A Grassmannian Packing Based on the Nordstrom-Robinson Code

Vaneet Aggarwal
Department of Electrical Engineering
Princeton University
Email: vaggarwa@princeton.edu

Alexei Ashikhmin
Statistics and Communications
Research Department
Bell Laboratories
Email: aea@research.bell-labs.com

A. Robert Calderbank
Department of Mathematics
Princeton University
Email: calderbank@math.princeton.edu

***Abstract*— We construct new families of Grassmannian packings associated with the binary Nordstrom-Robinson code. The constituent subspaces are associated with projection operators which which arise in the theory of quantum stabilizer codes. These Grassmannian packings find application as highly structured of dictionaries that admit fast algorithms for identifying sparse representations, and in noncoherent wireless communication with multiple antennas. The capacity of the noncoherent MIMO channel at both low and moderate SNR (under the constraint that only isotropically distributed unitary matrices are used for information transmission) is closely approximated by these packings.**

I. Introduction

Let Q_1, Q_2 be two M-dimensional subspaces of $\mathbb{C}^T, T \geq M$, and P_1, P_2 be the corresponding orthogonal projectors. Traditionally chordal or Frobenius distance is used to measure how far away Q_1 and Q_2 are from each other.

Definition 1: The chordal distance between Q_1 and Q_2 is the quantity

$$d(Q_1, Q_2) = d(P_1, P_2) = M - \mathrm{Tr}\,(P_1 P_2).$$

In this article we will use a slightly different definition of distance.

Definition 2:

$$d(Q_1, Q_2) = d(P_1, P_2) = \mathrm{Tr}\,(P_1) + \mathrm{Tr}\,(P_2) - 2\mathrm{Tr}\,(P_1 P_2).$$

The reasons for the change of distance definitions are the following. First, definition 2, unlike definition 1, is applicable for the case when $\mathrm{Tr}\,(P_1) \neq \mathrm{Tr}\,(P_2)$. Second, let us consider the linear space formed by linear operators acting in $\mathbb{C}^T$ with the inner product defined by $\mathrm{Tr}\,(A^\dagger B), A, B \in \mathbb{C}^T$. Then, remembering that for any projection operator $PP = P$ and $P^\dagger = P$, we see that definition 2 is the standard definition of the Euclidean distance in a vector space. Note also, that if $\mathrm{Tr}\,(P_1) = \mathrm{Tr}\,(P_2)$ then the distance computed according to definition 2 is just twice the distance computed according to definition 1.

We will construct and analyze Grassmannian packings with respect to distance metric 2.

Definition 3: An (T, M, L, d) Grassmannian packing is a collection of orthogonal projectors $P_1, \ldots, P_L$ acting on $\mathbb{C}^T$ such that

$$\begin{aligned} \mathrm{Tr}\,(P_i) &= M,\ 1 \leq i \leq L; \\ d(P_i, P_j) &= \mathrm{Tr}\,(P_i) + \mathrm{Tr}\,(P_j) - 2\mathrm{Tr}\,(P_i P_j) \geq d,\ \text{for} \\ &\quad 1 \leq i < j \leq L. \end{aligned}$$

The parameter

$$d = \min_{1 \leq i < j \leq L} \mathrm{Tr}\,(P_i) + \mathrm{Tr}\,(P_j) - 2\mathrm{Tr}\,(P_i P_j)$$

is the minimum distance of the packing.

We are motivated by two important applications. First, Grassmannian packings are highly structured examples of dictionaries, and the problem of finding sparse representations in non-orthogonal dictionaries has been considered by a number of authors (see for example [9] and references given there). The minimum distance of a packing determines the coherence of the dictionary, which is critical to the design of fast algorithms. The second application is to noncoherent wireless communication with multiple antennas.

In [2] and [3] we constructed Grassmannian packings associated with binary Reed-Muller codes $RM(r, m)$. These packings have $T = 2^m$ and $d = 2^{m-r}$, which coincide with the length and the minimum distance of $RM(r, m)$. The parameter M can be made equal to the weight of any codeword of $RM(r, m)$.

