Codes, Systems and Extension Theorems in the Hamming and Rank metric

Sijpesteijn, T.

T.J. Sijpesteijn

Codes, Systems and Extension Theorems in the Hamming and Rank metric

---

MSc Mathematics | Masterscriptie

Supervisor: Dr Peter Bruin

Universiteit Leiden

Mathematisch Instituut, Universiteit Leiden

Contents

Conventions & Notation

$\mathbb{Z}$	The integers.
$\mathbb{F}_q$	A finite field with q elements, with q a prime power.
$\mathrm{Mat}_{m\times n}(\mathbb{F}_q)$	The set of $m \times n$ matrices with entries in $\mathbb{F}_q$.
$V^\vee$	The dual of a vector space V.
k^*	The multiplicative group $k \setminus \{0\}$ for a field k.
$[n]$	The set $\{1, \ldots, n\} \subseteq \mathbb{Z}_{\geq 1}$.
π_i	The projection map on the i-th coordinate.
$A^\top$	The transpose of a matrix A.
$\mathrm{rowsp}(A)$ ..	The space generated by the rows of a matrix A.
$\mathrm{colsp}(A)$ ...	The space generated by the columns of a matrix A.
$\mathrm{supp}^{\mathrm{H}}(c)$ ...	The Hamming support of a codeword $c \in \mathbb{F}_q^n$.
$\mathrm{supp}^{\mathrm{rk}}(v)$ ..	The rank support of a codeword $v \in \mathbb{F}_{q^m}^n$.
$\mathrm{wt}^{\mathrm{H}}(c)$	The Hamming weight of a codeword $c \in \mathbb{F}_q^n$.
$\mathrm{wt}^{\mathrm{rk}}(v)$	The rank weight of a codeword $v \in \mathbb{F}_{q^m}^n$.
$\overline{x}$	The equivalence class of an object x.

Introduction

Coding theory is the field concerned with the study of codes and their properties. Codes are studied in a variety of disciplines, from mathematics to computer science and electrical engineering. Perhaps most importantly, codes can be used for error detection and correction in communication. This makes codes especially interesting objects of study in cryptography and information theory.

In this thesis, codes are considered in a more abstract way. Broadly speaking, a code is a collection of codewords along with a function that assigns to each codeword a nonnegative integer that we call its *weight*. Traditionally, coding theory is mostly concerned with Hamming-metric codes, where the notion of weight is given by the Hamming distance to the zero vector. Recently however, more and more research has been dedicated to codes with a different weight function known as the *rank metric*. Much of this recent work has aimed to transfer results from the Hamming-metric to the rank-metric setting. Especially the class of *vector rank-metric codes* seems to have analogues to quite a few classic results in Hamming-metric coding theory.

Structurally, this thesis revolves around two main chapters. The first concerns Hamming-metric codes and the second deals with (vector) rank-metric codes. Both chapters start by formally introducing the relevant code, which will then be linked to objects known as *systems* through a correspondence theorem. Then, both chapters investigate to what extent the respective weight functions determine the properties of a code. Lastly, the first chapter recalls MacWilliams' Extension Theorem in the Hamming setting, while the second chapter shows no such Extension Theorem exists in the rank-metric context.

Chapter 1

Hamming Codes and Projective Systems

This chapter will introduce Hamming-metric codes and some of their properties. More precisely, we will work towards stating and proving a result from [10], which concerns Hamming weight functions. To do so, we will define Hamming-metric $[n,k]_q$ codes and $[n,k]_q$ projective systems, as well as link these two notions through a correspondence theorem. Lastly, we will consider a result known as MacWilliams' Extension Theorem.

1.1 Hamming-metric $[n,k]_q$ codes

Definition 1.1.1. Let n,k be integers with $0 \leq k \leq n$. Let q be a prime power and consider the finite field $\mathbb{F}_q$. An $[n,k]_q$ *code* is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ such that $\dim_{\mathbb{F}_q} \mathcal{C} = k$.

In the coding theory literature, the statement above is usually taken to define *linear block* $[n,k]_q$ *codes*. Since neither nonlinear nor non-block codes are within our scope, we will simply refer to these objects as *codes*. Elements of a code are known as *codewords* or *code vectors*.

One of the most important notions associated with codes is that of weight, for which we make the following definitions.

Definition 1.1.2. Let $\mathcal{C}$ be an $[n,k]_q$ code and let $c \in \mathcal{C}$. Then the *Hamming*

support of c is defined as

$$\operatorname{supp}^{\mathrm{H}}(c) := \{\, i \in [n] \mid c_i \neq 0 \,\},$$

where c_i denotes the i-th coordinate of the vector c.

Definition 1.1.3. Let $\mathcal{C}$ be an $[n,k]_q$ code and let $c, d \in \mathcal{C}$. Then the *Hamming distance* between c and d is defined as

$$\delta^{\mathrm{H}}(c,d) =:= |\{\, i \in [n] \mid c_i \neq d_i \,\}|,$$

where c_i and d_i denote the i-th coordinate of the vectors c and d respectively.

It is easy to verify that this does indeed define a distance function or metric on $\mathbb{F}_q^n$. We always study codes with a metric rather than in isolation, so it makes sense to explicitly specify the metric for a given code. In this case, that means our objects of interest are will be referred to as *Hamming-metric* $[n,k]_q$ *codes*. In practice, coding theory often focuses on Hamming weight rather than Hamming distance, which is defined as follows.

Definition 1.1.4. Let $\mathcal{C}$ be an $[n,k]_q$ code. Then the *Hamming weight function* for $\mathcal{C}$ is defined by the following map:

$$\begin{aligned} \mathrm{wt}^{\mathrm{H}}_{\mathcal{C}} \colon \mathcal{C} &\longrightarrow \mathbb{Z}_{\geq 0} \\ c &\longmapsto |\operatorname{supp}^{\mathrm{H}}(c)| = \delta(c,0). \end{aligned}$$

Essentially, the Hamming weight function counts the number of indices in which a codeword differs from zero.

Remark. Each code has its own Hamming weight function, because different codes have a different domain for their weight function. Therefore, the subscript in the definition is indeed formally necessary. It is however usually clear from context which code, and thus which domain, we are talking about, so we will often suppress the subscript and simply write wt^{H}.

Example 1.1.5. Coding theory naturally occurs in computer science, especially the case $q = 2$. Consider for instance the set X consisting of all single bytes, i.e. bitstrings of length 8. Note that $X = \mathbb{F}_2^8$, meaning that X is a $[8,8]_2$ code. Furthermore, let $x \in X$ be given by $x = (0,0,1,0,1,1,0,1)$ and note that

$$\begin{aligned} \operatorname{supp}^{\mathrm{H}}(x) &= \{\, 3,5,6,8 \,\} \\ \mathrm{wt}^{\mathrm{H}}(x) &= 4. \end{aligned}$$

Next, we want to extend the notion of support from codewords to codes themselves. To do so, we make the following definition.

Definition 1.1.6. For a Hamming-metric $[n,k]_q$ code $\mathcal{C}$, we define

$$\mathrm{supp}^{\mathrm{H}}(\mathcal{C}) = \bigcup_{c\in\mathcal{C}} \mathrm{supp}^{\mathrm{H}}(c) \subseteq [n].$$

If $\mathrm{supp}^{\mathrm{H}}(\mathcal{C}) = [n]$, we say that $\mathcal{C}$ is *nondegenerate*. Otherwise, we the code is called *degenerate*.

Note that by definition, an $[n,k]_q$ code $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$ of $\mathbb{F}_q$-dimension k, meaning that $\mathcal{C}$ is isomorphic to $\mathbb{F}_q^k$. In particular, it is convenient to view such an isomorphism as a matrix.

Definition 1.1.7. Let $\mathcal{C}$ be a Hamming-metric $[n,k]_q$ code. A *generator matrix* for $\mathcal{C}$ is a full-rank matrix $G \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ whose rows generate $\mathcal{C}$, i.e. $\mathrm{rowsp}(G) = \mathcal{C}$. Equivalently, $\mathcal{C} = \{\, x\cdot G \mid x \in \mathbb{F}_q^k \,\}$.

So, a generator matrix for a code is a matrix whose rows are an $\mathbb{F}_q$-basis for the code. Note that any code has a generator matrix, but generator matrices are not generally unique. Also useful is the following observation:

Remark. Let $\mathcal{C}$ be a code and let $G_{\mathcal{C}}$ be a generator matrix for $\mathcal{C}$. Then $\mathcal{C}$ is nondegenerate if and only if every column of $G_{\mathcal{C}}$ has at least one nonzero entry.

Example 1.1.8. Consider the finite field $\mathbb{F}_7$. Let $G \in \mathrm{Mat}_{2\times 3}(\mathbb{F}_7)$ be given by

$$G = \begin{pmatrix} 0 & 1 & 2 \\ 5 & 0 & 1 \end{pmatrix}$$

Note that $\mathcal{C} = \{\, xG \mid x \in \mathbb{F}_7^2 \,\} \subseteq \mathbb{F}_7^3$ is a $[2,3]_7$ code. Consider the element $x = (2,3) \in \mathbb{F}_7$. We claim that that $c = xG$ is a codeword in $\mathcal{C}$ with Hamming weight 2. To see this, note that

$$c = xG = (2,3)\cdot \begin{pmatrix} 0 & 1 & 2 \\ 5 & 0 & 1 \end{pmatrix} = (1,2,0),$$

which clearly has 2 nonzero coordinates.

Next, we want a notion of equivalence for codes. Clearly, we want equivalent codes to have the same length and dimension and to exist over the same field. As with many notions of equivalence, it also makes sense to require the existence of a structure-preserving morphism. In the case of Hamming codes, the structure is Hamming weight. This all means that the following definition is natural.

Definition 1.1.9. Let $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^n$ be two Hamming-metric $[n,k]_q$ codes. We call $\mathcal{C}$ and $\mathcal{D}$ *equivalent* and write $\mathcal{C} \sim \mathcal{D}$ if there exists an $\mathbb{F}_q$-linear map $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

(i) For every $x \in \mathbb{F}_q^n$ we have $\mathrm{wt}^{\mathrm{H}}(x) = \mathrm{wt}^{\mathrm{H}}(\varphi(x))$

(ii) $\varphi[\mathcal{C}] = \mathcal{D}$

Example 1.1.10. Let $\mathcal{C}$ be an $[4,2]_5$ code generated by $G_{\mathcal{C}} = (1,1,1,1)$. Similarly, let $\mathcal{D}$ be an $[4,2]_5$ code generated by $G_{\mathcal{D}} = (4,4,4,4)$. Note that

$$\begin{aligned} \varphi\colon \mathbb{F}_5^4 &\longrightarrow \mathbb{F}_5^4 \\ x &\longmapsto 4x \end{aligned}$$

is clearly an $\mathbb{F}_5$-linear map. It is also easy to see that $\varphi[\mathcal{C}] = \mathcal{D}$, and weight is preserved because all nonzero codewords in $\mathcal{C}$ and $\mathcal{D}$ have Hamming weight 4. So $\mathcal{C} \sim \mathcal{D}$.

Characterising the equivalence of codes using weight-preserving maps is not the only way to do it. In the following, we will introduce an equivalent notion, which will turn out to be useful.

Definition 1.1.11. A square matrix is called *monomial* if it has precisely one nonzero element in every row and every column.

Definition 1.1.12. We define the group $\mathcal{A}(n,q)$ by setting $\mathcal{A}(n,q) := (\mathbb{F}_q^*)^n \rtimes S_n$, and note that that $\mathcal{A}(n,q)$ acts on $\mathbb{F}_q^n$ (and thus on $[n,k]_q$ codes) in the following way:

$$\begin{aligned} ((\mathbb{F}_q^*)^n \rtimes S_n) \times \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ ((\lambda, \sigma), c) &\longmapsto (\lambda_1 \sigma(c_1), \ldots, \lambda_n \sigma(c_n)), \end{aligned}$$

where λ_i and c_i denote the i-th component of λ and c respectively for $i \in [n]$.

Now, note that $\mathcal{A}(n,q)$ also acts on $n\times n$ matrices, by scalar multiplication and permutation of the columns. In that sense, we can interpret $\mathcal{A}$ as the subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ generated by diagonal and permutation matrices. In particular, note that for the identity matrix I_n, the matrix acquired by letting an element of $\mathcal{A}(n,q)$ act on I is a monomial matrix. It is also easy to see that any monomial matrix can be expressed as an element of $\mathcal{A}(n,q)$ acting on the identity matrix. So, $\mathcal{A}(n,q)$ may be identified with the set of $n \times n$ monomial matrices over $\mathbb{F}_q$, where the action on codes is given simply by multiplication from the right.

Proposition 1.1.13. Let $\mathcal{C}, \mathcal{D}$ be Hamming-metric $[n,k]_q$ codes. The following are equivalent:

(i) $\mathcal{C}$ and $\mathcal{D}$ are equivalent codes.

(ii) For every generator matrix $G_\mathcal{C}$ of $\mathcal{C}$, there exists a monomial matrix $M \in \mathcal{A}(n,q)$ such that $G_\mathcal{D} := G_\mathcal{C} \cdot M$ is a generator matrix for $\mathcal{D}$.

Proof. Suppose we are in situation (ii). Let $G_\mathcal{C}$ be some generator matrix fof $\mathcal{C}$ and let M be monomial such that $G_\mathcal{D} = G_\mathcal{C}$ generates $\mathcal{D}$. Right multiplication with the matrix M defines a linear map $\varphi_M \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$. Since any $c \in \mathcal{C}$ can be written as $xG_\mathcal{C}$ for some $x \in \mathbb{F}_q^k$, we get that

$$\varphi_M(c) = \varphi_M(xG_\mathcal{C}) = xG_\mathcal{C}M = xG_\mathcal{D} \in \mathcal{D}$$

for every $c \in \mathcal{C}$, meaning that $\varphi_M[\mathcal{C}] = \mathcal{D}$. It remains to be shown that φ_M preserves weight. Note that since M is monomial and acts from the right, it can only scale and permute columns, which will not affect the Hamming weight.

