DUALITY THEORY FOR SPACE-TIME CODES OVER FINITE FIELDS

DAVID GRANT AND MAHESH K. VARANASI

ABSTRACT. We further the study of the duality theory of linear space-time codes over finite fields by showing that the only finite linear temporal correlated codes with a duality theory are the column distance codes and the rank codes. We introduce weight enumerators for both these codes and show that they have MacWilliams-type functional equations relating them to the weight enumerators of their duals. We also show that the complete weight enumerator for finite linear sum-of-ranks codes satisfies such a functional equation. We produce an analogue of Gleason's Theorem for linear finite rank codes. Finally, we relate the duality matrices of $n \times n$ linear rank codes and length n vector codes under the Hamming metric.

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 transmitted over each of the M 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 one seeks to minimize the pair-error probability of decoding one codeword C_1 into another C_2. This probability will depend on how the wireless channel is modeled, but one can typically bound this probability by an asymptotic in the inverse of the signal-to-noise ratio ν, whose lead term is a multiple of $(1/\nu)^d$ for some integer d. We call $d = d(C_1, C_2)$ the *diversity* of the pair (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 $d_{\mathcal{S}}$.

Channels for which space-time codes have been considered and diversity order defined as above include:

EXAMPLE 1. Fast-fading Rayleigh channels with additive white Gaussian noise (AWGN). Here the diversity order $d(C_1, C_2)$ is the number of non-zero columns of $C_1 - C_2$.

EXAMPLE 2. Quasi-static fading Rayleigh channels with AWGN. Here $d(C_1, C_2) = \mathrm{rk}(C_1 - C_2)$, the rank of $C_1 - C_2$.

EXAMPLE 3. Channels which are a combination of those in Examples 1 and 2, a multiple block fading channel with AWGN, which is quasi-static for each of ℓ

2000 *Mathematics Subject Classification.* 94B05, 94B60, 11T71.

Key words and phrases. Linear codes, space-time codes, finite fields.

This work was partially supported by NSF grant CCF 0434410. The first named author was enjoying the hospitality of the Mathematical Sciences Research Institute as this paper was being completed. He would also like to thank Laurence Mailaender for continued encouragement.

blocks. Here each codeword C consists of ℓ matrices $\{C_i\}_{i=1}^{\ell}$, each of size $M \times \rho$. The diversity order $d(C_1, C_2)$ is $\sum_{i=1}^{\ell} \mathrm{rk}((C_1)_i - (C_2)_i)$.

EXAMPLE 4. Rayleigh fading channels with AWGN, where we allow for temporal correlation [2]. We need some notation. Let 1_{IJ} denote the $I \times J$ matrix whose entries are all 1. If D is an $M \times T$ matrix and B is of size $T \times T$, we let $D \sharp B$ be the $MT \times T$ matrix whose rows are indexed by the set $\{(i,j) | 1 \leq i \leq M, 1 \leq j \leq T\}$ ordered lexicographically, and whose columns are indexed by $1 \leq k \leq T$, and whose $(i,j)k$-th entry is $D_{ik}B_{jk}$. In other words, $D \sharp B = (D \otimes 1_{T1}) \odot (1_{M1} \otimes B)$, where $\odot$ and $\otimes$ respectively denote the Hadamard and Kronecker products. (Recall that if E is an $M \times T$ matrix and F is an $M' \times T'$ matrix, and if the sets $\{(i,i') | 1 \leq i \leq M, 1 \leq i' \leq M'\}$ and $\{(j,j') | 1 \leq j \leq T, 1 \leq j' \leq T'\}$ are ordered lexicographically, then the $(i,i')(j,j')$-th entry of $E \otimes F$ is $E_{ij}F_{i'j'}$.)

Let U denote the number of receive antennas. Suppose there is a $U \times M$ matrix $H(t)$ which describes the fading of the t^{th}-column of a codeword, for $1 \leq t \leq T$, and that the elements of $H(t)$ are i.i.d. zero-mean complex Gaussian variables, but that the T-length vector of each of the entries of $H(t)$ for $1 \leq t \leq T$ has a $T \times T$ temporal correlation matrix Σ. Write $\Sigma = B^*B$, where B^* is the conjugate transpose of B. Then in [11], using [2], it is shown that for codewords C_1, C_2,

$$d(C_1, C_2) = \mathrm{rk}\left((C_1 - C_2) \sharp B\right). \tag{1}$$

Then the diversity orders in Examples 1, 2, and 3 are all special cases of this formula for different choices of B (respectively, B is the $T \times T$ identity I_T; $B = 1_{TT}$; and B is the block diagonal matrix with ℓ blocks each consisting of $1_{\rho\rho}$).

Note that all the diversity orders in Examples 1–4 make sense for matrices in any ring. In a recent paper [11], the authors showed that there are appropriate notions of approximation, equivalence, and lifting, such that each space-time code above is arbitrarily well approximated by one lifted from an equivalent code over a finite field. This adds impetus to the study of space-time codes over finite fields.

Let q be a power of a prime and $\mathbb{F}_q$ denote the field with q elements. We call subsets of $\mathrm{Mat}_{M \times T}(\mathbb{F}_q)$, respectively endowed with the diversity orders from Examples 1–4 above, *finite column distance* codes, *finite rank codes*, *finite sum-of-ranks codes*, and *finite temporal correlated codes*, and denote their diversity orders as d_{cd}, d_{rk}, d_{sor}, and d_{tc}.

Not only can such finite codes be used in essence to build all space-time codes (see [12], [15], [18], [19], [20], and [21] for some constructions), they are interesting mathematical objects in their own right, with a long pedigree. Gabidulin [10] employed finite column distance and finite rank codes for studying crisscross errors in data storage. There is a longer history of finite rank codes, also referred to as q-codes. One of the crowning achievements in this area is the work of Delsarte, who proved a "MacWilliams Identity" for finite rank codes, both from the points of view of association schemes (see [3], [4]), and also from the point of view of character theory (see [5], [6]). Earlier, Campion had considered rank as a weight for square matrices [1].

The goal of this paper is to further the theory of duality for space-time codes over finite fields. We do this in two ways.

I) For any fixed B of size $T \times T$, we get a diversity order d_{tc}, which we can use to define a weight $w_{\mathrm{tc}}(C) = d_{\mathrm{tc}}(C, 0)$ on $\mathrm{Mat}_{M \times T}(\mathbb{F}_q)$. Recall that for a subspace $\mathcal{C}$

of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, its dual $\mathcal{C}^\perp$ is the orthogonal space to $\mathcal{C}$ with respect to the inner product $A \cdot B = \mathrm{Tr}(AB^t)$, where Tr denotes the trace and t denotes the transpose. For any subspace $\mathcal{C} \in \mathrm{Mat}_{M\times T}(F)$, we can define its spectrum with respect to $\mathrm{wt}_{\mathrm{tc}}$ as the vector $a = (a_i)$ of length $T+1$ where $a_i = \#\{C \in \mathcal{C} | \, \mathrm{wt}_{\mathrm{tc}}(C) = i\}$.

The minimum one needs for a "duality" theory is that $a(\mathcal{C}^\perp)$ is a function of $a(\mathcal{C})$ for every subspace $\mathcal{C}$ of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$. Our first result is, that up to some notions of equivalence we will make precise, the only finite temporal correlated codes which have a duality theory are those in Examples 1 and 2: the finite column distance codes, and the finite rank codes. (Though we will show that the finite sum-of-ranks codes of Example 3 satisfy a MacWilliams-type identity when the complete weight spectrum is considered.) As noted by Gabidulin, column distance codes can be interpreted as vector codes[1] of length T over $\mathbb{F}_{q^M}$ under the Hamming metric. This will enable us to interpret the duality theory of the former in terms of the duality theory of the latter. This lets us focus our attention on finite rank codes.

II) Although the "MacWilliams Identity" for linear finite rank codes was worked out by Delsarte 30 years ago, there is more to be done. He gave an explicit matrix β such that

$$a(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}\beta a(\mathcal{C}),$$

and proved that its entries were q-Krawtchouk polynomials [4], [5], [6]. This is a direct analogue of the corresponding result for linear vector codes under the Hamming metric, where there is a matrix α such that

$$a(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}\alpha a(\mathcal{C}),$$

and the entries of α are values of Krawtchouk polynomials.

But the MacWilliams identities for linear vector codes embody more than just the computation of the matrix α. They give a functional equation relating a generating function for the spectrum (the Hamming weight enumerator) to that of its dual. That explicit functional equation is crucial in:

i) Gleason's theorems for formally self-dual codes [22].

ii) The relationship between the MacWilliams identities and the functional equation of the Riemann theta function [9].

iii) Duursma's conjectures [7], [8].

Our second main result is to introduce a rank enumerator (different from the one considered by Delsarte [6]), which is a generating function for the spectrum of a finite rank code, and which has a functional equation relating it to the rank enumerator of the dual code. As a result, we can prove an analogue of Gleason's Theorem for formally self-dual finite rank codes. It should be possible to greatly extend this result (see the recent [23] to see far reaching generalizations of Gleason's Theorem for linear vector codes), but we will not attempt to do so here. It would also be wonderful to relate the functional equation of the rank enumerator to the functional equation of the symplectic theta function.

The paper is organized as follows. In the preliminary section 1, we set notation and give definitions, and discuss what we mean by "duality theory." In section 2 we give a summary of results and present some examples. In section 3 we prove the

[1]We employ the retronym "vector code" to describe a code with just one row, which before the advent of finite space-time codes, was just known as a "code."

claim above that in essence the only finite temporal correlated codes with a duality theory are the finite column distance codes and the finite rank codes. In section 4 we give a proof of the classical MacWilliams identity for linear vector codes that serves as a template of the proof for finite rank codes, which we derive in section 6. In section 5 we use the MacWilliams identity for linear vector codes to derive a similar identity for linear finite column distance codes. In section 7 we present a MacWilliams-type identity for the complete weight enumerator for finite sum-of-ranks codes. In section 8 we prove the analogue of Gleason's theorem for formally self-dual finite rank codes. In the final section 9 we explain how the matrices α and β are related, showing that the original MacWilliams identity can be considered a special case of the one for finite rank codes.

Some of the results of the paper were announced in [13].

