WEIGHT ENUMERATORS AND A MACWILLIAMS-TYPE IDENTITY FOR SPACE-TIME RANK CODES OVER FINITE FIELDS

DAVID GRANT
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF COLORADO AT BOULDER
BOULDER, CO 80309
GRANT@BOULDER.COLORADO.EDU AND
MAHESH VARANASI
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
UNIVERSITY OF COLORADO AT BOULDER
BOULDER, CO 80309
VARANASI@COLORADO.EDU

Abstract. Several authors have considered the analogue of space-time codes over finite fields, usually taking the distance between two matrices as the rank of their difference. We introduce a weight enumerator for these "finite rank codes," and show that there is a MacWilliams-type identity connecting the weight enumerator of a linear finite rank code to that of its dual. We do so with a proof of sufficient generality that it simultaneously derives the classical MacWilliams identity for linear block codes. Finally, we demonstrate a close relationship between the MacWilliams identity for linear finite rank codes and that for linear block codes.

Introduction

A space-time code $\mathcal{S}$ is a finite subset of the $M \times T$ complex matrices $\mathrm{Mat}_{M\times T}(\mathbb{C})$ used to describe the amplitude-phase modulation of a radio frequency carrier signal in a frame of T symbols received over each of the M transmit antennas. We call the set of entries of the matrices in $\mathcal{S}$ its *alphabet*.

The main design criterion in the construction of space-time codes is the error correcting capability of the code, so we seek to minimize the pair-error probability of decoding one codeword C_1 into another C_2. For quasi-static Rayleigh fading channels with Gaussian noise, one can bound this probability by an asymptotic in the inverse of the signal-to-noise ratio ρ, whose lead term is a multiple of $(1/\rho)^d$, where $d = d(C_1, C_2)$ is the rank of $C_1 - C_2$. The minimum value $d_{\mathcal{S}}$ for $d(C_1, C_2)$ over all $C_1 \neq C_2, C_1, C_2 \in \mathcal{S}$ is called the *diversity order* of $\mathcal{S}$. Hence one seeks to maximize $d_{\mathcal{S}}$.

We note that:

I) This diversity order makes sense for matrices over a finite field.

II) Each space-time code whose alphabet lies in the set of algebraic integers is an appropriately-defined lift from a corresponding space-time code over a finite field.

III) There is an appropriately-defined notion of equivalence of space-time codes such that each space-time codes is arbitrarily well approximated by an equivalent one whose alphabet lies in the set of algebraic integers.

The first-named author would like to thank the second-named author, Nigel Boston, Laurence Mailaender, and Judy Walker for continued encouragement. This work was partially supported by NSF grant CCF 0434410.

In a forthcoming paper [3], we make the notions in (II) and (III) precise and prove these assertions. Roughly speaking, what we prove in [3] is that the alphabet of $\mathcal{S}$ can be perturbed by an arbitrarily small amount such that it lies in the ring of integers $\mathcal{O}$ of some number field, and that this perturbation does not change the rank of the difference of any two codewords. Then there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that when the entries of the codewords are reduced mod $\mathfrak{p}$, the rank of the difference of any two codewords does not change. This set of reduced matrices now has entries in the finite field $\mathcal{O}/\mathfrak{p}$.

We conclude that each space-time code is in essence derived from one over a finite field. Thus the study of such codes over finite fields becomes a central object of investigation.

The main result of this paper is that these space-time codes have a rich theory over finite fields: in particular, each such linear code has a notion of a dual, and a weight enumerator that satisfies a MacWilliams-type identity relating it to the weight enumerator of its dual.

In section 1, we discuss previous work on space-time rank codes over finite fields and define the dual of a linear code. In section 2 we outline a quite general proof of MacWilliams-type identities for space-time codes with certain weights over finite fields. In section 3 we use this to give a proof of the classical MacWilliams identity for linear block codes. In section 4 we use the results of section 2 to show that the linear "finite rank codes" have appropriately defined weight enumerators that satisfy a MacWilliams-type identity, and give some examples in section 5. In the final section 6 we explain how these two duality relations are closely related.

1. Duality Theory for linear space-time codes over finite fields

Let q be a power of a prime, and $\mathbb{F}_q$ denote the field with q elements. Let $M, T \geq 1$, and $\mathcal{C} \subseteq \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$. We call $\mathcal{C}$ a *finite matrix code* over $\mathbb{F}_q$. If in addition $\mathcal{C}$ is an $\mathbb{F}_q$-vector space, we call it a *linear finite matrix code.* We define a *code structure* $d(C_1, C_2)$ on $\mathcal{C}$ to be any translation-invariant metric on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, i.e., one such that $d(C_1 + C_3, C_2 + C_3) = d(C_1, C_2)$ for all $C_1, C_2, C_3 \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$. Note that each code structure defines a weight $w(C_1) = d(C_1, 0)$, and that a code structure can be recovered from the weight via $d(C_1, C_2) = w(C_1 - C_2)$. So we will also think of the weight as the code structure.

Here we will only consider two code structures (others are detailed in [2]). The first is where $d(C_1, C_2) = \mathrm{rk}(C_1 - C_2)$, and we will call a finite matrix code endowed with this metric a *finite rank code.* The second is where $d(C_1, C_2)$ is the Hamming weight of $C_1 - C_2$ (i.e., the number of non-zero entries of $C_1 - C_2$), and we will call a finite matrix code endowed with this metric a *finite matrix Hamming code.* Concatenating rows or columns of these matrices shows that such codes are nothing more than block codes of length MT under the Hamming metric.

