

Duality of Codes Supported on Regular Lattices, with an Application to Enumerative Combinatorics

Alberto Ravagnani*

Institut de Mathématiques
Université de Neuchâtel
Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

Abstract

We introduce a general class of regular weight functions on finite abelian groups, and study the combinatorics, the duality theory, and the metric properties of codes endowed with such functions. The weights are obtained by composing a suitable support map with the rank function of a graded lattice satisfying certain regularity properties. A regular weight on a group canonically induces a regular weight on the character group, and invertible MacWilliams identities always hold for such a pair of weights. Moreover, the Krawtchouk coefficients of the corresponding MacWilliams transformation have a precise combinatorial significance, and can be expressed in terms of the invariants of the underlying lattice. In particular, they are easy to compute in many examples. Several weight functions traditionally studied in Coding Theory belong to the class of weights introduced in this paper. Our lattice-theory approach also offers a control on metric structures that a regular weight induces on the underlying group. In particular, it allows to show that every finite abelian group admits weight functions that, simultaneously, give rise to MacWilliams identities, and endow the underlying group with a metric space structure. We propose a general notion of extremality for (not necessarily additive) codes in groups endowed with semi-regular supports, and establish a Singleton-type bound. We then investigate the combinatorics and duality theory of extremal codes, extending classical results on the weight and distance distribution of error-correcting codes. Finally, we apply the theory of MacWilliams identities to enumerative combinatorics problems, obtaining closed formulæ for the number of rectangular matrices over a finite having prescribed rank and satisfying some linear conditions.

Introduction and motivations

In Coding Theory, a MacWilliams identity expresses a linear transformation between the partition enumerator of a code and the partition enumerator of its dual code. MacWilliams identities are named after F. J. MacWilliams, who first discovered in [25] relations of this type for linear codes endowed with the Hamming weight. Analogous identities were later established for other classes of codes, most notably for codes in groups (see [4, 12, 13, 27, 33, 34] and the references therein).

An additive code $\mathcal{C} \subseteq G$ is a subgroup of a finite abelian group G , and its dual code $\mathcal{C}^* \subseteq \hat{G}$ is its character-theoretic annihilator. Codes and dual codes are subsets of different ambient spaces, and therefore their enumerators refer in general to different partitions, say \mathcal{P} and \mathcal{Q} , on G and \hat{G} , respectively. When \mathcal{P} and \mathcal{Q} are “mutually compatible”, the \mathcal{P} -distribution of a code \mathcal{C} and

*E-mail: ravagnani@ece.utoronto.ca. The author was partially supported by the Swiss National Science Foundation through grant no. 200021_150207.
MSC subject classification: 11T71, 05A15, 06B05, 20K01.

the Q -distribution of the dual code \mathcal{C}^* determine each other. The linear relations between the partition distributions are expressed by certain complex numbers called Krawtchouk coefficients. Their existence is guaranteed by the compatibility property of the partitions, but giving explicit formulæ for them is difficult in general.

Most general works on MacWilliams identities for codes in groups focus on group partitions and their duals, as these determine the existence of a MacWilliams transformation. More precisely, it is known that a partition \mathcal{P} of a finite abelian group G induces a dual partition $\hat{\mathcal{P}}$ of the character group \hat{G} . Under a certain “compatibility” assumption (called Fourier-reflexivity), the partition enumerators of a code and of its dual code associated to \mathcal{P} and $\hat{\mathcal{P}}$, respectively, determine each other via a MacWilliams transformation (see [13, 33, 34] for details). Compatible pairs were proposed in [34] with the goal of simplifying the construction of abelian association schemes on groups.

In Coding Theory however, partitions of the ambient space are generally induced by weight functions having an information-theoretic significance. The main property that usually allows error correction is the *weight* function defined on the ambient group, rather than the *partition* it induces. A given group partition can be induced by many different weights, which in general will not have good properties from a Coding Theory viewpoint. For example, they will not endow the underlying group with a metric structure. Weight functions and induced partitions are therefore not equivalent information in general.

In this paper we focus our attention on weight functions, and address the problem of constructing *general* families of *numerical* weights on finite abelian groups (rather than partitions) that yield MacWilliams identities. We achieve this combining lattice theory and discrete Fourier analysis methods, introducing a general notion of support map. One of the advantages of our approach is that it offers a control (via lattice modularity) on metric space structures induced by the weight function on the ambient group. In a second part of this work we investigate how the theory of weights on groups relate to codes’ extremality. We close the paper with a section devoted to enumerative combinatorics problems on matrices. More in detail, this paper makes the following contributions.

In Section 3 we define a regular support σ as a function on a finite abelian group G that takes values in a graded lattice \mathcal{L} with certain regularity properties. A regular support naturally induces a weight function on G via the rank function of \mathcal{L} . We show that a regular support σ on G *canonically* induces a dual regular support σ^* on the character group \hat{G} , with values in the dual lattice \mathcal{L}^* . This defines in particular a canonical and numerical weight on \hat{G} via the rank function of \mathcal{L}^* . In contrast to previous works on codes in groups, our approach concentrates on numerical weights on the groups G and \hat{G} , rather than on partitions of them.

In Section 4 we show that the weight functions induced by a regular support and its dual support, respectively, always obey a MacWilliams identity. The result relies on the specific notion of dual support, as the definition of regular support on a group does not depend on the algebraic structure of the corresponding character group. The Krawtchouk coefficients of the MacWilliams transformation are integers with a precise combinatorial significance. More precisely, they can be expressed in terms of the combinatorial invariants of the support lattice \mathcal{L} .

As a secondary result, in Section 6 we revisit the theory of MacWilliams identities associated with many weights traditionally studied in Coding Theory, showing that such weight functions factor through a suitable support map having remarkable regularity properties.

In Section 5 we show that when the lattice associated with a regular support is modular, then the underlying group can be naturally endowed with a metric space structure. We then prove that one can systematically construct (over any finite abelian group) numerical weight functions that, *simultaneously*, yield MacWilliams identities, and endow the ambient group with a metric structure. This is particularly interesting from a Coding Theory perspective, as the triangle inequality is usually a key property enabling error correction.

In Section 7 we propose a general notion of extremality for codes in groups endowed with semi-regular support functions, establishing a generalized Singleton bound in this context. Our definition of extremality only relies on codes' cardinality, which is a fundamental code parameter from an information-theoretic viewpoint. This differs from previous general approaches, where extremal codes are defined in terms of their interaction with the dual code via algebraic properties of their inner distributions. We also study the combinatorics and duality theory of the codes attaining the Singleton-type bound, extending classical results to the general framework of codes in groups.

In Section 8 the theory of MacWilliams identities is applied to enumerative combinatorics problems, deriving explicit formulæ for the number of $k \times m$ matrices over \mathbb{F}_q having prescribed rank and satisfying certain linear conditions (e.g., having zeroes in a given set of diagonal entries). In particular, we answer a generalized question of R. Stanley.

1 Groups, Codes, and Weight Functions

Let $(G, +)$ be an abelian group. The **character group** of G , denoted by (\hat{G}, \cdot) , is the set of group homomorphisms $\chi : G \rightarrow \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ endowed with pointwise multiplication, i.e., for $\chi_1, \chi_2 \in \hat{G}$,

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g)\chi_2(g), \quad \text{for all } g \in G.$$

The neutral element of (\hat{G}, \cdot) is the **trivial character** $\varepsilon \equiv 1$ of G . The groups G and $\hat{\hat{G}}$ are canonically isomorphic via the map $\psi : G \rightarrow \hat{\hat{G}}$ defined, for $g \in G$, by $\psi(g)(\chi) := \chi(g)$ for all $\chi \in \hat{G}$. It is well-known that when $(G, +)$ is finite and abelian the groups $(G, +)$ and (\hat{G}, \cdot) are isomorphic, not canonically in general. In particular, $|G| = |\hat{G}|$. Notice that for all $n \geq 1$ we have $\widehat{\widehat{G}^n} = \hat{G}^n$, where $(\chi_1, \dots, \chi_n) \in \widehat{G}^n$ is defined, for all $(g_1, \dots, g_n) \in G^n$, by

$$(\chi_1, \dots, \chi_n)(g_1, \dots, g_n) := \prod_{i=1}^n \chi_i(g_i).$$

Definition 1. Let G be a finite abelian group. A **code** in G is a subgroup $\mathcal{C} \subseteq G$. The **dual** of \mathcal{C} is the code $\mathcal{C}^* := \{\chi \in \hat{G} : \chi(g) = 1 \text{ for all } g \in \mathcal{C}\} \subseteq \hat{G}$. We say that \mathcal{C} is **trivial** if $\mathcal{C} = \{0\}$ or $\mathcal{C} = G$. The code **generated** by codes $\mathcal{C}, \mathcal{D} \subseteq G$ is the code $\mathcal{C} + \mathcal{D} := \{c + d : c \in \mathcal{C}, d \in \mathcal{D}\} \subseteq G$.

The following remark summarizes some properties of duality. The proof is left to the reader.

Remark 2. Let $\mathcal{C} \subseteq G$ be a code. Then $|\mathcal{C}| \cdot |\mathcal{C}^*| = |G| = |\hat{G}|$. Moreover, identifying G and $\hat{\hat{G}}$ we have $\mathcal{C}^{**} = \mathcal{C}$. Finally, duality and sum of codes relate as follows.

1. Let $\mathcal{C}, \mathcal{D} \subseteq G$ be codes. Then $|\mathcal{C} + \mathcal{D}| \times |\mathcal{C} \cap \mathcal{D}| = |\mathcal{C}| \cdot |\mathcal{D}|$.
2. Let $\mathcal{C}_1, \dots, \mathcal{C}_t \subseteq G$ be codes, $t \geq 2$. We have $\bigcap_{i=1}^t \mathcal{C}_i^* = (\sum_{i=1}^t \mathcal{C}_i)^*$.

Definition 3. Let G be a finite abelian group. A **weight** on G is a function $\omega : G \rightarrow X$, where X is a finite non-empty set. The ω -**distribution** of a code $\mathcal{C} \subseteq G$ is the integer vector $(W_a(\mathcal{C}, \omega) : a \in X)$, where $W_a(\mathcal{C}, \omega) := |\{g \in \mathcal{C} : \omega(g) = a\}|$ for all $a \in X$.

A weight function on a group naturally induces a partition of it as follows.

Definition 4. Let $\omega : G \rightarrow X$ be a weight. For all $a \in \omega(G)$ define $P_a(\omega) := \{g \in G : \omega(g) = a\}$. Then

$$\mathcal{P}(\omega) := \bigsqcup_{a \in \omega(G)} P_a(\omega)$$

is the **partition** of G induced by ω . We say that weight functions $\omega : G \rightarrow X$ and $\omega' : G \rightarrow X'$ are **equivalent** if $\mathcal{P}(\omega) = \mathcal{P}(\omega')$, and in this case we write $\omega \sim \omega'$.

Let $\omega : G \rightarrow X$ and $\tau : \hat{G} \rightarrow Y$ be weights. We say that (ω, τ) is a **compatible pair** if for all $b \in \tau(\hat{G})$ and for all $g, g' \in G$ with $\omega(g) = \omega(g')$ one has

$$\sum_{\chi \in P_b(\tau)} \chi(g) = \sum_{\chi \in P_b(\tau)} \chi(g').$$

If this is the case, then the **Krawtchouk coefficients** associated to (ω, τ) are defined, for every $a \in \omega(G)$ and $b \in \tau(\hat{G})$, by

$$K(\omega, \tau)(a, b) := \sum_{\chi \in P_b(\tau)} \chi(g),$$

where $g \in G$ is any element with $\omega(g) = a$. When $a \notin \omega(G)$ or $b \notin \tau(\hat{G})$ we put $K(\omega, \tau)(a, b) := 0$.

Remark 5. Let $\omega : G \rightarrow X$, $\tau : \hat{G} \rightarrow Y$ be weights. Identifying G and \hat{G} one has $g(\chi) = \chi(g)$ for all $g \in G$ and $\chi \in \hat{G}$. Thus when (τ, ω) is a compatible pair the Krawtchouk coefficients associated to (τ, ω) are defined, for every $a \in \tau(\hat{G})$ and $b \in \omega(G)$, by

$$K(\tau, \omega)(a, b) = \sum_{g \in P_b(\omega)} \chi(g),$$

where $\chi \in \hat{G}$ is any character with $\tau(\chi) = a$. Again, if $a \notin \tau(\hat{G})$ or $b \notin \omega(G)$ then $K(\tau, \omega)(a, b) = 0$.