1. Preliminaries

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 $\mathbb{F}_q$. The elements of $\mathcal{C}$ are called its *codewords*. 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 function on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q) \times \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ to the non-negative integers 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 $\mathrm{wt}(C_1) = d(C_1, 0)$, and that a code structure can be recovered from the weight via $d(C_1, C_2) = \mathrm{wt}(C_1 - C_2)$. So we can also think of a weight, which for our purposes is any function from $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ to the non-negative integers, as a code structure. We let $\mathrm{wt}_{\mathrm{cd}}$, $\mathrm{wt}_{\mathrm{rk}}$, $\mathrm{wt}_{\mathrm{sor}}$, and $\mathrm{wt}_{\mathrm{tc}}$ be the weights corresponding to the four coding structures d_{cd}, d_{rk}, d_{sor}, and d_{tc} defined in the introduction.

Remark. One can define the Hamming weight wt_{H} of a matrix to be the number of its non-zero entries. Finite matrix codes also appear as the product of two vector codes, and in the definitions of the joint weight enumerator of vector codes and the multiple weight enumerator of a vector code.

Let wt be a code structure on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$. If n is the maximal integer in the image of wt, for any finite matrix code $\mathcal{C}$ we define its *spectrum* to be the row vector $a(\mathcal{C}) = (a_i(\mathcal{C}))$ of length $n + 1$, where

$$a_i(\mathcal{C}) = \#\{C \in \mathcal{C} |\, \mathrm{wt}(C) = i\},$$

for $0 \leq i \leq n$. We define the minimal weight of $\mathcal{C}$ as

$$d = \min_{A\in\mathcal{C},\ A\neq 0} (\mathrm{wt}(A)).$$

We say two finite matrix codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are *formally equivalent* if they have the same spectrum. We define $\mathcal{C}^\perp = \{D \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q) | C \cdot D = 0,\ \forall C \in \mathcal{C}\}$. If $\mathcal{C}$ is a linear finite matrix code of dimension k, we say that $\mathcal{C}$ has parameters $[M, T, k, d]$. If $\mathcal{C}$ is an $[M, T, k, d]$ code, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}$, and $C^\perp$ is an $[M, T, k', d']$ code, where $k + k' = MT$. We say a linear code is *formally self-dual* if it is formally equivalent to its dual.

Fix M and T. We say a weight on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ has a *duality theory* if for every finite linear matrix code $\mathcal{C}$, $a(\mathcal{C}^\perp)$ depends only on $a(\mathcal{C})$. If in addition, there is an integer matrix γ such that for every finite linear code $\mathcal{C}$,

$$|\mathcal{C}| a(\mathcal{C}^\perp) = a(\mathcal{C})\gamma,\ \gamma^2 = q^{MT} I_{n+1}, \tag{2}$$

then we say that wt satisfies a *MacWilliams identity*, and that γ is the *duality matrix* of wt. (If wt defines a metric association scheme on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, γ is the eigenmatrix of the scheme.) We call a weight wt *homogeneous* if $\mathrm{wt}(C) = \mathrm{wt}(eC)$ for any non-zero $e \in \mathbb{F}_q$ and all $C \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, and its image consists of all integers between 0 and n. Akin to an argument in section 3, one can show that for a homogeneous weight, the second condition in (2) follows from the first.

If $F = \{f_0, ..., f_n\}$ is a set of $\mathbb{Q}$-linearly independent functions in $\mathbb{Q}(t)$, for t an indeterminate, we call

$$\phi_F^{\mathrm{wt}}(\mathcal{C}) = \sum_{i=0}^{n} a_i(\mathcal{C}) f_i = \sum_{i=0}^{n} a_i f_i,$$

the *F-weight enumerator* of $\mathcal{C}$. If F is understood, and the weight has a name, like the Hamming weight or rank, we will call it the Hamming weight enumerator or rank enumerator, etc. An *involutary* automorphism $*$ of $\mathbb{Q}(t)$ is one of order 2. We let $F^* = \{f_0^*, ..., f_n^*\}$.

Suppose that wt satisfies a MacWilliams identity. We will say that it has a *MacWilliams functional equation* if there is a set F as above, an involutary automorphism $*$, and a function $\psi \in \mathbb{Q}(t)$, such that for every finite linear matrix code $\mathcal{C}$,

$$\phi_F^{\mathrm{wt}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|} \psi \phi_{F^*}^{\mathrm{wt}}(\mathcal{C}). \tag{3}$$

Plugging $\mathcal{C}^\perp$ in for $\mathcal{C}$ in (3) shows that $\psi\psi^* = q^{MT}$. Indeed, if wt has a MacWilliams functional equation with $\psi\psi^* = q^{MT}$, then it is not hard to see that if wt is homogeneous then it satisfies a MacWilliams identity.

Remark: The philosophical reason for the requirement that the functional equation be of the form (3) is worthy of debate. In light of Duursma's work relating Hamming weight enumerators of Goppa codes to zeta functions of these codes, a revisionist could say that the motivation is to emulate the functional equation of zeta functions of varieties over finite fields. Or, in light of the work relating Hamming weight enumerators of vector codes to modular forms, one could say in hindsight that one wanted to mirror the functional equation of a theta function. But in reality, we of course require this form because it is the one taken by the historical MacWilliams functional equation for the Hamming weight enumerators of linear vector codes.

2. Summary of results and examples

We define two weights, $\mathrm{wt}_1(C)$ and $\mathrm{wt}_2(C)$, on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ to be *equivalent* if one is a non-zero constant multiple of the other, or if $\mathrm{wt}_2(C)$ is the same as $\mathrm{wt}_1(D)$, where D is obtained from C by a sequence of operations that either transpose two of its columns or multiplies a column by a non-zero constant. The weight that maps every element of $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ to 0 is called the trivial weight.

Theorem 1. *Assume that the weight* $\mathrm{wt}_{\mathrm{tc}}$ *on* $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ *is non-trivial and has a duality theory for some choice of* B*. Then up to equivalence:*

i) $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{rk}}$*, or*

ii) $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{cd}}$*, or*

iii) $M = 1$*, and* $T = \rho\ell$*, for some* ρ *and* ℓ*, and* $\mathrm{wt}_{\mathrm{tc}}(C)$ *of the vector* $C = (c_1, ..., c_{\rho\ell})$ *is the number of non-zero rows in the* $\rho \times \ell$ *matrix* C' *whose* j*-th row*

is $(c_j, c_{j+\rho}, ..., c_{j+(\ell-1)\rho})$. *Thus* $\mathrm{wt}_{\mathrm{tc}}(C) = \mathrm{wt}_{\mathrm{cd}}((C')^t)$, *and* $\mathrm{wt}_{\mathrm{tc}}$ *is a disguised version of the column distance weight.*

This leads us to the next two theorems:

Theorem 2. *Let* $\mathcal{C}$ *be a linear* $M \times T$ *finite column distance code over* $\mathbb{F}_q$. *For* $0 \leq r \leq T$, *let* a_r *denote the number of codewords in* $\mathcal{C}$ *of column distance weight* r. *Let* $F = \{1, t, ..., t^T\}$, *so the column distance weight enumerator of* $\mathcal{C}$ *is* $\phi_F^{\mathrm{cd}}(\mathcal{C}) = \sum_{r=0}^{T} a_r t^r$. *Let* $t \to (1-t)/(1+(q^M-1)t)$ *induce an involutary automorphism* $*$ *of* $\mathbb{Q}(t)$. *Then*

$$\phi_F^{\mathrm{cd}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}(1+(q^M-1)t)^T \phi_{F^*}^{\mathrm{cd}}(\mathcal{C}).$$

Theorem 3. *Let* $\mathcal{C}$ *be a linear* $M \times T$ *finite rank code over* $\mathbb{F}_q$. *For any* $0 \leq r \leq \min(M,T)$, *let* a_r *be the number of codewords of* $\mathcal{C}$ *of rank* r, *and let* $f_r = \prod_{j=0}^{r-1}(\frac{t-q^j}{q^{\max(M,T)}-q^j})$. *Let* $F = \{f_0, ..., f_{\min(M,T)}\}$, *so the rank enumerator of* $\mathcal{C}$ *is* $\phi_F^{\mathrm{rk}}(\mathcal{C}) = \sum_{r=0}^{\min(M,T)} a_r f_r$. *Let* $t \to q^{\max(M,T)}/t$ *induce an involutary automorphism* $*$ *of* $\mathbb{Q}(t)$. *Then*

$$\phi_F^{\mathrm{rk}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|} t^{\min(M,T)} \phi_{F^*}^{\mathrm{rk}}(\mathcal{C}).$$

Although finite sum-of-ranks codes do not have a duality theory, there is a MacWilliams-type identity for their complete weight enumerators.

Theorem 4. *Let* $\mathcal{C}$ *be a linear* $M \times \rho\ell$ *finite sum-of-ranks code over* $\mathbb{F}_q$, *consisting of* ℓ *blocks of* $M \times \rho$ *matrices. For any* $0 \leq r_i \leq \min(M,\rho)$, $1 \leq i \leq \ell$, *let* $a_{(r_1,...,r_\ell)}$ *be the number of codewords* $[N_1|\cdots|N_\ell]$ *of* $\mathcal{C}$ *with* $\mathrm{rk}(N_i) = r_i$ *for all* $1 \leq i \leq \ell$, *and let* $f_{(r_1,...,r_\ell)} = \prod_{i=1}^{\ell} f_{r_i}(t_i)$, *where the* f_i *are as in Theorem 3 and the* t_i *are independent indeterminants. Let* $F = \{f_{(r_1,...,r_\ell)} | 0 \leq r_i \leq \min(M,\rho), 1 \leq i \leq \ell\}$. *Then the complete sum-of-ranks enumerator of* $\mathcal{C}$ *is*

$$\phi_F^{\mathrm{sor}}(\mathcal{C}) = \sum_{(r_1,...,r_\ell)} a_{(r_1,...,r_\ell)} f_{(r_1,...,r_\ell)},$$

where the sum is over $0 \leq r_i \leq \min(M,\rho)$, *and* $1 \leq i \leq \ell$. *Let* $t_i \to q^{\max(M,\rho)}/t_i$, $1 \leq i \leq \ell$, *induce an involutary automorphism of* $\mathbb{Q}(t_1, ..., t_\ell)$. *Then*

$$\phi_F^{\mathrm{sor}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}(t_1 \cdots t_\ell)^{\min(M,\rho)} \phi_{F^*}^{\mathrm{sor}}(\mathcal{C}).$$

Finally, we derive a close relationship between the duality matrices for vectors codes of length n under the Hamming metric and finite rank codes of size $n \times n$. Let $U_{t,m}$ denote the number of upper-triangular matrices of rank t and size $m \times m$ defined over $\mathbb{F}_q$.