The structure of finite rank codes was studied long before the advent of space-time codes, by Gabidulin some 30 years ago in studying criss-cross errors in storage [1]. We are indebted to Eric Moorhouse for pointing out to us that a finite rank code $\mathcal{C}$ with $T = M$ that satisfies $d(C_1, C_2) = M$ for all distinct non-trivial $C_1, C_2 \in \mathcal{C}$, is also nothing more than an "matrix spread set" studied in discrete geometry under a different guise (and that if in addition $\mathcal{C}$ is linear, then it is a semifield, i.e., a non-associative division algebra over $\mathbb{F}_q$.) The theory of finite rank codes as they relate to space-time codes was initiated in [4], [5], [6], [7], and [8].

Let $\mathcal{C}$ be a finite linear $M \times T$ code over $\mathbb{F}_q$ of dimension k and coding structure w. We define its minimal distance as $d = \min_{A\in\mathcal{C},\ A\neq 0} w(A)$, and say that $\mathcal{C}$ has parameters $[M, T, k, d]$.

There is a notion of a dual of any linear finite matrix code $\mathcal{C}$. On $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ we define the symmetric bilinear "inner product" $\ell(A,B)=\mathrm{tr}(AB^T)$, and then set

$$\mathcal{C}^\perp = \{B\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)|\ \ell(A,B)=0,\ \forall A\in\mathcal{C}\}.$$

Remark. This choice of product mirrors the standard inner product on real matrices. It is also the standard dot product of A and B thought of as vectors by concatenating their rows (or columns).

If $\mathcal{C}$ is a linear $[M,T,k,d]$-code, then $(\mathcal{C}^\perp)^\perp=\mathcal{C}$, and $\mathcal{C}^\perp$ is an $[M,T,k',d']$-code, where $k+k'=MT$. The main result of this paper is that a finite rank code has a generating function that serves as a weight enumerator, and that there is a functional equation relating the weight enumerator of a linear finite rank code to that of its dual that is analogous to the MacWilliams identity for linear block codes.

2. The general argument

We can now give an argument which simultaneously provides generalized MacWilliams-type identities for several classes of finite linear matrix codes over $\mathbb{F}_q$.

Let $\mathcal{P}=\{P_i|1\le i\le n\}$ be a partition of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, so that $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)=\cup_{i=1}^n P_i$, each $P_i\neq\emptyset$, and $P_i\cap P_j=\emptyset$ for $i\neq j$. We say $\mathcal{P}$ has *length* n. For $B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ we will write $\mathcal{P}(B)$ for the r such that $B\in P_r$. Since one way to partition $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ is by having a code structure w and taking each $\mathcal{P}_i$ to be the matrices of a fixed weight, by abuse of language, for any partition $\mathcal{P}$, if $\mathcal{P}(B)=r$, we will also refer to r as the *weight* of B. We assume throughout that each P_r is fixed by the multiplication of its elements by non-zero scalars in $\mathbb{F}_q$, and say in this case that $\mathcal{P}$ is *preserved by* $\mathbb{F}_q^*$. Let $\mathcal{C}_{M\times T}$ denote the set of linear $M\times T$ matrix codes over $\mathbb{F}_q$, and for any $\mathcal{C}\in\mathcal{C}_{M\times T}$ and $1\le r\le n$, define

$$a_r(\mathcal{C})=\#(\mathcal{C}\cap P_r).$$

Then we define $a:\mathcal{C}_{M\times T}\to\mathbb{Q}^n$ by $a(\mathcal{C})=(a_1(\mathcal{C}),...,a_n(\mathcal{C}))$. For any $A\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, let $[A]$ be the linear code generated by A. Let y_r denote the integer-valued vector of length n consisting of a 1 in the r^{th}-entry and a 0 in every other entry.

Lemma 1. *$a(\mathcal{C}_{M\times T})$ is a spanning set of $\mathbb{Q}^n$ as a $\mathbb{Q}$-vector space.*

Proof. Suppose that $\mathcal{P}(0)=s$. Then $a([0])=y_s$. For every $1\le r\le n$, $r\neq s$, choose a matrix $C_r\in\mathcal{P}_r$. Then $a([C_r])=(q-1)y_r+y_s$. Hence $a([0])$ and the $a([C_r])$ form a spanning set. □

We will say that $\mathcal{C}_1,\mathcal{C}_2\in\mathcal{C}_{M\times T}$ are *formally equivalent* if $a(\mathcal{C}_1)=a(\mathcal{C}_2)$. We will let $\mathbb{Q}(t)$ denote the field of rational function in t, that is, the field of ratios of polynomials in t with rational coefficients.

Let $F=\{f_r|1\le r\le n\}$ be elements of $\mathbb{Q}(t)$ which are linearly independent over $\mathbb{Q}$. Fix a $\mathcal{C}\in\mathcal{C}_{M\times T}$ and let $a_r=a_r(\mathcal{C})$. Then we define a $\mathcal{P}$-enumerator of C with respect to F to be

$$\phi_{F(t)}(\mathcal{C})=\sum_{r=1}^n a_r f_r.$$

Consider the double sum

$$S=\sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)}\Big(\sum_{A\in\mathcal{C}}\chi(\ell(A,B))\Big)f_{\mathcal{P}(B)},$$

where χ is a non-trivial character on $\mathbb{F}_q$. Recall that this means that χ is a non-trivial homomorphism from $\mathbb{F}_q$ to $\mathbb{C}^*$, so the sum $\sum_{x\in\mathbb{F}_q}\chi(xy)$ is q if $y=0$ but vanishes otherwise. Since ℓ is bilinear the inner sum in S is $|\mathcal{C}|$ if $B\in\mathcal{C}^\perp$, and vanishes if $B\notin\mathcal{C}^\perp$.

