Linear Transformations on Codes

David G. Glynn *
3 St. Winifreds Place,
Bryndwr, Christchurch 8005
New Zealand
Email: dglynn@mac.com

T. Aaron Gulliver, Senior Member, IEEE
Department of Electrical and Computer Engineering, University of Victoria,
P.O. Box 3055, STN CSC, Victoria, B.C., Canada V8W 3P6
Email:agullive@engr.uvic.ca

Manish K. Gupta, Member, IEEE
Department of Mathematics, University of Canterbury,
Private Bag 4800, Christchurch, New Zealand
Email:m.k.gupta@ieee.org

February 5, 2002

*This work was supported by the Marsden fund of the Royal Society of New Zealand.

Abstract

This paper studies and classifies linear transformations that connect Hamming distances of codes. These include irreducible linear transformations and their concatenations. Their effect on the Hamming weights of codewords is also studied. Both linear and non-linear codes over fields are considered.

We construct a family of pure binary quantum codes using these transformations. It is shown that optimal codes can be constructed using these transformations.

Keywords: Krawtchouk polynomials, linear transformations, non-linear codes, optimal codes, quantum codes

1 Introduction

Let $\mathbb{F}$ be a finite set called the *alphabet* (e.g., $\mathbb{F} = \{0, 1\}$ for binary codes). A *code* $\mathcal{C}$, of length n, over $\mathbb{F}$ is any non-empty subset of $\mathbb{F}^n$. If $\mathbb{F}$ has the structure of an additive group then $\mathcal{C}$ is *additive* if it is an additive subgroup of $\mathbb{F}^n$. If $\mathbb{F}$ has a ring structure then $\mathcal{C}$ is *linear* over $\mathbb{F}$ if it is additive and also closed under multiplication by elements of $\mathbb{F}$. An element of $\mathcal{C}$ is called a *codeword of* $\mathcal{C}$ and a *generator matrix* of $\mathcal{C}$ is a matrix whose rows generate $\mathcal{C}$.

In order to define dual codes we equip $\mathbb{F}$ with an *inner product* $(,)$ that satisfies the following conditions:

$$\begin{aligned} (x+y,z) &= (x,z)+(y,z), \\ (x,y+z) &= (x,y)+(x,z), \\ \text{if } (x,y) &= 0 \text{ for all } x \text{ then } y=0, \\ \text{if } (x,y) &= 0 \text{ for all } y \text{ then } x=0. \end{aligned}$$

Further we define a *conjugacy* operation or "involutory anti-automorphism" (which may be the identity), denoted by a bar, that satisfies

$$\overline{\overline{x}} = x, \overline{x+y} = \overline{x}+\overline{y}, \overline{xy} = \overline{x}\,\overline{y}.$$

The inner product then satisfies

$$(x,y) = \overline{(y,x)}, (ax,y) = (x,\overline{a}y).$$

Finally, the inner product of vectors $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$ in $\mathbb{F}^n$ is defined by

$$(x,y) = \sum_{i=1}^{n} (x_i, y_i).$$

The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as $\{x \in \mathbb{F}^n \mid (x,y) = 0 \text{ for all } y \in \mathcal{C}\}$ where (x,y) is the inner product of x and y. $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and $\mathcal{C}$ is *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. The *Hamming weight* $w_H(x)$ of a vector x in $\mathbb{F}^n$ is the number of non-zero components.

In this paper we study and classify linear transformations on a code that connect a weight of $\mathcal{C}$ to a weight in the transformed code. Such transformations also connect the distances between codewords in non-linear codes over fields in the same way. Section 2 contains some preliminaries and notation. The irreducible transformations are given in Section 3. Section 4 defines the concatenated transformations. Section 5 investigates applications of these transformations. The last section finishes with some conclusions.

2 Preliminaries and Notations

We list the families of codes which we will consider here. The standard notation is from [4]. Note that the list starts from (2) because there is no field of order 1.

(2) Binary linear codes: $\mathbb{F} = \mathbb{F}_2 = \{0,1\}$, with standard inner product $(x,y) = xy$, $\mathcal{C} =$ a subspace of $\mathbb{F}_2^n$.

(3) Ternary linear codes: $\mathbb{F} = \mathbb{F}_3 = \{0,1,2\}$, $(x,y) = xy$, $\mathcal{C} =$ a subspace of $\mathbb{F}_3^n$. Note that for families (2) and (3) an additive code is automatically linear.