Theorem 5. *Let* $[\alpha_{k\ell}]$ *denote the duality matrix for linear vector codes of length* n *over* $\mathbb{F}_q$ *under the Hamming metric, and* $[\beta_{rs}]$ *the duality matrix for* $n \times n$ *finite linear rank codes over* $\mathbb{F}_q$. *Then if* $V_{kr} = q^{\binom{n}{2}-\binom{n-k}{2}} U_{r-k,n-k-1}$, *we have*

$$[\alpha_{k\ell}] = q^{-\binom{n}{2}} [V_{kr}][\beta_{rs}][V_{\ell s}]^{-1}.$$

EXAMPLES.

I) *Representing extension fields.* 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 weight be maximal, that is, equal to $n = \min(M,T)$. For such codes, the Singleton bound constrains k to be at most n [10]. This leads one to consider $[M,T,n,n]$ codes where $n = \min(M,T)$.

Let us consider the case $M = T = 2$. The following are representations of $\mathbb{F}_{q^2}$ as 2×2 matrices over $\mathbb{F}_q$, considered in [10], [20].

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. 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

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

One easily checks that $t^2\phi_{F^*}^{\mathrm{rk}}(\mathcal{C})/q^2 = \phi_F^{\mathrm{rk}}(\mathcal{C}^\perp)$, where $*$ is induced by $t \to q^2/t$.

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 $\phi_F^{\mathrm{rk}}(\mathcal{C}) = \phi_F^{\mathrm{rk}}(\mathcal{C}^\perp) = \frac{t^2-(q+1)t+q^2}{q^2-q}$.

II) *Some formally self-dual linear rank codes.* Take $T \geq 2$. Consider the $2 \times T$ code $\mathcal{C}_1$ where the top row of a codeword is any vector in $(\mathbb{F}_q)^T$, but the bottom row is all zeros. It is formally self dual, and its rank enumerator, which we will call g_1, is $1+(q^T-1)(t-1)/(q^T-1) = t$. Now suppose T is odd, and let $\mathcal{C}_2$ consist of $2 \times T$ matrices which are $(T-1)/2$ concatenations of the 2×2 code in Example (I), and whose last column has a top entry which is arbitrary and a bottom entry which is zero. Then $\mathcal{C}_2$ is formally self-dual, $a_0(\mathcal{C}_2) = 1, a_1(\mathcal{C}_2) = q-1$, and $a_2(\mathcal{C}_2) = q^T - q$, so its rank enumerator, which we will call g_2, is

$$1 + (q-1)(t-1)/(q^T-1) + (q^T-q)(t-1)(t-q)/(q^T-1)(q^T-q) =$$

$$(t^2 - 2t + q^T)/(q^T-1).$$

If T is even, let $\mathcal{C}_3$ by the $1 \times T$ code consisting of codewords whose first $T/2$ entries are arbitrary, and whose remaining entries are all 0. Then $\mathcal{C}_3$ is formally self-dual, and its rank enumerator, which we will call g_3, is $1+(q^{T/2}-1)(t-1)/(q^T-1)$, so $g_3 = (t+q^{T/2})/(q^{T/2}+1)$. We will return to g_1, g_2 and g_3 in section 8.

III) *Relations to upper-triangular matrices.* Theorem 3 gives a nice recursive relation for $U_{t,m}$. 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 the rank enumerator $\phi_F^{\mathrm{rk}}(\mathcal{C}) = U_{0,2} + U_{1,2}\frac{t-1}{q^3-1} + U_{2,2}\frac{(t-1)(t-q)}{(q^3-1)(q^3-q)}$, and $\phi_F^{\mathrm{rk}}(\mathcal{C}^\perp) = U_{0,3} + U_{1,3}\frac{t-1}{q^3-1} + U_{2,3}\frac{(t-1)(t-q)}{(q^3-1)(q^3-q)} +$

$U_{3,3}\frac{(t-1)(t-q)(t-q^2)}{(q^3-1)(q^3-q)(q^3-q^2)}$. The fact that $t^3\phi_{F^*}^{\mathrm{rk}}(\mathcal{C})/q^3 = \phi_F^{\mathrm{rk}}(\mathcal{C}^\perp)$, where $*$ is induced by $t \to q^3/t$, implies, for instance, that

$$U_{1,3} = (\phi_F^{\mathrm{rk}}(\mathcal{C}^\perp)|_{t=q} - U_{0,3})(q^2+q+1) = (\phi_F^{\mathrm{rk}}(\mathcal{C})|_{t=q^2} - U_{0,2})(q^2+q+1) =$$

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

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

IV) *Column distance weight enumerators.* Let us now consider the code $\mathcal{C}$ in Example (I) as a column distance code. Then as before $\mathcal{C}$ is self-dual, and once again $a_0 = 1, a_1 = 0, a_2 = q^2-1$, so $\mathcal{C}$ is $[2,2,2,2]$. However the column distance weight enumerator is

$$\phi_F^{\mathrm{cd}}(\mathcal{C}) = \phi_F^{\mathrm{cd}}(\mathcal{C}^\perp) = 1 + (q^2-1)t^2,$$

and one easily checks that $(1+(q^2-1)t)^2\phi_{F^*}^{\mathrm{cd}}(\mathcal{C})/q^2 = \phi_F^{\mathrm{cd}}(\mathcal{C}^\perp)$, where $*$ is induced by $t \to (1-t)/(1+(q^2-1)t)$.

V) *Complete rank weight enumerators.* Let $c_1 = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$ and $c_2 = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right)$, thought of as partitioned matrices with 2 blocks of 2×2 matrices over $\mathbb{F}_q$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be respectively the vector spaces spanned by c_1 and c_2. Then the sum-of-ranks spectra of $\mathcal{C}_1$ and $\mathcal{C}_2$ are identical ($a_0 = 1, a_1 = 0, a_2 = q-1$), but as we will see in the next section, the spectra of their duals are not. Theorem 4 implies that they must have different complete weight enumerators.

Indeed, the complete weight enumerator of $\mathcal{C}_1$ is

$$\phi_F^{\mathrm{sor}}(\mathcal{C}_1) = 1 + (q-1)(t_1-1)(t_2-1)/(q^2-1)^2,$$

whereas the complete weight enumerator of $\mathcal{C}_2$ is

$$\phi_F^{\mathrm{sor}}(\mathcal{C}_2) = 1 + (q-1)(t_1-1)(t_1-q)/(q^2-1)(q^2-q).$$

Note that these differ even when we set $t_2 = t_1$.

3. Only two finite temporal correlated codes have duality theories

For a fixed matrix B of size $T \times T$, we have defined a weight on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$,

$$\mathrm{wt}_{\mathrm{tc}}(C) = \mathrm{rk}(C\sharp B),$$

where we recall that $D\sharp B = (D \otimes 1_{T1}) \odot (1_{M1} \otimes B)$.

The following can be verified directly from the definition of $\sharp$.

Lemma 1. *Let A, B, and N be matrices of sizes $M \times T$, $T \times T$, and $r \times T$, respectively. Then:*

a) $A\sharp B = (A \otimes I_T)(I_T\sharp B)$.

b) $(I_T \otimes N)(I_T\sharp B) = I_T\sharp NB$.

Recall that we defined two weights, $\mathrm{wt}_1(C)$ and $\mathrm{wt}_2(C)$, on $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ to be *equivalent* if one is a non-zero constant multiple of the other, or if $\mathrm{wt}_2(C)$ is the same as $\mathrm{wt}_1(D)$, where D is obtained from C by a sequence of operations that either transpose two of its columns or multiplies a column by a non-zero constant.

Theorem 1. *Assume that the weight* $\mathrm{wt}_{\mathrm{tc}}$ *on* $\mathrm{Mat}_{M\times T}(\mathbb{F}_q)$ *is non-trivial and has a duality theory for some choice of* B*. Then up to equivalence:*

i) $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{rk}}$*, or*

ii) $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{cd}}$*, or*

iii) $M = 1$*, and* $T = \rho\ell$*, for some* ρ *and* ℓ*, and* $\mathrm{wt}_{\mathrm{tc}}(C)$ *of the vector* $C = (c_1, ..., c_{\rho\ell})$ *is the number of non-zero rows in the* $\rho \times \ell$ *matrix* C' *whose* j*-th row is* $(c_j, c_{j+\rho}, ..., c_{j+(\ell-1)\rho})$*. Thus* $\mathrm{wt}_{\mathrm{tc}}(C) = \mathrm{wt}_{\mathrm{cd}}((C')^t)$*, and* $\mathrm{wt}_{\mathrm{tc}}$ *is a disguised version of the column distance weight.*

Proof. Assume that $\mathrm{wt}_{\mathrm{tc}}$ has a duality theory for some choice of B.

Step one: We can assume B *is of the form* $[I_\rho|B']$ *for some* $\rho \leq T$*.*

For any invertible $T \times T$ matrix N, $I_M \otimes N$ is invertible, and by Lemma 1 (a) and (b),

$$(I_M \otimes N)(A\sharp B) = (I_M \otimes N)(A \otimes I_T)(I_T\sharp B) = (A \otimes N)(I_T\sharp B) =$$
$$(A \otimes I_T)(I_T \otimes N)(I_T\sharp B) = (A \otimes I_T)(I_T\sharp NB) = A\sharp NB,$$

so without loss of generality, we can assume that B is in row-reduced echelon form.

Now let $\rho \geq 1$ be the rank of B, and $\tilde{B}$ the top ρ rows of B. Then we can identify the non-zero rows of $A\sharp B$ with $A\sharp\tilde{B}$, so we might as well extend our notion of weight to include matrices B of size $\rho \times T$, but then only consider B which are row reduced of rank ρ. Also, transposing two columns of B and doing the same to A acts in the same manner on $A\sharp B$. Likewise multiplying a column of B by a constant acts in the same manner on $A\sharp B$. So we can assume up to equivalence that B is of the form $[I_\rho|B']$.

Step two: We can assume every column of B' *has one non-zero entry.*

First we can assume B contains no zero columns. If not, as above, up to equivalence we can assume the last column is 0. Then the code $\mathcal{C}_1$ consisting of all $M \times T$ matrices whose T-th column vanishes and the code $\mathcal{C}_2$ consisting of all $M \times T$ matrices whose rows sum to zero, would have the same spectrum. Yet $\mathcal{C}_1^\perp$ consists only of vectors of weight 0, whereas $\mathcal{C}_2^\perp$ contains at least one element of non-zero weight.