Remark 6. Let $\omega : G \rightarrow X$, $\omega' : G \rightarrow X'$, $\tau : \hat{G} \rightarrow Y$ and $\tau' : \hat{G} \rightarrow Y'$ be weights with $\omega \sim \omega'$ and $\tau \sim \tau'$. There exist bijections $\pi : \omega'(G) \rightarrow \omega(G)$ and $\eta : \tau'(\hat{G}) \rightarrow \tau(\hat{G})$ such that $\omega = \pi \circ \omega'$ and $\tau = \eta \circ \tau'$. Moreover, it is easy to see that if (ω, τ) is a compatible pair, then (ω', τ') is also a compatible pair, and for all $a \in \omega'(G)$ and $b \in \tau'(\hat{G})$ one has

$$K(\omega', \tau')(a, b) = K(\omega, \tau)(\pi(a), \eta(b)).$$

Therefore the Krawtchouk coefficients associated to (ω', τ') are essentially the same as the Krawtchouk coefficients associated to (ω, τ) , up to a suitable bijection. For this reason most authors concentrate on group partitions when studying Krawtchouk coefficients in the context of additive codes.

In Coding Theory however, given a “numerical” weight function $\omega : G \rightarrow X \subseteq \mathbb{N}$, one naturally attempts to define a distance d_ω on G by setting $d_\omega(g, g') := \omega(g - g')$ for all $g, g' \in G$. This is usually crucial for error correction. It is easy to construct groups G and weights $\omega, \omega' : G \rightarrow X \subseteq \mathbb{N}$ such that $\omega \sim \omega'$, d_ω is a distance function, but $d_{\omega'}$ is not. This is the reason why in this work we concentrate on numerical weights, rather than on group partitions.

It is well known [33, Theorem 1] that compatible pairs of weights yield MacWilliams-type identities as follows.

Theorem 7 (MacWilliams Identities). Let G be a finite abelian group, and let $\omega : G \rightarrow X$ and $\tau : \hat{G} \rightarrow Y$ be weights. Assume that (ω, τ) is compatible. Then for all codes $\mathcal{C} \subseteq G$ we have

$$W_b(\mathcal{C}^*, \tau) = \frac{1}{|\mathcal{C}|} \sum_{a \in X} K(\omega, \tau)(a, b) W_a(\mathcal{C}, \omega).$$

for all $b \in Y$. In particular, the ω -distribution of \mathcal{C} determines the τ -distribution of \mathcal{C}^* .

Proof. By the definition of compatible pair, the partition $\mathcal{P}(\omega)$ is finer than $\widehat{\mathcal{P}(\tau)}$, the dual of the partition $\mathcal{P}(\tau)$ (see [13, Definition 2.1]). The result now follows from [13, Theorem 2.7]. \square

Notice that the identities of Theorem 7 express a linear transformation between the ω -distribution of the code $\mathcal{C} \subseteq G$ and the τ -distribution of its dual code $\mathcal{C}^* \subseteq \hat{G}$. The matrix of the linear transformation, $K(\omega, \tau)$, is called the **Krawtchouk matrix**. Its rows are indexed by $b \in Y$, and its columns are indexed by $a \in X$.

Remark 8. The fact that a pair (ω, τ) is compatible does not imply that (τ, ω) is compatible. This corresponds to the fact that the MacWilliams transformation is not invertible. The most interesting scenario is when both (ω, τ) and (τ, ω) are compatible, i.e., when ω and τ are **mutually** compatible.

We conclude this section by mentioning the product weight and the symmetrized weight induced by a weight function. See [13, 33] for a more complete analysis.

Definition 9. Let $\omega : G \rightarrow X$ be a weight, and let $n \geq 1$ be an integer.

1. The **product weight** on G^n associated to ω is the function $\omega^n : G^n \rightarrow X^n$ defined, for all (g_1, \dots, g_n) , by $\omega^n(g_1, \dots, g_n) := (\omega(g_1), \dots, \omega(g_n))$.
2. Assume that $X = \{0, \dots, r\}$ and for all $(c_1, \dots, c_n) \in X^n$ let $\text{cmp}(c) := (e_0, \dots, e_r)$, where $e_i := |\{1 \leq j \leq n : c_j = x_i\}|$ for all $0 \leq i \leq r$. The **symmetrized weight** on G^n associated to ω is the function $\omega_{\text{sym}}^n : G^n \rightarrow \{0, \dots, n\}^{r+1}$ defined, for all $(g_1, \dots, g_n) \in G^n$, by $\omega_{\text{sym}}^n(g_1, \dots, g_n) := \text{cmp}(\omega^n(g_1, \dots, g_n))$.

Compatibility of pairs is preserved by products and symmetrization.

Proposition 10. Let $\omega : G \rightarrow X$ and $\tau : \hat{G} \rightarrow Y$ be weights. Let $n \geq 1$, $r := |X|$ and $s := |Y|$. Assume that (ω, τ) is compatible. Write $K = K(\omega, \tau)$ for ease of notation. The following hold.

1. The pair (ω^n, τ^n) is compatible. Moreover, for $a = (a_1, \dots, a_n) \in X^n$ and $b = (b_1, \dots, b_n) \in Y^n$ we have

$$K(\omega^n, \tau^n)(a, b) = \prod_{j=1}^n K(a_j, b_j).$$

2. Assume $X = \{0, \dots, r\}$ and $Y = \{0, \dots, s\}$. The pair $(\omega_{\text{sym}}^n, \tau_{\text{sym}}^n)$, is compatible. Moreover, for $d = (d_0, \dots, d_r) \in \{1, \dots, n\}^{r+1}$ and $e \in \{1, \dots, n\}^{s+1}$ we have

$$K(\omega_{\text{sym}}^n, \tau_{\text{sym}}^n)(d, e) = \sum_{\substack{b \in Y^n \\ \text{cmp}(b) = e}} \prod_{j=1}^{d_0} K(0, b_j) \prod_{j=d_0+1}^{d_0+d_1} K(1, b_j) \cdots \prod_{j=d_0+\dots+d_{r-1}+1}^{d_0+\dots+d_r} K(r, b_j).$$

Proof. Let $(a_1, \dots, a_n) \in \omega^n(G^n)$ and $(b_1, \dots, b_n) \in \tau^n(\hat{G}^n)$. For any element $(g_1, \dots, g_n) \in G^n$ with $\omega^n(g_1, \dots, g_n) = (a_1, \dots, a_n)$ one has

$$\sum_{\substack{(\chi_1, \dots, \chi_n) \in \hat{G}^n \\ \tau^n(\chi_1, \dots, \chi_n) = (b_1, \dots, b_n)}} (\chi_1, \dots, \chi_n)(g_1, \dots, g_n) = \prod_{j=1}^n K(a_j, b_j). \quad (1)$$

This shows that (ω^n, τ^n) is a compatible pair, and proves the first formula in the statement. Now we study the symmetrized weight. Let $(d_0, \dots, d_r) \in \omega_{\text{sym}}^n(G^n)$ and $(e_0, \dots, e_s) \in \tau_{\text{sym}}^n(\hat{G}^n)$, and let $(g_1, \dots, g_n) \in G^n$ with $\omega_{\text{sym}}^n(g_1, \dots, g_n) = (d_0, \dots, d_r)$. Using (1) we compute

$$\sum_{\substack{(\chi_1, \dots, \chi_n) \in \hat{G}^n \\ \tau_{\text{sym}}^n(\chi_1, \dots, \chi_n) = (e_0, \dots, e_s)}} (\chi_1, \dots, \chi_n)(g_1, \dots, g_n) = \sum_{\substack{(b_1, \dots, b_n) \in Y^n \\ \text{cmp}(b_1, \dots, b_n) = (e_0, \dots, e_s)}} \prod_{j=1}^n K(a_j, b_j), \quad (2)$$

where $(a_1, \dots, a_n) := \omega^n(g_1, \dots, g_n)$. Up to a permutation of the entries of (a_1, \dots, a_n) , without loss of generality we may assume $a_i \leq a_{i+1}$ for all $1 \leq i \leq n-1$. Therefore (2) becomes

$$\sum_{\substack{b \in Y^n \\ \text{cmp}(b)=e}} \prod_{j=1}^{d_0} K(0, b_j) \prod_{j=d_0+1}^{d_0+d_1} K(1, b_j) \cdots \prod_{j=d_0+\dots+d_{r-1}+1}^{d_0+\dots+d_r} K(r, b_j).$$

The expression above only depends on (d_0, \dots, d_r) and (e_0, \dots, e_s) . This shows that $(\omega_{\text{sym}}^n, \tau_{\text{sym}}^n)$ is compatible, and proves the second formula in the statement. \square

Proposition 10 shows that the computation of the Krawtchouk coefficients of the pairs (ω^n, τ^n) and $(\omega_{\text{sym}}^n, \tau_{\text{sym}}^n)$ reduces to the computation of the Krawtchouk coefficients of (ω, τ) .

In the reminder of the paper we concentrate on numerical weight functions on finite abelian groups arising from lattices.

2 Regular Lattices

In this section we briefly recall some basic notions on posets and lattices, and propose a definition of regular lattice. See [31, Chapter 3] for a general introduction to posets. Throughout this paper we only treat finite lattices.

Given a poset (L, \leq) and $S, T \in L$, we write $S < T$ for $S \leq T$ and $S \neq T$. We write $S \triangleleft T$ if $S < T$ and there is no $U \in L$ with $S < U < T$. In this case we say that T **covers** S . Recall moreover that a **meet** of $S, T \in L$ is a maximal lower bound for both S and T . Similarly, a **join** of $S, T \in L$ is a minimal upper bound for both S and T .

Definition 11. A **lattice** is a poset (L, \leq) where every $S, T \in L$ have a unique meet and a unique join, denoted by $S \wedge T$ and $S \vee T$, respectively.

Meet and join of a lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ define two binary, commutative and associative operations $\wedge, \vee : L \times L \rightarrow L$. In particular, for any non-empty finite subset $M \subseteq L$, the lattice elements $\bigwedge \{S : S \in M\}$ and $\bigvee \{S : S \in M\}$ are well defined. When \mathcal{L} is **finite** (i.e., L is finite), we set $0_{\mathcal{L}} := \bigwedge \{S : S \in L\}$ and $1_{\mathcal{L}} := \bigvee \{S : S \in L\}$.

A finite lattice \mathcal{L} is **graded** of **rank** r if all maximal chains (with respect to \leq) in \mathcal{L} have the same length r . We denote the rank of a graded lattice \mathcal{L} by $\text{rk}(\mathcal{L})$.

Remark 12. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a finite graded lattice of rank r . There exists a unique function $\rho_{\mathcal{L}} : L \rightarrow \{0, \dots, r\}$, called the **rank function** of \mathcal{L} , with $\rho_{\mathcal{L}}(0_{\mathcal{L}}) = 0$ and $\rho_{\mathcal{L}}(T) = \rho_{\mathcal{L}}(S) + 1$ whenever $S \triangleleft T$ (see [31, page 281]). The function $\rho_{\mathcal{L}}$ is monotonic, i.e., $\rho_{\mathcal{L}}(S) \leq \rho_{\mathcal{L}}(T)$ whenever $S \leq T$. Moreover, $\rho_{\mathcal{L}}(L) = \{0, \dots, r\}$, and $0_{\mathcal{L}}$ and $1_{\mathcal{L}}$ are the only elements of rank 0 and r , respectively.

The **dual** of a lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ is the lattice $\mathcal{L}^* = (L, \preceq, \wedge, \vee)$, where $S \preceq T$ if and only if $T \leq S$, $\wedge := \vee$ and $\vee := \wedge$. If \mathcal{L} is finite (and so \mathcal{L}^* is finite) then $0_{\mathcal{L}^*} = 1_{\mathcal{L}}$ and $1_{\mathcal{L}^*} = 0_{\mathcal{L}}$. Clearly, $\mathcal{L}^{**} = \mathcal{L}$. Notice moreover that \mathcal{L} is graded if and only if \mathcal{L}^* is graded. If this is the case, then $\text{rk}(\mathcal{L}) = \text{rk}(\mathcal{L}^*)$ and $\rho_{\mathcal{L}^*}(S) = \text{rk}(\mathcal{L}) - \rho_{\mathcal{L}}(S)$ for all $S \in L$.

Definition 13. Let $\mathcal{L} = (L, \leq)$ be a finite poset. Then the **Möbius function** of \mathcal{L} is the map $\mu_{\mathcal{L}} : \{(S, T) \in L \times L : S \leq T\} \rightarrow \mathbb{Z}$ inductively defined by $\mu_{\mathcal{L}}(S, S) = 1$ for all $S \in L$, and

$$\mu_{\mathcal{L}}(S, T) = - \sum_{S \leq U < T} \mu_{\mathcal{L}}(S, U) \quad \text{for all } S, T \in L \text{ with } S < T.$$

Using the fact that a lattice \mathcal{L} and its dual lattice \mathcal{L}^* are anti-isomorphic, one can show that $\mu_{\mathcal{L}^*}(S, T) = \mu_{\mathcal{L}}(T, S)$ for all $S, T \in \mathcal{L}$ (see [30, Proposition 2.1.10]).