Now, suppose $\mathcal{C} \sim \mathcal{D}$ and let φ be the linear map this statement guarantees. Let $G_\mathcal{C}$ be some generator matrix for $\mathcal{C}$. Since φ preserves Hamming weight, each standard basis vector e_i is mapped to $\lambda_i e_j$ for some standard basis vector e_j and some scalar $\lambda_i \in \mathbb{F}_q^*$. If we take $\tau \in S_n$ to be the element such that $\varphi(e_i) = e_{\tau(i)}$ for every i and take $\lambda = (\lambda_1, \ldots, \lambda_n)^\top$, then $a = (\lambda, \tau) \in \mathcal{A}(n,q)$ is an element such that the action of a on $\mathcal{C}$ coincides with the map φ. By the remark from before, we can also view a as a monomial matrix M with the action of right multiplication. That means that we have $cM = \varphi(c)$ for all $c \in \mathcal{C}$. If we let P be the matrix associated to the linear map φ, then we have

$$xG_\mathcal{C}M = \varphi(xG_\mathcal{C}) = x(G_\mathcal{C}P),$$

for every $x \in \mathbb{F}_q^k$. Since φ is an isomorphism, we note that $G_{\mathcal{D}} := G_{\mathcal{C}}P$ is a generator matrix for $\mathcal{D}$ and we are done. □

More often than not, we find that the notion of generator matrices differing by a monomial matrix is the most useful characterisation of equivalence. In fact, some texts in the literature take this as the definition and call such codes *monomially equivalent*.

Lastly, we define a notion of duality for Hamming codes, which we will need later.

Definition 1.1.14. The *dual* of a Hamming-metric code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is given by

$$\mathcal{C}^{\perp} = \{\, v \in \mathbb{F}_q^n \mid u \cdot v^{\top} = 0 \text{ for all } u \in \mathcal{C} \,\}.$$

1.2 Projective $[n, k]_q$ systems

In this section, we will consider objects known as projective systems. In particular, we will work towards relating these projective systems to Hamming-metric codes in a very specific way. We follow the notion of projective systems as in [14]. In order to define what a projective system is, we will first need a number of definitions.

Firstly, we will introduce the notion of a *multiset*. Intuitively, a multiset is a set whose elements can appear more than once, i.e. a set with multiplicities. This can be formally defined as follows.

Definition 1.2.1. A *multiset* is a pair (M, μ) where M is a set and $\mu\colon M \to \mathbb{Z}_{\geq 0}$ is a map linking each element of M to a nonnegative integer. For any $m \in M$, we say that $\mu(m)$ is the *multiplicity* of m in M. The *cardinality* of M is defined by $|M| := \sum_{m \in M} \mu(m)$.

Example 1.2.2. Naively, we might consider the multiset X given by $X = \{\, a, b, b, b, c, c \,\}$. Formally, this set would be given by the pair (X, f), where

$$X = \{a, b, c\}, \qquad f\colon \begin{cases} a & \mapsto & 1 \\ b & \mapsto & 3 \\ c & \mapsto & 2 \end{cases}.$$

The following is a useful fact which we will use later.

Proposition 1.2.3. Let X be a set and $n \in \mathbb{Z}_{\geq 1}$. Let $\mathcal{M}$ denote the collection of all multisets with cardinality n and X as underlying set. Then $\mathcal{M} \cong X^n/S_n$.

Proof. Let $(M, f) \in \mathcal{M}$ be a multiset. Since M is finite, we can create a vector where each element of $m \in M$ occurs $f(m)$ times and the order is chosen in some arbitrary way. It is easy to see that this is indeed a vector in X^n. Considering its equivalence class under S_n gives us an element in the desired set.

For the converse, let $\overline{v} \in X^n/S_n$. Let $v \in X^n$ be some lift of $\overline{v}$. Now, define the map μ by setting

$$\begin{aligned} \mu \colon X &\longrightarrow \mathbb{Z}_{\geq 0} \\ x &\longmapsto |\{\, i \in [n] \mid x = v_i \,\}| \end{aligned}$$

Note that this is well-defined, because this definition of μ clearly does not depend on choice of lift v for $\overline{v}$. Furthermore, the two constructions above are clearly each other's inverse, so we are done. □

Example 1.2.4. Using this construction, we can rewrite the multiset from Example 1.2.2 as follows:

$$\overline{(b, a, b, b, c, c)} \in X^6/S_6.$$

As the final definition concerning multisets, we define what it means for two multisets to be the same.

Definition 1.2.5. Let (M, μ) and (N, ν) be two multisets. Then they are *equivalent* if there exists a bijection $f \colon M \to N$ such that $\nu = \mu \circ f$.

Recall that we need the notion of multisets in order to define projective systems. Before we can do so, we still need one more ingredient: projective spaces.

Definition 1.2.6. For a vector space V over a finite field $\mathbb{F}_q$, the *projectivisation* or *associated projective space* is given by

$$\mathbb{P}(V) = (V \setminus \{0\}) \,/\, \mathbb{F}_q^*,$$

where the group action of $\mathbb{F}_q^*$ on $V \setminus \{0\}$ is given by $(\lambda, x) \mapsto \lambda x$.

In the case that $V = \mathbb{F}_q^n$, we will sometimes write $\mathbb{P}_q^{n-1}$ for $\mathbb{P}(\mathbb{F}_q^n)$. Furthermore, if V is a vector space of dimension k, we say that $\mathbb{P}(V)$ is a projective space of dimension $k-1$. Now, we are in shape to define projective systems.

Definition 1.2.7. Let V be some k-dimensional vector space over $\mathbb{F}_q$ and consider the associated projective space $\mathbb{P}(V)$. A *projective* $[n,k]_q$ *system* is a multiset $\mathcal{P}$ with underlying set $\mathbb{P}(V)$, such that:

(i) $|\mathcal{P}| = n$

(ii) There exists no hyperplane $h \subseteq \mathbb{P}(V)$ such that h contains all elements of $\mathcal{P}$.

It will turn out that equivalence classes of nondegenerate codes are in a 1-to-1 correspondence with equivalence classes of projective systems. Before we formally state and prove this, we need to define when two projective systems are considered equivalent. First, note that any isomorphism of vector spaces $\varphi\colon V \to W$ induces a *projective isomorphism* $\mathbb{P}(V) \to \mathbb{P}(W)$ by $\overline{v} \mapsto \overline{\varphi(v)}$. We use this in the following definition.

Definition 1.2.8. We say that two projective $[n,k]_q$ systems $\mathcal{P}$ and $\mathcal{Q}$ with underlying sets in V and W respectively are *equivalent* if there exists a projective isomorphism $\varphi\colon \mathbb{P}(V) \to \mathbb{P}(W)$ such that $\varphi[\mathcal{P}] = \mathcal{Q}$. As usual, we denote the equivalence class of $\mathcal{P}$ by $\overline{\mathcal{P}}$.

Theorem 1.2.9 ([14], 1.1.6)**.** There is a 1-to-1 correspondence between the set of equivalence classes of nondegenerate Hamming-metric $[n,k]_q$ codes and the set of equivalence classes of projective $[n,k]_q$ systems.

Proof. Let $\mathcal{C}$ be a nondegenerate $[n,k]_q$ code. For any $i \in [n]$, let $\pi_i\colon \mathbb{F}_q^n \to \mathbb{F}_q$ denote the projection on the i-th coordinate. Since these maps are obviously linear, we find that $\pi_{i|\mathcal{C}} \in \mathcal{C}^\vee$ for all $i \in [n]$, where $\mathcal{C}^\vee$ denotes the dual vector space of linear maps $\mathcal{C} \to \mathbb{F}_q$. Furthermore, since $\mathcal{C}$ was assumed to be nondegenerate, we know that these projections are all nontrivial. For every $i \in [n]$ we now define P_i to be the equivalence class of $\pi_{i|\mathcal{C}}$ in $\mathbb{P}(\mathcal{C}^\vee)$ and we claim that $\mathcal{P} = \{ P_1, \ldots, P_n \}$ is a projective $[n,k]_q$ system. We need to show that there is no hyperplane $h \subseteq \mathbb{P}(\mathcal{C}^\vee)$ containing every P_i. For the sake of contradiction, suppose there is such a hyperplane h. In particular, we can see h as a hyperplane in $\mathcal{C}^\vee$, since hyperplanes are clearly invariant under proportionality of points. Furthermore, with standard linear algebra

duality arguments, we argue that every hyperplane in $\mathcal{C}^\vee$ corresponds to a linear map in $\mathcal{C}^{\vee\vee} \cong \mathcal{C}$, so h corresponds to a nonzero codeword $c_h \in \mathcal{C}$. We also have that $f \in h$ if and only if $f(c_h) = 0$. Using these facts, as well as the assumption that $P_i \in h$ for all $i \in [n]$, we write:

$$\begin{aligned} 0 &= \{\, i \in [n] \mid P_i \notin h \,\} \\ &= \left\{\, i \in [n] \;\middle|\; \pi_{i|C} \notin h \,\right\} \\ &= \left\{\, i \in [n] \;\middle|\; \pi_{i|C}(c_h) \neq 0 \,\right\} \\ &= \operatorname{wt} c_h, \end{aligned}$$

which is a contradiction since c_h has to be nonzero.

Now, we show that this construction does indeed map equivalent codes to equivalent projective systems. To see this, let $\mathcal{C}, \mathcal{D}$ be an equivalent $[n,k]_q$ codes and let $\mathcal{P} = \{\, P_1, \dots P_n \,\}$ and $\mathcal{Q} = \{\, Q_1, \dots Q_n \,\}$ be the projective systems obtained from codes $\mathcal{C}$ and $\mathcal{D}$ respectively. By definition of equivalence of codes, there exist $\sigma \in S_n$ and $a \in (\mathbb{F}_q^*)^n$ such that for every $c \in C$ there is precisely one $d \in D$ with $c = \sigma(a \odot d)$, where $\odot$ denotes element-wise multiplication. Now, let $i \in [n]$ arbitrary and let $j \in [n]$ denote the pre-image of i under σ. Note that

$$\pi_i(c) = \pi_i(\sigma(a \odot d)) = \pi_j(a \odot d) = a_j \pi_j(d).$$

Since our choice of i was arbitrary, we see that every $\pi_{i|\mathcal{C}} \in \mathcal{C}^\vee$ corresponds to a $a_j \pi_{j|\mathcal{D}}$ in $\mathcal{D}^\vee$. This means that every equivalence class $\overline{\pi_{i|\mathcal{C}}} \in \mathbb{P}(\mathcal{C}^\vee)$ corresponds to an equivalence class $\overline{\pi_{j|\mathcal{D}}} = \overline{\pi_i \circ \sigma} \in \mathbb{P}(\mathcal{D}^\vee)$. This is obviously an equivalence of projective systems, thus exactly what we wanted to show.

For the converse, let $\mathcal{P} = \{\, P_1, \dots, P_n \,\}$ be a projective system in $\mathbb{P}(V)$ for some $\mathbb{F}_q$-vector space V of dimension k. For any $i \in [n]$, we let v_i be an arbitrary lift of P_i to V and we consider the linear map

$$\begin{aligned} \varphi_{\mathcal{P}} \colon V^\vee &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(v_1), \dots, f(v_n)). \end{aligned}$$

We claim that this map is injective. To see this, suppose $\varphi_{\mathcal{P}}(f) = 0$. This implies $v_i \in \ker f$ for all $i \in [n]$. This in turn implies that $P_i \in \ker[f]$ for all $i \in [n]$, which is a contradiction since $\mathcal{P} = \{\, P_1, \dots, P_n \,\}$ is a projective system and $\ker[f]$ is a hyperplane. So $\ker \varphi_{\mathcal{P}} = 0$, i.e. $\varphi_{\mathcal{P}}$ is injective. Now,

we set $\mathcal{C} := \operatorname{im} \varphi_{\mathcal{P}}$ and note that $\dim \mathcal{C} = \dim V^\vee - \dim \ker \varphi_{\mathcal{P}} = k - 0$, so $\mathcal{C}$ is an $[n, k]_q$ code. Suppose $\mathcal{C}$ is degenerate. Then there is some $i \in [n]$ such that $f(v_i) = 0$ for all $f \in V^\vee$. This implies that $v_i = 0$, which is a contradiction because v_i is a lift of an element P_i in a projective space. So $\mathcal{C}$ is nondegenerate.

Now, suppose that $\mathcal{P} = \{ P_1, \dots, P_n \}$ and $\mathcal{Q} = \{ Q_1, \dots, Q_n \}$ are equivalent projective systems with underlying sets $\mathbb{P}(V)$ and $\mathbb{P}(V')$ respectively. Let $\Psi \colon \mathbb{P}(V) \to \mathbb{P}(V')$ be an isomorphism. It follows from the construction that $\operatorname{im} \varphi_{\mathcal{P}}$ and $\operatorname{im} \varphi_{\mathcal{Q}}$ can differ only by permutation (from the isomorphism Ψ) and by element-wise scalar multiplication (from choosing the lifts). So the codes we got differ exactly by elements from the subgroup generated S_n and $(\mathbb{F}_q^*)^n$, meaning they are equivalent.

It remains to be shown that the above constructions are each other's inverse up to equivalence. Too see this, consider a code $\mathcal{C}$ and its generator matrix $G_{\mathcal{C}}$. Let g_i denote the i-th column of $G_{\mathcal{C}}$ and let γ_i denote the linear map defined by taking the dot product with g_i. Now, note that the projection map $\pi_{i|\mathcal{C}}$ actually equals γ_i for all $i \in [n]$, meaning that the projective system corresponding to $\mathcal{C}$ can be seen as $\mathcal{P} = \{ \overline{\gamma_1}, \dots, \overline{\gamma_n} \}$. Now, we argue that constructing a code as above from $\mathbb{P}$ gives us a code $\mathcal{C}'$ equivalent to $\mathcal{C}$. To see this, let $v_1, \dots v_n$ be arbitrary lifts of $\overline{\gamma_1}, \dots, \overline{\gamma_n}$ and let V denote the matrix with the v_i as columns and note that

$$\begin{aligned}
\mathcal{C}' &= \operatorname{im} \varphi_{\mathcal{P}} \\
&= \left\{ f(v_1), \dots f(v_n) \;\middle|\; f \colon (\mathbb{F}_q^n)^{\vee\vee} \to (\mathbb{F}_q^n)^\vee \text{ linear map} \right\} \\
&= \left\{ v_1(x), \dots v_n(x) \;\middle|\; x \in \mathbb{F}_q^n \right\} \\
&= \operatorname{rowsp}(V).
\end{aligned}$$

Now, we note that V is clearly monomially equivalent to $G_{\mathcal{C}}$, i.e. $V = G_{\mathcal{C}} \cdot A$ for some $A \in \mathcal{A}(n, q)$. So $\mathcal{C} \sim \mathcal{C}$'. The argument in the other direction follows a similar vein. □

So, if we are looking to investigate nondegenerate Hamming-metric codes, it turns out that we may as well look into projective systems. In certain contexts, the combinatorial nature of these systems makes certain proofs and insights easier. Examples of this include constructions with weight functions, which we will consider in the following subsection.