(4^H) Quaternary linear codes: $\mathbb{F} = \mathbb{F}_4 = \{0,1,\omega,\omega^2\}$, where $\omega^2 + \omega + 1 = 0, \omega^3 = 1$, $\bar{x} = x^2$ for $x \in \mathbb{F}_4$, with the Hermitian inner product $(x,y) = x\bar{y}$, $\mathcal{C} =$ a subspace of $\mathbb{F}_4^n$. Note that for $x, y \in \mathbb{F}_4$,

$$(x+y)^2 = x^2 + y^2, x^4 = x.$$

(4^{H+}) Quaternary additive codes: $\mathbb{F} = \mathbb{F}_4$, with $(x,y) = trace(x\bar{y}) = xy^2 + yx^2$, $\mathcal{C} =$ an additive subgroup of $\mathbb{F}_4^n$.

(q^H) Linear codes over $\mathbb{F}_q$: $\mathbb{F} = \mathbb{F}_q =$ finite field with q elements where q is an even power of an arbitrary prime p, with $\bar{x} = x^{\sqrt{q}}$ for $x \in \mathbb{F}_q$, with the inner product $(x,y) = x\bar{y}$, $\mathcal{C} =$ a subspace of $\mathbb{F}_q^n$. Note that for $x, y \in \mathbb{F}_q$,

$$(x+y)^{\sqrt{q}} = x^{\sqrt{q}} + y^{\sqrt{q}}, x^q = x.$$

(q^E) Linear codes over $\mathbb{F}_q$, for q any prime power, with standard inner product $(x,y) = xy$.

($F2$) Additive codes over $\mathbb{F}_4$, with $(x,y) = x\bar{y}$.

Let $\mathcal{C}$ be a code over $\mathbb{F}_q$. For all $x \in \mathcal{C}$ let T be a linear transformation defined as $T(x) = xA$, where A is an appropriate matrix and x is a row vector. Let $T(\mathcal{C}) = \mathcal{C}'$ be the transformed code. We would like to classify all such transformations T that connect one distance of $\mathcal{C}$ to another distance of $\mathcal{C}'$. This give us a code with new parameters. If the code $\mathcal{C}$ is linear and $\mathcal{C} = \mathcal{C}'$, such a transformation is an Hamming isometry (follows from a classical result of MacWilliams [3]). Recently the result of MacWilliams has been extended to codes over rings by Wood [7]. For a combinatorial approach to Wood's result see [2].

We are interested in the case when $\mathcal{C} \neq \mathcal{C}'$. We also investigate inner products for which T preserves orthogonality. This is useful, for example, in constructing new quantum codes.

3 The Irreducible Transformation

Let $\mathbb{F} = \mathbb{F}_q = \{0, 1, \alpha_3, \ldots, \alpha_q\}$ be the finite field having q elements. Given $n \in \mathbb{N}$, let $0 \leq j \leq n$. For $n > 2$, define the matrix A_j^n inductively as

$$A_j^n = \left(\begin{array}{c|c|c|c|c} 11\cdots1 & 11\cdots1 & \cdots & 11\cdots1 & 00\cdots0 \\ \hline A_{j-1}^{n-1} & \alpha_3 A_{j-1}^{n-1} & \cdots & \alpha_q A_{j-1}^{n-1} & A_j^{n-1} \end{array} \right),$$

with the convention that A_j^{n-1} is absent for $j = n$, the blocks $\alpha_3 A_{j-1}^{n-1} \mid \cdots \mid \alpha_q A_{j-1}^{n-1}$ are absent for $j = 1$, and A_0^n is a zero column of length n. In particular, $A_1^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $A_2^2 = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha_3 & \alpha_4 & \alpha_5 & \cdots & \alpha_q \end{pmatrix}$. Clearly, the size of A_j^n is $n \times \binom{n}{j}(q-1)^{j-1}$, so applied to any code of length n gives a code of length $\binom{n}{j}(q-1)^{j-1}$. We call A_j^n a *j-weight irreducible* transformation.