Now we introduce regular lattices, which are central in our approach.

Definition 14. A finite graded lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ of rank r is **regular** if the following hold.

- (a) For all $T \in L$ and for all integers $0 \leq s \leq r$,
 - the number of $S \in L$ with $\rho_{\mathcal{L}}(S) = s$ and $S \leq T$ only depends on s and $\rho_{\mathcal{L}}(T)$,
 - the number of $S \in L$ with $\rho_{\mathcal{L}}(S) = s$ and $T \leq S$ only depends on s and $\rho_{\mathcal{L}}(T)$.
- (b) For all $S, T \in L$ with $S \leq T$, the Möbius function $\mu_{\mathcal{L}}(S, T)$ only depends on $\rho_{\mathcal{L}}(S)$ and $\rho_{\mathcal{L}}(T)$.

A regular lattice is shown in Figure 1 via its Hasse diagram. More examples will be given in Section 6. We also notice that property (a) of Definition 14 does not imply property (b). For example, let \mathcal{L} be the lattice whose Hasse diagram is depicted in Figure 2. Then \mathcal{L} satisfies property (a), as one can easily check. However, $\mu_{\mathcal{L}}(S_1, T_1) = 1$ and $\mu_{\mathcal{L}}(S_2, T_1) = 0$, violating property (b).

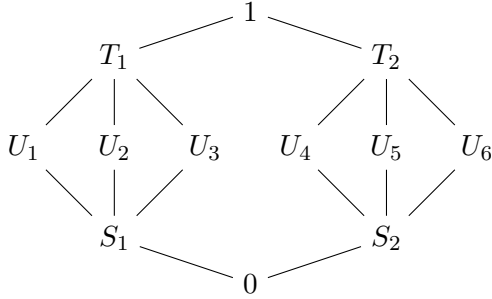


Figure 1: A regular lattice

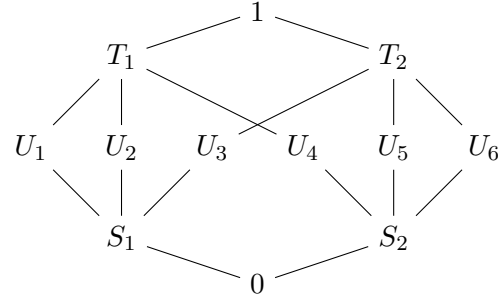


Figure 2: A non-regular lattice

We can now define the main combinatorial invariants of a regular lattice as follows.

Notation 15. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular lattice of rank r . For all integers $0 \leq s, t \leq r$ we define

$$\mu_{\leq}(s, t) := |\{S \in L : S \leq T, \rho_{\mathcal{L}}(S) = s\}| \quad \text{and} \quad \mu_{\geq}(s, t) := |\{S \in L : T \leq S, \rho_{\mathcal{L}}(S) = s\}|,$$

where $T \in L$ is any element with $\rho_{\mathcal{L}}(T) = t$. For any given integers $0 \leq s \leq t \leq r$ we also set

$$\mu_{\mathcal{L}}(s, t) := \mu_{\mathcal{L}}(S, T),$$

where $S, T \in L$ are arbitrary with $S \leq T$, $\rho_{\mathcal{L}}(S) = s$, and $\rho_{\mathcal{L}}(T) = t$. For $s > t$ we set $\mu_{\mathcal{L}}(s, t) := 0$.

Remark 16. A different notion of (semi)lattice regularity was proposed by Delsarte in [9]. The definition of Delsarte is motivated by applications to Coding Theory via association schemes, rather than Fourier analysis. Our approach and purposes are different from those of [9]. For example, support maps, duality and cardinality-related extremality notions are not treated in [9]. Notice moreover that in contrast to Delsarte's approach, in our setting the lattice structure is defined on an independent “support space”, rather than on the ambient group.

The following result easily follows from the definitions and from the properties of the Möbius function. It expresses the parameters of the dual of a regular lattice \mathcal{L}^* in terms of those of \mathcal{L} .

Proposition 17. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular lattice of rank r . Then $\mathcal{L}^* = (L, \preceq, \lambda, \gamma)$ is regular of rank r , and for all $0 \leq s, t \leq r$ we have

$$\mu_{\preceq}(s, t) = \mu_{\geq}(r - s, r - t), \quad \mu_{\succeq}(s, t) = \mu_{\leq}(r - s, r - t), \quad \text{and} \quad \mu_{\mathcal{L}^*}(s, t) = \mu_{\mathcal{L}}(r - t, r - s).$$

We conclude this section giving a sufficient condition for lattice regularity that does not involve the Möbius function. It can be used, for example, to easily test the regularity of the lattice represented in Figure 1.

Proposition 18. Let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a finite graded lattice. Assume that for every $S, T \in L$ with $S \leq T$ and for every $\rho_{\mathcal{L}}(S) \leq i \leq \rho_{\mathcal{L}}(T)$ the number $\{U \in L : S \leq U \leq T \text{ and } \rho_{\mathcal{L}}(U) = i\}$ only depends on i , $\rho_{\mathcal{L}}(S)$ and $\rho_{\mathcal{L}}(T)$. Then \mathcal{L} is regular.

Proof. Property (a) of Definition 14 is immediate, and property (b) can be proved by induction on $\rho_{\mathcal{L}}(T) - \rho_{\mathcal{L}}(S)$ using the definition of the Möbius function. \square

3 Regular Supports and Duality

In this section we propose a definition of regular support on a finite abelian group, and establish some preliminary properties that will be needed in the sequel. In particular, we show that a regular support on a finite abelian group G canonically induces a regular support on \hat{G} .

As we will see in Section 6, our definition of regular support generalizes both the Hamming and the rank support for codes endowed with the Hamming and the rank weight, respectively. This explains the use of the word “support” in this paper.

Notation 19. If G is a group, $\mathcal{L} = (L, \leq)$ is a poset and $\sigma : G \rightarrow L$ is any function, then for all $S \in L$ we set $G_{\sigma}(S) := \{g \in G : \sigma(g) \leq S\}$.

Definition 20. Let $(G, +)$ be a finite abelian group, and let $\mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular lattice. A **regular support** on G with values in \mathcal{L} is a function $\sigma : G \rightarrow L$ that satisfies the following.

- (A) $\sigma(g) = 0_{\mathcal{L}}$ if and only if $g = 0$.
- (B) $\sigma(g) = \sigma(-g)$ for all $g \in G$.
- (C) $\sigma(g_1 + g_2) \leq \sigma(g_1) \vee \sigma(g_2)$ for all $g_1, g_2 \in G$.
- (D) $G_{\sigma}(S_1 \vee S_2) = G_{\sigma}(S_1) + G_{\sigma}(S_2)$ for all $S_1, S_2 \in L$.
- (E) For all $S \in L$, $|G_{\sigma}(S)|$ only depends on $\rho_{\mathcal{L}}(S)$.

Notice that properties (A), (B) and (C) of Definition 20 imply that $G_{\sigma}(S)$ is a subgroup of G for any lattice element $S \in \mathcal{L}$.

Notation 21. We denote a regular support on G with values in \mathcal{L} by $\sigma : G \dashrightarrow \mathcal{L}$. Moreover, for all $0 \leq s \leq r$ we set

$$\gamma_{\sigma}(s) := |G_{\sigma}(S)|,$$

where $S \in L$ is any element with $\rho_{\mathcal{L}}(S) = s$. Given a lattice element $S \in L$ and a code $\mathcal{C} \subseteq G$, we also define $\mathcal{C}_{\sigma}(S) := G_{\sigma}(S) \cap \mathcal{C}$.

We can now show that the definition of regular support behaves well with respect to dualization. We start introducing some notation and establishing a preliminary lemma.

Notation 22. Let $\sigma : (G, +) \dashrightarrow \mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular support. Define $\sigma^* : \hat{G} \rightarrow L$ by

$$\sigma^*(\chi) := \bigvee \{S \in L : \chi \in G_\sigma(S)^*\}$$

for all $\chi \in \hat{G}$. Since $G_\sigma(0_{\mathcal{L}}) = \{0\}$ by property (A) of Definition 20, we have $\chi \in G_\sigma(0_{\mathcal{L}})^*$ for any $\chi \in \hat{G}$. This shows that $\sigma^*(\chi)$ is well defined. We regard σ^* as a function on \hat{G} with values in \mathcal{L}^* . In particular, according to Notation 19, for $S \in L$ we have

$$\hat{G}_{\sigma^*}(S) = \{\chi \in \hat{G} : \sigma^*(\chi) \leq S\}.$$

Lemma 23. Let $\sigma : (G, +) \dashrightarrow \mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular support. For all $\chi \in \hat{G}$ we have $\chi \in G_\sigma(\sigma^*(\chi))^*$. Equivalently, $\sigma^*(\chi)$ is the maximum $S \in L$ such that $\chi \in G_\sigma(S)^*$.

Proof. Let $\chi \in \hat{G}$ be any character. As already shown, $\{S \in L : \chi \in G_\sigma(S)^*\} \neq \emptyset$. Choose an enumeration $\{S \in L : \chi \in G_\sigma(S)^*\} = \{S_1, S_2, \dots, S_t\}$. By property (D) of Definition 20 and the associativity of the join, we have $G_\sigma(S_1 \vee S_2 \vee \dots \vee S_t) = G_\sigma(S_1) + G_\sigma(S_2) + \dots + G_\sigma(S_t)$. Therefore Remark 2 implies $G_\sigma(S_1 \vee S_2 \vee \dots \vee S_t)^* = G_\sigma(S_1)^* \cap G_\sigma(S_2)^* \cap \dots \cap G_\sigma(S_t)^*$. Since $\chi \in G_\sigma(S_i)^*$ for all $i \in \{1, \dots, t\}$, we have $\chi \in G_\sigma(\sigma^*(\chi))^*$, as claimed. \square

The following central theorem establishes the main properties of a regular support. In particular, it shows that a regular support on a group G with values in a lattice \mathcal{L} canonically induces a regular support on the character group \hat{G} , with values in the dual lattice \mathcal{L}^* .

Theorem 24. Let $\sigma : (G, +) \dashrightarrow \mathcal{L} = (L, \leq, \wedge, \vee)$ be a regular support. The following hold.

1. $G_\sigma(S)^* = \hat{G}_{\sigma^*}(S)$ for all $S \in L$.
2. The map $\chi \mapsto \sigma^*(\chi)$ defines a regular support $\sigma^* : (\hat{G}, \cdot) \dashrightarrow \mathcal{L}^* = (L, \leq, \wedge, \vee)$.
3. $\gamma_{\sigma^*}(s) = |G|/\gamma_\sigma(\text{rk}(\mathcal{L}) - s)$ for all $0 \leq s \leq \text{rk}(\mathcal{L})$.
4. Identifying \hat{G} and G , we have $\sigma^{**} = \sigma$.

Proof. 1. Take any $S \in L$. If $\chi \in G_\sigma(S)^*$ then, by definition, $S \leq \sigma^*(\chi)$, i.e., $\sigma^*(\chi) \leq S$. This shows that $G_\sigma(S)^* \subseteq \hat{G}_{\sigma^*}(S)$. Now assume that $\chi \in \hat{G}_{\sigma^*}(S)$, and let $g \in G_\sigma(S)$. We have $\sigma(g) \leq S \leq \sigma^*(\chi)$, hence $g \in G_\sigma(\sigma^*(\chi))$. Lemma 23 implies $\chi(g) = 1$, so $\hat{G}_{\sigma^*}(S) \subseteq G_\sigma(S)^*$.