1.3 Weight functions and equivalence

Let $\mathcal{C}$ be a Hamming-metric $[n,k]_q$ code. We know that $\mathcal{C}$ comes equipped with a Hamming weight function $\mathrm{wt}^{\mathrm{H}}\colon \mathcal{C} \to \mathbb{Z}_{\geq 0}$, which maps a codeword c to a nonnegative integer representing the number of coordinate positions in which c differs from 0. Such a $\mathcal{C}$ is itself the image of right-multiplication with a generator matrix $G_{\mathcal{C}}$, so we can also consider the composition

$$\mathbb{F}_q^k \xrightarrow{G_{\mathcal{C}}} \mathcal{C} \xrightarrow{\mathrm{wt}^{\mathrm{H}}} \mathbb{Z}.$$

More generally, we are interested in the following construction.

Definition 1.3.1. Let $\mathcal{G}^{\mathrm{H}}[n,k]_q$ be the set of generator matrices for nondegenerate Hamming $[n,k]_q$ codes, i.e.:

$$\mathcal{G}^{\mathrm{H}}[n,k]_q = \{\, G \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q) \mid \mathrm{rk}\, G = k \text{ and } G \text{ has no zero columns} \,\}.$$

We consider the following map, which associates to each generator matrix a weight function:

$$\begin{aligned} W^{\mathrm{H}}_{n,k}\colon \mathcal{G}^{\mathrm{H}}[n,k]_q &\longrightarrow \mathrm{Map}\big(\mathbb{F}_q^k, \mathbb{Z}_{\geq 0}\big) \\ G &\longmapsto [x \mapsto \mathrm{wt}^{\mathrm{H}}(xG)]. \end{aligned}$$

As Nogin argues in [10], it is a natural question to wonder to what extent the image of a generator matrix under the this function determines it. More precisely: given $W^{\mathrm{H}}(G)$, how much do we know about the code that G generates? It turns out that the W^{H} distinguishes generator matrices up to equivalence of the associated codes. This is captured in the following result.

Theorem 1.3.2 (Implicitly stated and proved in [10])**.** Let $\mathcal{C}$ and $\mathcal{D}$ be nondegenerate $[n,k]_q$ Hamming codes. Suppose there exist $G_{\mathcal{C}}, G_{\mathcal{D}} \in \mathcal{G}[n,k]_q$ that generate $\mathcal{C}$ and $\mathcal{D}$ respectively, such that $W^{\mathrm{H}}(G_{\mathcal{C}}) = W^{\mathrm{H}}(G_{\mathcal{D}})$. Then $\mathcal{C} \sim \mathcal{D}$.

We follow the proof in [10], using the machinery of projective $[n,k]_q$ systems we discussed previously. The proof proceeds as follows, though we split it up into two lemmas for clarity.

Lemma 1.3.3. Let $\mathcal{C}$ be a nondegenerate Hamming-metric $[n,k]_q$ code and let $(\mathcal{P},\nu)$ be the projective $[n,k]_q$ system associated to $\mathcal{C}$. Then for every $c \in \mathcal{C}$ we have

$$\mathrm{wt}^{\mathrm{H}}(c) = \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{c}) \neq 0}} \nu(f)$$

Proof. Let $\mathcal{C}$ be a nondegenerate Hamming-metric $[n,k]_q$ code. Let $\mathcal{P}$ be the projective $[n,k]_q$ system associated to $\mathcal{C}$ via the construction in Theorem 1.2.9, i.e. the elements of $\mathcal{P}$ are equivalence classes of projection maps $\pi_i \colon \mathcal{C} \to \mathbb{F}_q$. Let $\nu \colon \mathbb{P}(\mathcal{C}^\vee) \to \mathbb{Z}_{\geq 0}$ be the multiplicity function for the projective system $\mathcal{P}$. Let $c \in \mathcal{C}$ and consider

$$\begin{aligned}
\mathrm{wt}^{\mathrm{H}}(c) &= |\{\, i \in [n] \mid c_i \neq 0 \,\}| \\
&= |\{\, i \in [n] \mid \pi_i(c) \neq 0 \,\}| \\
&= |\{\, i \in [n] \mid \overline{\pi_i}(\overline{c}) \neq 0 \,\}| \\
&= \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{c}) \neq 0}} \nu(f),
\end{aligned}$$

and we are done. □

Essentially, we can interpret this as a way to construct a weight function from a given projective system. However, our question was in the other direction: how (much freedom do we have) to construct a code from a given weight function. Luckily, Nogin provides an answer to this question too, having found a way to invert the formula from Lemma 1.3.3.

Lemma 1.3.4. Let $\mathcal{C}$ be a nondegenerate Hamming-metric $[n,k]_q$ code and let $(\mathcal{P},\nu)$ be the projective $[n,k]_q$ system associated to $\mathcal{C}$. Then for every $f \in \mathcal{P}$, we have

$$\nu(f) = \frac{q \cdot \sum\limits_{\overline{c}} \mathrm{wt}^{\mathrm{H}}(c) - \sum\limits_{f(\overline{c})=0} \mathrm{wt}^{\mathrm{H}}(c)}{q^{k-1}}$$

Proof. First, consider the following equalities:

$$\sum_{\overline{c} \in \mathbb{P}(\mathcal{C})} \mathrm{wt}^{\mathrm{H}}(c) = \sum_{\overline{c} \in \mathbb{P}(\mathcal{C})} \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{c}) \neq 0}} \nu(f) = \sum_{f \in \mathbb{P}(\mathcal{C}^\vee)} \nu(f) \sum_{\substack{\overline{c} \in \mathbb{P}(\mathcal{C}) \\ f(\overline{c}) \neq 0}} 1.$$

In the above, the first equality holds by Lemma 1.3.3 and the second follows from a reordering of summation terms. Now, we look more closely at the expression $|\{\,\overline{c} \in \mathbb{P}(\mathcal{C}) \mid f(\overline{c}) = 0\,\}|$. Note that for fixed f, this expression essentially counts the number of points in $\mathbb{P}(\mathcal{C})$ that are not in the hyperplane h_f given by $h_f\colon f(x) = 0$. Let κ denote this number, i.e. $\kappa = |\{\,x \in \mathbb{P}(\mathcal{C}) \mid x \notin h_f\,\}|$. Then, note that a hyperplane in a projective space is itself a projective space of one dimension less. So, we write:

$$|\mathbb{P}(\mathcal{C})| = |\mathbb{P}_q^{k-1}| = \frac{q^k - 1}{q - 1}$$

$$|\{\,x \mid x \in h_f\,\}| = \frac{q^{k-1} - 1}{q - 1}$$

Using this, we find that:

$$\begin{aligned}
\kappa &= |\{\,x \in \mathbb{P}(\mathcal{C}) \mid x \notin h_f\,\}| \\
&= |\mathbb{P}(\mathcal{C})| - \{\,x \mid x \in h_f\,\}| \\
&= \frac{q^k - 1}{q - 1} - \frac{q^{k-1} - 1}{q - 1} \\
&= \frac{q^k - q^{k-1}}{q - 1} \\
&= q^{k-1}
\end{aligned}$$

Plugging this into the equation from before, we find that

$$\sum_{\overline{c} \in \mathbb{P}(\mathcal{C})} \mathrm{wt}^{\mathrm{H}}(c) = q^{k-1} \sum_{f \in \mathbb{P}(\mathcal{C}^\vee)} \nu(f). \tag{1.1}$$

Next, fix some $f_0 \in \mathbb{P}(\mathcal{C}^\vee)$. With a reasoning similar to the above sequence of equalities, we write

$$\sum_{\substack{\overline{c} \in \mathbb{P}(\mathcal{C}) \\ f_0(\overline{c}) = 0}} \mathrm{wt}^{\mathrm{H}}(c) = \sum_{\substack{\overline{c} \in \mathbb{P}(\mathcal{C}) \\ f_0(\overline{c}) = 0}} \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{c}) \neq 0}} \nu(f) = \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f \neq f_0}} \nu(f) \sum_{\substack{\overline{c} \in \mathbb{P}(\mathcal{C}) \\ f(\overline{c}) \neq 0 \\ f_0(\overline{c}) = 0}} 1.$$

Now, note that the equality $f_0(\overline{c}) = 0$ defines a hyperplane h in $\mathbb{P}(\mathcal{C})$ Since the dimension of a hyperplane is by definition one less than the ambient space,

we find that h is a space of dimension $\dim \mathbb{P}(\mathcal{C}) - 1 = \dim \mathcal{C} - 2 = k - 2$. So, the expression $|\{\, \bar{c} \in \mathbb{P}(\mathcal{C}) \mid f(\bar{c}) = 0 \,\}|$ counts the number of points outside a hyperplane in the $(k-2)$-dimensional space h. Using the same argument as above, except one dimension lower, we find that this number of points equals q^{k-2}. Substituting this gives us

$$\sum_{\substack{\bar{c} \in \mathbb{P}(\mathcal{C}) \\ f_0(\bar{c}) = 0}} \mathrm{wt}^{\mathrm{H}}(c) = q^{k-2} \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f \neq f_0}} \nu(f). \tag{1.2}$$

To find the desired result, we now combine (1.1) and (1.2). Specifically, taking $q \cdot (1.2) - (1.1)$ gives us the following expression for any f_0:

$$q \cdot \sum_{\substack{\bar{c} \in \mathbb{P}(\mathcal{C}) \\ f_0(\bar{c}) = 0}} \mathrm{wt}^{\mathrm{H}}(c) - \sum_{\bar{c} \in \mathbb{P}(\mathcal{C})} \mathrm{wt}^{\mathrm{H}}(c) = q^{k-1} \left(\sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f \neq f_0}} \nu(f) - \sum_{f \in \mathbb{P}(\mathcal{C}^\vee)} \nu(f) \right)$$

Changing signs on both sides and dividing by q^{k-1} gives us that:

$$\nu(f_0) = \sum_{f \in \mathbb{P}(\mathcal{C}^\vee)} \nu(f) - \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f \neq f_0}} \nu(f) = \frac{q \cdot \sum_{\bar{c} \in \mathbb{P}(\mathcal{C})} \mathrm{wt}^{\mathrm{H}}(c) - \sum_{\substack{\bar{c} \in \mathbb{P}(\mathcal{C}) \\ f_0(\bar{c}) = 0}} \mathrm{wt}^{\mathrm{H}}(c)}{q^{k-1}}.$$

Now simply substituting f for f_0 yields the desired equation. □

Recall that the above lemmas aimed at working towards a proof for Theorem 1.3.2. Now that both lemmas have been stated and proved, the proof of the theorem is relatively straightforward.

Proof of 1.3.2. Let $\mathcal{C}$ and $\mathcal{D}$ be nondegenerate $[n,k]_q$ Hamming codes. Suppose that $W^{\mathrm{H}}(G_\mathcal{C}) = W^{\mathrm{H}}(G_\mathcal{D})$ for some $G_\mathcal{C}, G_\mathcal{D} \in \mathcal{G}[n,k]_q$, which generate $\mathcal{C}$ and $\mathcal{D}$ respectively. We want to show that $\mathcal{C} \sim \mathcal{D}$. Note that by assumption, we have the following for all $x \in \mathbb{F}_q^k$:

$$\mathrm{wt}^{\mathrm{H}}(xG_\mathcal{C}) = \mathrm{wt}^{\mathrm{H}}(xG_\mathcal{D})$$

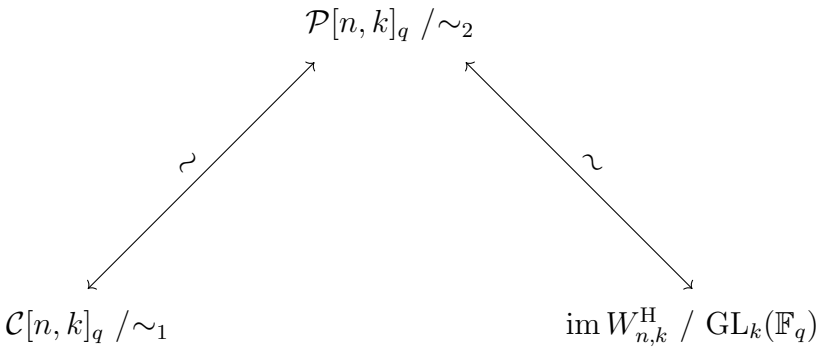
Now, let $(\mathcal{P}, \nu)$ and $(\mathcal{M}, \mu)$ be projective $[n,k]_q$ systems associated with $\mathcal{C}$ and $\mathcal{D}$ respectively. Using 1.3.4, we now write that for any $f \in \mathbb{P}(\mathbb{F}_q^k)$ we

have:

$$\begin{aligned} q^{k-1} \cdot \nu(f) &= q \cdot \sum_{\overline{c} \in \mathbb{P}(\mathcal{C})} \mathrm{wt}^{\mathrm{H}}(c) - \sum_{f(\overline{c})=0} \mathrm{wt}^{\mathrm{H}}(c) \\ &= q \cdot \sum_{\overline{x} \in \mathbb{P}\mathbb{F}_q^k} \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{C}}) - \sum_{f(\overline{c})=0} \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{C}}) \\ &= q \cdot \sum_{\overline{x} \in \mathbb{P}\mathbb{F}_q^k} \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{D}}) - \sum_{f(\overline{c})=0} \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{D}}) \\ &= q \cdot \sum_{\overline{d} \in \mathbb{P}(\mathcal{D})} \mathrm{wt}^{\mathrm{H}}(d) - \sum_{f(\overline{d})=0} \mathrm{wt}^{\mathrm{H}}(d) \\ &= q^{k-1} \cdot \mu(f) \end{aligned}$$

So, we find that $\nu(f) = \mu(f)$ for all $f \in \mathbb{P}(\mathbb{F}_q^k)$. This implies that $(\mathcal{P}, \nu) \sim (\mathcal{M}, \mu)$. By Theorem 1.2.9, we conclude that $\mathcal{C} \sim \mathcal{D}$. □

Summarising the last sections, we have found a 1-to-1 correspondence between the set of equivalence classes of nondegenerate $[n,k]_q$ codes and the set of equivalence classes of projective $[n,k]_q$ systems. Furthermore, we have found that to each of those equivalence classes we can associate an element from the image of W^{H} up to a choice of generator matrix. In diagram form, we have the following system of correspondences:



where

- $\mathcal{C}[n,k]_q$ denotes the set of nondegenerate Hamming $[n,k]_q$ codes and we have $\mathcal{C} \sim_1 \mathcal{D}$ if there exist an $\mathbb{F}_q$-linear weight preserving map $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\varphi[\mathcal{C}] = \mathcal{D}$.