It is natural to try to design Grassmannian packings that are related to other binary codes. In this article we make a first step in this direction by constructing Grassmannian packings that are associated with the binary Nordstrom-Robinson code. The Nordstrom-Robinson code is a nonlinear, distance invariant, code of length 16, size 256, and minimum distance 6. Codewords in the Nordstrom-Robinson code have weights $0, 6, 8, 10$, and 16. This code lies between codes $RM(1, 4)$ and $RM(2, 4)$, which have minimum distances 8 and 4 respectively. It is known that the Nordstrom-Robinson code is optimal. We also note that this code is the first code in the infinite family of nonlinear codes known as the Kerdock codes. A detailed description of the Nordstrom-Robinson code can be found in [8].

In this article we construct Grassmannian packings with $M = 6, 8$, or 10, $T = 16$ and $d = 6$, that is parameters

that correspond to the codeword weights, length and minimum distance of the Nordstrom-Robinson code.

II. Grassmannian Packings over Finite Fields

Our constructions of Grassmannian packings over $\mathbb{C}$ require good Grassmannian packings over $\mathbb{F}_2$, and we begin with some definitions.

The symplectic inner product of vectors $(\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}') \in \mathbb{F}_q^{2m}$ is defined by

$$(\mathbf{a},\mathbf{b}) * (\mathbf{a}',\mathbf{b}') = \mathbf{a}\cdot\mathbf{b}' \ominus \mathbf{a}'\cdot\mathbf{b}, \tag{1}$$

where $\cdot$ is defined by $(x_1,\ldots,x_n)\cdot(y_1,\ldots,y_n) = \sum_j x_j y_j$. An $[n,k]$ linear code C is self-orthogonal (with respect to the symplectic inner product) if for any $\mathbf{v},\mathbf{v}' \in C$ we have $\mathbf{v} * \mathbf{v}' = 0$.

We now define two Grassmannian spaces $G_q(n,m)$ and $GS_q(n,m)$.

Definition 4: The space $G_q(n,m)$ is the sets of all $[n,m]$ linear codes or equivalently the set of all m-dimensional subspaces in $\mathbb{F}_q^n$.

Definition 5: The space $GS_q(n,m)$ is the set of all $[n,m]$ self-orthogonal codes in $\mathbb{F}_q^n$.

Given two linear $[n,m]$ codes C and C', we define the distance $\mathrm{dist}\,(C,C')$ to be the dimension of the largest common subcode of C and C', i.e.

$$\begin{aligned} &\mathrm{dist}\,(C,C') \\ = \;& \max\{\dim(A) : A \text{ is a linear code}, A \in C\cap C'\}. \end{aligned} \tag{2}$$

Next we consider fundamental limits on packings in $G_2(n,m)$ and $GS_2(n,m)$ with respect to the distance defined by (2). In other words we would like to examine a set of $[n,m]$ linear codes $\{C_1,C_2,\ldots,C_L\}$ from $G_2(n,m)$ or from $GS_2(n,m)$ such that the size L is as large as possible and the minimum pairwise distance is also as large as possible.

We start by deriving upper bounds on the size of a packing as a function of the minimum distance. We recall the definition of an association scheme. Let $S = \{s_1,s_2,\ldots,s_l\}$ be a finite set and let $R_0,R_1,\ldots R_D$ be a set of relations defined on S.

Definition 6: The relations R_i define an association scheme if

- R_t is symmetric, that is $(s_i,s_j) \in R_t$ iff $(s_j,s_i) \in R_t$;
- $R_0,R_1,\ldots,R_D$ is a partition of $S\times S$;
- $R_0 = \{(s,s) : s \in S\}$
- For any $(s_t,s_r) \in R_k$ the number of $s \in S$ such that $(s,s_t) \in R_i$ and $(s,s_r) \in R_j$ is a constant p_{ij}^k that does not depend on a particular choice of s_t and s_r.

A comprehensive algebraic theory has been developed over the last 40 years for studying distance-regular graphs and association schemes. For an introduction into the theory of association schemes see for instance [4],[5].