Hence

$$S = |\mathcal{C}| \sum_{B \in \mathcal{C}^\perp} f_{\mathcal{P}(B)} = |\mathcal{C}| \sum_{s=1}^{n} b_s f_s = |\mathcal{C}| \phi_{F(t)}(\mathcal{C}^\perp),$$

where $b_s = a_s(\mathcal{C}^\perp)$.

On the other hand, exchanging the order of summation,

$$S = \sum_{A \in \mathcal{C}} \Big(\sum_{B \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(A,B)) f_{\mathcal{P}(B)} \Big).$$

Assumption 1. $\sum_{B \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(A,B)) f_{\mathcal{P}(B)}$ *depends only on* $\mathcal{P}(A)$.

We now assume that Assumption 1 holds. So then we can write

$$\sum_{B \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(A,B)) f_{\mathcal{P}(B)} = \sum_{s=1}^{n} \alpha_{rs} f_s,$$

for some α_{rs}, where $r = \mathcal{P}(A)$. Since $\mathcal{P}$ is preserved by $\mathbb{F}_q^*$ and ℓ is bilinear, we get that $\alpha_{rs} \in \mathbb{Z}$.

As a result, we get

$$S = \sum_{r,s=1}^{n} a_r \alpha_{rs} f_s,$$

so since the f_s are $\mathbb{Q}$-linearly independent,

$$|\mathcal{C}| b_s = \sum_{r=1}^{n} a_r \alpha_{rs}, \tag{1}$$

for all $1 \le s \le n$. Note that applying (1) to every $\mathcal{C}$ and its dual, Lemma 1 shows that $[\alpha_{rs}]$ is an invertible matrix, whose square is q^{MT} times the $n \times n$ identity matrix.

We now define a *dualizing sequence* $\mathcal{C}_k \in \mathcal{C}_{M\times T}$, $1 \le k \le n$ to be one such that:

i) $\mathcal{C}_k^\perp$ is formally equivalent to $\mathcal{C}_{n+1-k}$.

ii) If $p_{kr} = a_r(\mathcal{C}_k)$, then $[p_{kr}]$ is invertible.

We will call $[p_{rk}]$ the *associated matrix* of the dualizing sequence. Suppose that the dimension of $\mathcal{C}_k$ is e_k. We will call $\{e_k | 1 \le k \le n\}$, the *associated dimensions* of the dualizing sequence.

Now suppose we have a dualizing sequence. Applying (1) to every $\mathcal{C}_k$ we have

$$q^{e_k} p_{n-k,s} = |\mathcal{C}_k| a_s(\mathcal{C}_{n-k}) = |\mathcal{C}_k| a_s(\mathcal{C}_k^\perp) = |\mathcal{C}_k| b_s = \sum_{r=1}^{n} \alpha_{rs} p_{kr}.$$

So as matrices

$$\mathrm{antidiag}(q^{e_1}, ..., q^{e_n})[p_{ks}] = [p_{kr}][\alpha_{rs}],$$

where $\mathrm{antidiag}(q^{e_1}, ..., q^{e_n})$ is the $n \times n$ matrix $N = [n_{ij}]$ such that $n_{ij} = q^{e_i}$ if $j = n+1-i$ and vanishes otherwise. Hence:

$$[\alpha_{rs}] = [p_{kr}]^{-1} \mathrm{antidiag}(q^{e_1}, ..., q^{e_n})[p_{kr}]. \tag{2}$$

In order to replicate a functional equation for a $\mathcal{P}$-enumerator that resembles the classical MacWilliams identity, we take $*$ to be any involutary automorphism of $\mathbb{Q}(t)$ (i.e., an automorphism $*$ of $\mathbb{Q}(t)$ of order 2) and ψ to be any element of $\mathbb{Q}(t)$ such that $\psi\psi^* = q^{MT}$. Then we want a relation of the form

$$|\mathcal{C}| \phi_{F(t)}(\mathcal{C}^\perp) = \psi \phi_{F(t^*)}(\mathcal{C}), \tag{3}$$

to hold for every $\mathcal{C} \in \mathcal{C}_{M\times T}$. Again, by Lemma 1, from (1), (3) holds if and only if,

$$\psi f_r^* = \sum_{s=1}^{n} \alpha_{rs} f_s,$$

so by (2), if and only if

$$\psi g_k^* = q^{e_k} g_{n+1-k}, \tag{4}$$

where $g_k = \sum_{r=1}^{n} p_{kr} f_r$ for $1 \le k \le n$. Therefore if we have $\mathbb{Q}$-linearly independent g_k, $1 \le k \le n$, that satisfy (4), and if we find some dualizing sequence with associated matrix $[p_{kr}]$ and degrees $\{e_k\}$, and then define $[f_r] = [p_{kr}]^{-1}[g_k]$, then $\phi_{F(t)}$ will satisfy the functional equation (3).