2. The lattice \mathcal{L}^* is regular by Proposition 17, and the group (\hat{G}, \cdot) is finite and abelian. Let ε be the trivial character of G . By 1 we have $\hat{G}_{\sigma^*}(0_{\mathcal{L}^*}) = G_\sigma(1_{\mathcal{L}})^* = G^* = \{\varepsilon\}$, and this proves property (A) of Definition 20. For $\chi \in \hat{G}$ and $S \in L$ we have $\chi \in G_\sigma(S)^*$ if and only if $1/\chi \in G_\sigma(S)^*$. By definition of dual support, this gives property (B). Now take any $\chi_1, \chi_2 \in \hat{G}$, and let $g \in G_\sigma(\sigma^*(\chi_1)) \cap G_\sigma(\sigma^*(\chi_2))$. Lemma 23 implies $\chi_1(g) = \chi_2(g) = 1$, and so $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g) = 1$. Therefore

$$\chi_1 \cdot \chi_2 \in (G_\sigma(\sigma^*(\chi_1)) \cap G_\sigma(\sigma^*(\chi_2)))^* = G_\sigma(\sigma^*(\chi_1) \wedge \sigma^*(\chi_2))^*,$$

where the last equality directly follows from the definition of meet. As a consequence we have $\sigma^*(\chi_1) \wedge \sigma^*(\chi_2) \leq \sigma^*(\chi_1 \cdot \chi_2)$, i.e., $\sigma^*(\chi_1 \cdot \chi_2) \leq \sigma^*(\chi_1) \vee \sigma^*(\chi_2)$. This establishes property (C). Let $S_1, S_2 \in L$. By definition of meet we have $G_\sigma(S_1 \wedge S_2) = G_\sigma(S_1) \cap G_\sigma(S_2)$. Taking the duals, by Remark 2 we obtain $G_\sigma(S_1 \wedge S_2)^* = G_\sigma(S_1)^* \cdot G_\sigma(S_2)^*$, and part 1 of the statement gives $\hat{G}_{\sigma^*}(S_1 \wedge S_2) = \hat{G}_{\sigma^*}(S_1) \cdot \hat{G}_{\sigma^*}(S_2)$, i.e., $\hat{G}_{\sigma^*}(S_1 \vee S_2) = \hat{G}_{\sigma^*}(S_1) \cdot \hat{G}_{\sigma^*}(S_2)$. This is property (D). Let $S \in L$. By part 1 and Remark 2 we have $|\hat{G}_{\sigma^*}(S)| = |G|/|G_\sigma(S)|$. Hence $|\hat{G}_{\sigma^*}(S)|$ only depends on $\rho_{\mathcal{L}^*}(S) = \text{rk}(\mathcal{L}) - \rho_{\mathcal{L}}(S)$. This is property (E).

3. Let $r := \text{rk}(\mathcal{L}) = \text{rk}(\mathcal{L}^*)$. Take any element $S \in L$ with $\rho_{\mathcal{L}^*}(S) = s$. Part 1 and Remark 2 imply $\hat{G}_{\sigma^*}(S)^* = G_{\sigma}(S)$. Therefore $\gamma_{\sigma^*}(s) = |\hat{G}_{\sigma^*}(S)| = |G|/|\hat{G}_{\sigma^*}(S)^*| = |G|/|G_{\sigma}(S)| = |G|/\gamma_{\sigma}(s)$, as desired.
4. As before, part 1 and Remark 2 give $\hat{G}_{\sigma^*}(S)^* = G_{\sigma}(S)$ for all $S \in L$. Hence, for all $g \in G$,

$$\sigma^{**}(g) = \bigvee \{S \in L : g \in \hat{G}_{\sigma^*}(S)^*\} = \bigwedge \{S \in L : g \in G_{\sigma}(S)\} = \bigwedge \{S \in L : \sigma(g) \leq S\} = \sigma(g).$$

This concludes the proof. \square

Definition 25. The regular support $\sigma^* : (\hat{G}, \cdot) \dashrightarrow \mathcal{L}^*$ defined by part 2 of Theorem 24 and Notation 22 is called the **dual support** of σ .

Regular supports can be constructed over any finite abelian group G using as lattice any chain of subgroups of G . The regular support constructed in the following Example 26 will be used later to show the existence, over any finite abelian group, of the following objects: (i) weight functions yielding MacWilliams identities, (ii) Fourier-reflexive partitions, (iii) pairs of weights that, simultaneously, yield MacWilliams identities, and induce metric space structures on both the underlying groups.

Example 26 (Chain support). Let (L, \leq) be a finite chain, and let $S_0 < S_1 < \dots < S_r$ be the elements of L . For all $i, j \in \{0, \dots, r\}$ define $S_i \wedge S_j := S_{\min\{i, j\}}$ and $S_i \vee S_j := S_{\max\{i, j\}}$. Then $\mathcal{L} = (L, \leq, \wedge, \vee)$ is regular lattice of rank r with:

$$\mu_{\leq}(s, t) = \begin{cases} 1 & \text{if } s \leq t \\ 0 & \text{else} \end{cases} \quad \mu_{\geq}(s, t) = \begin{cases} 1 & \text{if } s \geq t \\ 0 & \text{else} \end{cases} \quad \mu_{\mathcal{L}}(s, t) = \begin{cases} 1 & \text{if } s = t \\ -1 & \text{if } t = s + 1 \\ 0 & \text{else} \end{cases}$$

for all $0 \leq s, t \leq r$. Now let $(G, +)$ be a finite abelian group, and let $\mathcal{L} = (L, \subseteq, \wedge, \vee)$ be a chain of subgroups of G , i.e., $\{0\} = G_0 \subsetneq G_1 \subsetneq \dots \subsetneq G_r = G$, endowed with the structure of regular lattice described above. The **chain support** $\sigma : G \dashrightarrow \mathcal{L}$ is the function $\sigma : G \rightarrow L$ defined, for all $g \in G$, by $\sigma(g) := G_i$, where $i = \min\{0 \leq j \leq r : g \in G_j\}$. It is easy to check that σ is a regular support. By definition, $G_{\sigma}(G_s) = G_s$ for all $0 \leq s \leq r$, and therefore $\gamma_{\sigma}(s) = |G_s|$ for all s . Moreover, for any $\chi \in \hat{G}$ we have $\sigma^*(\chi) = G_i$, where $i = \max\{0 \leq j \leq r : \chi \in G_j^*\}$.

Notice that not all regular supports on a group G arise from chains of subgroups of G . Other examples will be given in Section 6 when revisiting the theory of MacWilliams identities for certain classes of codes.

4 Compatible Weights from Regular Supports

In this section we show that a regular support $\sigma : G \dashrightarrow \mathcal{L}$ on a finite abelian group G induces a pair of compatible weights on G and \hat{G} , yielding MacWilliams identities. Moreover, we express the associated Krawtchouk coefficients in terms of the combinatorial invariants of the lattice \mathcal{L} , proving that they are integers with a precise combinatorial significance. As we will see, in many relevant examples the lattice invariants are very easy to determine. In particular, this allows to easily compute the Krawtchouk coefficients. The simplification relies on the specific fact that the weight functions on G and \hat{G} both factor through a regular support map. Whenever this happens, the following Theorem 29 gives an effective method to compute the Krawtchouk coefficients.

Remark 27. The fact that a regular support automatically yields MacWilliams identities is not obvious, as the definition of support is completely independent from the specific structure of the character group. This differs from previous approaches, where partitions yielding MacWilliams identities are defined (or characterized) in terms on their interaction with the character group.

We start observing that a regular support $\sigma : G \dashrightarrow \mathcal{L}$ induces a weight function on G via the rank function of \mathcal{L} .

Definition 28. Let $\sigma : (G, +) \dashrightarrow \mathcal{L}$ be a regular support. The **weight** on G **induced** by σ is the function $\omega_\sigma : G \rightarrow \{0, \dots, \text{rk}(\mathcal{L})\}$ defined by $\omega_\sigma(g) := \rho_{\mathcal{L}}(\sigma(g))$ for all $g \in G$.

We can now state our main result.

Theorem 29. Let $\sigma : (G, +) \dashrightarrow \mathcal{L}$ be a regular support, $r = \text{rk}(\mathcal{L})$. The following hold.

1. The pair $(\omega_{\sigma^*}, \omega_\sigma)$ is compatible. Moreover, for all $i \in \omega_{\sigma^*}(\hat{G})$ and $j \in \omega_\sigma(G)$ we have

$$K(\omega_{\sigma^*}, \omega_\sigma)(i, j) = \sum_{s=0}^r \gamma_\sigma(s) \mu_{\mathcal{L}}(s, j) \mu_{\leq}(s, r-i) \mu_{\geq}(j, s).$$

2. The pair $(\omega_\sigma, \omega_{\sigma^*})$ is compatible. Moreover, for all $i \in \omega_\sigma(G)$ and $j \in \omega_{\sigma^*}(\hat{G})$ we have

$$K(\omega_\sigma, \omega_{\sigma^*})(i, j) = |G| \sum_{s=0}^r \frac{1}{\gamma_\sigma(r-s)} \mu_{\mathcal{L}}(r-j, r-s) \mu_{\geq}(r-s, i) \mu_{\leq}(r-j, r-s).$$

In particular, the Krawtchouk coefficients associated to both the pairs $(\omega_{\sigma^*}, \omega_\sigma)$ and $(\omega_\sigma, \omega_{\sigma^*})$ are integers determined by the combinatorial invariants of \mathcal{L} and σ .

Proof. Throughout this proof, a sum over an empty set of indices is zero by definition. Let us first show part 1. Part 2 will follow easily. Fix any character $\chi \in \hat{G}$, and let $f, g : L \rightarrow \mathbb{C}$ be the complex-valued functions defined by

$$f(T) := \sum_{\substack{g \in G \\ \sigma(g)=T}} \chi(g), \quad g(T) := \sum_{S \leq T} f(S) \quad \text{for all } T \in L.$$

By the orthogonality relations of characters (see [24, Lemma 1.1.32]), for all $T \in L$ we have

$$g(T) = \sum_{S \leq T} f(S) = \sum_{g \in G_\sigma(T)} \chi(g) = \begin{cases} \gamma_\sigma(\rho_{\mathcal{L}}(T)) & \text{if } \chi \in G_\sigma(T)^* \\ 0 & \text{if } \chi \notin G_\sigma(T)^*. \end{cases}$$

Therefore applying the Möbius inversion formula (e.g., [31, Proposition 3.7.1]) to f and g we obtain

$$\begin{aligned} f(T) &= \sum_{\substack{S \leq T \\ \chi \in G_\sigma(S)^*}} \gamma_\sigma(\rho_{\mathcal{L}}(S)) \mu_{\mathcal{L}}(S, T) = \sum_{s=0}^r \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(\bar{S})=s \\ \chi \in G_\sigma(S)^*}} \gamma_\sigma(s) \mu_{\mathcal{L}}(S, T) \\ &= \sum_{s=0}^r \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(\bar{S})=s \\ \chi \in \hat{G}_{\sigma^*}(S)}} \gamma_\sigma(s) \mu_{\mathcal{L}}(S, T), \end{aligned}$$

where the last equality follows from part 1 of Theorem 24. Thus for all $0 \leq j \leq r$ one has

$$\begin{aligned} \sum_{\substack{g \in G \\ \omega_\sigma(g)=j}} \chi(g) &= \sum_{\substack{T \in L \\ \rho_{\mathcal{L}}(T)=j}} f(T) = \sum_{\substack{T \in L \\ \rho_{\mathcal{L}}(T)=j}} \sum_{s=0}^r \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(S)=s \\ \chi \in \hat{G}_{\sigma^*}(S)}} \gamma_\sigma(s) \mu_{\mathcal{L}}(S, T) \\ &= \sum_{s=0}^r \gamma_\sigma(s) \sum_{\substack{T \in L \\ \rho_{\mathcal{L}}(T)=j}} \sum_{\substack{S \leq T \\ \rho_{\mathcal{L}}(S)=s \\ \chi \in \hat{G}_{\sigma^*}(S)}} \mu_{\mathcal{L}}(S, T). \end{aligned}$$

By the regularity of \mathcal{L} , $\mu_{\mathcal{L}}(S, T) = \mu_{\mathcal{L}}(s, j)$ for all $S, T \in L$ with $S \leq T$, $\rho_{\mathcal{L}}(S) = s$ and $\rho_{\mathcal{L}}(T) = j$. Setting $\alpha(s, j, \chi) := |\{(S, T) \in L \times L : \rho_{\mathcal{L}}(S) = s, \rho_{\mathcal{L}}(T) = j, S \leq T, \sigma^*(\chi) \preceq S\}|$ we obtain

$$\sum_{\substack{g \in G \\ \omega_\sigma(g)=j}} \chi(g) = \sum_{s=0}^r \gamma_\sigma(s) \mu_{\mathcal{L}}(s, j) \alpha(s, j, \chi). \quad (3)$$

We now derive a more convenient expression for $\alpha(s, j, \chi)$. By definition,

$$\alpha(s, j, \chi) = \sum_{\substack{S \in L \\ \rho_{\mathcal{L}}(S)=s \\ \sigma^*(\chi) \preceq S}} |\{T \in L : \rho_{\mathcal{L}}(T) = j, S \leq T\}| = \sum_{\substack{S \in L \\ \rho_{\mathcal{L}}(S)=s \\ \sigma^*(\chi) \preceq S}} \mu_{\geq}(j, s) = \mu_{\leq}(s, \rho_{\mathcal{L}}(\sigma^*(\chi))) \mu_{\geq}(j, s).$$

By the properties of the rank of the dual lattice (see Section 2) and the definition of ω_{σ^*} , we have $\rho_{\mathcal{L}}(\sigma^*(\chi)) = r - \rho_{\mathcal{L}^*}(\sigma^*(\chi)) = r - \omega_{\sigma^*}(\chi)$. It follows $\mu_{\leq}(s, \rho_{\mathcal{L}}(\sigma^*(\chi))) = \mu_{\leq}(s, r - \omega_{\sigma^*}(\chi))$, hence $\alpha(s, j, \chi) = \mu_{\leq}(s, r - \omega_{\sigma^*}(\chi)) \mu_{\geq}(j, s)$. Substituting this expression for $\alpha(s, j, \chi)$ into (3) yields

$$\sum_{\substack{g \in G \\ \omega_\sigma(g)=j}} \chi(g) = \sum_{s=0}^r \gamma_\sigma(s) \mu_{\mathcal{L}}(s, j) \mu_{\leq}(s, r - \omega_{\sigma^*}(\chi)) \mu_{\geq}(j, s).$$

By Remark 5, this shows part 1.