The result is now trivial if $\rho = 1$ or $\rho = T$, so we take $1 < \rho < T$. Now let b be any column of B' which has more than one entry that does not vanish. Up to equivalence, we might as well assume it is the first column of B'. Let $\mathcal{C}_1$ be the code consisting of all $M \times T$ matrices whose first ρ columns are identical and all of whose other columns vanish, and $\mathcal{C}_2$ the code consisting of all $M \times T$ matrices whose first $\rho+1$ columns are identical and all of whose other columns vanish. Both codes have size q^M, contain only one matrix of weight 0, and the assumed shape of B guarantees that all other codewords have weight ρ. So the spectra of $\mathcal{C}_1$ and $\mathcal{C}_2$ are identical. Now let us consider how many elements of $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$ have weight 1. Note that the dual of $\mathcal{C}_1$ is the set of matrices of the form $[D|E]$ where the sum of the rows in D is 0 and E is any matrix of size $M \times (T - \rho)$. To have weight 1, we must have $D = 0$. Therefore the elements of weight 1 in $\mathcal{C}_1^\perp$ are all the elements of the form $[0|E]$ with $\mathrm{wt}([0|E]) = 1$. This contains the subset of all such $[0|E]$ where the first column of E vanishes, and a similar analysis shows that since b has more than one non-zero entry, this subset is precisely the set of elements of $\mathcal{C}_2^\perp$ of weight 1. So we get a contradiction if we can show that there is some E whose first column does not vanish such that $[0|E]$ has weight 1. Taking the last $T - \rho - 1$ columns of

E to be 0, and taking any entry of the first column of E to be non-zero does the trick. Multiplying b by a non-zero constant, we can assume up to equivalence that it consists of one entry which is 1, and that all the other entries vanish. If the 1 is in the i-th row we will denote the column as e_i.

Step three: We can assume $B = [I_\rho|\cdots|I_\rho]$.

If $\rho = 1$, this is clear. Assume $\rho > 1$. For $1 \leq k \leq T$, suppose that B contains $d_k \geq 1$ columns of the form e_k. Suppose for some $i \neq j$ that $d_i < d_j$. Let $\mathcal{C}_i$ be the code consisting of all $M \times T$ matrices which vanish except on the d_i columns corresponding to the columns of B which are e_i, and let $\mathcal{C}_j$ denote the code consisting of all $M \times T$ matrices which vanish except on a chosen d_i columns corresponding to columns of B which are e_j. Then $\mathcal{C}_i$ and $\mathcal{C}_j$ have the same spectrum. Now the number of elements in $\mathcal{C}_i^\perp$ of weight 1 is:

$$((q^M - 1)/(q-1)) \sum_{k \neq i} (q^{d_k} - 1).$$

However, the number of matrices in the dual of $\mathcal{C}_2^\perp$ of weight 1 is:

$$((q^M - 1)/(q-1))((q^{d_j - d_i} - 1) + \sum_{k \neq j} (q^{d_k} - 1)).$$

Since $q^{d_j} - 1 \neq (q^{d_i} - 1) + (q^{d_j - d_i} - 1)$, these numbers differ. Hence we have $d_i = \ell$ for all i and some ℓ. Up to equivalence we can exchange columns, which gives us the claim. Note that $T = \rho\ell$.

Step four: If $\rho > 1$ *and* $\ell > 1$*, then* $M = 1$

Note that exchanging columns of $B = [I_\rho|\cdots|I_\rho]$ to put the columns which are e_1 leftmost, and then e_2 next leftmost, etc., then we have $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{sor}}$, so what we are showing in this step is that there is no duality theory for sum-of-ranks codes if M, ρ, ℓ are all at least 2.

Assume that $\rho \geq 2$, $\ell \geq 2$, and that $M \geq 2$. We will think of every codeword as ℓ blocks of size $M \times \rho$, and the weight of a codeword as the sum of the ranks of these blocks.

Let $\mathcal{C}_1$ be the linear $M \times \rho\ell$ code consisting of the codewords whose last $\ell - 2$ blocks are arbitrary, and whose first block vanishes in every entry except the one in the first row and first column, which is arbitrary, and whose second block consists of matrices whose last row and last column vanish, but whose entries are otherwise arbitrary. Let $\mathcal{C}_2$ be the linear $M \times \rho\ell$ code consisting of the codewords whose last $\ell - 2$ blocks are arbitrary, whose second block vanishes, and whose first block consists of matrices whose first row and first column vanish, except that the entry in the first row and first column can be arbitrary, as can all the entries not in the first row or column. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same spectrum. Now let us count the number of codewords in $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$ whose weight is 1, that is, $a_1(\mathcal{C}_1^\perp)$ and $a_1(\mathcal{C}_2^\perp)$. Note that the last $\ell - 2$ blocks of $C_1^\perp$ and $C_2^\perp$ vanish. Let $e_{m,n}$ denote the number of $m \times n$ matrices with entries in $\mathbb{F}_q$ which have rank 1. Then $a_1(\mathcal{C}_1^\perp)$ is the number of codewords whose first block has rank 1 and whose second block vanishes, call it σ_{10}, plus the number whose second block has rank 1 and whose first block vanishes, call it σ_{01}. For a matrix in $C_1^\perp$ to have a first block of rank 1, the first row or first column of the block must vanish, so $\sigma_{1,0} = e_{M-1,\rho} + e_{M,\rho-1} - e_{M-1,\rho-1}$, to avoid double-counting those blocks whose first row and first column both vanish. Likewise, for

a matrix in $C_1^\perp$ to have a second block of rank 1, the last row or last column of the block must vanish (except for their last elements). So $\sigma_{0,1} = e_{M,1} + e_{1,\rho} - e_{1,1}$. Hence

$$a_1(\mathcal{C}_1^\perp) = \sigma_{10} + \sigma_{01} = e_{M-1,\rho} + e_{M,\rho-1} - e_{M-1,\rho-1} + e_{M,1} + e_{1,\rho} - e_{1,1}.$$

A similar (but simpler) analysis shows that

$$a_1(\mathcal{C}_2^\perp) = e_{M-1,1} + e_{1,\rho-1} + e_{M,\rho}.$$

Now $e_{m,n} = (q^m - 1)(q^n - 1)/(q - 1)$. So for $a_1(\mathcal{C}_1^\perp)$ to equal $a_2(\mathcal{C}_1^\perp)$, we must have

$$(q^{M-1} - 1)(q^\rho - 1) + (q^M - 1)(q^{\rho-1} - 1) - (q^{M-1} - 1)(q^{\rho-1} - 1) +$$
$$(q^M - 1)(q - 1) + (q^\rho - 1)(q - 1) - (q - 1)^2$$
$$= (q^{M-1} - 1)(q - 1) + (q^{\rho-1} - 1)(q - 1) + (q^M - 1)(q^\rho - 1).$$

This simplifies to

$$(q^{M-1} - 1)(q^{\rho-1} - 1) = 0,$$

giving us our contradiction.

Step five: Conclusion.

We conclude that if $\mathrm{wt}_{\mathrm{tc}}$ has a duality theory, then either:
1) $\rho = 1$, so $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{rk}}$, or
2) $\ell = 1$, so $\mathrm{wt}_{\mathrm{tc}} = \mathrm{wt}_{\mathrm{cd}}$, or
3) $M = 1$, and $T = \rho\ell$, for some ρ and ℓ, and $\mathrm{wt}_{\mathrm{tc}}(C)$ of the vector $C = (c_1, ..., c_{\rho\ell})$ is the number of non-zero rows in the $\rho \times \ell$ matrix C' whose j-th row is $(c_j, c_{j+\rho}, ..., c_{j+(\ell-1)\rho})$. □

Remark. We show in sections 5 and 6 that $\mathrm{wt}_{\mathrm{rk}}$ and $\mathrm{wt}_{\mathrm{cd}}$ do have duality theories, satisfy MacWilliams Identities, and have weight enumerators that satisfy MacWilliams functional equations.

4. The classical MacWilliams identity and functional equation

To motivate the definition of rank enumerators for finite rank codes, we will present a proof of the MacWilliams identity and functional equation for Hamming weight enumerators of linear vector codes over $\mathbb{F}_q$. The proof is hardly the most direct, but it is subject to generalization. We will also partake in an exercise in revisionist history: we will start off by pretending to not know precisely how we want to define the Hamming weight enumerator, and then let the desired shape of its functional equation (3) guide us to its definition.

Let $\mathcal{C}_n$ be the collection of linear vector codes of length n over $\mathbb{F}_q$, and $a_r = a_r(\mathcal{C})$ be the number of codewords of some $\mathcal{C} \in \mathcal{C}_n$ of Hamming weight r. Let $F = \{f_i | 0 \le i \le n\}$ be elements of $\mathbb{Q}(t)$ which are linearly independent over $\mathbb{Q}$, which are to be determined later. Then we have the Hamming weight enumerator of $\mathcal{C}$, $\phi_F^{\mathrm{H}}(\mathcal{C}) = \sum_{r=0}^n a_r f_r$.

Let $b_r = a_r(\mathcal{C}^\perp)$. Using character theory or Delsarte's work on association schemes [3], one gets that there is an $(n + 1) \times (n + 1)$ integer matrix $\alpha = [\alpha_{rs}]$, such that for every $\mathcal{C} \in \mathcal{C}_n$,

$$|\mathcal{C}| b_s = \sum_{r=0}^{n} a_r \alpha_{rs}, \tag{4}$$

for all $0 \leq s \leq n$. Let $w_r = (1, ..., 1, 0, ..., 0)$, the vector with r ones followed by $n - r$ zeros.

Considering for each $0 \leq r \leq n$ the linear code generated by w_r shows that the set of all $(a_0(\mathcal{C}), ..., a_n(\mathcal{C}))$, for $\mathcal{C} \in \mathcal{C}_n$, spans $\mathbb{Q}^{n+1}$. Hence applying (4) to every $\mathcal{C}$ and its dual shows that $[\alpha_{rs}]$ is an invertible matrix, whose square is $q^n I_{n+1}$. The matrix α is the Hamming weight duality matrix, but we will pretend for the moment that we do not know what it is, and present the following method for finding it.