The incidence matrices of the relations R_k span a D-dimensional commutative algebra (called the Bose-Mesner algebra).

The parameter D is called the diameter and the numbers p_{ij}^k are called the intersection numbers of the association scheme. The operator

$$L_k = \begin{bmatrix} p_{00}^k & p_{10}^k & \ldots & p_{D0}^k \\ p_{01}^k & p_{11}^k & \ldots & p_{D1}^k \\ \ldots & \ldots & \ldots & \ldots \\ p_{0D}^k & p_{1D}^k & \ldots & p_{DD}^k \end{bmatrix}, k = 0,\ldots,D,$$

describe multiplication by the incidence matrix of R_k in the Bose-Mesner algebra. Let $p_k(j), j = 0,\ldots,D$, be the set of eigenvalues of L_k. Define

$$P = \begin{bmatrix} p_0(0) & p_1(0) & \ldots & p_D(0), \\ p_0(1) & p_1(1) & \ldots & p_D(1), \\ \ldots & \ldots & \ldots & \ldots \\ p_0(D) & p_1(D) & \ldots & p_D(D). \end{bmatrix}$$

and

$$Q = \frac{1}{|S|}P^{-1} = \begin{bmatrix} q_0(0) & q_1(0) & \ldots & q_D(0), \\ q_0(1) & q_1(1) & \ldots & q_D(1), \\ \ldots & \ldots & \ldots & \ldots \\ q_0(D) & q_1(D) & \ldots & q_D(D). \end{bmatrix}$$

The following result is very useful for deriving bounds on subsets of association schemes. Let X be a subset of S and let the inner distribution of X be defined as

$$A_i = \frac{1}{|X|}|R_i \cap X^2|.$$

Then the numbers $A_0,A_1,...,A_D$ satisfy a set of $D+1$ linear inequalities, known as the Delsarte inequalities,

$$\frac{1}{|S|}\sum_{i=0}^{D} q_j(i)A_i \geq 0, j = 0,\ldots,D. \tag{3}$$

We will use these inequalities to derive bounds for packings in $G_2(n,m)$ and $GS_2(n,m)$.

Let $C,C' \in G_2(n,m)$ or $GS_2(n,m)$. We will say that $(C,C') \in R_i$ if $\mathrm{dist}\,(C,C') = i$.

Theorem 1: [4] With this definition of relation the sets $G_2(n,m)$ and $GS_2(n,m)$ are association schemes.
$G_2(n,m)$ is called the q-Johnson scheme and $GS_2(n,m)$ is called the association scheme of dual polar spaces (speaking more precisely, it is the association scheme of dual polar spaces with respect to the symplectic form).

Both schemes have the same diameter $D = m$ and the intersection numbers of these two schemes are known (for detailed information see [4],[5]). Thus we can compute the matrix Q and use the linear inequalities (3) to derive upper bounds on the size of a packing in $G_2(n,m)$ and $GS_2(n,m)$ as a function of the minimum distance.

In the next example we derive an upper bound on the size of a packing in $GS_2(6,3)$ with minimum distance 2.

The intersection numbers of $GS_2(6,3)$ are

$$\begin{array}{llll} p^0_{3,3}=64 & p^0_{3,2}=0 & p^0_{3,1}=0 & p^0_{3,0}=0 \\ p^0_{2,3}=0 & p^0_{2,2}=56 & p^0_{2,1}=0 & p^0_{2,0}=0 \\ p^0_{1,3}=0 & p^0_{1,2}=0 & p^0_{1,1}=14 & p^0_{1,0}=0 \\ p^0_{0,3}=0 & p^0_{0,2}=0 & p^0_{0,1}=0 & p^0_{0,0}=1 \end{array}$$

$$\begin{array}{llll} p^1_{3,3}=32 & p^1_{3,2}=32 & p^1_{3,1}=0 & p^1_{3,0}=0 \\ p^1_{2,3}=32 & p^1_{2,2}=12 & p^1_{2,1}=12 & p^1_{2,0}=0 \\ p^1_{1,3}=0 & p^1_{1,2}=12 & p^1_{1,1}=1 & p^1_{1,0}=1 \\ p^1_{0,3}=0 & p^1_{0,2}=0 & p^1_{0,1}=1 & p^1_{0,0}=0 \end{array}$$