- $\mathcal{P}[n,k]_q$ denotes the set of projective $[n,k]_q$ systems and we have $\mathcal{P} \sim_2 \mathcal{Q}$ if there exist an isomorphism $\psi\colon V \to W$ between the underlying sets such that $\psi[\mathcal{P}] = \mathcal{Q}$.
- $\operatorname{im} W^{\mathrm{H}}_{n,k}$ denotes the image of the map W^{H}, i.e. the set of Hamming weight functions $\mathbb{F}_q^k \to \mathbb{Z}_{\geq 0}$ of the form $x \mapsto \mathrm{wt}^{\mathrm{H}}(xG)$ for some nondegenerate generator matrix G. Two weight functions π, τ are considered equivalent if there exists an $A \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $\pi(x) = \tau(xA)$ for all $x \in \mathbb{F}_q^k$.

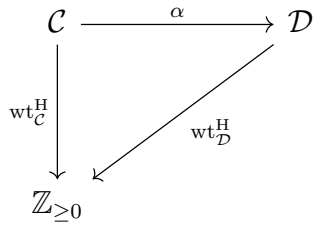
The equivalence on the left side is given by Theorem 1.2.9. For the right side, we have Lemmas 1.3.3 and 1.3.4.

1.4 MacWilliams' Extension Theorem

In this section, we will focus our attention on a result from the 1960s known as MacWilliams' Extension Theorem [9]. In particular, we will state the theorem and show how it relates to Theorem 1.3.2. Then, we will use the Extension Theorem to further relate codes, projective systems and weight functions.

We begin by making the following definition, which considers a different notion of equivalence between Hamming codes.

Definition 1.4.1. Let $\mathcal{C}$ and $\mathcal{D}$ be two nondegenerate $[n,k]_q$ codes. We say that $\mathcal{C}$ and $\mathcal{D}$ are *locally weight-equivalent* and write $\mathcal{C} \sim_w \mathcal{D}$ if there exists an $\mathbb{F}_q$-linear isomorphism $\alpha\colon \mathcal{C} \to \mathcal{D}$ such that $\mathrm{wt}^{\mathrm{H}}_{\mathcal{C}} = \mathrm{wt}^{\mathrm{H}}_{\mathcal{D}} \circ \alpha$. That is, if the following diagram commutes:



Remark. Note that the notion of local weight-equivalence is very similar to our classic notion of equivalence between codes in that both require the existence of a weight-preserving map. The only difference is that local weight-equivalance only requires a map from $\mathcal{C}$ to $\mathcal{D}$, whereas the classic notion of

equivalence requires a weight-preserving map on the ambient space $\mathbb{F}_q^n$ (which also maps $\mathcal{C}$ to $\mathcal{D}$).

Theorem 1.4.2 (MacWilliams' Extension Theorem, e.g. [8], 7.9.4)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be Hamming-metric $[n,k]_q$ codes and suppose $\mathcal{C} \sim_w \mathcal{D}$. Then $\mathcal{C} \sim \mathcal{D}$. Moreover, any weight-preserving map $\alpha\colon \mathcal{C} \to \mathcal{D}$ can be extended to a weight-preserving map $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$.

The statement can be proved in several different ways, e.g. 7.9.4 in [8]. In the following, we will focus on a weaker version of MacWilliams' Extension Theorem, aptly called Weak MacWilliams. In particular, we will show that this weak version of the Extension Theorem is closely related to Nogin's Theorem 1.3.2 from the previous section. Interestingly, Nogin's paper [10] does not explicitly mention this connection to the older result.

We begin by stating the Weak MacWilliams Theorem.

Theorem 1.4.3 (Weak MacWilliams)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be Hamming-metric $[n,k]_q$ codes and suppose $\mathcal{C} \sim_w \mathcal{D}$. Then $\mathcal{C} \sim \mathcal{D}$.

So, like the stronger version we mentioned earlier, this theorem states that $\mathcal{C} \sim_w \mathcal{D} \implies \mathcal{C} \sim \mathcal{D}$. However, in contrast to the actual Extension Theorem, it does not require that the maps guaranteed by the equivalences actually match up. Indeed, that is the reason for calling it Weak MacWilliams. Note that Weak MacWilliams follows trivially from MacWilliams' Extension Theorem.

First, we show that Weak MacWilliams implies Nogin's Theorem 1.3.2. To see this, let $\mathcal{C}, \mathcal{D}$ be $[n,k]_q$ codes with generator matrices $G_\mathcal{C}$ and $G_\mathcal{D}$ respectively. Suppose $W^{\mathrm{H}}(G_\mathcal{C}) = W^{\mathrm{H}}(G_\mathcal{D})$, i.e. $\mathrm{wt}^{\mathrm{H}}(xG_\mathcal{C}) = \mathrm{wt}^{\mathrm{H}}(xG_\mathcal{D})$ for every $x \in \mathbb{F}_q^k$. If we consider the map

$$\begin{aligned} \alpha\colon \mathcal{C} &\longrightarrow \mathcal{D} \\ xG_\mathcal{C} &\longmapsto xG_\mathcal{D}, \end{aligned}$$

then it is clear that α is an $\mathbb{F}_q$-linear map. Furthermore, it follows from our assumption that α is weight-preserving. Now, Theorem 1.4.3 gives us that $\mathcal{C} \sim \mathcal{D}$ and we are done.

Perhaps more interestingly, we note that the converse is also true: Theorem 1.4.3 follows rather easily from Theorem 1.3.2. To see this, first consider the following lemma.

Lemma 1.4.4. If $\mathcal{C}, \mathcal{D}$ are $[n,k]_q$ codes and $\alpha\colon \mathcal{C} \to \mathcal{D}$ is a weight-preserving $\mathbb{F}_q$-linear map, then α is bijective.

Proof. Note that

$$\begin{aligned}\ker\alpha &= \{\, c \in \mathcal{C} \mid \alpha(c) = 0 \,\} \\ &\subseteq \{\, c \in \mathcal{C} \mid \mathrm{wt}^{\mathrm{H}}(\alpha(c)) = 0 \,\} \\ &= \{\, c \in \mathcal{C} \mid \mathrm{wt}^{\mathrm{H}}(c) = 0 \,\} \\ &= \{\, 0 \,\}\end{aligned}$$

So α is injective, and by finiteness, it is also surjective. □

Now, we use this lemma and Theorem 1.3.2 to prove the weak version of MacWilliams' Extension Theorem.

Proof of 1.4.3. Let $\alpha\colon \mathcal{C} \to \mathcal{D}$ be a weight-preserving map. Let $G_{\mathcal{C}}$ be a generator matrix for $\mathcal{C}$ and let $g_{\mathcal{C}}\colon \mathbb{F}_q^k \to \mathcal{C}$ be the associated map, i.e. right-multiplication with $G_{\mathcal{C}}$. Let $g_{\mathcal{D}} := \alpha \circ g_{\mathcal{C}}$ and note that this is surjective as a composition of surjective maps (by assumption and 1.4.4). So $g_{\mathcal{D}}$ is a surjective linear map from $\mathbb{F}_q^k$ to $\mathcal{D}$. If we let $G_{\mathcal{D}}$ be the associated matrix (for right multiplication), then that is a generator matrix for $\mathcal{D}$. Now, using the fact that α is weight-preserving, for every $x \in \mathbb{F}_q^n$ we have:

$$\begin{aligned}W^{\mathrm{H}}(G_{\mathcal{D}})(x) &= \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{D}}) \\ &= \mathrm{wt}^{\mathrm{H}}(g_{\mathcal{D}}(x)) \\ &= \mathrm{wt}^{\mathrm{H}}((\alpha \circ g_{\mathcal{C}})(x)) \\ &= \mathrm{wt}^{\mathrm{H}}(g_{\mathcal{C}}(x)) \\ &= \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{C}}) \\ &= W^{\mathrm{H}}(G_{\mathcal{C}})(x).\end{aligned}$$

Since this holds for all $x \in \mathbb{F}_q^n$, we get that $W^{\mathrm{H}}(G_{\mathcal{C}}) = W^{\mathrm{H}}(G_{\mathcal{D}})$. Using 1.3.2, it follows that $\mathcal{C} \sim \mathcal{D}$. □

Note that the converse of the above implication is also obviously true: to show that $\mathcal{C} \sim \mathcal{D} \implies \mathcal{C} \sim_w \mathcal{D}$, we can simply restrict the domain of a weight-preserving map $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ to $\mathcal{C}$ and we are done. Using this, we can expand the figure of correspondences from the previous section in the following way:

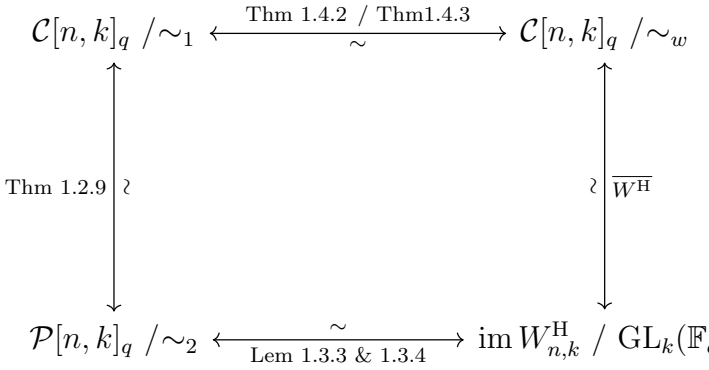


Figure 1.1: Figure of equivalences for the Hamming metric

Recall that $\sim_1$ and $\sim_2$ refer to the standard equivalence relations for codes and projective systems we defined earlier. We also consider two weight functions π, τ in $\operatorname{im} W^{\mathrm{H}}$ equivalent if there exists some $A \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $\pi(x) = \tau(xA)$ for all $x \in \mathbb{F}_q$. Furthermore, the left and bottom arrows were already introduced in the previous section. Only the top and right arrows remain to be discussed.

The top arrow follows directly from the Weak MacWilliams Theorem 1.4.3 (and the remark that the converse direction is trivial). For the arrow on the right, we consider the following map:

$$\begin{aligned} \overline{W^{\mathrm{H}}_{n,k}} \colon \mathcal{C}[n,k]_q\ /\!\sim_w &\longrightarrow \operatorname{im} W^{\mathrm{H}}_{n,k}\ /\ \mathrm{GL}_k(\mathbb{F}_q) \\ \overline{\mathcal{C}} &\longmapsto \overline{W^{\mathrm{H}}(G_{\mathcal{C}})}, \end{aligned}$$

where $G_{\mathcal{C}}$ is some generator matrix for the code $\mathcal{C}$. First, we have to show that this map is well-defined. First, we show that the choice of generator matrix has no effect. So, let G_1 and G_2 be two generator matrices for a nondegenerate Hamming code $\mathcal{C}$. Note that by definition of a generator matrix, there has to exist some $A \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $G_2 = AG_2$. This implies that

$$W^{\mathrm{H}}(G_1)(x) = \mathrm{wt}^{\mathrm{H}}(xG_1) = \mathrm{wt}^{\mathrm{H}}(xAG_2) = W^{\mathrm{H}}(G_2)(xA),$$

that is, $W^{\mathrm{H}}(G_1) \sim W^{\mathrm{H}}(G_2)$. Now, we also have to show that if $\mathcal{C} \sim_w \mathcal{D}$, then $\overline{\mathcal{C}}$ and $\overline{\mathcal{D}}$ map to the same element. Note that we are free to choose

generator matrices by the previous argument. So, let $G_{\mathcal{C}}$ be some generator matrix for $\mathcal{C}$. Note that by assumption, there exists some weight preserving $\alpha\colon \mathcal{C} \to \mathcal{D}$. Since α is linear, we can let P be the associated matrix and note that $G_{\mathcal{D}} := G_{\mathcal{C}}P$ is a generator matrix for $\mathcal{D}$. In particular, for any $x \in \mathbb{F}_q^k$ we can write:

$$W^{\mathrm{H}}(G_{\mathcal{C}})(x) = \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{C}}) = \mathrm{wt}^{\mathrm{H}}(\alpha(xG_{\mathcal{C}})) = \mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{D}}) = W^{\mathrm{H}}(G_{\mathcal{D}})(x),$$

so we have $W^{\mathrm{H}}(G_{\mathcal{C}}) = W^{\mathrm{H}}(G_{\mathcal{D}})$ and we conclude that the map is well-defined.

Now, it remains to be shown that $\overline{W^{\mathrm{H}}}$ is bijective. Surjectivity follows easily. For injectivity, suppose we have generator matrices $G_{\mathcal{C}}$ and $G_{\mathcal{D}}$ for codes $\mathcal{C}$ and $\mathcal{D}$ and some $A \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $\mathrm{wt}^{\mathrm{H}}(xG_{\mathcal{C}}) = \mathrm{wt}^{\mathrm{H}}(xAG_{\mathcal{D}})$ for all $x \in \mathbb{F}_q^k$. Let $\alpha\colon \mathcal{C} \to \mathcal{D}$ be defined by $c \mapsto cA$. Note that α is clearly weight preserving and linear, so $\mathcal{C} \sim_w \mathcal{D}$. So we are done.

Chapter 2

Rank-metric codes and $[n, k]_{q^m/q}$ systems

Traditionally, the field of coding theory has tended to focus on Hamming-metric codes. However, recent research has seen increased interest in a different type of code known as *rank-metric codes* (e.g. [12], [11], [6]). Rank-metric codes were introduced independently by Gabidulin [5] and Delsarte [4]. In this chapter, we will mostly consider a special kind of rank-metric codes known as vector rank-metric codes. In particular, we will go through many of the same motions as in the previous chapter and investigate which of those constructions have an analogue in the vector rank-metric setting.