We call a sequence of codes $\mathcal{C}_k \in \mathcal{C}_n$, $0 \leq k \leq n$, a *dualizing sequence* if it satisfies:

i) The dimension of $\mathcal{C}_k$ is k.
ii) $\mathcal{C}_k^{\perp}$ is equivalent to $\mathcal{C}_{n-k}$.
iii) If $p_{kr} = a_r(\mathcal{C}_k)$, $0 \leq r, k \leq n$, then $[p_{kr}]$ is invertible.

We now claim that the matrix $[\alpha_{rs}]$ is completely determined by a dualizing sequence. Indeed, applying (4) to every $\mathcal{C}_k$ in a dualizing sequence, we have

$$q^k p_{n-k,s} = |\mathcal{C}_k| a_s(\mathcal{C}_{n-k}) = |\mathcal{C}_k| a_s(\mathcal{C}_k^{\perp}) = |\mathcal{C}_k| b_s = \sum_{r=0}^{n} p_{kr}\alpha_{rs}.$$

So as matrices,

$$\text{antidiag}(1, q, ..., q^n)[p_{ks}] = [p_{kr}][\alpha_{rs}],$$

where $\text{antidiag}(\gamma_0, ..., \gamma_n)$ denotes the $(n+1) \times (n+1)$ matrix N whose rows and columns are indexed by $\{0, ..., n\}$, and such $N_{i,n-i} = \gamma_i$ for $0 \leq i \leq n$, and $N_{ij} = 0$ for $j \neq n - i$.

Hence

$$[\alpha_{rs}] = [p_{kr}]^{-1}\text{antidiag}(1, q, ..., q^n)[p_{ks}]. \tag{5}$$

Our goal is to show that the Hamming weight has a MacWilliams functional equation. To proceed, we have several tasks ahead of us: choosing a dualizing sequence, and choosing a set F, an involutary automorphism $*$, and a function ψ such that $\psi\psi^* = q^n$, and such that (3) holds. We will take $*$ to be the involutary automorphism induced by the map $t \to q/t$, and $\psi = t^n$. Now again, since $(a_0(\mathcal{C}), ..., a_n(\mathcal{C}))$ for $\mathcal{C} \in \mathcal{C}_n$ spans $\mathbb{Q}^{n+1}$, multiplying (4) by f_s and summing on s shows that (3) holds if and only if

$$t^n f_r^* = \sum_{s=0}^{n} \alpha_{rs} f_s.$$

By (5), this holds if and only if

$$t^n g_k^* = q^k g_{n-k}, \tag{6}$$

where $g_k = \sum_{r=0}^{n} p_{kr} f_r$ for $0 \leq k \leq n$. We note that (6) has the rather lovely solution $g_k = t^k$, which in turn means that if we find some dualizing sequence, and then *define* $[p_{kr}]$ in terms of it, and then *define* $[f_r] = [p_{kr}]^{-1}[t^k]$, then ϕ_F^{H} will satisfy the functional equation,

$$\phi_F^{\text{H}}(\mathcal{C}^{\perp}) = \frac{1}{|\mathcal{C}|} t^n \phi_{F^*}^{\text{H}}(\mathcal{C}), \tag{7}$$

for every $\mathcal{C} \in \mathcal{C}_n$. Let us now compute $[p_{kr}]$ for some dualizing sequence. Let

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

Then it is clear that $\mathcal{C}_k$ satisfies conditions (i) and (ii) of being a dualizing sequence, and that

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

for $k \geq r$, and otherwise is 0. If $s_{rj} = (-1)^{r-j}\binom{r}{j}/(q-1)^r$ for $r \geq j$ and is otherwise 0, then $\sum_{r=0}^{n} p_{kr}s_{rj} = 0$ if $k < j$, and if $k \geq j$,

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

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

where δ_{kj} is the Kronecker delta. So $\mathcal{C}_k$ is a dualizing sequence, and following the prescription above, we set $f_r = \sum_{j=0}^{n} s_{rj}t^j = ((1-t)/(1-q))^r$. With this choice of F, (7) holds, and we get:

Theorem (MacWilliams). *Let $\mathcal{C}$ be a linear finite vector code of length n over $\mathbb{F}_q$. For $0 \leq r \leq n$, let a_r be the number of codewords of $\mathcal{C}$ of rank r, and let $f_r = ((1-t)/(1-q))^r$. Let $F = \{f_0, ..., f_n\}$ so the Hamming weight enumerator $\phi_F^{\mathrm{H}}(\mathcal{C}) = \sum_{r=0}^{n} a_r f_r$. Let $t \to q/t$ induce an involutary automorphism $*$ of $\mathbb{Q}(t)$. Then*

$$\phi_F^{\mathrm{H}}(\mathcal{C}^{\perp}) = \frac{1}{|\mathcal{C}|}t^n\phi_{F^*}^{\mathrm{H}}(\mathcal{C}).$$

Now letting $u = (1-t)/(1-q)$, so $t = 1+(q-1)u$, the map $* : t \to q/t$ corresponds to $u \to (1-u)/(1+(q-1)u)$. So (3) holds with $f_r = t^r$, $0 \leq r \leq n$, $\psi = (1+(q-1)t)^n$, and $*$ induced by $t \to (1-t)/(1+(q-1)t)$, which gives the typical statement of the MacWilliams functional equation for linear finite vector codes [22].

Note that (5) gives us the entries of the duality matrix:

$$\alpha_{rs} = \sum_{j=0}^{n} s_{rj}q^j p_{n-j,s} = (q-1)^{s-r}\sum_{j=0}^{n}(-1)^{r-j}\binom{r}{j}\binom{n-j}{s}q^j,$$

which is easily recognized as the value at s of the r^{th} Krawtchouk polynomial. Indeed, for an indeterminate z,

$$\sum_{s=0}^{n}\alpha_{rs}z^s = (1-q)^{-r}\sum_{j=0}^{r}\binom{r}{j}(-q)^j\sum_{s=0}^{n-j}\binom{n-j}{s}z^s(q-1)^s =$$

$$\frac{(1+(q-1)z)^n}{(1-q)^r}\sum_{j=0}^{r}\binom{r}{j}\left(\frac{-q}{1+(q-1)z}\right)^j =$$

$$(1+(q-1)z)^{n-r}(1-z)^r = \sum_{s=0}^{n}\sum_{j=0}^{s}\binom{r}{j}\binom{n-r}{s-j}(-1)^j(q-1)^{s-j}z^s.$$

So $\alpha_{rs} = \sum_{j=0}^{s}\binom{r}{j}\binom{n-r}{s-j}(-1)^j(q-1)^{s-j}$, which is the expression on line 53 of page 151 of [22].

5. Duality for column distance codes

Let us recall Gabidulin's method for considering an $M \times T$ finite column distance code over $\mathbb{F}_q$ as a vector code of length T over $\mathbb{F}_{q^M}$ under the Hamming metric.

Take $N \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, and let $v_1, ..., v_M$ be the rows of N. If we choose a basis $\mathcal{B} = \{b_1, ..., b_M\}$ for $\mathbb{F}_{q^M}$ over $\mathbb{F}_q$, then we can consider $\sigma_{\mathcal{B}}(N) = \sum_{i=1}^{M} b_i v_i$ as a vector of length T over $\mathbb{F}_{q^M}$. This gives a bijection $\sigma_{\mathcal{B}} : \mathrm{Mat}_{M\times T}(\mathbb{F}_q) \to (\mathbb{F}_{q^M})^T$, whose inverse we denote by $\tau_{\mathcal{B}}$. Furthermore, $\mathrm{wt}_{\mathrm{cd}}(N) = \mathrm{wt}_{\mathrm{H}}(\sigma_{\mathcal{B}}(N))$.

So $\sigma_{\mathcal{B}}$ induces a $1-1$ correspondence from finite $M \times T$ column distance codes over $\mathbb{F}_q$ to vector codes of length T over $\mathbb{F}_{q^M}$ under the Hamming metric. Note, however, that if $\mathcal{C}$ is linear over $\mathbb{F}_q$, then $\sigma_{\mathcal{B}}(\mathcal{C})$ is not necessarily linear over $\mathbb{F}_{q^M}$. For example, for any basis $\mathcal{B}$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, the column distance code $\mathcal{C}$ in Example (IV) of section 2 is $\mathbb{F}_q$-linear, but $\sigma_{\mathcal{B}}(\mathcal{C})$ is not $\mathbb{F}_{q^2}$-linear. Hence linear finite column distance codes need separate study.

In particular, a MacWilliams identity and functional equation for finite linear column distance codes do not follow directly from those for linear vector codes. However, we will see that they do follow not *that* indirectly.

Since the trace $\mathrm{Tr}_{\mathbb{F}_{q^M}/\mathbb{F}_q}$ from $\mathbb{F}_{q^M}$ to $\mathbb{F}_q$ is surjective, for every non-trivial additive character $\chi : \mathbb{F}_q \to \mathbb{C}^*$ the induced character $\chi' = \chi \circ \mathrm{Tr}_{\mathbb{F}_{q^M}/\mathbb{F}_q} : \mathbb{F}_{q^M} \to \mathbb{C}^*$ is non-trivial.

Also note that if $\mathcal{B}' = \{b'_1, ..., b'_M\}$ is the dual basis to $\mathcal{B}$, i.e., $\mathrm{Tr}_{\mathbb{F}_{q^M}/\mathbb{F}_q}(b_i b'_j) = \delta_{ij}$, then for $A, D \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, $A \cdot D$ coincides with the trace from $\mathbb{F}_{q^M}$ to $\mathbb{F}_q$ of the standard dot product $\cdot$ of the vectors $\sigma_{\mathcal{B}}(A)$ and $\sigma_{\mathcal{B}'}(D)$.