$$\begin{array}{llll} p^2_{3,3}=32 & p^2_{3,2}=24 & p^2_{3,1}=8 & p^2_{3,0}=0 \\ p^2_{2,3}=24 & p^2_{2,2}=28 & p^2_{2,1}=3 & p^2_{2,0}=1 \\ p^2_{1,3}=8 & p^2_{1,2}=3 & p^2_{1,1}=3 & p^2_{1,0}=0 \\ p^2_{0,3}=0 & p^2_{0,2}=1 & p^2_{0,1}=0 & p^2_{0,0}=0 \end{array}$$

$$\begin{array}{llll} p^3_{3,3}=28 & p^3_{3,2}=28 & p^3_{3,1}=7 & p^3_{3,0}=1 \\ p^3_{2,3}=28 & p^3_{2,2}=21 & p^3_{2,1}=7 & p^3_{2,0}=0 \\ p^3_{1,3}=7 & p^3_{1,2}=7 & p^3_{1,1}=0 & p^3_{1,0}=0 \\ p^3_{0,3}=1 & p^3_{0,2}=0 & p^3_{0,1}=0 & p^3_{0,0}=0 \end{array}$$

Let $\mathcal{P}$ be a packing in $GS_2(6,3)$ with distance distribution (or equivalently the inner distribution) $A_0=1, A_i, i=1,2,3$. Using the intersection numbers p^k_{ij} we construct matrices P and further Q and conclude that the numbers A_i must satisfy the inequalities

$$\begin{aligned} 15-\frac{15}{2}A_1+\frac{15}{4}A_2-\frac{15}{8}A_3 &\geq 0 \\ 84-6A_1-6A_2-\frac{21}{4}A_3 &\geq 0 \\ 35+\frac{25}{2}A_1+\frac{5}{4}A_2-\frac{35}{8}A_3 &\geq 0 \end{aligned}$$

We assume that the minimum distance of $\mathcal{P}$ is equal to 2 and therefore $A_1=0$. Thus we can formulate the following linear program:

$$\text{maximize: } 1+A_2+A_3$$

subject to the constrains:

$$\begin{aligned} 15A_0+\frac{15}{4}A_2-\frac{15}{8}A_3 &\geq 0, \\ 84A_0-6A_2-\frac{21}{4}A_3 &\geq 0, \\ 35A_0+\frac{5}{4}A_2-\frac{35}{8}A_3 &\geq 0, \end{aligned}$$

The optimal solution of this problem is $A_2=28, A_3=16$ and therefore $|\mathcal{P}|\leq 45$.

Similarly, for packings with minimum distance 2 in $GS_2(8,4)$ we obtain $A_2=700, A_3=3600, A_4=2176$ and therefore $|\mathcal{P}|\leq 6477$.

In the following tables we present several upper bounds on the size of packings in $G_2(n,m)$ and $GS_2(n,m)$ for several small values of n and m.

$G_2(n,m)$:

$n,m/d$	1	2	3	4	5
6,3:	1395	93	9	.	.
8,4:	200787	6477	2159/7	17	.
10,5:	109221651	1733677	40953	5621/5	33

$GS_2(n,m)$:

$n,m/d$	1	2	3	4	5
6,3:	135	45	9	.	.
8,4:	2295	765	255/7	17	.
10,5:	75735	25245	8416/7	1815	33

We are not aware of constructions of good packings in either $G_q(n,m)$ or $GS_q(n,m)$. With the help of a computer search we have constructed packings with minimum distance 2 in $GS_2(6,3)$ and $GS_2(8,4)$. The first packing has size 31 and the second, which we denote $\mathcal{P}^0_{8,4}$, has size 387. We see from the table that the constructions are about 2 times smaller than the corresponding upper bounds. This means that we lose less than one information bit compared to the best possible scenario.