Remark. In the existing literature, the term *rank-metric code* is rather ambiguous. Depending on the author and even the specific paper, it may refer to two different objects, which the present thesis distinguishes by the terms *matrix rank-metric code* and *vector rank-metric code* for clarity.

2.1 Matrix rank-metric codes

The most general type of rank metric codes are the matrix rank-metric codes, which we define as follows.

Definition 2.1.1. Let n, k, m be integers with $0 \leq k < n, m$. Let q be a prime power and consider the finite field $\mathbb{F}_q$. An $[m, n, k]_q$ *matrix rank-metric code* is an $\mathbb{F}_q$-linear subspace $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ such that $\dim_{\mathbb{F}_q} \mathcal{C} = k$.

An element $X \in \mathcal{C}$ is known as a (matrix rank-metric) *codeword*. So, where a Hamming code is a collection of vectors over $\mathbb{F}_q$, a matrix rank-metric code is a collection of matrices over $\mathbb{F}_q$. As in the Hamming case, we do not consider rank-metric codes in isolation: we need a weight function. First, we define a notion of support.

Definition 2.1.2. Let $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ be an $[m, n, k]_q$ matrix rank-metric code and let $X \in \mathcal{C}$. The *rank support* of X is defined as

$$\mathrm{supp}^{\mathrm{mrk}}(X) := \mathrm{rowsp}(X)$$

Like for Hamming-metric codes, we use the support to define a weight function.

Definition 2.1.3. Let $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ be an $[m, n, k]_q$ matrix rank-metric code and let $X, Y \in \mathcal{C}$. The *rank distance* between X and Y is defined as

$$\delta^{\mathrm{mrk}}(X, Y) := \dim_{\mathbb{F}_q} \mathrm{supp}^{\mathrm{mrk}}(X - Y)$$

Since $\dim_{\mathbb{F}_q} \mathrm{supp}^{\mathrm{mrk}}(X - Y) = \dim_{\mathbb{F}_q} \mathrm{rowsp}(X - Y) = \mathrm{rk}(X - Y)$, it is clear why these objects are called rank-metric codes. Again, following familiar footsteps, we use the appropriate distance function to define a weight function in the context of matrix rank-metric codes.

Definition 2.1.4. Let $\mathcal{C} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ be a matrix rank-metric code and let $X \in \mathcal{C}$. The *rank weight function* for $\mathcal{C}$ is defined as follows:

$$\begin{aligned} \mathrm{wt}^{\mathrm{mrk}}_{\mathcal{C}} \colon \mathcal{C} &\longrightarrow \mathbb{Z}_{\geq 0} \\ X &\longmapsto \delta^{\mathrm{mrk}}(X, 0) \end{aligned}$$

As was the case for Hamming-metric codes, we could also define the weight in terms of support rather than distance, by observing that

$$\mathrm{wt}^{\mathrm{mrk}}_{\mathcal{C}}(X) = \delta^{\mathrm{mrk}}(X, 0) = \mathrm{rk}(X) = \dim_{\mathbb{F}_q} \mathrm{supp}^{\mathrm{mrk}}(X)$$

Remark. Like in the Hamming case, the domain of the weight function is usually clear from context. For that reason, we will often suppress the subscript in the notation for ease of reading.

Remark. In our definition of matrix rank-metric codes, we deviate slightly from the existing literature. Most authors define (matrix) rank-metric codes as k-dimensional subsets of $\mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ instead of $\mathrm{Mat}_{m\times n}(\mathbb{F}_q)$. We chose the latter option because it makes it makes certain analogies to Hamming-metric codes more clear. Note that the rank-metric is invariant under transposition anyways, so our deviation is indeed minor.

Example 2.1.5. Let $\mathcal{C}$ be the matrix rank-metric code $\mathrm{Mat}_{2\times 3}(\mathbb{F}_3)$ (where $n = k = 3$). Note:

$$\text{if } X = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 0 \end{pmatrix}, \text{ then } \mathrm{wt}^{\mathrm{mrk}}(X) = 2$$

$$\text{if } Y = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}, \text{ then } \mathrm{wt}^{\mathrm{mrk}}(Y) = 1$$

In the following sections, we will often consider equivalence classes of codes rather than specific codes. To define when two codes are to be considered equivalent, we consider:

Definition 2.1.6. Two rank-metric codes $X, Y \in \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ are called *equivalent* if there exists a $\mathbb{F}_q$-linear weight-preserving map $\varphi\colon \mathrm{Mat}_{m\times n}(\mathbb{F}_q) \to \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ such that $\varphi(X) = Y$. In such cases, we write $X \sim Y$.

Note that in this context, a weight-preserving morphism refers to a homomorphism that respects rank weight/distance.

2.2 Vector rank-metric codes

Although matrix rank-metric codes are interesting objects in their own right, we will presently not investigate their properties much further. Instead, we will focus on so-called *vector rank-metric codes*, which are more similar to Hamming codes in a number of ways. Consider the following definitions.

Definition 2.2.1. Let $0 < k \leq n$ be integers. Let m be an integer and q a prime power. A *vector rank-metric code* is an $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. The integer n is known as the *code length* and the *dimension* of $\mathcal{C}$ is its dimension as an $\mathbb{F}_{q^m}$ vector space. In particular, we call a code with these parameters an $[n, k]_{q^m/q}$ code. An element $c \in \mathcal{C}$ is known as a (vector rank-metric) *codeword*.

Again, we note that for such objects to make sense as codes worthy of study, we would like notions of distance, support, weight and equivalence. Rather than defining these properties explicitly, we follow e.g. [7] and find a way to embed vector rank-metric codes into the space of matrix rank-metric codes. This will allow us to import the notions already defined to the current case.

Definition 2.2.2. Let $\Gamma = \{ \gamma_1, \ldots, \gamma_m \}$ be an $\mathbb{F}_q$-basis for the vector space $\mathbb{F}_{q^m}$ and let $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$. For every $1 \leq j \leq n$ we have $v_j \in \mathbb{F}_{q^m}$, so we can use the basis Γ to write

$$v_j = \sum_{i=1}^{m} \nu_{ij} \ \gamma_i$$

where $\nu_{ij} \in \mathbb{F}_q$ for all $1 \leq j \leq m$ and all $1 \leq i \leq n$. Now, by slight abuse of notation, we define the following map:

$$\begin{aligned} \Gamma \colon \mathbb{F}_{q^m}^n &\longrightarrow \mathrm{Mat}_{m\times n}(\mathbb{F}_q) \\ v &\longmapsto (\nu_{ij})_{\substack{1\leq i\leq m,\\ 1\leq j\leq n}} \end{aligned}$$

i.e. $\Gamma(v) \in \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ is the $m \times n$ matrix whose j-th column represents the j-th coordinate of v, expanded over the basis Γ. We therefore say that $\Gamma(v)$ is the *matrix associated with the vector v with respect to the basis* Γ.

Remark. Note that the above definition differs from the one found in most of the literature (e.g. [1]). In particular, because of our choice of definition for matrix rank-metric codes, the usual definition of $\Gamma(v)$ is exactly the transpose of our definition.

We illustrate this embedding in the following example.

Example 2.2.3. Consider the field $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$. Concretely, we have

$$\mathbb{F}_{2^3} = \{ 0, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, 1 \}.$$

Note that $\Gamma = \{ 1, \alpha, \alpha^2 \}$ is an $\mathbb{F}_2$-basis for $\mathbb{F}_{2^3}$. Consider the element $v \in \mathbb{F}_{2^3}^2$ given by $v = (\alpha^2, \alpha+1)$. Note that

$$v = (\alpha^2, \alpha+1) = (0\cdot 1 + 0\cdot\alpha + 1\cdot\alpha^2, 1\cdot 1 + 1\cdot\alpha + 0\cdot\alpha^2).$$

From this, we deduce that

$$\Gamma(v) = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Using a map Γ in this way, we are able to link each vector rank-metric codeword to a matrix rank-metric codeword. We now extend this idea from codewords to entire codes.

Definition 2.2.4. Let $\Gamma = \{ \gamma_1, \ldots, \gamma_m \}$ be an $\mathbb{F}_q$-basis for the vector space $\mathbb{F}_{q^m}$ and let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric code. Then we say that $\Gamma(\mathcal{C}) := \{ \Gamma(v) \mid v \in \mathcal{C} \}$ is the *rank-metric code associated to C with respect to* Γ.

Proposition 2.2.5. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric $[n,k]_{q/q^m}$ code and let Γ, Δ be two $\mathbb{F}_q$-bases for $\mathbb{F}_{q^m}$. For any $v \in \mathcal{C}$ we have that

$$\mathrm{rowsp}(\Gamma(v)) = \mathrm{rowsp}(\Delta(v)).$$

Proof. Let $\Gamma = \{ \gamma_1, \ldots \gamma_m \}$ and $\Delta = \{ \delta_1, \ldots, \delta_m \}$. It is easy to see that

$$(\gamma_1, \ldots \gamma_m) \cdot \Gamma(v) = v = (\delta_1, \ldots, \delta_m) \cdot \Delta(v)$$

This implies that the row spaces are identical. □

Now, we make a number of definitions, the purpose of which is to 'import' constructions from the matrix rank-metric to the vector rank-metric setting. Note that this is all well-defined as a consequence of Proposition 2.2.5, since that proposition guarantees that the following is independent of choice of basis Γ.

Definition 2.2.6. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric $[n,k]_{q/q^m}$ code and let Γ be an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^m}$. For $v, w \in \mathcal{C}$, we define the vector rank-metric distance, weight and support as follows:

(i) $\delta^{\mathrm{vrk}}(v,w) := \delta^{\mathrm{mrk}}(\Gamma(v), \Gamma(w))$

(ii) $\mathrm{supp}^{\mathrm{vrk}}(v) := \mathrm{supp}^{\mathrm{mrk}}(\Gamma(v))$

(iii) $\mathrm{wt}^{\mathrm{vrk}}(v) := \mathrm{wt}^{\mathrm{mrk}}(\Gamma(v))$

In what follows, we will write δ^{rk}, $\mathrm{supp}^{\mathrm{rk}}$ and $\mathrm{wt}^{\mathrm{rk}}$ respectively for the distance, support and weight functions on both matrix and vector rank-metric codes, since they are clearly linked and it will be clear from context what we mean.

Proposition 2.2.7. Let $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ be a rank-metric codeword. Then $\mathrm{wt}^{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \mathrm{span}_{\mathbb{F}_q}(\{ v_1, \ldots, v_n \})$.

Proof. Let Γ be an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^m}$. We write:

$$\begin{aligned}\mathrm{wt}^{\mathrm{rk}}(v) &= \mathrm{wt}^{\mathrm{rk}}(\Gamma(v)) \\ &= \dim_{\mathbb{F}_q} \mathrm{rowsp}(\Gamma(v)) \\ &= \dim_{\mathbb{F}_q} \mathrm{colsp}(\Gamma(v)) \\ &= \dim_{\mathbb{F}_q} \mathrm{span}_{\mathbb{F}_q}(\{ v_1, \ldots, v_n \}),\end{aligned}$$

and we are done. □

Like we did in the case of the Hamming metric, we extend the notion of support from codewords to codes themselves. In particular, we define the support of $\mathcal{C}$ to be the sum of $\mathrm{supp}^{\mathrm{rk}}(v)$ for all $v \in \mathcal{C}$.

Definition 2.2.8. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric $[n,k]_{q/q^m}$ code. Then the *support* of $\mathcal{C}$ is defined by

$$\mathrm{supp}^{\mathrm{rk}}(\mathcal{C}) := \sum_{v \in \mathcal{C}} \mathrm{supp}^{\mathrm{rk}}(v) \subseteq \mathbb{F}_q^n.$$

Definition 2.2.9. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric $[n,k]_{q/q^m}$ code. We say that $\mathcal{C}$ is *nondegenerate* if $\mathrm{supp}^{\mathrm{rk}}(\mathcal{C}) = \mathbb{F}_q^n$. We say that $\mathcal{C}$ is *degenerate* otherwise.

Taking into account the results above, we can view vector-rank metric codes as matrix-rank metric codes (up to a choice of basis) with a more rigid structure, in the sense that they more strongly resemble Hamming-metric codes. For instance, like for Hamming-metric codes, every $[n,k]_{q^m/q}$ vector rank-metric code $\mathcal{C}$ has a (not necessarily unique) *generator matrix* $G_{\mathcal{C}} \in \mathrm{Mat}_{k \times n}(\mathbb{F}_{q^m})$, i.e. a matrix $G_{\mathcal{C}}$ such that $\mathcal{C} = \{ x \cdot G_{\mathcal{C}} \mid x \in \mathbb{F}_{q^m}^k \}$.

Proposition 2.2.10. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric $[n,k]_{q/q^m}$ code and let $G_{\mathcal{C}}$ be some generator matrix for $\mathcal{C}$. Then $\mathcal{C}$ is nondegenerate if and only if the columns of $G_{\mathcal{C}}$ are linearly independent over $\mathbb{F}_q$.

Proof. Suppose there exists an $\mathbb{F}_q$-linear relation between the columns of $G_{\mathcal{C}}$. By definition of a generator matrix, this implies a linear relation between the coordinates of every vector $v \in \mathcal{C}$. In turn, this means that there is linear relation between the columns of $\Gamma(v)$ for every $v \in \mathcal{C}$. Crucially, this linear relation between the columns is the same for every $\Gamma(v)$. Note that:

$$\operatorname{supp}^{\mathrm{rk}}(\mathcal{C}) = \sum_{v \in \mathcal{C}} \operatorname{supp}^{\mathrm{rk}}(v) = \sum_{v \in \mathcal{C}} \operatorname{rowsp}(\Gamma(v)),$$

and it is clear that the right hand side cannot be the whole space $\mathbb{F}_q^n$.

For the converse, we essentially reverse the argument. If $\mathcal{C}$ is nondegenerate, then $\sum_v \operatorname{rowsp}(\Gamma(v)) \subsetneqq \mathbb{F}_q^n$. So there is a linear dependence in the columns of $\Gamma(v)$ for every v, implying a linear relation between the columns of $G_{\mathcal{C}}$.

□

We now define what it means for two vector rank-metric codes to be equivalent.