Now let $\mathcal{C}$ be a finite linear $M \times T$ column distance code over $\mathbb{F}_q$. For $0 \le r \le T$, let $a_r = a_r(\mathcal{C})$ denote the number of codewords in $\mathcal{C}$ of column weight r. Following the standard character theoretic proof of MacWilliams identities, consider the double sum

$$S = \sum_{D\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} t^{\mathrm{wt}_{\mathrm{cd}}(D)} \sum_{A\in\mathcal{C}} \chi(A \cdot D) = \sum_{D\in\mathcal{C}^\perp} |\mathcal{C}| t^{\mathrm{wt}_{\mathrm{cd}}(D)} = |\mathcal{C}| \sum_{r=0}^{T} a_r(\mathcal{C}^\perp) t^r.$$

On the other hand, exchanging the order of summation,

$$\begin{aligned} S &= \sum_{A\in\mathcal{C}} \sum_{D\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(A \cdot D) t^{\mathrm{wt}_{\mathrm{cd}}(D)} \\ &= \sum_{A\in\mathcal{C}} \sum_{D\in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi'(\sigma_{\mathcal{B}}(A) \cdot \sigma_{\mathcal{B}'}(D)) t^{\mathrm{wt}_{\mathrm{H}}(\sigma_{\mathcal{B}'}(D))} \\ &= \sum_{A\in\mathcal{C}} \sum_{E\in(\mathbb{F}_{q^M})^T} \chi'(\sigma_{\mathcal{B}}(A) \cdot E) t^{\mathrm{wt}_{\mathrm{H}}(E)}. \end{aligned}$$

If $\mathrm{wt}_{\mathrm{H}}(\sigma_{\mathcal{B}}(A)) = r$, there is a non-singular $T \times T$ matrix U with entries in $\mathbb{F}_{q^M}$ such that $\sigma_{\mathcal{B}}(A)U = w_r$. Since $\sigma_{\mathcal{B}}(A) \cdot E = \sigma_{\mathcal{B}}(A)U \cdot E(U^{-1})^t$, and $E \to E(U^{-1})^t$ is a permutation of $(\mathbb{F}_{q^M})^T$, this last inner sum depends only on r. Hence it is of the form $\sum_{s=0}^{T} \epsilon_{rs} t^s$ for some algebraic integers ϵ_{rs}. Since all conjugates of $\chi'(\sigma_{\mathcal{B}}(A)\cdot E)$ are of the form $\chi'(\sigma_{\mathcal{B}}(A) \cdot E)^m = \chi'(\sigma_{\mathcal{B}}(mA) \cdot E)$ for some m prime to q, the ϵ_{rs} are rational integers.

Therefore

$$|\mathcal{C}| \sum_{r=0}^{T} a_r(\mathcal{C}^\perp) t^r = \sum_{r,s=0}^{T} \epsilon_{rs} a_r(\mathcal{C}) t^s,$$

so

$$a_s(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}\sum_{r=0}^{T} a_r(\mathcal{C})\epsilon_{rs}.$$

Since the Hamming weight spectra of the $\mathbb{F}_{q^M}$-linear vector codes of length T span $\mathbb{Q}^{T+1}$, applying this to $\mathcal{C} = \tau_{\mathcal{B}}(\mathcal{C}')$ for every $\mathbb{F}_{q^M}$-linear code $\mathcal{C}'$ in $(\mathbb{F}_{q^M})^T$ shows that the duality matrix $[\epsilon_{rs}]$ is the same as the one for linear vector codes of length T over $\mathbb{F}_{q^M}$ under the Hamming metric. Hence as in section 4, letting $f_r = ((1-t)/(1-q^M))^r$, $0 \le r \le T$, we get

$$\phi_F^{\mathrm{cd}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}t^T\phi_{F^*}^{\mathrm{cd}}(\mathcal{C}),$$

where $\phi_F^{\mathrm{cd}}(\mathcal{C}) = \sum_{r=0}^{T} a_r((1-t)/(1-q^M))^r$, and $*$ is induced by $t \to q^M/t$. Now letting $u = (1-t)/(1-q^M)$, so $t = 1+(q^M-1)u$, the map $* : t \to q^M/t$ corresponds to $u \to (1-u)/(1+(q^M-1)u)$. Hence we get:

Theorem 2. *Let $\mathcal{C}$ be a linear $M \times T$ finite column distance code over $\mathbb{F}_q$. For $0 \le r \le T$, let a_r denote the number of codewords in $\mathcal{C}$ of column distance weight r. Let $F = \{1, t, ..., t^T\}$, so the column distance weight enumerator of $\mathcal{C}$ is $\phi_F^{\mathrm{cd}}(\mathcal{C}) = \sum_{r=0}^{T} a_r t^r$. Let $t \to (1-t)/(1+(q^M-1)t)$ induce an involutary automorphism $*$ of $\mathbb{Q}(t)$. Then*

$$\phi_F^{\mathrm{cd}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}(1+(q^M-1)t)^T\phi_{F^*}^{\mathrm{cd}}(\mathcal{C}).$$

6. A MacWilliams functional equation for rank enumerators

Let $n = \min(M, T)$, and let $\mathcal{C}_{M\times T}$ denote the set of linear $M \times T$ finite rank codes over $\mathbb{F}_q$. For any $\mathcal{C} \in \mathcal{C}_{M\times T}$ and $0 \le r \le n$, let $a_r = a_r(\mathcal{C})$ denote the number of codewords in $\mathcal{C}$ of rank r. Then we define $a : \mathcal{C}_{M\times T} \to \mathbb{Q}^{n+1}$ by $a = (a_0, ..., a_n)$. For $0 \le r \le n$, let W_r denote the matrix which is I_r for its first r rows and columns and whose other entries all vanish. For any $A \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, let $\{A\}$ be the linear code generated by A. Considering $\{W_r\}$ for $0 \le r \le n$ shows:

Lemma 2. *$a(\mathcal{C}_{M\times T})$ is a spanning set of $\mathbb{Q}^{n+1}$ as a $\mathbb{Q}$-vector space.*

Let $F = \{f_r | 0 \le r \le n\}$ 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 as before we define an F-rank enumerator $\phi_F^{\mathrm{rk}}(\mathcal{C}) = \sum_{r=1}^{n} a_r f_r$.

By either character theory or using association schemes, Delsarte [4], [6] showed that there is an integer $(n+1)\times(n+1)$ matrix $\beta = [\beta_{rs}]$ such that for every $\mathcal{C} \in \mathcal{C}_{M\times T}$, we have

$$|\mathcal{C}|b_s = \sum_{r=0}^{n} a_r\beta_{rs}, \tag{8}$$

for all $0 \le s \le n$, where $b_s = a_s(\mathcal{C}^\perp)$. Note that applying (8) to every $\mathcal{C}$ and its dual, Lemma 2 shows that $[\beta_{rs}]$ is an invertible matrix, whose square is $q^{MT}I_{n+1}$.

Following the template of section 4, we now define a *dualizing sequence* $\mathcal{C}_k \in \mathcal{C}_{M\times T}$, $0 \le k \le n$ to be one such that:

i) $\mathcal{C}_k^\perp$ is formally equivalent to $\mathcal{C}_{n-k}$.
ii) If $p_{kr} = a_r(\mathcal{C}_k)$, then $[p_{kr}]$ is invertible.

We will call $[p_{kr}]$ the *associated matrix* of the dualizing sequence. Suppose that the dimension of $\mathcal{C}_k$ is e_k. We will call $\{e_k\}$, $0 \leq k \leq n$, the *associated dimensions* of the dualizing sequence.

Now suppose we have a dualizing sequence. Applying (8) to every $\mathcal{C}_k$ we have

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

So as matrices

$$\text{antidiag}(q^{e_0}, ..., q^{e_n})[p_{ks}] = [p_{kr}][\beta_{rs}],$$

hence,

$$[\beta_{rs}] = [p_{kr}]^{-1} \text{antidiag}(q^{e_0}, ..., q^{e_n})[p_{ks}]. \tag{9}$$

Take $*$ to be any involutary automorphism of $\mathbb{Q}(t)$ and ψ any function such that $\psi\psi^* = q^{MT}$. Then as in (3), we want a $*$ and ψ such that the MacWilliams functional equation,

$$|\mathcal{C}| \phi_F^{\text{rk}}(\mathcal{C}^{\perp}) = \psi \phi_{F^*}^{\text{rk}}(\mathcal{C}), \tag{10}$$

holds for every $\mathcal{C} \in \mathcal{C}_{M \times T}$. Again by Lemma 2, multiplying (8) by f_s and summing on s shows that (10) holds if and only if,

$$\psi f_r^* = \sum_{s=0}^{n} \beta_{rs} f_s,$$

so by (9), if and only if

$$\psi g_k^* = q^{e_k} g_{n-k}, \tag{11}$$

where $g_k = \sum_{r=0}^{n} p_{kr} f_r$ for $0 \leq k \leq n$. Hence if we find some dualizing sequence, with associated matrix $[p_{kr}]$ and dimensions e_k, and an involutary automorphism $*$ and a function ψ such that $\psi\psi^* = q^{MT}$, and g_k satisfying (11), and then *define* $[f_r] = [p_{kr}]^{-1}[g_k]$, then ϕ_F^{rk} will satisfy (10).

If $M \geq T$, $n = T$, and we let $\mathcal{C}_k$ be the collection of partitioned matrices $(N|0_{M,T-k})$, where $N \in \text{Mat}_{M \times k}$. If $M \leq T$, $n = M$, and we let C_k be the collection of the transposes of the partitioned matrices $(N|0_{T,M-k})$ where $N \in \text{Mat}_{T \times k}$. 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 use a classical calculation [17] that shows that $p_{kr} = \begin{bmatrix} k \\ r \end{bmatrix} \begin{bmatrix} m \\ r \end{bmatrix} \mu_r (-1)^r q^{\binom{r}{2}}$, if $r \leq k$, where:

$$\mu_r = (1-q) \cdots (1-q^r), \ \begin{bmatrix} k \\ r \end{bmatrix} = \mu_k / \mu_r \mu_{k-r}, \tag{12}$$

and $m = \max(M, T)$. If $r > k$, $p_{kr} = 0$. Here $\begin{bmatrix} k \\ r \end{bmatrix}$ is the classical *generalized binomial coefficient* or *q-binomial coefficient*. For any $N \geq 0$ it satisfies the Newton identity [14],

$$\prod_{i=0}^{N-1} (1 + q^i x) = \sum_{i=0}^{N} \begin{bmatrix} N \\ i \end{bmatrix} q^{\binom{i}{2}} x^i. \tag{13}$$

Let $s_{rj} = (-1)^{r-j} \begin{bmatrix} r \\ j \end{bmatrix} q^{\binom{r-j}{2}} / \frac{\mu_m}{\mu_{m-r}} (-1)^r q^{\binom{r}{2}}$ for $j \leq r$, and $s_{rj} = 0$ if $j > r$. Then by (12) and (13), $\sum_{r=0}^{n} p_{kr} s_{rj} = 0$ if $k < j$, and if $k \geq j$,

$$\sum_{r=0}^{n} p_{kr} s_{rj} = \sum_{r=j}^{k} \begin{bmatrix} k \\ r \end{bmatrix} \begin{bmatrix} r \\ j \end{bmatrix} q^{\binom{r-j}{2}} (-1)^{r-j} = \sum_{r=j}^{k} \begin{bmatrix} k-j \\ r-j \end{bmatrix} \begin{bmatrix} k \\ k-j \end{bmatrix} q^{\binom{r-j}{2}} (-1)^{r-j} =$$