We will use the packing $\mathcal{P}^0_{8,4}$ to construct Grassmannian packings over $\mathbb{C}$. We will also use packings $\mathcal{P}^1_{8,4}, \mathcal{P}^2_{8,4}, \ldots, \mathcal{P}^6_{8,4}$ of sizes $270, 266, 257, 231, 220$, and 187 respectively that were found by computer search. All of these packings are from $GS_2(8,4)$, all have minimum distance 2 and any two packings are disjoint, i.e.

$$\mathcal{P}^i_{8,4}\cap\mathcal{P}^j_{8,4}=0.$$

III. The Extraspecial Group

Let σ_x, σ_y, and σ_z be the Pauli matrices, given by

$$\sigma_x=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_y=\begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix},$$

and consider linear operators E with the following form

$$E=e_1\otimes\ldots\otimes e_m,\ e_j\in\{I_2,\sigma_x,\sigma_y,\sigma_z\}.$$

We form the extra-special group $\mathcal{E}_m$ of order 4^{m+1}, which is realized as a group of the linear operators $\alpha E, \alpha=\pm 1,\pm i$. (For a detailed description of the extra-special group and its use for construction of quantum codes see [7], [6], [1].)

The group $\overline{\mathcal{E}}_m$ is isomorphic to the binary vector space $\mathbb{F}_2^{2m}$. We associate with binary vectors $(\mathbf{a},\mathbf{b})\in\mathbb{F}_2^{2m}$ operators $E_{(\mathbf{a},\mathbf{b})}$ defined by

$$E_{(\mathbf{a},\mathbf{b})}=e_1\otimes\ldots\otimes e_m, \tag{4}$$

$$\text{where } e_j=\begin{cases} I_2, & a_i=0,b_i=0, \\ \sigma_x, & a_i=1,b_i=0, \\ \sigma_z, & a_i=0,b_i=1, \\ \sigma_y, & a_i=1,b_i=1. \end{cases}$$

It is easy to check that

$$E_{(\mathbf{a},\mathbf{b})}E_{(\mathbf{a}',\mathbf{b}')}=(-1)^{\mathbf{b}\cdot\mathbf{a}'}i^{\mathbf{a}\cdot\mathbf{b}'+\mathbf{a}'\cdot\mathbf{b}}E_{(\mathbf{a}\oplus\mathbf{a}',\mathbf{b}\oplus\mathbf{b}')}. \tag{5}$$

It is also easy to check that

$$E_{(\mathbf{a},\mathbf{b})}E_{(\mathbf{a}',\mathbf{b}')} = (-1)^{(\mathbf{a},\mathbf{b})*(\mathbf{a}',\mathbf{b}')}E_{(\mathbf{a}',\mathbf{b}')}E_{(\mathbf{a},\mathbf{b})}. \quad (6)$$

In other words $E_{(\mathbf{a},\mathbf{b})}$ and $E_{(\mathbf{a}',\mathbf{b}')}$ commute iff $(\mathbf{a},\mathbf{b})$ and $(\mathbf{a}',\mathbf{b}')$ are orthogonal with respect to the symplectic inner product (1).

Let C be an $[2m,k]$ self-orthogonal code. Obviously C is isomorphic to a commutative subgroup S of $\mathcal{E}_m$.

Since C is self-orthogonal S can be constructed as as follows. Let vectors $\mathbf{c}_1,\ldots,\mathbf{c}_k$ form a basis of C. Then $S =< E_{\mathbf{c}_1},\ldots,E_{\mathbf{c}_k} >$. The subgroup S consists of operators of the form $\beta_{\mathbf{c}}E_{\mathbf{c}}, \mathbf{c}\in C, \beta_{\mathbf{c}} = \pm 1$. If $\mathbf{c} = \mathbf{c}_{i_1}+\mathbf{c}_{i_2}+\ldots+\mathbf{c}_{i_t}, \mathbf{c}\in C$ then $\beta_{\mathbf{c}}$ should be chosen so that $\beta_{\mathbf{c}}E_{\mathbf{c}} = E_{\mathbf{c}_{i_1}}\cdot\ldots\cdot E_{\mathbf{c}_{i_2}}$. We will always assume that the lexicographically first set of k independent vectors of C is chosen as the basis. After this assumption the group S corresponding to C becomes unique. In the next section we will always assume that the operators $E_{\mathbf{v}}$ are taken with appropriately chosen constants $\beta_{\mathbf{c}}$.