In summary, we have proved:

Theorem 1. *Let $\mathcal{P}$ be a partition of length n of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ preserved by $\mathbb{F}_q^*$. Suppose χ is a non-trivial character of $\mathbb{F}_q$ such that Assumption 1 holds. Let $*$ be an involutary automorphism of $\mathbb{Q}(t)$ and $\psi \in \mathbb{Q}(t)$ be such that $\psi\psi^* = q^{MT}$. Suppose we have a dualizing sequence for $\mathcal{P}$ with associated matrix $[p_{kr}]$ and dimensions $\{e_k\}$. Further suppose that we have a set of $\mathbb{Q}$-linearly independent functions $g_1, ..., g_n \in \mathbb{Q}(t)$ such that $\psi g_k^* = q^{e_k} g_{n+1-k}$. Set $[f_r] = [p_{kr}]^{-1}[g_k]$. Then we have*

$$|\mathcal{C}|\phi_{F(t)}(\mathcal{C}^\perp) = \psi\phi_{F(t^*)}(\mathcal{C}).$$

The partitions which apply in the theorem will often be the orbits under a group action. In this case, we can prove the following.

Theorem 2. *Let G be a group that acts on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$. We assume that G contains a subgroup H isomorphic to $\mathbb{F}_q^*$, and that identifying H and $\mathbb{F}_q^*$, the action restricted to $\mathbb{F}_q^*$ is just scalar multiplication. We also assume that G has an automorphism ρ of order 2, such that ρ is adjoint for $\ell(A, B)$, i.e.,*

$$\ell(gA, B) = \ell(A, \rho(g)B),$$

for all $g \in G$ and $A, B \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$. Suppose that we have a dualizing sequence for the partition $\mathcal{P}$ consisting of the orbits under the action of G, with associated matrix $[p_{kr}]$ and dimensions $\{e_k\}$. Let n be the length of $\mathcal{P}$. Let $*$ be an involutary automorphism of $\mathbb{Q}(t)$ and $\psi \in \mathbb{Q}(t)$ be such that $\psi\psi^* = q^{MT}$. Suppose we have a set of $\mathbb{Q}$-linearly independent functions $g_1, ..., g_n \in \mathbb{Q}(t)$, such that $\psi g_k^* = q^{e_k} g_{n+1-k}$. Set $[f_r] = [p_{kr}]^{-1}[g_k]$. Then we have

$$|\mathcal{C}|\phi_{F(t)}(\mathcal{C}^\perp) = \psi\phi_{F(t^*)}(\mathcal{C}).$$

Proof. All we have to check is that Assumption 1 holds for $\mathcal{P}$ and some non-trivial character χ. For each $1 \le r \le n$, let γ_r be a chosen element in P_r. Take $A \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ and suppose $\mathcal{P}(A) = r$. Then there is a $g \in G$ such that $A = g\gamma_r$. Note that for every B, $\ell(A, B) = \ell(g\gamma_r, B) = \ell(\gamma_r, \rho(g)B)$, and the map $B \to \rho(g)B$ is a bijection of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ that preserves orbits under G. Hence we can rewrite the sum

$$\sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(A, B)) f_{\mathcal{P}(B)} = \sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(\gamma_r, \rho(g)B)) f_{\mathcal{P}(B)} =$$

$$\sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(\gamma_r, \rho(B))) f_{\mathcal{P}(\rho(B))} = \sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(\gamma_r, B)) f_{\mathcal{P}(B)},$$

which depends only on $\mathcal{P}(A)$. Hence Assumption 1 holds, and the proof follows from Theorem 1. $\square$

Remark. At the core of a duality relation is the necessity that the enumerator of a linear code completely determine the enumerator of its dual code. We can see then that Assumption 1 is necessary for any sort of duality relation to hold. Indeed,

$$\sum_{B\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(\ell(A,B)) f_{\mathcal{P}(B)} = \sum_{B\in[A]^\perp} f_{\mathcal{P}(B)} - \sum_{(B\notin[A]^\perp)/\mathbb{F}_q^*} f_{\mathcal{P}(B)}$$

$$= \frac{1}{q-1}\Big(\sum_{B\in[A]^\perp}(q-1)f_{\mathcal{P}(B)} - \sum_{B\notin[A]^\perp} f_{\mathcal{P}(B)}\Big)$$

$$= \frac{1}{q-1}\Big(\sum_{B\in[A]^\perp} q f_{\mathcal{P}(B)} - \sum_{B\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} f_{\mathcal{P}(B)}\Big),$$

which if an enumerator is determined by that of a dual, must only depend on the enumerator of $[A]$, which is to say, it must only depends on $\mathcal{P}(A)$. In fact, if (3) does hold, we get that

$$\frac{1}{q-1}\Big(\sum_{B\in[A]^\perp} q f_{\mathcal{P}(B)} - \sum_{B\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} f_{\mathcal{P}(B)}\Big) = \frac{1}{q-1}(q\phi_{F(t)}([A]^\perp) - \phi_{F(t)}([0]^\perp))$$

$$= \frac{1}{q-1}(\psi\phi_{F(t^*)}([A]) - \psi\phi_{F(t^*)}([0])) = \psi f_{\mathcal{P}(A)}(t^*),$$

which quite clearly depends only on $\mathcal{P}(A)$.

3. The classical MacWilliams identity

We can recover a proof of the classical MacWilliams identity by applying Theorem 2. We consider finite linear Hamming matrix codes and take $M = 1$, so these are just traditional linear block codes of length T under the Hamming metric. Let $GL_T(\mathbb{F}_q)$ denote the general linear group of invertible $T\times T$ matrix with entries in $\mathbb{F}_q$. We apply Theorem 2 by taking $G = DP$, where D is the subgroup of diagonal matrices in $GL_T(\mathbb{F}_q)$, P is the subgroup generated by permutation matrices, G acts via matrix multiplication on the right of $(\mathbb{F}_q)^T$, and ρ consists of taking transposes. We get a partition of $\mathbb{F}_q^T$ of length $T+1$, with each orbit consisting of vectors of a fixed Hamming weight.