By Theorem 24, σ^* is a regular support, and $\sigma^{**} = \sigma$ when identifying G and \hat{G} . Therefore part 2 follows from part 1 applied to $\sigma^* : \hat{G} \dashrightarrow \mathcal{L}^*$, along with Proposition 17.

We conclude observing that the Krawtchouk coefficients are indeed integers, as for all $0 \leq s \leq r$ the numbers $\gamma_\sigma(s)$ and $\gamma_\sigma(r - s)$ express the cardinality of subgroups of G . \square

Let $\sigma : G \dashrightarrow \mathcal{L}$ be a regular support. In the language of [13], the partitions $\mathcal{P}(\omega_\sigma)$ and $\mathcal{P}(\omega_{\sigma^*})$ are both Fourier-reflexive and mutually dual, as the following result shows. We do not go into the details of the proof.

Theorem 30. Let $\sigma : G \dashrightarrow \mathcal{L}$ be a regular support. The partitions $\mathcal{P}(\omega_\sigma)$ and $\mathcal{P}(\omega_{\sigma^*})$ are both Fourier-reflexive and mutually dual.

Combining Example 26, Theorem 29 and Theorem 30 we obtain in particular the following result of [34], which shows the existence of Fourier-reflexive partitions on any finite abelian group.

Corollary 31 (Fourier-reflexive partitions via subgroups). Let $(G, +)$ be a finite abelian group, and let $\{0\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G$ be a chain of subgroups of G . Then

$$\{0\} \sqcup \bigsqcup_{i=1}^r G_i \setminus G_{i-1}$$

is a Fourier-reflexive partition of G of cardinality $r + 1$.

The Fourier-reflexivity of the partitions constructed in the previous corollary was first shown in [34, Theorem 6]. Notice however that our focus is on numerical weight functions and metric space structure associated with these partitions, which are not investigated in [34]. As we will see in the next section, the partitions of Corollary 31 are induced by weight functions that endow the underlying group with a metric structure.

This feature is relevant from a Coding Theory perspective.

5 Metric Structures

Under certain assumptions on the lattice \mathcal{L} , the weight ω_σ induced by a regular support $\sigma : G \dashrightarrow \mathcal{L}$ automatically induces a distance d_{ω_σ} on G . This is particularly interesting for applications in Coding Theory, as the triangle inequality is usually a key property enabling error correction.

Recall that a finite lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ is **modular** if for all $S, T, U \in L$ with $S \leq U$ one has $S \vee (T \wedge U) = (S \vee T) \wedge U$. Notice that if \mathcal{L} is modular, then so is \mathcal{L}^* .

The following result shows that regular supports taking values in modular lattices induce a metric space structure on the underlying group.

Proposition 32. Let $\sigma : (G, +) \dashrightarrow \mathcal{L}$ be a regular support. If \mathcal{L} is modular, then the function $d_{\omega_\sigma} : G \times G \rightarrow \mathbb{N}$ defined by $d_{\omega_\sigma}(g, g') := \omega_\sigma(g - g')$ for all $g, g' \in G$ is a distance function.

Proof. Write $d := d_{\omega_\sigma}$. Let $g, g' \in G$. By definition, $d(g, g') = 0$ if and only if $\rho_{\mathcal{L}}(\sigma(g - g')) = 0$. By the properties of $\rho_{\mathcal{L}}$ (Remark 12), this happens if and only if $\sigma(g - g') = 0$, i.e., by property (A) of Definition 20, if and only if $g = g'$. By property (B) of Definition 20 we have $d(g, g') = \omega_\sigma(g - g') = \rho_{\mathcal{L}}(\sigma(g - g')) = \rho_{\mathcal{L}}(\sigma(g' - g)) = \omega_\sigma(g' - g) = d(g', g)$. Now let $h, g, g' \in G$. The rank function of a modular lattice $\mathcal{L} = (L, \leq, \wedge, \vee)$ satisfies $\rho_{\mathcal{L}}(S \vee T) = \rho_{\mathcal{L}}(S) + \rho_{\mathcal{L}}(T) - \rho_{\mathcal{L}}(S \wedge T)$ for all $S, T \in L$ (see [31], page 287). Thus by property (C) of Definition 20 we have

$$d(g, g') = \omega_\sigma(g - g') = \omega_\sigma(g - h - (g' - h)) \leq \rho_{\mathcal{L}}(\sigma(g - h) \vee \sigma(g' - h)) \leq d(g, h) + d(h, g').$$

This concludes the proof. \square

Remark 33. Assume that $\sigma : (G, +) \dashrightarrow \mathcal{L}$ is a regular support, with \mathcal{L} modular. Then by Theorem 24 the support $\sigma^* : (\hat{G}, \cdot) \dashrightarrow \mathcal{L}^*$ is regular as well, where \mathcal{L}^* is modular. Applying Theorem 29 and Proposition 32 to σ and σ^* , we obtain that the weights ω_σ and ω_{σ^*} are bi-compatible, and induce metric space structures on G and \hat{G} , respectively. This constructs a pair of metric ambient spaces and, *simultaneously*, yields MacWilliams identities for additive codes.

The following example shows that the construction presented in Remark 33 can be explicitly realized over any finite abelian group, by choosing a suitable support lattice.

Example 34 (Chain support, continued). Let $(G, +)$ be a finite abelian group, and let \mathcal{L} be a chain $\{0\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G$ of subgroups of G endowed with the lattice structure described in Example 26. Then \mathcal{L} is modular. Denote by $\sigma : G \dashrightarrow \mathcal{L}$ the associated chain support. As observed in Example 26, σ is regular. Therefore d_{ω_σ} is a distance on G by Proposition 32. By Theorem 24, σ^* is a regular support. Moreover, since \mathcal{L} is modular, \mathcal{L}^* is modular. Hence by Proposition 32 $d_{\omega_{\sigma^*}}$ is a distance on \hat{G} . By Theorem 29, $(\omega_\sigma, \omega_{\sigma^*})$ and $(\omega_{\sigma^*}, \omega_\sigma)$ are compatible pairs such that both d_{ω_σ} and $d_{\omega_{\sigma^*}}$ are distance functions.

We conclude the example giving a more explicit description of ω_{σ^*} . Let ν be the chain support on the character group \hat{G} associated to the chain $\{1\} = G_r^* \subsetneq G_{r-1}^* \subsetneq \cdots \subsetneq \hat{G}$. We claim that $\omega_\nu = \omega_{\sigma^*}$ (in particular, the dual of a chain support is a chain support as well). Indeed, as already mentioned

in Example 26, for a fixed $\chi \in \hat{G}$ we have $\sigma^*(\chi) = G_i$, where $i = \max\{0 \leq j \leq r : \chi \in G_j^*\}$. Thus, by definition, $\omega_{\sigma^*}(\chi) = \rho_{\mathcal{L}^*}(\sigma^*(\chi)) = r - i$. On the other hand,

$$\omega_\nu(\chi) = \min\{0 \leq j \leq r : \chi \in G_{r-j}^*\} = r - \max\{0 \leq j \leq r : \chi \in G_j^*\} = r - i = \omega_{\sigma^*}(\chi).$$

Remark 35. If $(G, +)$ is a finite abelian group, and $d : G \times G \rightarrow \mathbb{R}$ is a distance on G , then d can be extended to a distance function d^n on the cartesian product G^n by setting

$$d^n((g_1, \dots, g_n), (g'_1, \dots, g'_n)) := \sum_{i=1}^n d(g_i, g'_i) \quad \text{for all } (g_1, \dots, g_n), (g'_1, \dots, g'_n) \in G^n.$$

It is easy to check that d^n is indeed a distance function. Therefore a regular support σ on G taking values in a modular lattice \mathcal{L} automatically produces metric space structures on both G^n and \hat{G}^n .

6 MacWilliams Identities in Coding Theory

In this section we show that many weight functions traditionally studied in Coding Theory are induced by suitable regular supports up to equivalence. We also apply Theorem 29 to easily compute the corresponding Krawtchouk coefficients with a unified combinatorial method. Most of such coefficients have been computed by other authors employing *ad hoc* techniques in the past. Theorem 29 provides a general method that applies to different contexts. Some connections between these examples of weights and the general theory of group partitions have been studied in [13, 33, 34].

Observe moreover that the case of the rank weight (Example 39) is particularly interesting, as the standard method to compute the associated Krawtchouk coefficients is quite sophisticated [10]. Theorem 29 allows to compute them in a simple way, and to give them a precise combinatorial interpretation.

The following Examples 36 and 39 also show that the MacWilliams identities for codes endowed with the Hamming and the rank weight can be seen as two simple instances of the same result.

Example 36 (Additive codes with the Hamming weight). Let $n \geq 1$ be a positive integer, and let $[n] := \{1, \dots, n\}$. Then $\mathcal{L} = (2^{[n]}, \subseteq, \cap, \cup)$ is a regular lattice of rank n . The rank function of \mathcal{L} is the cardinality of sets. The parameters of \mathcal{L} are given by

$$\mu_\subseteq(s, t) = \binom{t}{s}, \quad \mu_\supseteq(s, t) = \binom{n-t}{s-t}, \quad \mu_{\mathcal{L}}(s, t) = \begin{cases} (-1)^{t-s} & \text{if } s \leq t \\ 0 & \text{if } s > t \end{cases}$$

for all $0 \leq s, t \leq n$. The formula for $\mu_{\mathcal{L}}(s, t)$ can be easily proved by induction on $t - s$ with the aid of the Binomial Theorem (page 24 of [31]). See [31, Example 3.8.3] for a different proof using the product of chains. Let $(G, +)$ be a finite abelian group. Define the **Hamming support** $\sigma_H : G^n \rightarrow 2^{[n]}$ by $\sigma_H(g_1, \dots, g_n) := \{i \in [n] : g_i \neq 0\}$ for all $(g_1, \dots, g_n) \in G^n$. It is a regular support. The weight induced on G^n by the Hamming support is the **Hamming weight** ω_H . For $S \subseteq [n]$ and $(\chi_1, \dots, \chi_n) \in \hat{G}^n$ we have $(\chi_1, \dots, \chi_n) \in G_\sigma^n(S)^*$ if and only if χ_s is the trivial character of G for all $s \in S$. Therefore $\sigma_H^*(\chi_1, \dots, \chi_n) = \{i \in [n] : \chi_i \text{ is trivial}\}$. It follows

$$\omega_{\sigma_H^*}(\chi_1, \dots, \chi_n) = n - |\{i \in [n] : \chi_i \text{ is trivial}\}| = |\{i \in [n] : \chi_i \text{ is not trivial}\}|.$$

Thus in the following we write $\omega_{\sigma_H^*} = \omega_H$. Theorem 29 allows to compute the Krawtchouk coefficients for the Hamming weight as

$$K(\omega_H, \omega_H)(i, j) = \sum_{s=0}^n (-1)^{j-s} |G|^s \binom{n-i}{s} \binom{n-s}{j-s}$$

for all $0 \leq i, j \leq n$. By Theorem 7, for every code $\mathcal{C} \subseteq G^n$ and for all $0 \leq j \leq n$ we have

$$W_j(\mathcal{C}^*, \omega_H) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^n W_i(\mathcal{C}, \omega_H) \sum_{s=0}^n (-1)^{j-s} |G|^s \binom{n-i}{s} \binom{n-s}{j-s}.$$

These are the “MacWilliams identities for the Hamming weight over a group”.