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

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 exponents $e_k = km$. 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 $\psi g_k^* = q^{km} g_{n-k}$. Hence if in the manner prescribed above we set $[f_r] = [p_{kr}]^{-1} g_k$, then by (13), $f_r =$

$$\sum_{j=0}^{n} s_{rj}t^j = \frac{\mu_{m-r}}{\mu_m}\sum_{j=0}^{r}\begin{bmatrix}r\\ j\end{bmatrix}q^{\binom{j}{2}}(-q^{1-r}t)^j = \frac{\mu_{m-r}}{\mu_m}\prod_{j=0}^{r-1}(1-q^{-j}t) = \prod_{j=0}^{r-1}\left(\frac{t-q^j}{q^m-q^j}\right),$$

and we have shown with our choices of $*$, ψ, and F, (10) holds:

Theorem 3. *Let $\mathcal{C}$ be a linear $M \times T$ finite rank code over $\mathbb{F}_q$. For any $0 \le r \le \min(M,T)$, let a_r be the number of codewords of $\mathcal{C}$ of rank r, and let $f_r = \prod_{j=0}^{r-1}\left(\frac{t-q^j}{q^{\max(M,T)}-q^j}\right)$. Let $F = \{f_0, ..., f_{\min(M,T)}\}$, so the rank enumerator of $\mathcal{C}$ is $\phi_F^{\mathrm{rk}}(\mathcal{C}) = \sum_{r=0}^{\min(M,T)} a_r f_r$. Let $t \to q^{\max(M,T)}/t$ induce an involutary automorphism $*$ of $\mathbb{Q}(t)$. Then*

$$\phi_F^{\mathrm{rk}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}t^{\min(M,T)}\phi_{F^*}^{\mathrm{rk}}(\mathcal{C}).$$

The entries β_{rs} are values of q-Krawtchouk polynomials, whose formulation is due to Delsarte [4]. Delsarte computed the β_{rs} in two different ways [4], [6], and Stanton [24] gave a different method of computing them (which he traces back to work of Carlitz and Hodges [16].) We do not see how to immediately reduce our formula (9) for β_{rs} to any previously known formulas for q-Krawtchouk polynomials.

Remark: For use in the next section, there is a consequence of Theorem 4 we would like to note. Let χ be any non-trivial additive character on $\mathbb{F}_q$, and f_r as in Theorem 3. Fix an $A \in \mathrm{Mat}_{M\times T}(\mathbb{F}_q)$, and let $S = \sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(A\cdot B) f_{\mathrm{rk}(B)}$. Using the standard character theoretic argument akin to that in section 5, for any finite rank code $\mathcal{C}$ we get that

$$|\mathcal{C}|\phi_F^{\mathrm{rk}}(\mathcal{C}^\perp) = \sum_{A\in\mathcal{C}}\sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} \chi(A\cdot B) f_{\mathrm{rk}(B)}.$$

Applying this to $\mathcal{C} = \{A\}$ and $\mathcal{C} = \{0\}$ gives,

$$q\phi_F^{\mathrm{rk}}(\{A\}^\perp) = (q-1)S + \sum_{B\in\mathrm{Mat}_{M\times T}(\mathbb{F}_q)} f_{\mathrm{rk}(B)} = (q-1)S + \phi_F^{\mathrm{rk}}(\{0\}^\perp).$$

Hence by Theorem 3,

$$S = \frac{q\phi_F^{\mathrm{rk}}(\{A\}^\perp) - \phi_F^{\mathrm{rk}}(\{0\}^\perp)}{q-1} = \frac{t^{\min(M,T)}\phi_{F^*}^{\mathrm{rk}}(\{A\}) - t^{\min(M,T)}\phi_{F^*}^{\mathrm{rk}}(\{0\})}{q-1}$$

$$= \frac{t^{\min(M,T)}}{q-1}(1+(q-1)f^*_{\mathrm{rk}(A)} - 1) = t^{\min(M,T)} f^*_{\mathrm{rk}(A)}.$$

7. An identity for finite sum-of-ranks codes

As we saw in the remark of section 3, unless $M = 1$, or $\rho = 1$, or $\ell = 1$, finite sum-of-ranks codes do not have a duality theory. As a consolation, we do get a nice duality relationship for the *complete sum-of-ranks enumerator* of a linear $T \times \rho\ell$ code over $\mathbb{F}_q$, i.e., where if each N_i is of size $M \times \rho$, the weight wt of $[N_1|...|N_\ell]$ is the vector $\mathrm{wt}([N_1|...|N_\ell]) = (\mathrm{rk}(N_1), ..., \mathrm{rk}(N_\ell))$.

Indeed, let $\mathcal{C}$ be a linear $M \times \rho\ell$ finite sum-of-ranks code over $\mathbb{F}_q$, each codeword consisting of ℓ blocks of $M \times \rho$ matrices. For any $0 \leq r_i \leq \min(M, \rho)$, $1 \leq i \leq \ell$, let $a_{(r_1,...,r_\ell)}$ be the number of codewords $[N_1|\cdots|N_\ell]$ of $\mathcal{C}$ with $\mathrm{rk}(N_i) = r_i$ for all $1 \leq i \leq \ell$. Let $t_1, ..., t_\ell$ be independent indeterminants, and $f_r(t) = \prod_{j=0}^{r-1}(\frac{t-q^j}{q^m-q^j})$, $m = \max(M, \rho)$, as for finite rank codes, and define $f_{\mathrm{wt}([N_1|...|N_\ell])} = \prod_{i=1}^{\ell} f_{\mathrm{rk}(N_i)}(t_i)$. Let $n = \min(M, \rho)$, and let $F = \{f_{(r_1,...,r_\ell)} | 0 \leq r_i \leq n, 1 \leq i \leq \ell\}$. Define the complete sum-of-ranks enumerator of $\mathcal{C}$ to be

$$\phi_F^{\mathrm{sor}}(\mathcal{C}) = \sum_{(r_1,...,r_\ell)} a_{(r_1,...,r_\ell)} f_{(r_1,...,r_\ell)},$$

where the sum is over $0 \leq r_i \leq n$, and $1 \leq i \leq \ell$.

Then as in section 4, for any non-trivial additive character χ on $\mathbb{F}_q$ we get,

$$|\mathcal{C}|\phi_F^{\mathrm{sor}}(\mathcal{C}^\perp) = \sum_{A=[A_1|...|A_\ell]\in\mathcal{C}} \Big(\sum_{B=[B_1|...|B_\ell]\in \mathrm{Mat}_{M\times\rho\ell}(\mathbb{F}_q)} \chi(A \cdot B) f_{\mathrm{wt}(B)} \Big) =$$

$$\sum_{A=[A_1|...|A_\ell]\in\mathcal{C}} \prod_{i=1}^{\ell} \sum_{B_i \in \mathrm{Mat}_{M\times\rho}(\mathbb{F}_q)} \chi(A_i \cdot B_i) f_{\mathrm{rk}(B_i)},$$

by the homomorphic property of χ, since $A \cdot B = \sum_{i=1}^{\ell} A_i \cdot B_i$. We can now use the remark of the last section to rewrite this as:

$$|\mathcal{C}|\phi_F^{\mathrm{sor}}(\mathcal{C}^\perp) = \sum_{A=[A_1|...|A_\ell]\in\mathcal{C}} \prod_{i=1}^{\ell} {t_i}^n f_{\mathrm{rk}(A_i)}(q^m/t_i) =$$

$$(t_1 \cdots t_\ell)^n \sum_{A\in\mathcal{C}} f^*_{\mathrm{wt}(A)} = (t_1 \cdots t_\ell)^n \phi_{F^*}^{\mathrm{sor}}(\mathcal{C}),$$

where $*$ is the involutary automorphism of $F(t_1, ..., t_\ell)$ which sends each t_i to q^m/t_i. Hence we get:

Theorem 4. *Let $\mathcal{C}$ be a linear $M \times \rho\ell$ finite sum-of-ranks code over $\mathbb{F}_q$, each codeword consisting of ℓ blocks of $M \times \rho$ matrices. For any $0 \leq r_i \leq \min(M, \rho)$, $1 \leq i \leq \ell$, let $a_{(r_1,...,r_\ell)}$ be the number of codewords $[N_1|\cdots|N_\ell]$ of $\mathcal{C}$ with $\mathrm{rk}(N_i) = r_i$ for all $1 \leq i \leq \ell$, and let $f_{(r_1,...,r_\ell)} = \prod_{i=1}^{\ell} f_{r_i}(t_i)$, where the f_i are as in Theorem 3. Let $F = \{f_{(r_1,...,r_\ell)} | 0 \leq r_i \leq \min(M, \rho), 1 \leq i \leq \ell\}$. Then the complete sum-of-ranks enumerator of $\mathcal{C}$ is*

$$\phi_F^{\mathrm{sor}}(\mathcal{C}) = \sum_{(r_1,...,r_\ell)} a_{(r_1,...,r_\ell)} f_{(r_1,...,r_\ell)},$$

where the sum is over $0 \leq r_i \leq \min(M, \rho)$, and $1 \leq i \leq \ell$. Let $t_i \to q^{\max(M,\rho)}/t_i$, $1 \leq i \leq \ell$, induce an involutary automorphism of $\mathbb{Q}(t_1, ..., t_\ell)$. Then

$$\phi_F^{\mathrm{sor}}(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}(t_1 \cdots t_\ell)^{\min(M,\rho)} \phi_{F^*}^{\mathrm{sor}}(\mathcal{C}).$$

8. An analogue of Gleason's Theorem

Because of the functional equation of the rank enumerator, there is an analogue of Gleason's Theorem for linear finite rank codes [22]. First let us introduce the homogeneous version of the rank enumerator for $M \times T$ codes. Without loss of generality, we take $M \leq T$. It is

$$f_{\mathcal{C}}^{\mathrm{rk}}(X,Y) = Y^M \phi_F^{\mathrm{rk}}(\mathcal{C})|_{t=X/Y},$$

where we always take the choice of F as in Theorem 3. Using this, we can now rewrite the MacWilliams functional equation for rank enumerators as

$$f_{\mathcal{C}^\perp}^{\mathrm{rk}}(X,Y) = \frac{1}{|\mathcal{C}|} f_{\mathcal{C}}^{\mathrm{rk}}(q^T Y, X).$$