Remark 1 *Note that each column of A_j^n has a fixed Hamming weight j and is taken from the generator matrix of a q-ary simplex code of dimension n. Also, A_1^n is the identity matrix of order n.*

The next theorem tells us about the effect the j-weight irreducible transformation on the Hamming weights of a code $\mathcal{C}$ of length n. The q-ary Krawtchouk polynomials are defined in [4]. For $j = 0, 1, 2, \ldots$, the Krawtchouk polynomials $K_j(x)$ are defined by

$$K_j(x; n, q) := K_j(x) := \sum_{k=0}^{j} (-1)^k \binom{x}{k} \binom{n-x}{j-k} (q-1)^{j-k},$$

where

$$\binom{x}{k} := \frac{x(x-1)\cdots(x-k+1)}{k!}, \ (x \in \mathbb{R}).$$

Theorem 1 *Let $\mathbf{c} \in \mathcal{C}$ be a codeword of weight i. Then the weight of a transformed codeword in $\mathcal{C}'$ is $\frac{1}{q}\{K_j(0) - K_j(i)\}$.*

Proof. Let w_k be the number of homogeneous vectors of length k (non-zero vectors determined up to multiplication by a scalar), with all non-zero components and a non-zero component sum, and let v_k the number of these vectors of non-zero components with a component sum of zero. Then $v_k + w_k = (q-1)^{k-1}$, while $v_k = w_{k-1}$, since the last component

of a vector with zero component sum is determined by the first $k-1$ components. Thus, $w_1 = 1$ and $v_1 = 0$, and since $w_k = (q-1)^{k-1} - w_{k-1}$ we obtain

$$w_k = (q-1)^{k-1} - (q-1)^{k-2} + \ldots + (-1)^{k-1}.$$

Since $w_k((q-1)+1) = (q-1)^k - (-1)^k$ it must be that

$$w_k = ((q-1)^k - (-1)^k)/q.$$

The proof of the distance formula is completed as follows. If we fix a vector of weight i of length n over $GF(q)$, then the weight of the transformed vector under A_j^n is the number of homogeneous vectors of weight j that have a non-zero inner product with the vector of weight i. Now, we can assume, by reasons of symmetry, that the vector of weight i is the vector with i 1's in the first i components and 0's in the remaining $n-i$ components. Let $F_j(i)$ be the weight of the transformed codeword $c' := cA_j^n$. Then we obtain the following formula by counting over vectors with k non-zero components in the first i, and with $j-k$ non-zero components in the remaining $n-i$:

$$F_j(i) = \sum_{k=0}^{\min(i,j)} \binom{i}{k}\binom{n-i}{j-k}(q-1)^{j-k} w_k,$$

where w_k is as above. Thus

$$\begin{aligned}
F_j(i) &= \textstyle\sum_{k=0}^{\min(i,j)} \binom{i}{k}\binom{n-i}{j-k}(q-1)^{j-k}((q-1)^k - (-1)^k)/q \\
&= q^{-1}\textstyle\sum_{k=0}^{\min(i,j)} \binom{i}{k}\binom{n-i}{j-k}(q-1)^{j-k}(q-1)^k - q^{-1}K_j(i) \\
&= q^{-1}\textstyle\sum_{k=0}^{\min(i,j)} \binom{i}{k}\binom{n-i}{j-k}(q-1)^{j} - q^{-1}K_j(i) \\
&= q^{-1}(q-1)^j\textstyle\sum_{k=0}^{\min(i,j)} \binom{i}{k}\binom{n-i}{j-k} - q^{-1}K_j(i) \\
&= q^{-1}(q-1)^j\binom{n}{j} - q^{-1}K_j(i),
\end{aligned}$$

since $\sum_k \binom{i}{k}\binom{n-i}{j-k} = \binom{n}{j}$. Then the formula follows since $K_j(0) = (q-1)^j\binom{n}{j}$. □

Remark 2 *If $q = 2$ then the weight w of any codeword of $\mathcal{C}$ will go to weight $w(n-w)$ of some codeword of $\mathcal{C}'$ by the irreducible transformation A_2^n.*

Note that a linear code is always mapped to a linear code, but a non-linear code may be mapped to a linear or a non-linear code depending upon whether the kernel (the set of vectors mapped to zero), of A_j^n is trivial or non-trivial. The kernel of A_j^n is non-trivial if and only if there exists i, $1 \le i \le n$ such that $K_j(0) = K_j(i)$. We have the following straightforward but useful result.