The main task before us to find a dualizing sequence. We claim that

$$\mathcal{C}_k = \{(x_1, ..., x_k, 0, ..., 0) | x_i \in \mathbb{F}_q\},$$

$0 \le k \le n$, is a dualizing sequence.

Indeed, the dimension of $\mathcal{C}_k$ is k, and $\mathcal{C}_k^\perp$ is equivalent to $\mathcal{C}_{n-k}$. Now let us set $p_{kr} = a_r(\mathcal{C}_k)$, and show that $[p_{kr}]$ is invertible. A computation shows for $k \ge r$,

$$p_{kr} = \binom{k}{r}(q-1)^r,$$

and otherwise is 0. If $s_{rj} = (-1)^{r-j}\binom{r}{j}/(q-1)^r$ for $r \ge j$ and is otherwise 0, then

$$\sum_{r=0}^{n} p_{kr}s_{rj} = \sum_{r=j}^{k}\binom{k}{r}\binom{r}{j}(-1)^{r-j} = \sum_{r=j}^{k}\binom{k-j}{r-j}\binom{k}{k-j}(-1)^{r-j} =$$

$$\binom{k}{j}\sum_{r=j}^{k}\binom{k-j}{r-j}(-1)^{r-j} = \binom{k}{j}(1+(-1))^{k-j} = \binom{k}{j}\delta_{kj} = \delta_{kj},$$

where δ_{kj} is the Kronecker delta. Hence $[p_{kr}]$ is invertible with inverse $[s_{rj}]$, and $\mathcal{C}_k$ forms a dualizing sequence with associated matrix $[p_{kr}]$ and associated dimensions $e_k = k$.

We now take $t \to q/t$ as the involutary automorphism of $\mathbb{Q}(t)$. Then taking $\psi = t^T$, and $g_k = t^k$, $0 \le k \le n$, we have $\psi(t^*)^k = q^k t^{n-k}$, so setting $f_r = \sum_{j=0}^n s_{rj} t^j = ((1-t)/(1-q))^r$ and applying Theorem 2 we get:

Theorem 3. *(MacWilliams) Let $\mathcal{C}$ be a linear block code of length T over $\mathbb{F}_q$, let a_r be the number of codewords of $\mathcal{C}$ of Hamming weight r, and set $\phi_{\mathcal{C}}(t) = \sum_{r=0}^T a_r (\frac{1-t}{1-q})^r$. Then*

$$\phi_{\mathcal{C}^\perp}(t) = \frac{1}{|\mathcal{C}|} t^T \phi_{\mathcal{C}}(q/t).$$

This is equivalent to the usual statement of the MacWilliams identity for linear block codes. Indeed letting $u = (1-t)/(1-q)$, then $t = 1 + (q-1)u$, and the map $* : t \to q/t$ corresponds to $u \to (1-u)/(1+(q-1)u)$. So (3) holds with $\psi = (1+(q-1)u)^n$ and $f_r = u^r$, which is the typical statement of the MacWilliams identity [10].

4. A MacWilliams-type identity for weight enumerators of finite rank codes

We now prove a MacWilliams-type identity for what we will call the *rank enumerator* of a finite rank code, which is to say, the weight enumerator where the weight of a matrix is its rank. In terms of the language of section 2, the rank enumerator of a code is the $\mathcal{P}$-enumerator when P_r consists of the $M \times T$ matrices with entries in $\mathbb{F}_q$ of rank r, for $0 \le r \le \min(M, T)$. Let $n = \min(M, T)$, so the partition $\mathcal{P}$ has length $n+1$.

We can proceed by using Theorem 2 since $\mathcal{P}$ is the set of orbits under a group action. Indeed, let $G = GL_M(\mathbb{F}_q) \times GL_T(\mathbb{F}_q)$, where the second factor acts as multiplication on the right of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ and the first factor acts on the left via multiplication by the transpose. Then the orbits under G give rise to $\mathcal{P}$, G has a subgroup isomorphic to $\mathbb{F}_q^*$ which acts as scalar multiplication, and if ρ consists of taking transposes of each factor, then it is an automorphism of order 2 which is an adjoint for ℓ. The main task for applying Theorem 2 is to compute $[p_{kr}]$ for some dualizing sequence.

Let $\mathcal{C}_k$ be the collection of partitioned matrices $(N|0_{M,T-k})$ where $N \in \mathrm{Mat}_{M\times k}(\mathbb{F}_q)$ if $M \ge T$, and the transpose of this collection if $M \le T$. In either case, we have $0 \le k \le n$. Then it is clear that $\mathcal{C}_k^\perp$ is formally equivalent to $\mathcal{C}_{n-k}$. To see that $\mathcal{C}_k$ forms a dualizing sequence, we resort to the known calculation of the number of matrices over $\mathbb{F}_q$ of fixed size and rank [11], which shows that $p_{kr} = a_r(\mathcal{C}_k) = [{k \atop r}][{m \atop r}]\phi_r(-1)^r q^{\binom{r}{2}}$, for $r \le k$, where:

$$\phi_r = (1-q)\cdots(1-q^r),\ [{k \atop r}] = \phi_k/\phi_r\phi_{k-r}, \tag{5}$$

and $m = \max(M, T)$. Here $[{k \atop r}]$ is the classical *generalized binomial coefficient* or *q-binomial coefficient.* For any N it satisfies the Newton identity [9]

$$\prod_{i=0}^{N-1}(1+q^i x) = \sum_{i=0}^{N}[{N \atop i}]q^{\binom{i}{2}}x^i. \tag{6}$$