Definition 2.2.11. Let $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^n$ be two rank-metric $[n,k]_{q^m/q}$ codes. We call $\mathcal{C}$ and $\mathcal{D}$ equivalent and write $\mathcal{C} \sim \mathcal{D}$ if there exists an $\mathbb{F}_q$-linear map $\varphi\colon \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ such that

(i) For every $x \in \mathbb{F}_{q^m}^n$ we have $\operatorname{wt}^{\mathrm{rk}}(x) = \operatorname{wt}^{\mathrm{rk}}(\varphi(x))$

(ii) $\varphi[\mathcal{C}] = \mathcal{D}$

In the Hamming case, we considered other characterisations of equivalent codes. Most notably, we found that any equivalence between codes can be expressed as a monomial matrix. In the rank-metric setting, we have a similar, though slightly more involved result.

Proposition 2.2.12 ([3], 1)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be two vector rank-metric $[n,k]_{q/q^m}$ codes. Then a map $\varphi\colon \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ with $\varphi[\mathcal{C}] = \mathcal{D}$ is weight-preserving if and only if there exist $\omega \in \mathbb{F}_{q^m}^*$ and $\Omega \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\varphi(x) = \omega x \Omega$ for all $x \in \mathbb{F}_{q^m}^n$.

Proof. First, let $\omega \in \mathbb{F}_{q^m}^*$. Using Proposition 2.2.7, we observe that for any $x \in \mathbb{F}_{q^m}^n$ we have:

$$\begin{aligned} \operatorname{wt}^{\mathrm{rk}}(\omega \cdot x) &= \dim_{\mathbb{F}_q} \operatorname{span}_{\mathbb{F}_q}(\{\, \omega \cdot x_1, \ldots, \omega \cdot x_n \,\}) \\ &= \dim_{\mathbb{F}_q} \operatorname{span}_{\mathbb{F}_q}(\{\, x_1, \ldots, x_n \,\}) \\ &= \operatorname{wt}^{\mathrm{rk}}(x), \end{aligned}$$

so scalar multiplication is weight-preserving. Similarly, elements of $\mathrm{GL}_n(\mathbb{F}_q)$ do not affect rank-weight either. We conclude that a mapping of the form $c \mapsto \omega c \Omega$ is weight-preserving.

For the converse, let $\varphi\colon \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ be a weight-preserving map such that $\varphi[\mathcal{C}] = \mathcal{D}$. Let M be the associated matrix in the canonical basis. That is, for all $x \in \mathbb{F}_{q^m}^n$ we have

$$\varphi(x) = xM, \text{ where } M = \begin{pmatrix} \text{—} & \varphi(e_1) & \text{—} \\ \text{—} & \varphi(e_2) & \text{—} \\ & \vdots & \\ \text{—} & \varphi(e_n) & \text{—} \end{pmatrix}$$

Since φ is weight-preserving, we find that

$$1 = \mathrm{wt}^{\mathrm{rk}}(e_i) = \mathrm{wt}^{\mathrm{rk}}(\varphi(e_i)) = \mathrm{wt}^{\mathrm{rk}}(M_i) = \dim_{\mathbb{F}_q} \mathrm{span}_{\mathbb{F}_q}(\{ M_{i,1}, \ldots, M_{i,n} \}),$$

where M_i denotes the i-th row of the matrix M. If we consider M_1, this means that the n elements differ only by multiplication with a scalar in $\mathbb{F}_q$. So, at a later stage, we can pull out a scalar $\omega \in \mathbb{F}_{q^m}$ so that $\omega^{-1} M_{1,j} \in \mathbb{F}_q$ for all $1 \leq j \leq n$.

Now, let $i \in \{ 2, \ldots n \}$. Like before, we argue that the dimension of the span of the elements of row M_i equals 1, since $M_i = \varphi(e_i)$, and the weight of e_i is clearly 1 (and φ is weight-preserving by assumption). Again similar to before, there exists some element $\lambda \in \mathbb{F}_{q^m}$ such that $\lambda^{-1} M_{i,j} \in \mathbb{F}_q$ for all $1 \leq j \leq n$. Now, let $\rho = e_1 + e_i$. Note that ρ has rank weight 1. We write:

$$\begin{aligned} \varphi(\rho) &= \varphi(e_1 + e_i) \\ &= \varphi(e_1) + \varphi(e_i) \\ &= M_1 + M_i \\ &= (M_{1,1} + M_{i,1}, M_{1,2} + M_{i,2}, \ldots, M_{1,n} + M_{i,n}). \end{aligned}$$

Note that the left hand side has rank weight 1 as φ is weight-preserving. So the entries in the vector on the right hand side are also linearly dependent. Without loss of generality, we assume $M_{1,1} + M_{i,1} \neq 0$ and all other entries are some $\mathbb{F}_q$-multiple of this entry.

Let $j \in \{0, \ldots, n\}$ and consider the j-th entry in the vector $f(\rho)$, i.e. $M_{1,j} + M_{i,j}$. By assumption, there exists some $\alpha \in \mathbb{F}_q$ such that $M_{1,j} + M_{i,j} = \alpha(M_{1,1} + M_{i,1})$. Rewriting this, we find the following expression:

$$M_{1,j} - \alpha M_{1,1} = -M_{i,j} + \alpha M_{i,1}$$

Note that the left hand side of this equation is an element of $\mathbb{F}_q$, since we saw that $M_{1,1}, M_{1,j} \in \mathbb{F}_q$ as well as $\alpha \in \mathbb{F}_q$. The right hand side, in turn, is an element of $\lambda\mathbb{F}_q$. Since left and right hand side refer to the same element, this must be an element in $\mathbb{F}_q \cap \lambda\mathbb{F}_q$. This is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q$, meaning either $\mathbb{F}_q$ itself or the trivial subspace. Suppose the latter is the case. Then $M_{1,j} - \alpha M_{1,1} = 0$, i.e. $M_{1,j} = \alpha M_{1,1}$. This would mean the i-th row is a multiple of the first row, implying the matrix M is not of full rank. However, since φ is a bijection, M is invertible, so this is false. Instead, we get that $\mathbb{F}_q \cap \lambda\mathbb{F}_q = \mathbb{F}_q$. This means $\lambda \in \mathbb{F}_q$, so the elements of the i-th row are in $\mathbb{F}_q$. Since i was chosen arbitrarily, this means every row has entries in $\mathbb{F}_q$ and we are done.

□

This proposition gives us a characterisation of equivalent codes which is easier to work with in certain contexts, as we will see later. Lastly, we define a notion of duality for vector rank-metric codes.

Definition 2.2.13. The *dual* of a vector rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is given by

$$\mathcal{C}^\perp = \{ v \in \mathbb{F}_{q^m}^n \mid u \cdot v^\top = 0 \text{ for all } u \in \mathcal{C} \}$$

2.3 $[n, k]_{q/q^m}$ systems

In section 1.2 we noted the existence of a 1-to-1 correspondence between equivalence classes of nondegenerate $[n, k]_q$ Hamming-metric codes and equivalence classes of projective $[n, k]_q$ systems. In this section, we will prove a similar result for equivalence classes of $[n, k]_{q^m/q}$ vector rank-metric codes and $[n, k]_{q^m/q}$ systems. We start by following the definition from [11]:

Definition 2.3.1. An $[n, k]_{q^m/q}$ *system* is a linear $\mathbb{F}_q$-space $\mathcal{U} \subseteq \mathbb{F}_{q^m}^k$ such that

(i) $\dim_{\mathbb{F}_q} \mathcal{U} = n$

(ii) There exists no hyperplane $h \subseteq \mathbb{F}_{q^m}^k$ such that h contains all elements of $\mathcal{U}$

Since we are interested in equivalence classes of systems, we introduce an appropriate notion of equivalence in the following definition.

Definition 2.3.2. Two $[n,k]_{q^m/q}$ systems $\mathcal{U}$ and $\mathcal{U}'$ are equivalent if there exists an $\mathbb{F}_{q^m}$-isomorphism $\varphi\colon \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^k$ such that $\varphi[\mathcal{U}] = \mathcal{U}'$.

Theorem 2.3.3 ([11], Thm 2)**.** There is a 1-to-1 correspondence between the set of equivalence classes of nondegenerate vector rank-metric $[n,k]_{q/q^m}$ codes and the set of equivalence classes of $[n,k]_{q/q^m}$ systems.

Proof. Consider some equivalence class of $[n,k]_{q^m/q}$ systems and let $\mathcal{U}$ be some arbitrary system in that class. Since $\mathcal{U}$ is a subspace of dimension n by assumption, we can take a basis $(u_1, u_2, \dots u_n)$ where $u_i \in \mathbb{F}_{q^m}^k$ for all $1 \leq i \leq n$. Now, we define a matrix G by setting

$$G := \begin{pmatrix} | & | & \cdots & | \\ u_1 & u_2 & \dots & u_n \\ | & | & \cdots & | \end{pmatrix}$$

Since every u_i is a vector of length k, we find that $G \in \mathrm{Mat}_{k\times n}(\mathbb{F}_{q^m})$. Let $\mathcal{C}$ be the code generated by G. We have to prove that G is full rank and defines a nondegenerate code.

Suppose G is not of full rank. Then there linearly dependent rows, i.e. there exists some $\kappa \in \mathbb{F}_{q^m}^*$ such that $\kappa u_i^\top = 0$ for all $i \in [n]$. But then the hyperplane $h_\kappa \subseteq \mathbb{F}_{q^m}^k$ defined by $h_\kappa\colon \kappa x^\top = 0$ contains all points in $\mathcal{U}$ which is a contradiction. So G has full rank. Now, note that by Proposition 2.2.10, a degenerate code has an $\mathbb{F}_q$-linear dependency between the columns of any generator matrix. However, since the columns in the matrix G are basis elements, there cannot be a linear dependence. So G defines a nondegenerate code.

We have yet to prove that equivalent systems are mapped to equivalent codes. To see this, note that the bases of equivalent systems differ by an element from $\mathrm{GL}_k(\mathbb{F}_{q^m})$ that is the matrix representation of an isomorphism φ. It is easy to see that the generator matrices acquired from these two bases differ by the same matrix and thus define equivalent codes.

For the other direction, consider some equivalence class of nondegenerate codes and let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ rank-metric code in that class. Let G be

a generator matrix for $\mathcal{C}$ and consider its columns $g_1, \ldots, g_n$. Let $\mathcal{U}$ be the $\mathbb{F}_q$-span of the set $\{ g_1, \ldots, g_n \}$. We claim that $\mathcal{U}$ is a $[n,k]_{q^m/q}$ system. First, note that

$$\dim_{\mathbb{F}_{q^m}} \mathcal{U} = \dim_{\mathbb{F}_{q^m}} \operatorname{span}_{\mathbb{F}_{q^m}}(\{ g_1, \ldots, g_n \}) = \operatorname{rk} G = k,$$

because G is full rank as a generator matrix. Since any hyperplane in $\mathbb{F}_{q^m}^k$ is by definition of dimension $k-1$, it can never contain all points in $\mathcal{U}$, as that space has a higher dimension. Secondly, we need to show that the $\mathbb{F}_q$-dimension of $\mathcal{U}$ equals n, i.e. that the g_i are linearly independent. This follows from Proposition 2.2.10 and the fact that $\mathcal{C}$ is nondegenerate.
We claim that this construction sends equivalent codes to equivalent systems. The argument for this is identical to the one we considered in the other direction.

Lastly, it remains to be shown that these maps are each other's inverse. But this is clear from construction and we are done. □

2.4 Rank-Weight Functions

Recall that in Section 1.3, rather than a Hamming weight function $\mathrm{wt}^{\mathrm{H}} \colon \mathcal{C} \to \mathbb{Z}$ we studied the properties of the following function:

$$\begin{aligned} W_{n,k}^{\mathrm{H}} \colon \mathcal{G}^{\mathrm{H}}[n,k]_q &\longrightarrow \operatorname{Map}\big(\mathbb{F}_q^k, \mathbb{Z}_{\geq 0}\big) \\ G &\longmapsto [x \mapsto \mathrm{wt}^{\mathrm{H}}(xG)], \end{aligned}$$

where we recall that

$$\mathcal{G}^{\mathrm{H}}[n,k]_q = \{ G \in \operatorname{Mat}_{k\times n}(\mathbb{F}_q) \mid \operatorname{rk} G = k \text{ and } G \text{ has no zero columns} \}.$$

We will now consider an analogous construction for the rank-metric case.

$$\mathcal{G}^{\mathrm{rk}}[n,k]_{q^m/q} = \left\{ G \in \operatorname{Mat}_{k\times n}(\mathbb{F}_{q^m}) \;\middle|\; \begin{array}{l} \operatorname{rk} G = k \text{ and the columns of } G \\ \text{are } \mathbb{F}_q\text{-linearly independent} \end{array} \right\}$$

Now, we will define a map that has the above set as its domain.

$$\begin{aligned} W_{n,k}^{\mathrm{rk}} \colon \mathcal{G}^{\mathrm{rk}}[n,k]_{q^m/q} &\longrightarrow \operatorname{Map}\big(\mathbb{F}_q^k, \mathbb{Z}_{\geq 0}\big) \\ G &\longmapsto [x \mapsto \mathrm{wt}^{\mathrm{rk}}(xG)], \end{aligned}$$

Recall that in the Hamming case, we were able to express the weight function of a code in terms of the associated projective system. More specifically, we found that

$$\mathrm{wt}^{\mathrm{H}}(c) = \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{c}) \neq 0}} \nu(f)$$

For now, we take a different path and consider the following result from [1], which we include here without proof.

Lemma 2.4.1 ([1], 3.7)**.** Let $\mathcal{C}$ be a nondegenerate rank-metric $[n,k]_{q^m/q}$ code and let $G_{\mathcal{C}}$ be a generator matrix for $\mathcal{C}$. For any nonzero $v \in \mathbb{F}_{q^m}^k$ we have that

$$\mathrm{wt}^{\mathrm{rk}}(vG_{\mathcal{C}}) = n - \dim_{\mathbb{F}_q}(\mathcal{U} \cap (\mathrm{span}_{\mathbb{F}_{q^m}}(v))^\perp),$$

where $\mathcal{U}$ is the $[n,k]_{q^m/q}$ system associated to $G_{\mathcal{C}}$, i.e. the $\mathbb{F}_q$-span of the columns of G and $(\mathrm{span}_{\mathbb{F}_{q^m}}(v))^\perp$ refers to the dual of the code generated by v.