Proposition 1 *Let $\mathcal{C}$ be a q-ary code and let A_j^n be the irreducible transformation on $\mathcal{C}$ yielding $\mathcal{C}'$. Then $\mathcal{C}'$ will be additive if for all $\alpha, \beta \in \mathcal{C}$ we have $\alpha + \beta + Ker(A_j^n) \bigcap \mathcal{C} \neq \{0\}$. In particular, it means that $\mathcal{C}'$ is an additive code if there exists $\gamma \in \mathcal{C}$ such that $\alpha + \beta - \gamma \in Ker(A_j^n)$. Further an additive code $\mathcal{C}'$ will be linear if for all $\alpha \in \mathcal{C}$ and $\lambda \in \mathbb{F}$ we have $\lambda\alpha + Ker(A_j^n) \bigcap \mathcal{C} \neq \{0\}$.*

For a q-ary linear code $\mathcal{C} : [n, k]_q$ with generator matrix $G_{k\times n}$, the generator matrix of the new code $\mathcal{C}' \left[\binom{n}{j}(q-1)^{j-1}, k\right]_q$ is GA_j^n. Note that the length of the new code $\mathcal{C}'$ under A_j^n is $K_j(0)/(q-1)$.

Remark 3 *If the number of words of weight j in $C^\perp$ is n_j it is possible (by deleting zero columns) to reduce the length by $n_j/(q-1)$. For a linear code $\mathcal{C}$, every word of $\mathcal{C}'$ will be repeated* $\dim(Ker(A_j^n) \cap \mathcal{C})$ *times. By omitting repetitions the dimension of $\mathcal{C}'$ can be assumed to be k minus this value. For example, if $q = 2$ and the linear code contains the all-one vector, then for all even j the dimension of $\mathcal{C}'$ is reduced by* 1.

After some investigation, it appears that many very good codes can be constructed by this method. By "good" we usually mean "close to the Griesmer bound".

As an example from geometry, consider the ovoid in $PG(3, 3)$ having 10 points, no three collinear (an elliptic quadric). The corresponding code, with generator matrix coming from the 10 column vectors, has parameters [10,4,6]. A hyperplane (here a plane) intersects the set in 1 or 4 points, and so corresponds to words of weight $10-1 = 9$ and $10-4 = 6$. Using the irreducible transformation A_j^n with $j = 3$ we obtain a constant weight [480,4,324] code that is 12 times the simplex code [40,4,27] over GF(3).

Geometrically, the transformation for $j = 2$ is the same as taking every pair of points of a given set, and finding all the points on the chords (but not the first pair). Thus we have $q-1$ points for each pair. If chords overlap then we count points with the given multiplicity.

For $j = 3$, look at every three points in the set, and find all the $(q-1)^2$ points in the plane determined by the points, but not on the lines of the triangle determined by them.

Now we consider the types of orthogonality that are preserved by the transformations. For example, for $q = 3$ the next result shows that $\mathcal{C}'$ is self-orthogonal with respect to the standard inner-product if $\mathcal{C}$ is self-orthogonal with respect to this inner-product.

Theorem 2 *For ternary linear codes i.e, for the family* (3)*, each irreducible transformation A_j^n $(1 \leq j \leq n)$ preserves self-orthogonality.*

Proof. The case $j = 1$ is trivial. It is sufficient to prove that for each $2 \leq j \leq n$, we have $A_j^n \left(A_j^n\right)^t \equiv \binom{n-1}{j-1} 2^{j-1} I_n \pmod 3$. The proof is by induction on n. Clearly it is true

for $n = 1$ and $n = 2$. Assume that it holds for each $2 \leq j \leq n-1$. Let $\mathbf{1}$ denote the all-ones vector of length $\binom{n-1}{j-1}2^{j-2}$. Then we have

$$\begin{aligned} A_j^n \left(A_j^n\right)^t &= \left(\begin{array}{c|c} 2(\mathbf{1}\mathbf{1}^t) & \mathbf{1}(A_{j-1}^{n-1})^t + 2\mathbf{1}(A_{j-1}^{n-1})^t) \\ \hline A_{j-1}^{n-1}\mathbf{1}^t + 2A_{j-1}^{n-1}\mathbf{1}^t & 2A_{j-1}^{n-1}\left(A_{j-1}^{n-1}\right)^t + A_j^{n-1}(A_j^{n-1})^t \end{array}\right) \\ &\equiv \binom{n-1}{j-1}2^{j-1}I_n \pmod 3 \text{ by induction hypothesis.} \end{aligned}$$

□

Remark 4 *Any ternary code which is monomially equivalent to a ternary self-orthogonal code is also self-orthogonal.*

The next result shows that the stabilizer matrix for an additive quantum code is taken to another one.