Note $p_{kr} = 0$ if $r > k$. If $s_{rj} = (-1)^{r-j}[{r \atop j}]q^{\binom{r-j}{2}}/\frac{\phi_m}{\phi_{m-r}}(-1)^r q^{\binom{r}{2}}$, for $r \ge j$, and $s_{rj} = 0$ for $r < j$, then by (5) and (6),

$$\sum_{r=0}^{n} p_{kr}s_{rj} = \sum_{r=j}^{k}[{k \atop r}][{r \atop j}]q^{\binom{r-j}{2}}(-1)^{r-j} = \sum_{r=j}^{k}[{k-j \atop r-j}][{k \atop k-j}]q^{\binom{r-j}{2}}(-1)^{r-j} =$$

$$[{k \atop j}]\sum_{r=j}^{k}[{k-j \atop r-j}]q^{\binom{r-j}{2}}(-1)^{r-j} = [{k \atop j}]\prod_{i=0}^{k-j-1}(1+q^i(-1)) = [{k \atop j}]\delta_{kj} = \delta_{kj}.$$

So $[p_{kr}]$ is invertible, and $[s_{rj}]$ is its inverse, and $\mathcal{C}_k$ is a dualizing sequence with associated matrix $[p_{kr}]$ and associated dimensions $e_k = q^{km}$. Let $* : t \to q^m/t$ be an involutary automorphism of $\mathbb{Q}(t)$, $\psi = t^n$, and $g_k = t^k$ for $0 \le k \le n$. Then $\psi\psi^* = q^{mn} = q^{MT}$, and $\psi g_k^* = t^{km} g_{n-k}$. Hence Theorem 2 applies, so if we set $[f_r] = [p_{kr}]^{-1} g_k$, then by (6),

$$f_r = \sum_{j=0}^{n} s_{rj} t^j = \frac{\phi_{m-r}}{\phi_m} \sum_{j=0}^{r} [{r \atop j}] q^{\binom{j}{2}} (-q^{1-r}t)^j = \frac{\phi_{m-r}}{\phi_m} \prod_{j=0}^{r-1} (1 - q^{-j}t) = \prod_{j=0}^{r-1} (\frac{t - q^j}{q^m - q^j}).$$

This motivates the following:

Definition 1. *Let $\mathcal{C}$ be an $M \times T$ finite linear rank code over $\mathbb{F}_q$. For any $0 \le r \le \min(M,T)$, let $f_r = \prod_{j=0}^{r-1} (\frac{t-q^j}{q^{\max(M,T)} - q^j})$, and define the rank enumerator of $\mathcal{C}$ to be*

$$\phi_{\mathcal{C}}(t) = \sum_{r=0}^{\min(M,T)} a_r f_r,$$

where a_r is the number of elements of $\mathcal{C}$ of rank r.

Finally, Theorem 2 gives us:

Theorem 4. *Let $\mathcal{C}$ be a $M \times T$ linear finite rank code over $\mathbb{F}_q$. Then*

$$\phi_{\mathcal{C}^\perp}(t) = \frac{1}{|\mathcal{C}|} t^{\min(M,T)} \phi_{\mathcal{C}}(q^{\max(M,T)}/t).$$

5. Some examples.

I) Typically the best space-time codes are those whose diversity order is maximal. The corresponding property for linear $M \times T$ finite rank codes is that their minimal distance be maximal, that is, equal to $n = \min(M,T)$. For such codes, the Singleton bound ([1], [7]) constrains k to be at most n. This leads one to consider $[M,T,n,n]$-codes where $n = \min(M,T)$. Let's consider the case $M = T = 2$.

i) q is odd. Take $e \in \mathbb{F}_q$ to be a non-square. Then

$$\mathcal{C} = \{\begin{pmatrix} a & b \\ be & a \end{pmatrix} | a, b \in \mathbb{F}_q\}$$

is a $[2,2,2,2]$-code (constructed in [1] and [7]). Its dual is

$$\mathcal{C}^\perp = \{\begin{pmatrix} c & de \\ -d & -c \end{pmatrix} | c, d \in \mathbb{F}_q\},$$

which is also a $[2,2,2,2]$-code. Let a_r and b_r denote respectively the number of elements of $\mathcal{C}$ and $\mathcal{C}^\perp$ of rank r. Then $a_0 = b_0 = 1$, $a_1 = b_1 = 0$, and $a_2 = b_2 = q^2 - 1$, so $\mathcal{C}$ and $\mathcal{C}^\perp$ are formally self dual. We get

$$\phi_{\mathcal{C}}(t) = \phi_{\mathcal{C}^\perp}(t) = 1 + 0 \cdot \frac{t-1}{q^2-1} + (q^2-1)\frac{(t-1)(t-q)}{(q^2-1)(q^2-q)} = \frac{t^2 - (q+1)t + q^2}{q^2 - q}.$$

One easily checks that $t^2 \phi_{\mathcal{C}}(q^2/t)/q^2 = \phi_{\mathcal{C}^\perp}(t)$.

ii) q is even. Take $e \in \mathbb{F}_q$ such that $x^2 + x + e$ is an irreducible polynomial. Then

$$\mathcal{C} = \{\begin{pmatrix} a & b \\ be & a+b \end{pmatrix} | a, b \in \mathbb{F}_q\}, \mathcal{C}^\perp = \{\begin{pmatrix} c & c+de \\ d & c \end{pmatrix} | c, d \in \mathbb{F}_q\},$$

are both $[2,2,2,2]$-codes. Again $\phi_{\mathcal{C}}(t) = \phi_{\mathcal{C}^\perp}(t) = \frac{t^2-(q+1)t+q^2}{q^2-q}$.