Example 37 (Linear codes with the Hamming weight). Take $G = \mathbb{F}_q$ in Example 36. Define the **orthogonal code** of a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ by $\mathcal{C}^\perp := \{v \in \mathbb{F}_q^n : \langle w, v \rangle = 0 \text{ for all } w \in \mathcal{C}\}$, where $\langle \cdot, \cdot \rangle$ is the standard inner product of \mathbb{F}_q^n . One can show that $W_j(\mathcal{C}^\perp, \omega_H) = W_j(\mathcal{C}^*, \omega_H)$ for all linear codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ (for a proof, see the following Example 39, where the same property is established for the more complicated case of rank-metric codes). By Example 36, for all $0 \leq j \leq n$ we have

$$W_j(\mathcal{C}^\perp, \omega_H) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^n W_i(\mathcal{C}, \omega_H) \sum_{s=0}^n (-1)^{j-s} |G|^s \binom{n-i}{s} \binom{n-s}{j-s}.$$

These are the “MacWilliams identities for linear codes with the Hamming weight”. See for instance Chapter 5 of [27] or Chapter 7 of [19] for equivalent formulations.

Example 38 (Modified exact weight). Let $(G, +)$ be a non-trivial finite abelian group. Denote by σ the chain support on G associated to the chain $\{0\} \subsetneq G$ (see Example 26). Let $\omega_\sigma : G \rightarrow \{0, 1\}$ be the induced weight. By the second part of Example 34, ω_{σ^*} is the weight on \hat{G} induced by the chain support associated to the chain $\{1\} \subsetneq \hat{G}$. If $n \geq 2$ and $G = \mathbb{F}_2$, then the n -th product weight of ω_σ is the **exact weight** on \mathbb{F}_2^n (see [27, page 147]). For a general G , we obtain a weight that partitions the elements of G^n according to the positions of their non-zero entries. With the aid of Theorem 29 and Example 26 one computes the Krawtchouk coefficients for $(\omega_\sigma, \omega_{\sigma^*})$ and $(\omega_{\sigma^*}, \omega_\sigma)$ as

$$K(\omega_\sigma, \omega_{\sigma^*})(i, j) = K(\omega_{\sigma^*}, \omega_\sigma)(i, j) = \begin{cases} 1 & \text{if } j = 0 \\ -1 & \text{if } j = 1 \text{ and } i = 1 \\ |G| - 1 & \text{if } j = 1 \text{ and } i = 0 \end{cases}$$

for all $i, j \in \{0, 1\}$. Proposition 10 also allows to compute the coefficients for the product and symmetrized weights.

Example 39 (Linear codes with the rank weight). Let $1 \leq k \leq m$ be integers, and let $G := \text{Mat}$ be the vector space of $k \times m$ matrices over \mathbb{F}_q . Denote by \mathcal{L} the set of all subspaces of \mathbb{F}_q^k . Then $\mathcal{L} = (L, \subseteq, \cap, +)$ is a regular lattice of rank k . Notice that the join is the sum of subspaces. The rank function of \mathcal{L} is given by $\rho_{\mathcal{L}}(V) = \dim(V)$ for all $V \subseteq \mathbb{F}_q^k$ (see [31, page 281]). The parameters of \mathcal{L} are, for all $0 \leq s, t \leq k$,

$$\mu_{\subseteq}(s, t) = \begin{bmatrix} t \\ s \end{bmatrix}, \quad \mu_{\supseteq}(s, t) = \begin{bmatrix} k-t \\ s-t \end{bmatrix}, \quad \mu_{\mathcal{L}}(s, t) = \begin{cases} (-1)^{t-s} q^{\binom{t-s}{2}} & \text{if } s \leq t \\ 0 & \text{if } s > t, \end{cases}$$

where the symbols in squared brackets are the q -ary binomial coefficients (see, e.g., [1]). The formula for $\mu_{\mathcal{L}}(s, t)$ can be proved by induction on $t - s$ with the aid of the Gaussian Binomial Theorem ([31, equation (1.87) on page 74]). An elegant argument that uses the fact that \mathcal{L} is a geometric lattice can be found in [31, Example 3.10.2]. Denote by $\text{colsp}(M) \subseteq \mathbb{F}_q^k$ the space generated by the columns of a matrix $M \in \text{Mat}$. Then $M \mapsto \text{colsp}(M)$ is a regular support $\sigma_{\text{rk}} : \text{Mat} \dashrightarrow \mathcal{L}$ with $\gamma_\sigma(s) = q^{ms}$ for all $0 \leq s \leq k$ (see [28, Lemma 26]). It is called the **rank support**. Let $\omega_{\text{rk}} := \omega_{\sigma_{\text{rk}}}$

be the **rank weight**, and set $\omega_{\text{rk}}^* := \omega_{\sigma_{\text{rk}}^*}$ for ease of notation. Note that $\omega_{\sigma_{\text{rk}}}(M) = \text{rk}(M)$ for all $M \in \text{Mat}$. By Theorem 29, the Krawtchouk coefficients of $(\omega_{\text{rk}}, \omega_{\text{rk}}^*)$ and $(\omega_{\text{rk}}^*, \omega_{\text{rk}})$ are

$$K(\omega_{\text{rk}}, \omega_{\text{rk}}^*)(i, j) = K(\omega_{\text{rk}}^*, \omega_{\text{rk}})(i, j) = \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}, \quad 0 \leq i, j \leq k. \quad (4)$$

Recall that the **trace-product** of matrices $M, N \in \text{Mat}$ is $\langle M, N \rangle := \text{Tr}(MN^t)$, where Tr is the trace of matrices, and the superscript t denotes transposition. The **orthogonal code** of a linear code $\mathcal{C} \subseteq \text{Mat}$ is $\mathcal{C}^\perp := \{M \in \text{Mat} : \langle N, M \rangle = 0 \text{ for all } N \in \mathcal{C}\}$. It can be shown that if $\mathcal{C} \subseteq \text{Mat}$ is a linear code, then $W_j(\mathcal{C}^\perp, \omega_{\text{rk}}) = W_j(\mathcal{C}^*, \omega_{\text{rk}}^*)$ for all $0 \leq j \leq k$ (see below). Therefore combining Theorem 7 and equation (4) we obtain

$$W_j(\mathcal{C}^\perp, \omega_{\text{rk}}) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^k W_i(\mathcal{C}, \omega_{\text{rk}}) \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}$$

for all $0 \leq j \leq k$. These are the “MacWilliams identities for linear codes with the rank weight”, first established by Delsarte in [10]. Rank-metric codes were recently re-discovered for applications in linear network coding (see [29]).

We conclude this example showing that if $\mathcal{C} \subseteq \text{Mat}$ is an \mathbb{F}_q -linear code, then for all $0 \leq j \leq k$ we have $W_j(\mathcal{C}^\perp, \omega_{\text{rk}}) = W_j(\mathcal{C}^*, \omega_{\text{rk}}^*)$. Fix a non-trivial character $\chi \in \hat{\mathbb{F}}_q$, and define the group isomorphism

$$f : \text{Mat} \rightarrow \widehat{\text{Mat}}, \quad f(M)(N) := \chi(\text{Tr}(MN^t)) \text{ for all } M, N \in \text{Mat}.$$

It is easy to see that for any linear code $\mathcal{C} \subseteq \text{Mat}$ we have

$$f(\mathcal{C}^\perp) = \mathcal{C}^*. \quad (5)$$

Let $g : L \rightarrow L$ be the map that sends an \mathbb{F}_q^k -subspace U to its dual U^\perp with respect to the standard inner product of \mathbb{F}_q^k . Note that $g = g^{-1}$. For all $M \in \text{Mat}$ we have

$$\sigma_{\text{rk}}^*(f(M)) = \bigvee \{S \in L : f(M) \in \text{Mat}_{\sigma_{\text{rk}}}(S)^*\} = \bigvee \{S \in L : M \in \text{Mat}_{\sigma_{\text{rk}}}(S)^\perp\},$$

where the last equality follows from (5) applied to the linear code $\text{Mat}_{\sigma_{\text{rk}}}(S)$. By [28, Lemma 27] and the definition of g one has $\text{Mat}_{\sigma_{\text{rk}}}(S)^\perp = \text{Mat}_{\sigma_{\text{rk}}}(S^\perp) = \text{Mat}_{\sigma_{\text{rk}}}(g(S))$. Therefore

$$\sigma_{\text{rk}}^*(f(M)) = \bigvee \{S \in L : M \in \text{Mat}_{\sigma_{\text{rk}}}(g(S))\} = \bigvee \{S \in L : S \subseteq g(\sigma_{\text{rk}}(M))\} = g(\sigma_{\text{rk}}(M)).$$

As a consequence, $g(\sigma_{\text{rk}}^*(f(M))) = \sigma_{\text{rk}}(M)$. Thus all the arrows in the following diagram commute, showing that the ω_{rk} -distribution of \mathcal{C}^\perp coincides with the ω_{rk}^* -distribution of \mathcal{C}^* .

$$\begin{array}{ccc} \text{Mat} & \xrightarrow{f} & \widehat{\text{Mat}} \\ \sigma_{\text{rk}} \downarrow & & \downarrow \sigma_{\text{rk}}^* \\ L & \xleftarrow{g} & L \\ \rho_{\mathcal{C}} \swarrow & & \swarrow \rho_{\mathcal{C}^*} \\ & \mathbb{N} & \end{array}$$

Example 40 (Lee weight on \mathbb{Z}_4). The **Lee weight** on \mathbb{Z}_4 is the function $\omega_{\text{Lee}} : \mathbb{Z}_4 \rightarrow \{0, 1, 2\} \subseteq \mathbb{N}$ defined by $\omega_{\text{Lee}}(0) := 0$, $\omega_{\text{Lee}}(1) = \omega_{\text{Lee}}(3) := 1$ and $\omega_{\text{Lee}}(2) := 2$. See [17] and [22] or Chapter 12 of [19] and the references within. Denote by σ the chain support on \mathbb{Z}_4 associated to the chain $\{0\} \subsetneq \mathbb{Z}_2 \subsetneq \mathbb{Z}_4$. Then $\omega_{\text{Lee}} \sim \omega_\sigma$. Let $\zeta \in \mathbb{C}$ be a primitive fourth root of unity. Define the map $\psi : \mathbb{Z}_4 \rightarrow \hat{\mathbb{Z}}_4$ by $\psi(a)(b) := \zeta^{ab}$ for all $a, b \in \mathbb{Z}_4$. Then ψ is a group isomorphism, and it is natural to define the **Lee weight** on $\hat{\mathbb{Z}}_4$ by $\omega_{\text{Lee}}^* := \omega_{\text{Lee}} \circ \psi^{-1}$. A direct computation shows $\omega_\sigma = \omega_{\sigma^*} \circ \psi$, and therefore $\omega_{\text{Lee}}^* = \omega_{\text{Lee}} \circ \psi^{-1} \sim \omega_\sigma \circ \psi^{-1} = \omega_{\sigma^*} \circ \psi \circ \psi^{-1} = \omega_{\sigma^*}$. Thus the Krawtchouk coefficients associated to $(\omega_{\text{Lee}}, \omega_{\text{Lee}}^*)$ are the same as the Krawtchouk coefficients associated to $(\omega_\sigma, \omega_{\sigma^*})$, up to a permutation. They can be explicitly computed combining Example 26 and Theorem 29 as follows. We write K_{Lee} for $K(\omega_{\text{Lee}}, \omega_{\text{Lee}}^*)$.

$$\begin{array}{lll} K_{\text{Lee}}(0, 0) = 1 & K_{\text{Lee}}(0, 1) = 2 & K_{\text{Lee}}(0, 2) = 1 \\ K_{\text{Lee}}(1, 0) = 1 & K_{\text{Lee}}(1, 1) = 0 & K_{\text{Lee}}(1, 2) = -1 \\ K_{\text{Lee}}(2, 0) = 1 & K_{\text{Lee}}(2, 1) = -2 & K_{\text{Lee}}(2, 2) = 1. \end{array}$$

Proposition 10 also allows to compute the Krawtchouk coefficients for the **symmetrized Lee weight** on the product group \mathbb{Z}_4^n , for $n \geq 1$ (see e.g. [17]).

Example 41 (Homogeneous weight on certain Frobenius rings). We denote the socle and the Jacobson radical of a finite (possibly non-commutative) Frobenius ring R by $\text{soc}(R)$ and $\text{rad}(R)$, respectively. See [21, Chapter 16] for the main properties of Frobenius rings, or [15] and [14] for a Coding Theory approach. It is known that $\text{rad}(R)$ is a two-sided ideal, and that $\text{soc}(R) \cong R/\text{rad}(R)$ as left and right R -modules. Moreover, if R is local, i.e., $\text{rad}(R)$ is the unique maximal left and right ideal of R , then $R/\text{rad}(R)$ is a field, called the **residue field**.