Theorem 3 *For quaternary linear codes i.e, for the family (4^H) and for quaternary additive codes i.e, for the family (4^{H+}), each irreducible transformation A_j^n $(1 \leq j \leq n)$ preserves self-orthogonality.*

Proof. The result is obvious for $j = 1$. It is sufficient to prove that for each $2 \leq j \leq n$, we have $A_j^n \left(A_j^n\right)^\star = \binom{n-1}{j-1}3^{j-1}I_n$, where $\star$ denotes transpose and conjugate. Since $GF(4)$ has characteristic 2, $\binom{n-1}{j-1}3^{j-1} = 0$ or 1. Hence the trace-orthogonality will also be preserved. Now the proof is by induction on n. Clearly it is true for $n = 1$ and $n = 2$. Assume that it holds for each $2 \leq j \leq n-1$. Let $\mathbf{1}$ denote the all-one vector of length $\binom{n-1}{j-1}3^{j-2}$. Then we have

$$\begin{aligned} A_j^n \left(A_j^n\right)^\star &= \left(\begin{array}{c|c} 3(\mathbf{1}\mathbf{1}^\star) & (1+\omega+\bar{\omega})\mathbf{1}(A_{j-1}^{n-1})^\star \\ \hline (1+\omega+\bar{\omega})A_{j-1}^{n-1}\mathbf{1}^\star & 3A_{j-1}^{n-1}\left(A_{j-1}^{n-1}\right)^\star + A_j^{n-1}(A_j^{n-1})^\star \end{array}\right) \\ &= \binom{n-1}{j-1}3^{j-1}I_n, \text{ by induction.} \end{aligned}$$

□

Remark 5 *Any additive quaternary code equivalent to a trace-orthogonal additive quaternary code is also trace-orthogonal.*

Thus given a binary additive quantum code with parameters $[[n, k]]$, the transformed quantum code will have parameters $\left[\left[\binom{n}{j}3^{j-1}, \binom{n}{j}3^{j-1} - n + k\right]\right]$ [1].

The following lemma shows a connection between the transformations A_j^n and the distance of a quantum code.

Lemma 1 *Let $\mathcal{C}$ be an $[[n,k,d]]$ pure binary quantum code. Then the dual distance of the corresponding additive code $\left(n, 2^{n-k}\right)$ is given by $d = \min\{j \mid 1 \leq j \leq n\}$ such that there exists a column with components 0 or 1 in the transformed stabilizer matrix of $\mathcal{C}$ via the irreducible transformation A_j^n.*

Proof. The distance of a pure quantum code is given by the minimum non-zero weight of a word in the dual code to the code generated by the stabilizer matrix. This word corresponds to a linear combination of the columns of the stabilizer matrix that is a vector with components 0 or 1. This is because the elements of trace 0 in $GF(4)$ are 0 and 1. □

Theorem 4 *The minimum distance d' of the transformed quantum code $\left[\left[\binom{n}{j}3^{j-1}, \binom{n}{j}3^{j-1} - n + k\right]\right]$ is at most 3. Moreover $d' = 1$ if $j = d$.*

Proof. Consider any j columns in the stabilizer matrix of the pure binary quantum code $[[n,k,d]]$. Multiplying these columns by the following 3 columns of weight j with $n-j$ zero rows omitted (these are the three columns of A_j^n of weight j)

$$\begin{matrix} 1 & 1 & 1 \\ 1 & \omega & \bar{\omega} \\ \vdots & \vdots & \vdots \\ 1 & \omega & \bar{\omega} \end{matrix},$$

we get 3 dependent columns in the transformed stabilizer matrix thus yielding a vector of weight 3 in the dual. Hence $d' \leq 3$. If $j = d$, then Lemma 1 implies that the distance of the new quantum code is 1.

□

If after the transformation we obtain a quantum code of distance 1 or 2, we can always change it to a quantum code of increased distance by looking at the dependencies among the columns of the stabilizer matrix of the quantum code. For example, we have the following lemma.

Lemma 2 *It should be possible to transform the distance 2 quantum codes to quantum codes of distance at least 3.*

Proof. Let $[[n,k,2]]$ be the pure binary quantum code with associated additive code $\mathcal{C}:\ (n, 2^{n-k})$. Then there exists a vector $(0,\ldots,0,\bar{\alpha},\ldots,\bar{\beta},\ldots,0) \in \mathcal{C}^{\perp}$ with $\alpha, \beta \neq 0$ and there exist two columns in the stabilizer matrix with coordinates (x,y) such that we have $\alpha x + \beta y \in \{0,1\}$. The transformation $(x,y) \mapsto \alpha x + \beta y + \text{trace}(\beta \text{y})\omega$ will collapse the two columns of the stabilizer to one. Repeating this operation should increase the distance of

the code. Note that there are similar operations that collapse n columns to $n-1$, for any n, as long as the corresponding n columns have a non-trivial linear combination that is a vector of $0's$ and $1's$ [5]. □

In the next section we return to a more general discussion, and remove the restriction to quantum codes. The focus is mainly on classical linear and non-linear codes.