II) Theorem 4 gives a nice recursive relation for $U_{t,m}$, the number of $m \times m$ upper-triangular matrices with entries in $\mathbb{F}_q$ of rank t. For example, let $\mathcal{C}$ be the vector space of all 3×3 lower-triangular matrices with entries in $\mathbb{F}_q$ whose diagonal entries are all

0, which is a $[3,3,3,1]$-code. Then $\mathcal{C}^{\perp}$ is the vector space of all 3×3 upper-triangular matrices with entries in $\mathbb{F}_q$, which is a $[3,3,6,1]$-code. Then

$$\phi_{\mathcal{C}}(t) = U_{0,2} + U_{1,2}\frac{t-1}{q^3-1} + U_{2,2}\frac{(t-1)(t-q)}{(q^3-1)(q^3-q)},$$

$$\phi_{\mathcal{C}^{\perp}}(t) = U_{0,3} + U_{1,3}\frac{t-1}{q^3-1} + U_{2,3}\frac{(t-1)(t-q)}{(q^3-1)(q^3-q)} + U_{3,3}\frac{(t-1)(t-q)(t-q^2)}{(q^3-1)(q^3-q)(q^3-q^2)}.$$

The fact that $t^3\phi_{\mathcal{C}}(q^3/t)/q^3 = \phi_{\mathcal{C}^{\perp}}(t)$ implies, for instance, that

$$U_{1,3} = (\phi_{\mathcal{C}^{\perp}}(q) - U_{0,3})(q^2+q+1) = (\phi_{\mathcal{C}}(q^2) - U_{0,2})(q^2+q+1) =$$

$$(q^2+q+1)(U_{1,2}\frac{q^2-1}{q^3-1} + U_{2,2}\frac{(q^2-1)(q^2-q)}{(q^3-1)(q^3-q)}) = U_{1,2}(q+1) + U_{2,2},$$

since $U_{0,3} = U_{0,2} = 1$. Noting that $U_{2,2} = (q-1)^2 q$ gives $U_{1,2} = q^3 - U_{0,2} - U_{2,2} = (q-1)(2q+1)$. Hence by the above, $U_{1,3} = (q-1)(3q^2+2q+1)$.

6. Relationship between the duality relations for linear block codes and linear finite rank codes.

From the point of view of Theorem 1 and its proof, it becomes apparent that there are two requirements for our derivation of a MacWilliams-type identity (3) for a partition $\mathcal{P}$ of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ that is preserved by $\mathbb{F}_q^*$. The first is that $\mathcal{P}$ satisfies Assumption 1, which gives rise to the integer matrix $[\alpha_{rs}]$. The second is the existence of a dualizing sequence, which produces the associated matrix $[p_{kr}]$ and associated dimensions $\{e_k\}$, which give the factorization (2). Of course, given the factorization (2) without a dualizing sequence, one could still use it to write down the MacWilliams-type identity (3).

So in a sense, the matrix $[\alpha_{rs}]$ is the more fundamental object, in that it gives the relationship between the weights of a linear matrix code and that of its dual without requiring the existence of an enumerator that satisfies a MacWilliams-type identity. We will call the matrix $[\alpha_{rs}]$ the *duality matrix* of $\mathcal{P}$.

We now compare the duality matrices for linear block codes of length n under the Hamming metric (which is given by values of Krawtchouk polynomials [10]) and for finite linear $M\times T$ rank codes. We show that taking $M=T=n$, one duality matrix is similar to a constant multiple of the other. This follows from the results of section 3 and 4, but we will give a more conceptual and precise approach.

Let $\mathcal{C}_n = \mathcal{C}_{1\times n}$. We define a map $\phi : \mathcal{C}_n \to \mathcal{C}_{n\times n}$ by defining $\phi(\mathcal{C})$ for $\mathcal{C} \in \mathcal{C}_n$ to be the set up all upper-triangular matrices whose vector of diagonal entries consists of codewords in $\mathcal{C}$. We will let $\tilde{\mathcal{C}}$ denote $\phi(\mathcal{C})$. It is not hard to see that if the dimension of $\mathcal{C}$ is k, then the dimension of $\tilde{\mathcal{C}}$ is $k + q^{\binom{n}{2}}$. It is also clear that $\widetilde{\mathcal{C}^{\perp}} \subseteq ((\tilde{\mathcal{C}})^{\perp})^T$. Since they both have dimension $n-k+\binom{n}{2} = n^2 - (k+\binom{n}{2})$, we have that $\widetilde{\mathcal{C}^{\perp}} = ((\tilde{\mathcal{C}})^{\perp})^T$.

Now for any $\mathcal{C} \in \mathcal{C}_n$, let $a_r = a_r(\mathcal{C})$, $b_r = a_r(\mathcal{C}^{\perp})$, $\tilde{a}_r = a_r(\tilde{\mathcal{C}})$, $\tilde{b}_r = a_r(\tilde{\mathcal{C}}^{\perp}) = a_r(\widetilde{\mathcal{C}^{\perp}})$, where the first two weights denote the number of codewords of Hamming weight r and the latter weights denote the number of codewords of rank r. Then from (1) we have

$$|\mathcal{C}|[b_0,...,b_n] = [a_0,...,a_n][\alpha_{rs}],\ \ |\tilde{\mathcal{C}}|[\tilde{b}_0,...,\tilde{b}_n] = [\tilde{a}_0,...,\tilde{a}_n][\tilde{\alpha}_{rs}], \tag{7}$$

where $[\alpha_{rs}]$ and $[\tilde{\alpha}_{rs}]$ are respectively the duality matrices for $\mathcal{C}_n$ and $\mathcal{C}_{n\times n}$.