Let $R := R_1 \times R_2 \times \cdots \times R_n$, where each R_i is a finite local Frobenius ring. Then $R_i/\text{rad}(R_i) \cong \text{soc}(R_i)$ as left and right R_i -modules. We assume that all the residue fields $R_i/\text{rad}(R_i)$ have the same order q . Then R is Frobenius with $\text{soc}(R) = \prod_{i=1}^n \text{soc}(R_i)$. The values of the **homogeneous weight** $\omega_{\text{hom}} : R \rightarrow \mathbb{R}$ (see [8, 15, 18]) on R were explicitly computed in [14, Proposition 3.8] as

$$\omega_{\text{hom}}(a) = \begin{cases} 1 - \left(\frac{-1}{q-1}\right)^{\text{wt}(a)} & \text{if } a \in \text{soc}(R) \\ 1 & \text{otherwise,} \end{cases}$$

where $\text{wt}(a) := |\{1 \leq i \leq n : a_i \neq 0\}|$ is the weight of $a = (a_1, \dots, a_n)$.

From now on we assume $q \geq 3$. In particular, we have $\omega_{\text{hom}}(a) = 0$ if and only if $a = 0$. Let $[n+1] := \{1, \dots, n+1\}$, and $L := \{S \subseteq [n+1] : n+1 \notin S\} \cup \{[n+1]\}$. Then $\mathcal{L} = (L, \subseteq, \cap, \cup)$ is a regular lattice of rank $n+1$, where the rank function is given by the cardinality of sets. It is easy to see that the parameters of \mathcal{L} are, for all $0 \leq s, t \leq n+1$,

$$\begin{aligned} \mu_{\subseteq}(s, t) &= \begin{cases} \binom{t}{s} & \text{if } s \leq t \leq n \\ \binom{n}{s} & \text{if } s \leq n, t = n+1 \\ 1 & \text{if } s = t = n+1 \\ 0 & \text{if } s > t, \end{cases} & \mu_{\supseteq}(s, t) &= \begin{cases} \binom{n-t}{s-t} & \text{if } t \leq s \leq n \\ 1 & \text{if } t \leq s = n+1 \\ 0 & \text{if } s < t, \end{cases} \\ \mu_{\mathcal{L}}(s, t) &= \begin{cases} (-1)^{t-s} & \text{if } s \leq t \leq n \\ 0 & \text{if } t < s, \text{ or } t = n+1 \text{ and } s < n \\ -1 & \text{if } t = n+1, s = n. \end{cases} \end{aligned}$$

The formula for $\mu_{\mathcal{L}}(s, t)$ can be proved by induction on $t-s$ using the Binomial Theorem, as in Example 36. Define $\sigma : R \rightarrow L$ by $\sigma(a) := [n+1]$ if $a \notin \text{soc}(R)$, and $\sigma(a) := \{1 \leq i \leq n : a_i \neq 0\}$ if

$a \in \text{soc}(R)$. One can check that $\sigma : R \dashrightarrow \mathcal{L}$ is a regular support with

$$\gamma_\sigma(s) = \begin{cases} q^s & \text{if } s \leq n \\ |R| & \text{if } s = n+1 \end{cases}$$

for all $0 \leq s \leq n+1$. Moreover, $\omega_\sigma \sim \omega_{\text{hom}}$. By Theorem 30, in the language of [13] we have

$$\widehat{\mathcal{P}(\omega_{\text{hom}})} = \mathcal{P}(\omega_{\sigma^*}).$$

Therefore the Krawtchouk matrix \mathbf{K} associated to the homogeneous weight partition (see Section 4 of [14] for the definition) is given by

$$\mathbf{K}_{ij} := K(\omega_{\sigma^*}, \omega_\sigma)(i, j) \tag{6}$$

for all $0 \leq i, j \leq n+1$.

When $n = 1$, the ring $R = R_1$ is a finite local Frobenius ring, and with the aid of Theorem 29 one can easily compute

$$\mathbf{K} = \begin{bmatrix} 1 & q-1 & |R|-q \\ 1 & q-1 & -q \\ 1 & -1 & 0 \end{bmatrix}.$$

The same matrix appears in [5] and [14] for $R = \mathbb{Z}_8$.

Combining equation (6) and Theorem 29, one obtains new explicit formulæ for the Krawtchouk coefficients associated to the homogeneous weight, along with a combinatorial interpretation for them. Since \mathcal{L} is modular, by Proposition 32 the weight function ω_σ automatically induces a distance function on R .

Note that for some simple Frobenius rings it is possible to express the homogeneous weight via a suitable chain support on the ring. For example, the homogeneous weight on a finite local Frobenius ring R is equivalent to the chain support associated to the chain $0 \subsetneq \text{soc}(R) \subsetneq R$ (see [3] or [14] for the values of the homogeneous weight on such rings).

It is known (see [14, Section 4]) that the partition induced by the homogeneous weight on more general Frobenius rings is not Fourier-reflexive. In particular, there is no regular support defined on these rings that induces the homogeneous weight. This is the case, for example, of the ring $\mathbb{Z}/546\mathbb{Z}$ (see [14, Example 4.6] for details).

7 Extremality

In this section we study subsets $\mathcal{C} \subseteq G$ that are not necessarily subgroups of G . We consider a slightly more general setting than the one we investigated in the previous sections, relaxing the definition of regular support (see the following Notation 43). We establish a generalized Singleton bound for subsets $\mathcal{C} \subseteq G$. We call “extremal” the codes attaining the Singleton bound. This yields a cardinality-related notion of extremality for codes in groups, that extend the concept of MDS code and MRD rank-metric code. Our specific interest in codes’ cardinality is motivated by the fact that this fundamental parameter reflects the code’s rate.

We show that if \mathcal{C} is an extremal set, then the weight distribution of any translate of \mathcal{C} and the distance distribution of \mathcal{C} coincide. Moreover, they can be expressed in terms of the combinatorial invariants of the underlying lattice. Finally, we prove that if \mathcal{C} is an extremal subgroup (i.e., an extremal code), then the dual code \mathcal{C}^* is extremal as well.

Remark 42. Our approach extends classical results on the distance distributions of extremal codes to the weight distributions of their translates. Notice that full knowledge of the weight distributions of the translates of a code gives information on the distance distribution of the code itself. However, the converse is not true in general, and the weight distributions of the translates of a code need an independent analysis. For MDS codes endowed with the Hamming weight, this analysis is carried out e.g. in [2] with an elegant simple argument.

Notation 43. In this section $(G, +)$ is a finite abelian group, and $\mathcal{L} = (L, \leq, \wedge, \vee)$ denotes a finite graded lattice of rank r that satisfies property (a) of Definition 14. Moreover, $\sigma : G \rightarrow L$ is a function that satisfies properties (A), (B), (C) and (E) of Definition 20. We simply denote by $\omega : G \rightarrow \{0, \dots, r\}$ the function defined by $\omega(g) := \rho_{\mathcal{L}}(\sigma(g))$ for all $g \in G$. We follow the notation of the previous sections, unless specified differently. In particular, we set $\mathcal{C}_{\sigma}(S) := \{g \in \mathcal{C} : \sigma(g) \leq S\}$ for any (possibly non-additive) subset $\mathcal{C} \subseteq G$ and $S \in L$.

In the sequel we investigate combinatorial properties of subsets $\mathcal{C} \subseteq G$ that are not necessarily subgroups of G .

Definition 44. Let $\mathcal{C} \subseteq G$ be any subset with $|\mathcal{C}| \geq 2$. The **minimum weight** and the **minimum distance** of \mathcal{C} are, respectively,

$$w_{\omega}(\mathcal{C}) := \min\{\omega(g) : g \in \mathcal{C}, g \neq 0\}, \quad d_{\omega}(\mathcal{C}) := \min\{\omega(g - g') : g, g' \in \mathcal{C}, g \neq g'\}.$$

The **weight** and **distance distributions** of \mathcal{C} are the integer vectors $(W_i(\mathcal{C}, \omega) : i = 0, \dots, r)$ and $(D_i(\mathcal{C}, \omega) : i = 0, \dots, r)$, respectively, where

$$W_i(\mathcal{C}, \omega) := |\{g \in \mathcal{C} : \omega(g) = i\}|, \quad D_i(\mathcal{C}, \omega) := \frac{1}{|\mathcal{C}|} |\{(g, g') \in \mathcal{C}^2 : \omega(g - g') = i\}|$$

for all $i \in \{0, \dots, r\}$.

Notice that we do not require the map $G \times G \rightarrow \{0, \dots, r\}$ given by $(g, g') \mapsto \omega(g - g')$ to be a distance function on G .

Remark 45. It is easy to check that if $\mathcal{C} \subseteq G$ is a subgroup (i.e., a code) then $W_i(\mathcal{C}, \omega) = D_i(\mathcal{C}, \omega)$ for all $i = 0, \dots, r$. In particular, if $|\mathcal{C}| \geq 2$ then $w_{\omega}(\mathcal{C}) = d_{\omega}(\mathcal{C})$.

We start with a Singleton-type bound of combinatorial flavor.

Proposition 46. Let $\mathcal{C} \subseteq G$ be a subset with $|\mathcal{C}| \geq 2$. We have $|\mathcal{C}| \leq |G|/\gamma_{\sigma}(d_{\omega}(\mathcal{C}) - 1)$.

Proof. Take any $S \in L$ with $\rho_{\mathcal{L}}(S) = d_{\omega}(\mathcal{C}) - 1$. Such an S always exists by definition of rank of a graded poset. For all $g \in \mathcal{C}$ define

$$[g] := g + G_{\sigma}(S) = \{g + h : h \in G_{\sigma}(S)\} \subseteq G.$$

By definition of minimum distance we have $[g] \cap [g'] = \emptyset$ for all $g, g' \in \mathcal{C}$ with $g \neq g'$. Therefore

$$|G| \geq \left| \bigcup_{g \in \mathcal{C}} [g] \right| = \sum_{g \in \mathcal{C}} |[g]| = \sum_{g \in \mathcal{C}} |G_{\sigma}(S)| = |\mathcal{C}| \cdot \gamma_{\sigma}(d_{\omega}(\mathcal{C}) - 1),$$

and the bound follows. □

Definition 47. A subset $\mathcal{C} \subseteq G$ is **extremal** if $|\mathcal{C}| \geq 2$ and it attains the bound of Proposition 46.

The remainder of the section is devoted to the combinatorial properties of extremal sets. We start with a preliminary result.

Lemma 48. Let $\mathcal{C} \subseteq G$ be an extremal subset. Let $S \in L$ be any element with $s := \rho_{\mathcal{L}}(S) \geq d_{\omega}(\mathcal{C})$. Then

$$|\mathcal{C}_{\sigma}(S)| = \frac{|\mathcal{C}| \gamma_{\sigma}(s)}{|G|}.$$

Proof. Let $T \in L$ with $T \leq S$ and $\rho_{\mathcal{L}}(T) = d_{\omega}(\mathcal{C}) - 1$. Such a T always exists by definition of graded posets. We clearly have $G_{\sigma}(T) \subseteq G_{\sigma}(S)$. Define the maps

$$\mathcal{C} \xrightarrow{\pi_1} G/G_{\sigma}(T) \xrightarrow{\pi_2} G/G_{\sigma}(S)$$

as follows. The function π_1 is the composition of the inclusion $\mathcal{C} \rightarrow G$ and the projection on the quotient group $G \rightarrow G/G_{\sigma}(T)$. The map π_2 is given by $g + G_{\sigma}(T) \mapsto g + G_{\sigma}(S)$, and it is a well defined group homomorphism, as $G_{\sigma}(T) \subseteq G_{\sigma}(S)$.

We claim that π_1 is a bijection. Indeed, assume that there exist $g, g' \in \mathcal{C}$ with $\pi_1(g) = \pi_1(g')$, i.e., $g + G_{\sigma}(T) = g' + G_{\sigma}(T)$. Then $g - g' \in G_{\sigma}(T)$, hence $\omega(g - g') \leq \rho_{\mathcal{L}}(T) = d_{\omega}(\mathcal{C}) - 1$. It follows $g = g'$, i.e., π_1 is injective. Since \mathcal{C} is extremal, we have $|\mathcal{C}| = |G|/\gamma_{\sigma}(d_{\omega}(\mathcal{C}) - 1) = |G|/G_{\sigma}(T)$, and so π_1 is a bijection, as claimed.