IV. Construction

Recall that a boolean function $g(x_1,\ldots,x_{2t})$ of $2t$ variables is called bent if

$$\hat{G}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^{2t}}(-1)^{\mathbf{u}\cdot\mathbf{x}+g(\mathbf{x})} = \pm 2^t, \quad \mathbf{u}\in\mathbb{F}_2^{2t}. \quad (7)$$

Let $\mathbf{F}\in\mathbb{C}^{2^{2m}}$. We enumerate entries of $\mathbf{F}$ by vectors $\mathbf{b}\in\mathbb{F}_2^{2m}$ ordered lexicographically. Suppose that the entries $F_{\mathbf{b}}$ satisfy the following properties:

- The nonzero entries of $\mathbf{F}$ have the values

$$F_{\mathbf{b}} = \begin{cases} 2^{-1}+\widehat{a}_{\mathbf{b}}2^{-t-1}, & \mathbf{b}=\mathbf{0},\\ \widehat{a}_{\mathbf{b}}2^{-t-1}, & \mathbf{b}\neq\mathbf{0}, \end{cases} \quad (8)$$

  where $\widehat{a}_{\mathbf{b}} = \pm 1$.

- The vectors $\mathbf{b}$ such that $F_{\mathbf{b}}\neq\mathbf{0}$ form a linear $[2m,2t]$ self-orthogonal code C.
- Let ψ be a linear isomorphism from $\mathbb{F}_2^{2t}$ into C. Set $\widehat{\mathbf{a}} = [\widehat{a}_{\psi(\mathbf{u})}]$, where the vectors $\mathbf{u}$ are ordered lexicographically in $\mathbb{F}_2^{2t}$. Then $\widehat{\mathbf{a}}$ (or equivalently the vector $\mathbf{a}$ obtained from $\widehat{\mathbf{a}}$ by reverse exponentiation) is a bent function f.

In [3] the following theorem was proven.

Theorem 2: The operator

$$P_{C,f} = \sum_{\mathbf{b}\in\mathbb{F}_2^{2m}} F_{\mathbf{b}}E_{\mathbf{b}} \quad (9)$$

is an orthogonal projector and $\mathrm{Tr}\,(P) = 2^{m-1}\pm 2^{m-t-1}$.

Example 1: Let $m=4, t=2$ and

$$\begin{aligned}&\mathbf{F}\\ =\ &(\frac{3}{8},-\frac{1}{8},-\frac{1}{8},\frac{1}{8},-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{1}{8},-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{1}{8},\frac{1}{8},\frac{1}{8},\\ &\frac{1}{8},-\frac{1}{8},0,\ldots,0).\end{aligned}$$

It is easy to see that the nonzero entries of $\mathbf{F}$ form a linear $[8,4]$ self-orthogonal code and their signs form a bent function of the length 16 (the sign corresponding to the zeroth entry is -1 according to (9)). Hence, using this vector in (9) we obtain a projection operator with trace 6.

Similarly, let $\mathbf{F}$ be such that $\mathbf{F_0} = 2^{-1}$, with the absolute value of the other nonzero entries equal to 2^{-t-1}, and with their indices $\mathbf{b}$ forming a *coset* $\mathbf{v}+C$ of a linear $[2m,2t]$ self-orthogonal code C, and their signs forming a bent function (where the entry in position zero is excluded). In [3] it is shown that one can construct the projection operator $P_{C,\mathbf{v},f}$ as

$$P_{C,\mathbf{v},f} = F_{\mathbf{0}}I_{2^m} + \sum_{\mathbf{b}\in C} c_{\mathbf{b}}E_{\mathbf{b}\oplus\mathbf{v}}, \quad (10)$$

and that $\mathrm{Tr}\,(P_{C,\mathbf{v},f}) = 2^{m-1}$. In (10) the coefficients $c_{\mathbf{b}}$ are determined by the nonzero entries of $\mathbf{F}$, but not always equal to them (for details see Theorem 6 of [3]).