Let $U_{t,m}$ denote the number of upper-triangular matrices of rank t and size $m\times m$ defined over $\mathbb{F}_q$ (which can be calculated recursively, as in example (II) of section 5). Let M be an $n\times n$ upper-triangular matrix which has u non-zero diagonal entries $d_{j_1,j_1},...,d_{j_u,j_u}$. Let M' denote the $(n-u)\times(n-u)$ upper-triangular matrix gotten by removing the $j_1^{st},...,j_u^{th}$ rows and columns of M. Note that all the diagonal entries of M' are 0, so its rank is the same as that of the $(n-u-1) \times (n-u-1)$ upper-triangular matrix M'' gotten by removing the diagonal and principal subdiagonal of M'. Then the rank of M is u plus the rank of M''. Note that the rank of M is independent of its $\binom{n}{2} - \binom{n-u-1}{2}$ non-diagonal entries that lie in its $j_1^{st}, ..., j_u^{th}$ rows and columns. Hence

$$\tilde{a}_r = \sum_{k=0}^{r} a_k q^{\binom{n}{2} - \binom{n-k-1}{2}} U_{r-k,n-k-1}.$$

Now let $V_{kr} = q^{\binom{n}{2} - \binom{n-k-1}{2}} U_{r-k,n-k-1}$. Then we have that

$$[\tilde{a}_0, ..., \tilde{a}_n] = [a_0, ..., a_n][V_{kr}], \text{ and } [\tilde{b}_0, ..., \tilde{b}_n] = [b_0, ..., b_n][V_{kr}]. \tag{8}$$

Putting (7) and (8) together we have

$$[a_0, ..., a_n][V_{kr}][\tilde{\alpha}_{rs}] = [\tilde{a}_0, ..., \tilde{a}_n][\tilde{\alpha}_{rs}] = |\tilde{\mathcal{C}}|[\tilde{b}_0, ..., \tilde{b}_n] =$$
$$|\mathcal{C}| q^{\binom{n}{2}} [b_0, ..., b_n][V_{kr}] = q^{\binom{n}{2}} [a_0, ..., a_n][\alpha_{rs}][V_{kr}]. \tag{9}$$

Let w_r be the vector of length n whose first r entries are 1 and whose remaining entries are 0. Now considering $\phi([w_r])$ for each $0 \le r \le n$, shows, as in the proof of Lemma 1, that $[\tilde{a}_0, ..., \tilde{a}_n]$ is a spanning set of $\mathbb{Q}^{n+1}$ as $\mathcal{C}$ varies. Hence from (9) we have that

$$[V_{kr}][\tilde{\alpha}_{rs}] = q^{\binom{n}{2}} [\alpha_{rs}][V_{kr}],$$

and from (8) that $[V_{kr}]$ is invertible. Therefore we have shown:

Theorem 5. *Let $[\alpha_{rs}]$ denote the duality matrix for linear block codes of length n over $\mathbb{F}_q$ under the Hamming metric, and $[\tilde{\alpha}_{rs}]$ the duality matrix for $n \times n$ finite linear rank codes over $\mathbb{F}_q$. Then*

$$[\alpha_{rs}] = q^{-\binom{n}{2}} [V_{kr}][\tilde{\alpha}_{rs}][V_{kr}]^{-1}.$$

This implies that the classical MacWilliams identity for linear block codes can be derived from the MacWilliams-type identity for finite linear rank codes, so the latter can be considered a generalization of the former.

References

[1] Gabidulin. *Theory of codes with maximal rank distance*. Problems of Information Transmission, **21**, No. 1 (1985), 1–12.

[2] D. Grant, M. K. Varanasi. *Duality Theory for Space-Time Codes over Finite Fields*, in preparation.

[3] D. Grant, M. K. Varanasi. *Algebraic Space-Time Codes*, in preparation.

[4] A. R. Hammonds and H. El Gamal. *On the theory of space-time codes for PSK modulation.* IEEE Trans. Inform. Theory **46**. No. 2 (2000), 524–542.

[5] Y. Liu, M. P. Fitz, and O. Y. Takeshita. *A rank criterion for QAM space-time codes*. IEEE Trans. Inform. Theory **48**. No. 12, (2002), 3062–3079.

[6] H-f. Lu, P. V. Kumar. *Rate-Diversity tradeoff of space-time codes with fixed alphabet and optimal constructions for PSK modulation*. IEEE Trans. Inform. Theory **49**. No. 10, (2003), 2747–2751.

[7] H-f. Lu, P. V. Kumar. *A unified construction of space-time codes with optimal rate-diversity tradeoff.* IEEE Trans. Inform. Theory **51**. No. 5, (2005).

[8] P. Lusina, E. Gabidulin, M. Bosert. *Maximal Rank Distance Codes as Space-Time Codes*. IEEE Trans. Inform. Theory **49**. No. 10, (2003), 2757–2760.

[9] I. G. MacDonald *Symmetric functions and Hall polynomials*, 2nd edition. Oxford University Press, 1995.

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

[11] T. Migler, K. E. Morrison, M. Ogle. *Weight and rank of matrices over finite fields*. Preprint.