For example, if we call G_1, G_2, and G_3 respectively the homogeneous versions of g_1, g_2, and g_3 from Example (II) of section 2, for the codes C_1, C_2, and C_3, then they are:

$$G_1 = f_{\mathcal{C}_1}^{\mathrm{rk}}(X,Y) = XY,$$
$$G_2 = f_{\mathcal{C}_2}^{\mathrm{rk}}(X,Y) = (X^2 - 2XY + q^T Y^2)/(q^T - 1),$$
$$G_3 = f_{\mathcal{C}_3}^{\mathrm{rk}}(X,Y) = (X + q^{T/2} Y)/(q^{T/2} + 1).$$

Suppose now that $\mathcal{C}$ is formally self-dual. Then $|\mathcal{C}| = q^{MT/2}$, and MT is necessarily even. We get

$$f_{\mathcal{C}}^{\mathrm{rk}}(X,Y) = f_{\mathcal{C}}^{\mathrm{rk}}(q^{T/2} Y, q^{-T/2} X),$$

so $f_{\mathcal{C}}^{\mathrm{rk}}(X,Y)$ is invariant under the involution $(X,Y) \to (q^{T/2}Y, q^{-T/2}X)$. It follow from a calculation in Chapter 19, Section 2 of [22], that the ring of homogeneous polynomials invariant under this transformation has a generator of degree 1 and a generator of degree 2. Suppose T is even. One candidate for the former is G_3, and G_1 will work for the latter. Since they are algebraically independent, they generate the full ring of homogeneous polynomials invariant under this involution. If T is odd, then M is necessarily even, so $f_{\mathcal{C}}^{\mathrm{rk}}(X,Y)$ is also invariant under the involution $(X,Y) \to (-X,-Y)$. Another calculation in Chapter 19, Section 2 of [22], shows that now the ring of homogeneous polynomials invariant under both these involutions is generated by two polynomials of degree 2. Note that G_1 and G_2 are invariant under both these involutions, and algebraically independent, so generate the full ring of invariants.

So in both cases we have come up with $M \times T$ codes whose homogeneous rank enumerators generate the full ring of invariant homogeneous polynomials, but that does not imply that every monomial in the generators occurs as a rank enumerator. Unlike the case of vector codes under the Hamming metric, one cannot relate the rank enumerator of a direct sum of two finite rank codes to the product of their rank enumerators. Also, since the involutions, and hence their invariants, depend on T, they only apply to formally self-dual $M \times T$ codes for fixed T and with $M \leq T$.

9. Relationship between the duality relations for linear vector codes and linear finite rank codes.

We will now compare the duality matrices for linear vector codes of length n under the Hamming metric and for finite linear $M \times T$ rank codes. We will show that taking $M = T = n$, one duality matrix is similar to a constant multiple of the other. As in sections 4 and 6, let $\mathcal{C}_n$ denote the collection of all linear vector codes

of length n over $\mathbb{F}_q$, and $\mathcal{C}_{n\times n}$ the collection of all linear $n\times n$ finite space-time codes over $\mathbb{F}_q$. We define a map $\lambda : \mathcal{C}_n \to \mathcal{C}_{n\times n}$ by defining $\lambda(\mathcal{C})$ 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 $\lambda(\mathcal{C})$. It is not hard to see that if the dimension of $\mathcal{C}$ is k, then the dimension of $\tilde{\mathcal{C}}$ is $k+\binom{n}{2}$. 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 $a_r = a_r(\mathcal{C})$, $b_r = a_r(\mathcal{C}^\perp)$, $\tilde{a}_r = \tilde{a}_r(\tilde{\mathcal{C}})$, $\tilde{b}_r = \tilde{a}_r(\tilde{\mathcal{C}}^\perp) = \tilde{a}_r(\widetilde{\mathcal{C}^\perp})$, where for $D \in \mathcal{C}_n$, $a_r(D)$ denotes the number of codewords of D of Hamming weight r, and for $D \in \mathcal{C}_{n\times n}$, $\tilde{a}_r(D)$ denotes the number of codewords of rank r. Then from (4) and (18) we have

$$|\mathcal{C}|[b_0,...,b_n] = [a_0,...,a_n][\alpha_{rs}],\ |\tilde{\mathcal{C}}|[\tilde{b}_0,...,\tilde{b}_n] = [\tilde{a}_0,...,\tilde{a}_n][\beta_{rs}], \tag{14}$$

where $[\alpha_{rs}]$ and $[\beta_{rs}]$ are respectively the duality matrices for $\mathcal{C}_n$ under the Hamming weight and for $\mathcal{C}_{n\times n}$ under the rank weight. 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 (III) of section 2).

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 $\binom{n}{2}-\binom{n-u}{2}$ non-diagonal entries that lie in its $j_1^{st},...,j_u^{th}$ rows and columns. Hence

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

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

$$[\tilde{a}_0,...,\tilde{a}_n] = [a_0,...,a_n][V_{kr}],\ \text{and}\ [\tilde{b}_0,...,\tilde{b}_n] = [b_0,...,b_n][V_{kr}]. \tag{15}$$

Putting (14) and (15) together we have

$$[a_0,...,a_n][V_{kr}][\beta_{rs}] = [\tilde{a}_0,...,\tilde{a}_n][\beta_{rs}] = |\tilde{\mathcal{C}}|[\tilde{b}_0,...,\tilde{b}_n] =$$

$$|\mathcal{C}|q^{\binom{n}{2}}[b_0,...,b_n][V_{\ell s}] = q^{\binom{n}{2}}[a_0,...,a_n][\alpha_{k\ell}][V_{\ell s}]. \tag{16}$$

As in section 4, let $w_r = (1,...,1,0,...,0)$, the vector with r ones followed by $n-r$ zeros. Considering $\lambda(\{w_r\})$ for each $0 \le r \le n$, shows that $[\tilde{a}_0,...,\tilde{a}_n]$ forms a spanning set of $\mathbb{Q}^{n+1}$ as $\mathcal{C}$ varies. Hence from (16) we have that

$$[V_{kr}][\beta_{rs}] = q^{\binom{n}{2}}[\alpha_{k\ell}][V_{\ell s}],$$

and from (15) that $[V_{kr}]$ is invertible. Therefore we have shown:

Theorem 5. *Let $[\alpha_{k\ell}]$ denote the duality matrix for linear vector codes of length n over $\mathbb{F}_q$ under the Hamming metric, and $[\beta_{rs}]$ the duality matrix for $n\times n$ finite linear rank codes over $\mathbb{F}_q$. Then if $V_{kr} = q^{\binom{n}{2}-\binom{n-k}{2}} U_{r-k,n-k-1}$, we have*

$$[\alpha_{k\ell}] = q^{-\binom{n}{2}}[V_{kr}][\beta_{rs}][V_{\ell s}]^{-1}.$$

Remarks. 1) This implies that the classical MacWilliams identity for linear vector codes can be derived from the MacWilliams identity for finite linear rank codes, so the latter can be considered a generalization of the former.

2) Rewriting Theorem 5 as $[\beta_{rs}] = q^{\binom{n}{2}}[V_{kr}]^{-1}[\alpha_{k\ell}][V_{\ell s}]$, gives another formula for values of q-Krawtchouk polynomials attached to square matrices.

References

[1] P. Campion. *Linear codes with given automorphism groups.* Discrete Math. 3 (1972), 33–45.

[2] P. Dayal, M. Varanasi, *Unified multi-antenna code design for fading channels with spatio-temporal correlations.* Proc. Asilomar Conf. on Signals, Systems and Computers, Monterey, CA, Nov. 2004.

[3] P. Delsarte, *An algebraic approach to the association schemes of coding theory*. Philips Res. Rep. Suppl. No. 10, (1973).

[4] P. Delsarte, *Association schemes and t-designs in regular semilattices*, J. Comb. Theory Ser. A 20 (1976), no. 2, 230–243.

[5] P. Delsarte, *Properties and applications of the recurrence* $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n) + q^kF(i,k,n)$, SIAM J. Appl. Math, **31**, No. 2. (1976), 262–270.

[6] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory.* J. Combin. Theory Ser. A **25** (1978), 226–241.

[7] I. Duursma, *From weight enumerators to zeta functions*. Discrete Appl. Math. 111 (2001), no. 1-2, 55–73.

[8] I. Duursma, *A Riemann hypothesis analogue for self-dual codes*. Codes and association schemes (Piscataway, NJ, 1999), 115–124, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 56, Amer. Math. Soc., Providence, RI, 2001.

[9] W. Eberling, *Lattices and codes*, Friedr. Vieweg & Sohn, Braunschweig, 2nd Ed., 2002.

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

[11] D. Grant and M. Varanasi, *The Equivalence of Space-Time Codes and Codes defined over Finite Fields and Galois Rings*, submitted.

[12] D. Grant and M. Varanasi, *Non-associative division algebras and the construction of space-time codes.* In preparation.

[13] D. Grant and M. Varanasi, *Weight enumerators and a MacWilliams-type identity for space-time rank codes over finite fields.* Proceedings of the 43rd Annual Allerton Conference on Communication, Control, and Computing, Urbana, IL, October 2005.

[14] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 5th edition, 1980.

[15] 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.

[16] J. Hodges. *Exponential sums for symmetric matrices in a finite field.* Arch. Math. 7 (1956), 116–121.

[17] G. Landsberg, *Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe*. Journal für die reine und angewandte Mathematik **111** (1893), 87–88.

[18] 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.

[19] P. Lusina, E. Gabidulin, M. Bossert. *Maximal rank distance codes as space-time codes*. IEEE Trans. Inform. Theory **49**. No. 10, (2003), 2757–2760.

[20] 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.

[21] 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), 1709–1730.

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

[23] G. Nebe, E/ Rains, and N. J. A. Sloane. *Self-Dual Codes and Invariant Theory.* Algorithms and Computation in Mathematics. Springer, 2006.

[24] D. Stanton. *A partially ordered set and q-Krawtchouk polynomials.* J. Combin. Theory, Ser. A **30**, (1981), 276–284.

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395 USA
E-mail address: grant@colorado.edu

Department of Electrical and Computer Engineering, University of Colorado at Boulder, Boulder, Colorado 80309-0425 USA
E-mail address: varanasi@colorado.edu