane, we appear to obtain packings in \( G(m, 2) \) containing

\[
\frac{1}{12}(2^i - 1) \prod_{r=0}^{i} (2^r + 2)
\]

planes, with minimal distance 1, for \( m = 2^i, \ i \geq 1. \)

On the other hand, if the initial subspace is that generated by the first \( m/4 \) coordinate vectors, we appear to obtain packings in \( G(m, m/4) \) containing

\[
\frac{1}{12}(m - 2)(m - 1)(m + 2)(m + 4)
\]

subspaces, with minimal distance \( \sqrt{m/8} \), for \( m = 2^i, \ i \geq 2. \) The first member of this sequence is the packing of 24 lines in \( \mathbb{R}^4 \) formed from the diameters of a pair of dual 24-cells.

We hope to discuss these packings (which appear to be a kind of Grassmannian analogue of Reed-Muller codes and Barnes-Wall lattices) in a subsequent paper.

Acknowledgements

We thank J. H. Conway and W. M. Kantor for helpful discussions about the groups and R. H. Hardin for assistance with experiments on the computer.
References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. W. Shor, T. Sleator, J. Smolin and H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A., 52 (1995), 3457–3467.

[2] E. S. Barnes and N. J. A. Sloane, New lattice packings of spheres, Canad. J. Math. 35 (1983), 117–130.

[3] E. S. Barnes and G. E. Wall, Some extreme forms defined in terms of Abelian groups, J. Australian Math. Soc., 1 (1959), 47–63.

[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] W. Bosma and J. Cannon, Handbook of Magma Functions, Sydney, May 22, 1995.

[7] W. Bosma, J. J Cannon and G. Mathews, Programming with algebraic structures: Design of the Magma language, In: M. Giesbrecht (ed.), Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation, Oxford, July 20–22, 1994. Association for Computing Machinery, 1994, 52–57.

[8] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, J. Symb. Comp., to appear, 1996.

[9] 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., 1997, to appear.

[10] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A, to appear.

[11] 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.
[12] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 2nd ed., 1993.

[13] G. D. Forney, Jr., Coset codes — part II: binary lattices and related codes, *IEEE Trans. Information Theory*, 34 (1988), 1152–1187.

[14] G. E. Wall, On Clifford collineation, transform and similarity groups IV, *Nagoya Math. J.*, 21 (1962), 199–222.