For example we may take the vector ($m=4, t=2$)

$$\begin{aligned}&\mathbf{F}\\ =\ &(\frac{1}{2},0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ &-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{1}{8},-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{1}{8},-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{1}{8},\frac{1}{8},\\ &\frac{1}{8},\frac{1}{8},-\frac{1}{8},0,\ldots,0)\end{aligned}$$

to construct a projection operator with trace 8.

In [3] we suggested using all $[2m,2t], t=1,\ldots,m/2$, self-orthogonal codes and all bent functions of degree 2. As a result we obtained Grassmannian packings with $T=2^m$ and minimum distance 2^{m-2} that correspond to the parameters of $RM(2,m)$ codes. We also established an algebraic relation between these packings and codes $RM(2,2m)$.

Choosing $m=2$ in the construction from [3] we obtain a Grassmannian packing with $T=16$ and $d=4$. In this work we would like to construct packings with $T=16$ and $d=6$. To achieve this minimum distance we have to restrict the set of bent functions. A natural choice is the bent functions that belong to the Nordstrom-Robinson code. The weight of these function is either 6 or 10. Hence using any $[8,4]$ linear self-orthogonal code C and a bent function from the Nordstrom-Robinson code, using Theorem 2, we obtain a projector with trace 6 or 10. If instead of C we take any of its cosets we obtain a projector with trace 8.

To guarantee that the minimum distance is 6 we first consider projections constructed from one and the same $[8,4]$ linear self-orthogonal code C.

Theorem 3: Let f and f' be bent functions from the Nordstrom-Robinson code. Then

$$\mathrm{Tr}\,(P_{C,f}P_{C,f'}) \leq 3$$

and

$$\mathrm{Tr}\,(P_{C,\mathbf{v},f}P_{C,\mathbf{v},f'}) \leq 3$$

and therefore $d(P_{C,f},P_{C,f'})\geq 6,\ d(P_{C,\mathbf{v},f},P_{C,\mathbf{v},f'})\geq 6$.

Unfortunately, in order to maintain a minimum distance of 6 we can not take all $[8,4]$ linear self-orthogonal codes. For

instance let C be generated by vectors

$$\begin{array}{cccccccc}(0 & 0 & 0 & 0 & 0 & 0 & 0 & 1)\\ (0 & 0 & 0 & 0 & 0 & 0 & 1 & 0)\\ (0 & 0 & 0 & 0 & 0 & 1 & 0 & 0)\\ (0 & 0 & 0 & 0 & 1 & 0 & 0 & 0)\end{array}$$

and C' be generated by vectors

$$\begin{array}{cccccccc}(0 & 0 & 0 & 0 & 0 & 0 & 0 & 1)\\ (0 & 0 & 0 & 0 & 0 & 0 & 1 & 0)\\ (0 & 0 & 0 & 0 & 0 & 1 & 0 & 0)\\ (1 & 0 & 0 & 0 & 0 & 0 & 0 & 0)\end{array}$$

Straightforward computations show that for some bent function f we have

$$\mathrm{Tr}\,(P_{C,f}P_{C',f}) = 4$$

and therefore $d(P_{C,f}, P_{C',f}) = 2$. To keep the minimum distance equal to 6 we have to use linear codes that are well separated from each other as formulated in the following theorem.

Theorem 4: Let C and C' be from a packing $\mathcal{P} \in GS_2(8,4)$ with minimum distance 2. Let $\mathbf{v}$ and $\mathbf{v}'$ be nonzero, not necessary different, vectors from $\mathbb{F}_2^{2m}$. Then for any f we have

$$\mathrm{Tr}\,(P_{C,f}P_{C',f}) \leq 3,$$

and

$$\mathrm{Tr}\,(P_{C,\mathbf{v},f}P_{C',\mathbf{v}',f}) \leq 3.$$

and therefore $d(P_{C,f}, P_{C',f}) \geq 6$, $d(P_{C,\mathbf{v},f}, P_{C',\mathbf{v}',f}) \geq 6$.