4 Concatenated Transformations

This section considers linear transformations which are concatenations of some transformations from the set $\left\{A_j^n \mid 0 < j \leq n\right\}$ of the j-weight irreducible transformations A_j^n. One such transformation is obtained by taking the concatenation of all A_j^n for $1 \leq j \leq n$ yielding the generator matrix of a q-ary simplex code S_n. Let $A(n,q) = \left[A_2^n \mid A_3^n \mid \cdots \mid A_j^n \mid \cdots \mid A_n^n\right]$ be the full concatenation for all $2 \leq j \leq n$. We can also define this linear transformation $A(n,q)$ inductively by

$$A(n,q) = \left(\begin{array}{c|c|c|c|c|c|c|c} 11\cdots1 & \alpha_3\alpha_3\cdots\alpha_3 & \cdots & \alpha_q\alpha_q\cdots\alpha_q & 00\cdots0 & 11\cdots1 & \cdots & \alpha_q\alpha_q\cdots\alpha_q \\ \hline I_{n-1} & I_{n-1} & \cdots & I_{n-1} & A(n-1,q) & A(n-1,q) & \cdots & A(n-1,q) \end{array}\right),$$

with

$$A(2,q) = \begin{pmatrix} 1 & \alpha_3 & \alpha_4 & \cdots & \alpha_q \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix},$$

which has $q-1$ columns. Clearly the size of the matrix $A(n,q)$ will be $n \times \left(\frac{q^n-1}{q-1} - n\right)$. The length of a new code after the concatenated transformation $A(n,q)$ will be $\left(\frac{q^n-1}{q-1} - n\right)$.

The next theorem tells us that the j-weight irreducible transformations A_j^n and their concatenations are all such possible linear transformations that connect distances of $\mathcal{C}$ and $\mathcal{C}'$. Note that we consider permutations of the columns of A_j^n and multiplying the columns by nonzero constants as giving equivalent linear transformations. In addition, $j = 1$ gives the monomial transformation.

Theorem 5 *All linear transformations on the words of length n over $GF(q)$ that take a word of weight w to a word of weight $f(w)$, where f is some function, are equivalent to the irreducible transformations A_j^n and their concatenations.*

Proof. Consider an incidence matrix X of the points versus the hyperplanes of the finite projective space $PG(n-1,q)$. The rows of X correspond to the points, coordinatised by the homogeneous vectors of length n over $GF(q)$, while the columns correspond to the hyperplanes, coordinatised similarly by the (dual) homogeneous vectors of length n over $GF(q)$. There is a one in a certain position of X if the corresponding point and hyperplane

are incident, or equivalently the inner product of the two coordinate vectors is zero. (This is a *flag* of the geometry.) Otherwise, if the point and hyperplane are not incident (an *antiflag*, the position in that position of X is zero. Here the crucial fact is that $det(X) \neq 0$. This follows from the theory of symmetric designs, since the hyperplanes of $PG(n-1,q)$ are the blocks of a well-known symmetric design having parameters $(v,k,\lambda) = ((q^n-1)/(q-1), (q^{n-1}-1)/(q-1), (q^{n-2}-1)/(q-1))$. Then it is known that the formula for the determinant of the incidence matrix for a symmetric (v,k,λ) is $\pm k(k-\lambda)^{(v-1)/2} \neq 0$ [4].

Next, reorder the rows and columns of X so that they fall into groups that correspond to the various weights of the corresponding coordinate vectors. Thus the first n rows of X will correspond to the n unit vectors, the next $\binom{n}{2}(q-1)$ rows will correspond to the points with coordinates of weight 2, etc, so that the columns are in groups of similar weights. There are n groupings for the rows, and n for the columns.

For any $1 \leq i \leq n$ let c_i denote the row vector of length n with 0's everywhere except for those columns corresponding to hyperplanes of weight i. Then let the subspace of $GF(q)^n$ generated by these n vectors c_i be C. For each $1 \leq j \leq n$ there is a certain element of C, defined as r_j, which is the sum of the rows of X within the j'th row-group (corresponding to the points of weight j of $PG(n-1,q)$). The reason is that $r_j \in C$ is equivalent to the fact that the mapping A_j^n is distance-connecting (which was shown previously). Now the rows of X are linearly independent, and since the sums of the rows that create the vectors r_j are disjoint, we see that $r_1, \ldots, r_n$ are n linearly independent vectors, which in fact must form a basis for C, since $\dim(C) \leq n$ but also $\dim(C) \geq n$. Thus $\dim(C) = n$.