Before moving on, let us observe that this result can actually be considered as the analogue of Lemma 1.3.3. In particular, this lemma states that for a nondegenerate Hamming-metric $[n,k]_q$ code $\mathcal{C}$, with associated projective system $(\mathcal{P}, \nu)$ we have the following equation for every $x \in \mathcal{C}$:

$$\mathrm{wt}^{\mathrm{H}}(x) = \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{x}) \neq 0}} \nu(f)$$

Note that we can easily rewrite this to

$$\mathrm{wt}^{\mathrm{H}}(x) = \sum_{f \in \mathbb{P}(\mathcal{C}^\vee)} \nu(f) - \sum_{\substack{f \in \mathbb{P}(\mathcal{C}^\vee) \\ f(\overline{x}) = 0}} \nu(f) \tag{2.1}$$

By standard linear algebra duality arguments, we know that any element w in a vector space W corresponds to a map g_w in the dual space $W^\vee$ (by taking the inner product) and vice versa. Note that this correspondence can be imported into the projectivised space. Using this, we note that every

$f \in \mathbb{P}(\mathcal{C}^\vee)$ (with $f(\overline{c}) = 0$) corresponds to an element $c_f \in \mathbb{P}(\mathcal{C})$ (with $c \cdot \overline{x}^\top = 0$. Now, let $\mathcal{Q}$ be a projective $[n,k]_q$ system with underlying set $\mathbb{P}(\mathcal{C})$ and multiplicity function μ such that $\mu(c_f) = \nu(f)$ for all $c_f \in \mathbb{P}(\mathcal{C})$. We can now rewrite (2.1) into:

$$\begin{aligned}
\mathrm{wt}^{\mathrm{H}}(x) &= \sum_{c \in \mathbb{P}(\mathcal{C})} \mu(c) - \sum_{\substack{c \in \mathbb{P}(\mathcal{C}) \\ c \cdot \overline{x}^\top = 0}} \nu(c) \\
&= |\mathcal{Q}| - \sum_{\substack{c \in \mathbb{P}(\mathcal{C}) \\ c \cdot \overline{x}^\top = 0}} \mu(c) \\
&= n - \sum_{v \in \mathrm{span}(x)^\perp} \mu(\overline{v}),
\end{aligned}$$

where $\mathrm{span}(x)^\perp$ denotes the Hamming code dual to the 1-dimensional code generated by x. This shows a striking resemblance to the result in Lemma 2.4.1.

Like in the Hamming case, 2.4.1 gives us a way to construct a weight-function from a given system - or from a given nondegenerate code, since the latter two are equivalent. In the Hamming case, we saw also Nogin's inversion formula 1.3.4, which allowed us to construct a projective system (again: or a nondegenerate code) from a given weight function. More concretely, we concluded that a given weight function defines a code up to equivalence. It turns out that in the rank-metric setting, such a result is not available. We will prove this claim in the next section.

2.5 No Extension Theorem

In the Hamming case, MacWilliams' Extension Theorem states that any weight-preserving map between codes extends to a weight-preserving map in the ambient space. In e.g. [2], the authors show (Example 2.9(a)) that the MacWilliams Extension Theorem does not hold in general for what the present thesis calls matrix rank-metric codes. It could however still be the case that the statement does hold for vector rank-metric codes. The statement would then look as follows:

Idea 2.5.1 (MacWilliams' Extension Theorem Analogue for vector rank–metric codes)**.** There is a weight-preserving $\mathbb{F}_{q^m}$-linear map φ between vector rank metric $[n,k]_q^m/q$ codes $\mathcal{C}$ and $\mathcal{D}$ if and only if there exist $\omega \in \mathbb{F}_{q^m}^*$ and $\Omega \in \mathrm{GL}_n(\mathbb{F}_q)$ such that for all $c \in \mathcal{C}$ we have $\varphi(c) = \omega \cdot c \cdot \Omega$.

Unfortunately, this statement turns out to be false, as shown in the following counterexample with $k = 1, n = 2, q = 2, m = 4$:

Example 2.5.2. We identify the field $\mathbb{F}_{2^4}$ with $\mathbb{F}_2(\alpha)$, where $\alpha^4 + \alpha + 1 = 0$. Let $\mathcal{C} \subseteq \mathbb{F}_{2^4}^2$ be the vector rank-metric code given by $\mathcal{C} = \{\, xG_{\mathcal{C}} \mid x \in \mathbb{F}_{2^4} \,\}$, where $G_{\mathcal{C}} = \begin{pmatrix} 1 & \alpha \end{pmatrix}$ denotes the generator matrix. Now, consider the following matrix:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$$

and consider the induced map φ defined by:

$$\begin{aligned} \varphi \colon \mathcal{C} &\longrightarrow \mathbb{F}_{2^4}^2 \\ c &\longmapsto cA. \end{aligned}$$

Let $\mathcal{D} \subseteq \mathbb{F}_{2^4}^2$ be the code defined as the image of φ. We claim that $\varphi \colon \mathcal{C} \to \mathcal{D}$ is weight-preserving. To see this, note that every nonzero element $c \in \mathcal{C}$ is of the form $c = \lambda(1, \alpha)$ for some $\lambda \in \mathbb{F}_{2^4}$ and so has rank-weight 2. We write

$$\varphi(c) = \varphi(\lambda(1,\alpha)) = \lambda(1,\alpha)A = \lambda(1,\alpha^2),$$

which also has rank-weight 2, proving the claim.

So, we have a map $\varphi \colon \mathcal{C} \to \mathcal{D}$ such that $\mathrm{wt}^{\mathrm{rk}}(c) = \mathrm{wt}^{\mathrm{rk}}(\varphi(c))$ for all $c \in \mathcal{C}$. We claim that there are no $\omega \in \mathbb{F}_{2^4}^*$ and $\Omega \in \mathrm{GL}_2(\mathbb{F}_2)$ such that $\varphi(c) = c \cdot \omega\Omega$ for all $c \in \mathcal{C}$. To see this, consider the element $c = (1, \alpha)$ and note that $\varphi(c) = (1, \alpha^2)$. We exhaust all possibilities:

(1) Suppose $\Omega = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then $c \cdot \omega\Omega = (\omega, \omega + \omega\alpha)$. This implies $\omega = 1$ and $\omega + \alpha\omega = \alpha^2$ which is a contradiction.

(2) Suppose $\Omega = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Then $c \cdot \omega\Omega = (\omega\alpha, \omega + \omega\alpha)$. This implies $\omega\alpha = 1$ and $\omega + \alpha\omega = \alpha^2$. The first equation implies $\omega = \alpha^{-1} = \alpha^3 + 1$ and substituting this in the second implies $\alpha^3 + 1 + \alpha^4 + \alpha = \alpha^3 = \alpha^2$ which is a contradiction.

(3) Suppose $\Omega = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $c \cdot \omega\Omega = (\omega + \omega\alpha, \omega)$. This implies $\omega + \omega\alpha = 1$ and $\omega = \alpha^2$. Substituting the latter into the former gives $\alpha^2 + \alpha^3 = 1$, which is a contradiction.

(4) Suppose $\Omega = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Then $c \cdot \omega\Omega = (\omega + \omega\alpha, \omega\alpha)$. This implies $\omega + \omega\alpha = 1$ and $\omega\alpha = \alpha^2$. The latter implies $\omega = \alpha$ and substituting this into the former gives $\alpha + \alpha^2 = 1$, which is a contradiction.

(5) Suppose $\Omega = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $c \cdot \omega\Omega = (\omega, \omega\alpha)$. This implies $\omega = 1$ and $\omega\alpha = \alpha^2$, which is a contradiction.

(6) Suppose $\Omega = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $c \cdot \omega\Omega = (\omega\alpha, \omega)$. This implies $\omega\alpha = 1$ and $\omega = \alpha^2$, which gives a contradiction when we substitute the latter into the former.

This exhausts all possibilities for $\Omega \in \mathrm{GL}_2(\mathbb{F}_2)$, thus concluding the proof that no suitable ω and Ω exist.

Remark. By way of driving the point home, we show that an Extension Theorem does indeed hold for the same code in the Hamming setting. So, consider the Hamming-metric code $\mathcal{C} \subseteq \mathbb{F}_{2^4}^2 \cong \mathbb{F}_2[\alpha]$ given by the generator matrix $G_{\mathcal{C}} = \begin{pmatrix} 1 & \alpha \end{pmatrix}$. Again, consider the map φ defined by right multiplication with the matrix A given by

$$\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$$

Let $\mathcal{D}$ be the image of φ. Note that $\varphi \colon \mathcal{C} \to \mathcal{D}$ is weight-preserving by the same argument as in the rank-metric case: any nonzero element of $\mathcal{C}$ has Hamming weight 2, as does any nonzero element of $\mathcal{D}$. Now, we claim that φ can be extended to a weight-preserving monomial map of the ambient space i.e. $\mathbb{F}_{2^4}^2 \to \mathbb{F}_{2^4}^2$. This is obvious because the matrix A is already monomial. In particular, the weight-preserving map φ is generated by the unit element in S_n and the scalar $(1, \alpha) \in (\mathbb{F}_{2^4}^*)^2$.

So, we now know that there is no analogue to MacWilliams' Extension Theorem in the vector rank-metric case. Recall that in the Hamming-metric setting, we also discussed a statement we called Weak MacWilliams (1.4.3), which said that $\mathcal{C} \sim_w \mathcal{D} \implies \mathcal{C} \sim \mathcal{D}$. That is, if there exists a weight preserving linear map $\mathcal{C} \to \mathcal{D}$, then there exists a weight-preserving linear map $\mathbb{F}_q^n \to \mathbb{F}_q^n$ that sends $\mathcal{C}$ to $\mathcal{D}$. In contrast to the (strong) MacWilliams'

Extension Theorem, the weak version does not assert that these maps coincide on $\mathcal{C}$. So, the counterexample 2.5.2 shows no analogue of MacWilliams' Extension Theorem holds in the rank-metric setting, but it does not necessarily disprove the rank-metric equivalent of Weak MacWilliams: we have seen that weight-preserving maps from $\mathcal{C} \to \mathcal{D}$ do not generally extend to weight-preserving maps in the ambient space, but it may be the case that some other weight-preserving map exists. The obvious question is the following: do we have an analogue of Weak MacWilliams in the rank-metric? The answer turns out to be negative, essentially by using the same counterexample.

Corollary 2.5.3 (No Weak MacWilliams Analogue)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be vector rank-metric $[n,k]_{q^m/q}$ codes. Suppose there is a weight-preserving $\mathbb{F}_{q^m}$-linear map $\varphi\colon \mathcal{C} \to \mathcal{D}$. Then this does not necessarily mean that there exists a weight-preserving $\mathbb{F}_{q^m}$-linear map $\psi\colon \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ that sends $\mathcal{C}$ to $\mathcal{D}$.

Proof. Consider the setting of Example 2.5.2. That is, we consider the code $\mathcal{C} \subseteq \mathbb{F}_{2^4}^n \cong \mathbb{F}_2(\alpha)$ given by $\mathcal{C} = \{\, xG_{\mathcal{C}} \mid x \in \mathbb{F}_{2^4} \,\}$, where $\alpha^4 + \alpha + 1 = 0$ and $G_{\mathcal{C}} = \begin{pmatrix} 1 & \alpha \end{pmatrix}$. Again, φ denotes right multiplication with the matrix A and we set $\mathcal{D} = \operatorname{im}\varphi$. Note that $\varphi\colon \mathcal{C} \to \mathcal{D}$ is a weight-preserving map. To prove the statement, we need to show that there exists no weight-preserving map $\psi\colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ with $\psi[\mathcal{C}] = \mathcal{D}$.

For the sake of contradiction, suppose such a map ψ does exist. Since $\mathcal{D}$ is a 1-dimensional space over $\mathbb{F}_{2^4}$, we find that all elements of $\mathcal{D}$ are $\mathbb{F}_{2^4}$-multiples of each other. In particular, the linearity of the maps φ and ψ implies that there exists some $\lambda \in \mathbb{F}_{2^4}^*$ such that $\psi(c) = \lambda\varphi(c)$ for all $c \in \mathcal{C}$. Note that by Proposition 2.2.12, there exist $\omega \in \mathbb{F}_{2^4}^*, \Omega \in \mathrm{GL}_2(\mathbb{F}_2)$ such that for all $x \in \mathbb{F}_{q^m}^n$ we have $\psi(x) = \omega x \Omega$. So, we can write for every $c \in \mathcal{C}$:

$$\lambda\varphi(c) = \psi(c) = \omega c \Omega$$

Now if we set $\omega' = \omega/\lambda \in \mathbb{F}_{2^4}^*$, we get $\varphi(c) = \omega' c \Omega$ for every $c \in \mathcal{C}$. But this contradicts our result from Example 2.5.2, where we found that φ could not be expressed in terms of such ω' and Ω. So no such map ψ can exists and we are done. □

So, we do not have an analogue of Weak MacWilliams in the rank-metric setting, either. As a final question, we might wonder whether an analogue of Nogin's Theorem 1.3.2 exists. It turns out that again, this is not the case. The proof follows by essentially the same argument as that in Theorem 1.4.3.

Corollary 2.5.4 (No Nogin Analogue)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be nondegenerate vector rank-metric $[n,k]_{q^m/q}$ codes. Suppose that $W^{\mathrm{rk}}(\mathcal{C}) = W^{\mathrm{rk}}(\mathcal{D})$. Then we do not necessarily have $\mathcal{C} \sim \mathcal{D}$.

Proof. For the sake of contradiction, suppose that the antecedent does indeed imply that $\mathcal{C} \sim \mathcal{D}$. We use this statement to prove rank-metric Weak MacWilliams, which is a contradiction because Corollary 2.5.3 shows that no such theorem can hold.