Finally we need one more observation. The total number of bent function of the length 16 and weight 6 is 28×16. They can be partitioned into 28 cosets of $RM(1,4)$. Choosing 7 'good' cosets and combining them with $RM(1,4)$ we obtain the Nordstrom-Robinson code. Our observation is that we can divide these 28 cosets to obtain 8 nonlinear codes with parameters of the Nordstrom-Robinson code with each pair of nonlinear codes having one coset in common. For instance, the 28 cosets can be distributed into following 8 non-linear codes:

$$\begin{array}{cccccccc}\{ & 854 & 1589 & 5234 & 5912 & 4427 & 4654 & 1388 & \}\\ \{ & 874 & 5924 & 5234 & 4382 & 1628 & 1337 & 4679 & \}\\ \{ & 874 & 1334 & 4724 & 5912 & 5198 & 4397 & 1619 & \}\\ \{ & 857 & 5159 & 4724 & 4382 & 5954 & 1594 & 1388 & \}\\ \{ & 854 & 5924 & 1379 & 4637 & 5198 & 1594 & 4472 & \}\\ \{ & 869 & 1334 & 5954 & 5147 & 1628 & 4654 & 4472 & \}\\ \{ & 857 & 1589 & 1379 & 5147 & 4679 & 4397 & 6014 & \}\\ \{ & 869 & 5159 & 1619 & 4637 & 4427 & 1337 & 6014 & \}\end{array}$$

(We present only one representative for each coset in the decimal notation- for example, 854 represents the bent function

$$(0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0)$$

which is the binary representation of 854 in 16 bits.). This further means that we can partition these 28 cosets into 7 sets of 'good' cosets (denoted by $\mathcal{NR}_i$, i=0,1,..6) containing 7, 6, 5, 4, 3, 2, 1 cosets respectively.

Now we are in the position to define the Grassmannian packing $\mathcal{GNR}$. We give the definition for the case of $\mathrm{Tr}\,(P) = 6$. The case $\mathrm{Tr}\,(P) = 8$ and $\mathrm{Tr}\,(P) = 10$ are similar.

Definition 7: $\mathcal{GNR}$:

- take any $[8,4]$ linear self-orthogonal code from $\mathcal{P}^i_{8,4}, i = 0,1,2,3,4,5,6$;
- take any bent function of $f \in \mathcal{NR}_i$, $\mathrm{wt}\,(f) = 6$;
- use (9) or (10) to construct a projector operator.

It is not difficult to see that the parameters of $\mathcal{GNR}$ are $T = 16, d = 6$, and $M = 6, 8$, or 10. If $M = 6$ or 10 we have $L = 128112$ and if $M = 8$ we have $L = 1921680$.

REFERENCES

[1] A. Ashikhmin and E. Knill, " Nonbinary quantum stabilizer codes," *IEEE Trans. Information Theory,* **47**, (2001), pp. 3065–3072.

[2] A. Ashikhmin and A. R. Calderbank, "Space-Time Reed-Muller Codes for Noncoherent MIMO Transmission," *International Symposium on Information Theory,* Adelaide, Australia, 2005, pp. 1952–1956.

[3] A. Ashikhmin, A. R. Calderbank, V. Kewlin, " Multidimensional Second Order Reed-Muller Codes as Grassmannian Packings," *International Symposium on Information Theory*, Seattle, Washington, USA. 2005, pp. 1001–1005.

[4] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*. The Bejamin/Publishing Company, Inc., London, 1984.

[5] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*. Springer-Verlag Berlin Heidelberg, 1989.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.,* **78**, (1997), pp. 405–409.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via codes over $GF(4)$," *IEEE Trans. on Inform.Theory,* **44**, (1998), pp. 1369–1387.

[8] F.J. MacWilliams and N.J.A Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.

[9] J. A. Tropp, "Greed is Good: Algorithmic Results for Sparse Approximation,"*IEEE Trans. on Inform.Theory,* **50**, (2004), pp. 2231–2242.