Now any linear distance-connecting mapping operating on a vector of length n over $GF(q)$ has a matrix the columns of which correspond to a multiset of m points of $PG(n-1,q)$, and these points correspond to m rows of X with the property that the sum of these rows is in C. Therefore these rows are a linear combination of the vectors c^j. The linear independence of the rows of X gives us the result that the m rows are equal to the union of groups corresponding to constant weight points of $PG(n-1,q)$. This fact is equivalent to the statement of the theorem.

□

5 Applications

We have applied these linear transformations to various codes and in many cases obtained optimal linear codes in the sense of the Griesmer bound. We also found very many near optimal codes (in fact in most cases), particularly long codes that are near the Griesmer bound. For example, a $[5,4,2]_7$ code is transformed to $[360,4,304]_7$ and $[1080,4,912]_7$ codes, whereas the Griesmer bound gives minimum distance 356 and 1065, respectively. Some of

Table 1: Linear Codes over $GF(q)$ and Their Transformations.

$\mathcal{C} : [n, k, d]_q$	A_j^n	$\mathcal{C}' : \left[\binom{n}{j}(q-1)^{j-1}, k, d'\right]_q$
$[4, 3, 2]_2$	A_2^4	$[6, 2, 4]_2$ optimal
$[4, 3, 2]_2$	A_3^4	$[16, 2, 10]_2$ optimal
$[5, 2, 2]_2$	A_2^5	$[10, 4, 4]_2$ optimal
$[7, 6, 2]_2$	A_3^7	$[35, 6, 16]_2$ optimal
$[8, 7, 2]_2$	A_3^8	$[56, 7, 26]_2$ optimal
$[10, 9, 2]_2$	A_2^{10}	$[120, 9, 56]_2$ optimal
$[6, 3, 3]_3$ no words of weight 6	A_2^6	$[30, 3, 20]_3$ optimal and Griesmer
$[7, 6, 2]_3$	A_3^7	$[140, 6, 90]_3$ optimal
$[5, 3, 3]_7$ Griesmer	A_2^5	$[60, 3, 50]_7$ optimal and Griesmer

the results are given in Table 1.

Consider the binary non-linear Kerdock Code $K(m) : \left(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2}\right)$, for even $m \geq 4$ with weight distribution

i	$A(i)$
0	1
$2^{m-1} - 2^{(m-2)/2}$	$2^m(2^{m-1} - 1)$
2^{m-1}	$2^{m+1} - 2$
$2^{m-1} + 2^{(m-2)/2}$	$2^m(2^{m-1} - 1)$
2^m	1

.

Applying $A_2^{2^m}$ to this distribution yields a two weight binary code $(2^{m-1}(2^m - 1), 2^{2m-1}, 2^{m-2}(2^m - 1))$ with weight distribution

i	$A(i)$
0	1
2^{2m-2}	$2^m - 1$
$2^{2m-2} - 2^{m-2}$	$2^m(2^{m-1} - 1)$

.

The above transformed code is non-linear from Proposition 1 since they are linear only if for all $\alpha, \beta \in K(m)$ we have either $\alpha + \beta$ or $\alpha + \beta + 1 \in K(m)$. There exist unique optimal two weight binary linear MacDonald codes $(k = 2m - 1, u = m - 1)[2^{m-1}(2^m - 1), 2m - 1, 2^{m-2}(2^m - 1)]$ with this weight distribution. We have not been able to determine if the above non-linear codes are equivalent to the MacDonald codes.

It would be nice if one could obtain a code meeting the Griesmer bound from a code meeting the Griesmer bound by these transformations. However this is not true in general,

for example, the code $[5, 2, 4]_7$ meets the Griesmer bound but the transformed code with A_2^5 is a $[60, 2, 50]_7$ code which does not meet the Griesmer bound. However, the output of the distance matrix suggests that very good codes can be constructed by this method, and this has been confirmed by the codes we have constructed.