Let $\varphi\colon \mathcal{C} \to \mathcal{D}$ be a weight-preserving $\mathbb{F}_{q^m}$-linear isomorphism. Let $G_{\mathcal{C}}$ be a generator matrix for $\mathcal{C}$ and let $g_{\mathcal{C}}\colon \mathbb{F}_{q^m}^k \to \mathcal{C}$ be the associated map. Now, let $g_{\mathcal{D}}\colon \mathbb{F}_{q^m}^k \to \mathcal{D}$ be defined by $g_{\mathcal{D}} = \varphi \circ g_{\mathcal{C}}$ and let $G_{\mathcal{D}}$ be the associated matrix. Clearly, $G_{\mathcal{D}}$ is a generator matrix for $\mathcal{D}$. For any $x \in \mathbb{F}_{q^m}^k$, we can write

$$\begin{aligned} W^{\mathrm{rk}}(\mathcal{D})(x) &= \mathrm{wt}^{\mathrm{rk}}(xG_{\mathcal{D}}) \\ &= \mathrm{wt}^{\mathrm{rk}}(g_{\mathcal{D}}(x)) \\ &= \mathrm{wt}^{\mathrm{rk}}((\varphi \circ g_{\mathcal{C}})(x)) \\ &= \mathrm{wt}^{\mathrm{rk}}(g_{\mathcal{C}}(x)) \\ &= \mathrm{wt}^{\mathrm{rk}}(xG_{\mathcal{C}}) \\ &= W^{\mathrm{rk}}(\mathcal{C})(x), \end{aligned}$$

which implies that $W^{\mathrm{rk}}(\mathcal{C}) = W^{\mathrm{rk}}(\mathcal{D})$. By assumption, our this implies that $\mathcal{C} \sim \mathcal{D}$. But then we just showed that the existence of a weight-preserving map $\mathcal{C} \to \mathcal{D}$ impies the existence of a weight-preserving map on the ambient space, also sending $\mathcal{C}$ to $\mathcal{D}$, i.e. Weak MacWilliams. This is a contradiction with the previous corollary and we are done. □

As a final step, let us create the rank-metric equivalent of Figure 1.1. First, we introduce the following pieces of notation.

- $\mathcal{C}[n,k]_{q^m/q}$ denotes the set of nondegenerate rank-metric $[n,k]_{q^m/q}$ codes and we have
  - $\mathcal{C} \sim_1 \mathcal{D}$ if there exist an $\mathbb{F}_{q^m}$-linear weight-preserving map $\varphi\colon \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ such that $\varphi[\mathcal{C}] = \mathcal{D}$.
  - $\mathcal{C} \sim_w \mathcal{D}$ if there exist an $\mathbb{F}_{q^m}$-linear weight-preserving map $\varphi\colon \mathcal{C} \to \mathcal{D}$.

- $\mathcal{U}[n,k]_{q^m/q}$ denotes the set of $[n,k]_{q^m/q}$ systems and we have $\mathcal{U} \sim_2 \mathcal{U}'$ if there exist an $\mathbb{F}_{q^m}$-isomorphism $\psi\colon \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^k$ such that $\psi[\mathcal{U}] = \mathcal{U}'$.
- $\operatorname{im} W_{n,k}^{\mathrm{rk}}$ denotes the image of the map $W_{n,k}^{\mathrm{rk}}$, i.e. the set of rank weight functions $\mathbb{F}_q^k \to \mathbb{Z}_{\geq 0}$ of the form $x \mapsto \mathrm{wt}^{\mathrm{rk}}(xG)$ for some nondegenerate generator matrix G over $\mathbb{F}_{q^m}$. Two weight functions π, τ are considered equivalent if there exists an $A \in \mathrm{GL}_k(\mathbb{F}_q)$ such that $\pi(x) = \tau(xA)$ for all $x \in \mathbb{F}_q^k$.

Now, we find the following diagram:

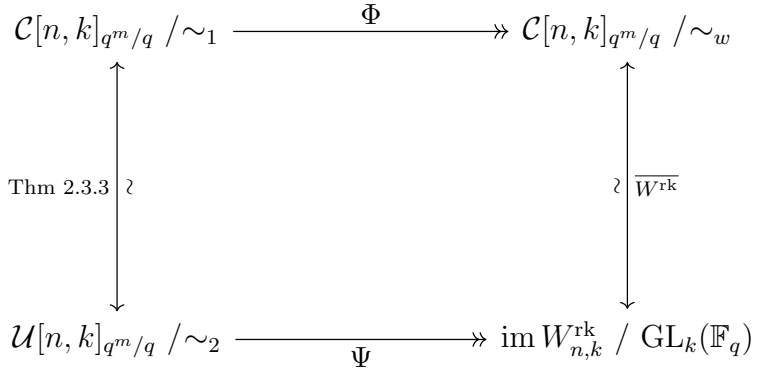


Figure 2.1: Figure of equivalences for the rank metric

So, like in Figure 1.1, we have 1-to-1 correspondences over the vertical arrows. However, in contrast to the Hamming setting, the horizontal arrows Φ and Ψ are not 1-to-1 correspondences. In particular, these maps from left to right are surjective, but not injective. Consider:

$$\begin{array}{rccc} \Phi\ :\ & \mathcal{C}[n,k]_{q^m/q}\ /\!\sim_1 & \longrightarrow & \mathcal{C}[n,k]_{q^m/q}\ /\!\sim_w \\ & \overline{\mathcal{C}} & \longmapsto & \overline{\mathcal{C}}, \end{array}$$

where the $\overline{\mathcal{C}}$ on the left denotes the equivalence class under $\sim_1$ and the $\overline{\mathcal{C}}$ on the right denotes the equivalence class under $\sim_w$. This map is well-defined, because $\mathcal{C} \sim_1 \mathcal{D}$ implies $\mathcal{C} \sim_w \mathcal{D}$. Furthermore, Φ is also clearly surjective. However, the map is not injective because of Corollary 2.5.3. Similarly, consider:

$$\begin{array}{rccl} \Psi & : & \mathcal{U}[n,k]_{q^m/q} \,/\!\sim_2 & \longrightarrow & W^{\mathrm{rk}}_{n,k} \,/\, \mathrm{GL}_k(\mathbb{F}_q) \\ & & \overline{\mathcal{U}} & \longmapsto & \overline{f}, \end{array}$$

where f is the map given by $v \mapsto n - \dim_{\mathbb{F}_q}(\mathcal{U} \cap (\mathrm{span}_{\mathbb{F}_{q^m}}(v))^{\perp})$ as in Lemma 2.4.1. The lemma implies that this is well-defined and surjective. Again, the map is not injective, because of Corollary 2.5.4.

Chapter 3

Discussion

In the previous section, we showed that there is no analogue of MacWilliams' Extension Theorem in the rank-metric setting. In particular, we provided a counterexample for the case $k = 1$, $n = 2$, $q = 2$, $m = 4$. Now, this is but a single counterexample, which immediately brings to mind a few new questions:

- Can we find more counterexamples?
- How many counterexamples are there?
- Are the counterexamples related in some way?
- Given parameters k, n, q and m, can we define a set of rank-metric $[n, k]_{q^m/q}$ codes for which an extension theorem does hold?

Unfortunately, we were unable to make much progress on these questions. We did find several more counterexamples using the SageMath code included in the appendix. However, the scope of the counterexamples is very limited, because the calculations quickly become infeasible as parameter sizes increase - at least, using the present code.

As for the fourth question listed above: the same problem of computational infeasibility arises. In order to brute-force check whether the Extension Theorem holds for certain parameter sets, we have to check every generator matrix and every possible weight-preserving map thereon. Using SageMath (see Appendix), we were able to do this for some sets with small parameters,

n	k	q	m	Result:
n=2	k=1	q=2	m=2	Statement holds
n=2	k=1	q=2	m=3	Statement holds
n=2	k=1	q=3	m=2	Statement holds
n=2	k=1	q=2	m=4	Counterexamples found
n=2	k=1	q=3	m=4	Counterexamples found

Table 3.1: Extension of weight-preserving maps in rank-metric

as shown in Table 3.1. Interestingly, it turns out that the Extension Theorem does hold for certain small parameters sets. The reason for this is not completely clear and could be subject to further research.

Appendix

Hunting for counterexamples

In order to hunt for counterexamples for the extension of weight-preserving maps in the rank-metric setting, the present thesis used the SageMath software. SageMath is a free, open-source mathematical software package [13]. Luckily the latest versions of SageMath include support for rank-metric codes, which made the implementation of our code relatively painless.

```
import random as rd

def is_weight_preserving(M, C): # M is a matrix, C is a code
    for x in C:
        if C.rank_weight_of_vector(x) != C.rank_weight_of_vector(x*M):
            return False
    return True

def check_if_rewriteable(M, F, C, Omega): # in terms of alpha and omega?
    for alpha in F:
        for omega in Omega:
            found_solution = True
            for x in C.basis():   # suffices by linearity
                if alpha*x*omega != x*M:
                    found_solution = False
                    break
            if found_solution:
```

```
                return alpha, omega
    return False, False


def check_code(C, F, nr_tries, n, q): # for a code, do some maps work
    P = MatrixSpace(F,n) # linear maps from C to F_(q^m)^n
    Omega = GL(n,GF(q)).list() # Calculate once to save time

    for counter in range(nr_tries):
        print("\t Map #",counter)
        M = P.random_element()
        if not is_weight_preserving(M,C):
            print("\t\t not weight-preserving")
            continue
        alpha, omega = check_if_rewriteable(M, F, C, Omega)
        if not alpha or not omega:
            print("\t\t COUNTEREXAMPLE: right-mult. w/ \n ", M, "\n\n\n")
        else:
            print("\t\t Can be rewritten....")



def main(nr_gen_matrices, nr_tries_per_matrix, q, m, k, n):
    F.<a> = GF(q^m)

    for i in range(nr_gen_matrices):
        gen_matrix = random_matrix(F, k, n)
        while gen_matrix == matrix(k,n):
            gen_matrix = random_matrix(F, k, n) # nontrivial codes
        print("Code ", i, ":\n\n")
        print(gen_matrix)
        C = codes.LinearRankMetricCode(gen_matrix, GF(q))
        check_code(C, F, nr_tries_per_matrix, n, q)
        print("----------------------\n")

def get_parameters(max_size):
    k = max_size
```

```
55      n = max_size # so they start too big
56      while k*n > max_size: # calculations quickly become infeasible...
57          k = rd.randint(1,3)
58          n = rd.randint(k, k+3)
59      return k,n
60
61
62  for experiment in range(1000):
63      nr_gen_matrices = 5
64      nr_tries_per_matrix = 5
65      q = 3
66      m = 4
67      k, n = get_parameters(4)
68      print("--------------------------")
69      print("EXPERIMENT NR", experiment, ":q=",q,"m=",m,"k=",k,",n=",n)
70      print("--------------------------")
71      main(nr_gen_matrices, nr_tries_per_matrix, q, m, k, n)
```

Verifying statement for small parameter sets

As shown in in Table 3.1, it turns out that weight-preserving maps between two vector rank-metric codes can be extended to weight-preserving maps on the ambient space for certain smaller parameter sets. We acquired this result by simply brute forcing all possible codes (i.e. generator matrices) for these codes and checking whether weight-preserving maps can be extended. This was done using the below script. Note that it is extremely similar to the code above for finding counterexamples. Yet, we decided to include it in its entirety for purposes of clarity.

```
def is_weight_preserving(M, C): # M is a matrixc, C is a code
    for x in C:
        if C.rank_weight_of_vector(x) != C.rank_weight_of_vector(x*M):
            return False
    return True

def check_if_rewriteable(M, F, C, Omega): # in terms of alpha and omega?
    for alpha in F:
        for omega in Omega:
            found_solution = True
            for x in C.basis():   # suffices by linearity
                if alpha*x*omega != x*M:
                    found_solution = False
                    break
            if found_solution:
                return alpha, omega
    return False, False


def check_code(C, F, n, q, Maps, Omega): # for a code, do some maps work

    for j, M in enumerate(Maps):
        if not is_weight_preserving(M,C):
            continue
        alpha, omega = check_if_rewriteable(M, F, C, Omega)
        if not alpha or not omega:
```

```
            print("\t\t COUNTEREXAMPLE: right-mult. w/ \n ", M, "\n\n\n")
    print("All weight-preserving maps can be rewritten...")


def main(q,m):
    k = 1
    n = 2

    F.<a> = GF(q^m)
    Gens = MatrixSpace(F, k, n) # set of generator matrices
    Maps = GL(n,F).list() # maps from C to D are invertible
    Omega = GL(n, GF(q)) # options for omega

    for i,gen_matrix in enumerate(Gens):
        if gen_matrix == matrix(k,n):
            continue # nontrivial codes
        print("Code ", i, ": " , gen_matrix, "\n\n")
        C = codes.LinearRankMetricCode(gen_matrix, GF(q))
        check_code(C, F, n, q, Maps, Omega)
        print("----------------------\n")
```

Bibliography

[1] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani, *Linear cutting blocking sets and minimal codes in the rank metric*, Journal of Combinatorial Theory, Series A, 192 (2022), p. 105658.

[2] A. Barra and H. Gluesing-Luerssen, *MacWilliams extension theorems and the local–global property for codes over Frobenius rings*, Journal of Pure and Applied Algebra, 219 (2015), pp. 703–728.

[3] T. P. Berger, *Isometries for rank distance and permutation group of Gabidulin codes*, IEEE Trans. Inf. Theory, 49 (2003), pp. 3016–3019.

[4] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, Journal of Combinatorial Theory, Series A, 25 (1978), pp. 226–241.

[5] E. Gabidulin, *Theory of codes with maximum rank distance (translation)*, Problems of Information Transmission, 21 (1985), pp. 1–12.

[6] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani, *Rank-metric codes and q-polymatroids*, Journal of Algebraic Combinatorics, 52 (2019), pp. 1–19.

[7] E. Gorla and A. Ravagnani, *Codes endowed with the rank metric*, 2017. arXiv:1710.02067.

[8] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2010.

[9] J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, The Bell System Technical Journal, 42 (1963), pp. 79–94.

[10] D. Nogin, *Weight functions and generalized Hamming weights of linear codes*, Problems of Information Transmission, 41 (2005), pp. 91–104.

[11] T. H. Randrianarisoa, *A geometric approach to rank metric codes and a classification of constant weight codes*, Designs, Codes, and Cryptography, 88 (2020), pp. 1331–1348.

[12] A. Ravagnani, *Rank-metric codes and their duality theory*, Designs, Codes, and Cryptography, 80 (2015), pp. 197–216.

[13] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022. `https://www.sagemath.org`.

[14] M. Tsfasman, S. Vlăduț, and D. Nogin, *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs vol. 139, American Mathematical Society, Providence, RI, 2007.