Some distance matrices are given below. Let $N := N(n, q)$ denote the row vector of length n with j^{th} entry $\binom{n}{j}(q-1)^{j-1}$ for all $1 \leq j \leq n$ and let $D := D(n, q)$ denote the distance matrix with $(i, j)^{th}$ entry $\frac{1}{q}\{K_j(0) - K_j(i)\}$ for every $1 \leq i \leq n$ and $1 \leq j \leq n$. Note that the entry in the $(i, j)^{th}$ position of D is the weight of a vector of weight i under the transformation A_j^n and that the j^{th} entry of N is the length of the code under the irreducible transformation A_j^n.

For $q = 2$, and $n = 7$

$$N = [7, 21, 35, 35, 21, 7, 1]$$

and

$$D = \begin{bmatrix} 1 & 6 & 15 & 20 & 15 & 6 & 1 \\ 2 & 10 & 20 & 20 & 10 & 2 & 0 \\ 3 & 12 & 19 & 16 & 9 & 4 & 1 \\ 4 & 12 & 16 & 16 & 12 & 4 & 0 \\ 5 & 10 & 15 & 20 & 11 & 2 & 1 \\ 6 & 6 & 20 & 20 & 6 & 6 & 0 \\ 7 & 0 & 35 & 0 & 21 & 0 & 1 \end{bmatrix}.$$

For $q = 3$, and $n = 5$

$$N = [5, 20, 40, 40, 16]$$

and

$$D = \begin{bmatrix} 1 & 8 & 24 & 32 & 16 \\ 2 & 13 & 30 & 28 & 8 \\ 3 & 15 & 27 & 24 & 12 \\ 4 & 14 & 24 & 29 & 10 \\ 5 & 10 & 30 & 25 & 11 \end{bmatrix}.$$

For $q = 4$, and $n = 3$

$$N = [3, 9, 9]$$

and

$$D = \begin{bmatrix} 1 & 6 & 9 \\ 2 & 8 & 6 \\ 3 & 6 & 7 \end{bmatrix}.$$

For $q = 4$, and $n = 5$

$$N = [5, 30, 90, 135, 81]$$

and

$$D = \begin{bmatrix} 1 & 12 & 54 & 108 & 81 \\ 2 & 20 & 72 & 108 & 54 \\ 3 & 24 & 70 & 96 & 63 \\ 4 & 24 & 64 & 104 & 60 \\ 5 & 20 & 70 & 100 & 61 \end{bmatrix}.$$

For $q = 4$, and $n = 6$

$$N = [6, 45, 180, 405, 486, 243]$$

and

$$D = \begin{bmatrix} 1 & 15 & 90 & 270 & 405 & 243 \\ 2 & 26 & 132 & 324 & 378 & 162 \\ 3 & 33 & 142 & 306 & 351 & 189 \\ 4 & 36 & 136 & 296 & 372 & 180 \\ 5 & 35 & 130 & 310 & 361 & 183 \\ 6 & 30 & 140 & 300 & 366 & 182 \end{bmatrix}.$$

Note that the distance of the transformed code for many transformations (both irreducible and their concatenations), can be obtained by looking at the distance matrices and adding columns. Finally, we conjecture that the determinant of $D(n, q)$ is always $(-q)^{\binom{n}{2}}$ and so D is non-singular.

6 Conclusions

In this paper, we have classified all linear transformations on q-ary codes that connect the Hamming distances of codes of different lengths. In addition, we have applied the irreducible transformations to obtain many optimal and near optimal codes. We also constructed a class of binary additive quantum codes of distance at most 3. The most important property of these transformations is that they can be applied to any code, linear or non-linear, to obtain good codes.

Acknowledgement. The authors would like to thank Patrick Solé for pointing out the work of MacWilliams [3] and Jay A. Wood [7], and for the useful communication [6].

References

[1] 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*, Vol. 44, pp. 1369-1387, 1998.

[2] M. Greferath and S. E. Schmidt. "Finite-ring combinatorics and MacWilliams' equivalence theorem," *J. Comb. Theory*, Series A, Vol. 92, pp 17-28, 2000.

[3] F. J. MacWilliams, *Combinatorial Properties of Elementary Abelian Groups*, Ph.D. Thesis, Radcliffe College, Cambridge, MA, 1962.

[4] V. Pless and W. C. Huffman (Eds.) *The Handbook of Coding Theory*. North-Holland, New York, 1998.

[5] D. G. Glynn, "Improving the distance of quantum codes," preprint, 2002.

[6] P. Solé, Private communication, 4 Dec. 2001.

[7] J. A. Wood, "The structure of linear codes of constant weight," *Trans. American Math. Society*, Vol. 354, pp. 1007-1026, 2002.