Since both π_1 and π_2 are surjective, the map $\pi := \pi_2 \circ \pi_1$ is surjective as well. Moreover, as π_1 is bijective and π_2 is a surjective group homomorphism, we have $|\pi^{-1}(0)| = |\pi^{-1}(x)|$ for all $x \in G/G_{\sigma}(S)$. Therefore

$$|\mathcal{C}| = \left| \bigcup_{x \in G/G_{\sigma}(S)} \pi^{-1}(x) \right| = \sum_{x \in G/G_{\sigma}(S)} |\pi^{-1}(x)| = \sum_{x \in G/G_{\sigma}(S)} |\pi^{-1}(0)| = \frac{|G|}{\gamma_{\sigma}(s)} \cdot |\mathcal{C}_{\sigma}(S)|,$$

where the last equality follows from the definition of $\mathcal{C}_{\sigma}(S)$. This shows the lemma. \square

Theorem 49. Let $\mathcal{C} \subseteq G$ be an extremal subset of minimum distance $d := d_{\omega}(\mathcal{C})$ and $0 \in \mathcal{C}$. Define the integer matrix P of size $(r - d + 1) \times (r - d + 1)$ by $P_{ij} := \mu_{\geq}(d + i - 1, d + j - 1)$ for all $i, j \in \{1, \dots, r - d + 1\}$. Then P is invertible, and the weight distribution of \mathcal{C} is given by

$$W_0(\mathcal{C}, \omega) = 1, \quad W_i(\mathcal{C}, \omega) = 0 \text{ for } 1 \leq i \leq d - 1,$$

$$\begin{pmatrix} W_d(\mathcal{C}, \omega) \\ W_{d+1}(\mathcal{C}, \omega) \\ \vdots \\ W_r(\mathcal{C}, \omega) \end{pmatrix} = P^{-1} \begin{pmatrix} |\mathcal{C}| \mu_{\leq}(d, r) \gamma_{\sigma}(d) / |G| - \mu_{\geq}(d, 0) \\ |\mathcal{C}| \mu_{\leq}(d + 1, r) \gamma_{\sigma}(d + 1) / |G| - \mu_{\geq}(d + 1, 0) \\ \vdots \\ |\mathcal{C}| \mu_{\leq}(r, r) \gamma_{\sigma}(r) / |G| - \mu_{\geq}(r, 0) \end{pmatrix}.$$

In particular, the weight distribution of \mathcal{C} only depends on $|G|$, $d_{\omega}(\mathcal{C})$, and on the combinatorial invariants of \mathcal{L} and σ .

Proof. Take any $s \in \{d, \dots, r\}$ and write $d := d_{\omega}(\mathcal{C})$. We will count the elements of the set

$$\mathcal{A} := \{(g, S) : g \in \mathcal{C}, S \in L, \rho_{\mathcal{L}}(S) = s, \sigma(g) \leq S\}$$

in two different ways. On the one hand, by Lemma 48 we have

$$|\mathcal{A}| = \sum_{\substack{S \in L \\ \rho_{\mathcal{L}}(S) = s}} |\mathcal{C}_{\sigma}(S)| = \mu_{\leq}(s, r) \frac{|\mathcal{C}| \gamma_{\sigma}(s)}{|G|}.$$

Since $0 \in \mathcal{C}$, by definition of \mathcal{A} we have

$$|\mathcal{A}| = \sum_{i=0}^s \sum_{\substack{g \in \mathcal{C} \\ \omega(g)=i}} |\{S \in L : \rho_{\mathcal{L}}(S) = s, \sigma(g) \leq S\}| = \mu_{\geq}(s, 0) + \sum_{i=d}^s W_i(\mathcal{C}, \omega) \mu_{\geq}(s, i).$$

Therefore

$$\sum_{i=d}^s W_i(\mathcal{C}, \sigma) \mu_{\geq}(s, i) = \mu_{\leq}(s, r) \frac{|\mathcal{C}| \gamma_{\sigma}(s)}{|G|} - \mu_{\geq}(s, 0), \quad s \in \{d, \dots, r\}. \quad (7)$$

Observe that (7) is a system of $r - d + 1$ linear equations in the unknowns $W_d(\mathcal{C}, \omega), \dots, W_r(\mathcal{C}, \omega)$. The matrix of the system is precisely P , which is lower triangular with all ones on the diagonal. \square

Remark 50. Following the notation of Theorem 49, when \mathcal{L} also satisfies property (b) of Definition 14 the weight distribution of an extremal subset $\mathcal{C} \subseteq G$ with $d = d_{\omega}(\mathcal{C})$ and $0 \in \mathcal{C}$ can be expressed as

$$W_i(\mathcal{C}, \sigma) = \sum_{s=0}^{d-1} \mu_{\mathcal{L}}(s, i) \mu_{\leq}(s, i) + \sum_{s=d}^i \mu_{\mathcal{L}}(s, i) \mu_{\leq}(s, i) \frac{|\mathcal{C}| \gamma_{\sigma}(s)}{|G|}, \quad d \leq i \leq r.$$

We do not go into the details of the proof. In the context of codes endowed with the rank metric, to our best knowledge the previous formula is new. As we will see in Corollary 51, it generalizes a result by Delsarte on the distance distribution of extremal codes (see [10, Theorem 5.6]).

If $\mathcal{C} \subseteq G$ is a non-empty subset and $h \in G$, we define the **translate** of \mathcal{C} by h as the set $\mathcal{C}_h := \{g - h : g \in \mathcal{C}\} \subseteq G$.

Corollary 51. Let $\mathcal{C} \subseteq G$ be an extremal subset of minimum distance $d := d_{\omega}(\mathcal{C})$. For all $h \in \mathcal{C}$ we have $W_i(\mathcal{C}_h, \omega) = D_i(\mathcal{C}, \omega)$ for $i \in \{0, \dots, r\}$.

Proof. For all $i \in \{0, \dots, r\}$ one has

$$D_i(\mathcal{C}, \omega) = \frac{1}{|\mathcal{C}|} |\{(g, g') \in \mathcal{C}^2 : \omega(g - g') = i\}| = \frac{1}{|\mathcal{C}|} \sum_{g' \in \mathcal{C}} |\{g \in \mathcal{C} : \omega(g - g') = i\}| = \frac{1}{|\mathcal{C}|} \sum_{g' \in \mathcal{C}} W_i(\mathcal{C}_{g'}, \omega).$$

Let $h \in \mathcal{C}$ be any element. It is easy to see that the translate \mathcal{C}_h has the same distance distribution as \mathcal{C} . In particular, \mathcal{C}_h is extremal. Moreover, since $0 \in \mathcal{C}_h$, its weight distribution is given by Theorem 49, and it does not depend on $h \in \mathcal{C}$. Therefore for all $h \in \mathcal{C}$ and $i \in \{0, \dots, r\}$ one has

$$D_i(\mathcal{C}, \omega) = \frac{1}{|\mathcal{C}|} \cdot |\mathcal{C}| \cdot W_i(\mathcal{C}_h, \omega) = W_i(\mathcal{C}_h, \omega),$$

as claimed. \square

Remark 52. Combining Theorem 49 and Corollary 51 we obtain generalizations of classical results on the distance distribution of the translates of cardinality-optimal codes to the general context of additive codes in groups.

We conclude this section showing that if \mathcal{C} is an extremal code (i.e., a subgroup of G) and σ also satisfies property (D) of Definition 20, then the dual of \mathcal{C} is an extremal code as well. Note that property (b) of Definition 14 is still not required, and thus \mathcal{L} is not a regular lattice in general.

Lemma 53. Let $\mathcal{C} \subseteq G$ be a code, and assume that σ also satisfies property (D) of Definition 20. Take any $S \in L$, and let $s := \rho_{\mathcal{L}}(S)$. We have

$$|\mathcal{C}_{\sigma}(S)| = \frac{|\mathcal{C}| \cdot |\mathcal{C}_{\sigma^*}^*(S)|}{\gamma_{\sigma^*}(r - s)}.$$

Proof. By definition, $\mathcal{C}_{\sigma}(S) = G_{\sigma}(S) \cap \mathcal{C}$. Remark 2 implies

$$|\mathcal{C}_{\sigma}(S)| = \frac{|G_{\sigma}(S)| \cdot |\mathcal{C}|}{|G_{\sigma}(S) + \mathcal{C}|} = \frac{|G_{\sigma}(S)| \cdot |\mathcal{C}| \cdot |(G_{\sigma}(S) + \mathcal{C})^*|}{|G|}. \quad (8)$$

Again by Remark 2 we have $|(G_{\sigma}(S) + \mathcal{C})^*| = |G_{\sigma}(S)^* \cap \mathcal{C}^*| = |\hat{G}_{\sigma^*}(S) \cap \mathcal{C}^*|$, where the last equality follows from Theorem 24 (whose proof does not require property (b) of Definition 14). Since $\hat{G}_{\sigma^*}(S) \cap \mathcal{C}^* = \mathcal{C}_{\sigma^*}^*(S)$ by definition, equation (8) can be written as

$$|\mathcal{C}_{\sigma}(S)| = \frac{|G_{\sigma}(S)| \cdot |\mathcal{C}| \cdot |\mathcal{C}_{\sigma^*}^*(S)|}{|G|}.$$

By Theorem 24 we have $|G|/|G_{\sigma}(S)| = |G|/\gamma_{\sigma}(s) = \gamma_{\sigma^*}(r - s)$, and the result follows. \square

Theorem 54. Let $\mathcal{C} \subseteq G$ be a non-trivial extremal code, and assume that σ also satisfies property (D) of Definition 20. Then $d_{\omega_{\sigma^*}}(\mathcal{C}^*) \geq r - d_{\omega_{\sigma}}(\mathcal{C}) + 2$, and the code \mathcal{C}^* is extremal.

Proof. Let $d := d_{\omega_{\sigma}}(\mathcal{C})$ and $d^* := d_{\omega_{\sigma^*}}(\mathcal{C}^*)$. Since \mathcal{C} is extremal, we have $|\mathcal{C}| = |G|/\gamma_{\sigma}(d - 1)$. Remark 2 and Theorem 24 (whose proof does not require property (b) of Definition 14) imply

$$|\mathcal{C}^*| = \gamma_{\sigma}(d - 1) = |\hat{G}|/\gamma_{\sigma^*}(r - d + 1). \quad (9)$$

Let $S \in L$ be any element with $\rho_{\mathcal{L}^*}(S) = r - d + 1$. Then $\rho_{\mathcal{L}}(S) = r - (r - d + 1) = d - 1$, and so $\mathcal{C}_{\sigma}(S) = \{0\}$. Lemma 53 gives

$$|\mathcal{C}_{\sigma^*}^*(S)| = \frac{|\mathcal{C}_{\sigma}(S)| \cdot \gamma_{\sigma^*}(r - d + 1)}{|\mathcal{C}|} = 1,$$

where the last equality easily follows from equation (9) and Remark 2. Therefore $\mathcal{C}_{\sigma^*}^*(S) = \{0\}$, and the minimum weight/distance of \mathcal{C}^* satisfies $d^* \geq r - d + 2$. In particular, $\gamma_{\sigma^*}(d^* - 1) \geq \gamma_{\sigma^*}(r - d + 1)$. Combining Proposition 46 applied to \mathcal{C}^* and σ^* with equation (9) we obtain

$$\frac{|\hat{G}|}{\gamma_{\sigma^*}(r - d + 1)} \geq \frac{|\hat{G}|}{\gamma_{\sigma^*}(d^* - 1)} \geq |\mathcal{C}^*| = \frac{|\hat{G}|}{\gamma_{\sigma^*}(r - d + 1)}.$$

It follows $|\mathcal{C}^*| = |\hat{G}|/\gamma_{\sigma^*}(d^* - 1)$, i.e., \mathcal{C}^* is extremal. \square

8 Enumerative Problems of Matrices

In this section we show how one can apply the MacWilliams identities for the rank weight to answer some open enumerative combinatorics questions on matrices over a finite field. In particular, we answer a generalized question of R. Stanley on the number of matrices with given rank and zero diagonal entries.

Following the notation of Example 39, in the sequel k and m are integers with $1 \leq k \leq m$, and \mathbb{F}_q is the finite field with q elements. We denote by Mat the km -dimensional space of $k \times m$ matrices over \mathbb{F}_q . Given an integer $s \geq 1$, we set $[s] := \{1, \dots, s\}$. The rank support on Mat is denoted by σ_{rk} ,

and ω_{rk} is the rank weight. We write “rank-distribution” for “ ω_{rk} -distribution”. All dimensions in this section are computed over \mathbb{F}_q .

Recall that the **trace-product** of matrices $M, N \in \text{Mat}$ is $\langle M, N \rangle := \text{Tr}(MN^t)$, where Tr denotes the trace of matrices and t denotes transposition. The **orthogonal** of a linear code $\mathcal{C} \subseteq \text{Mat}$ is the linear code $\mathcal{C}^\perp = \{M \in \text{Mat} : \langle M, N \rangle = 0 \text{ for all } N \in \mathcal{C}\}$. Notice that for any linear code \mathcal{C} one has $\{M^t : M \in \mathcal{C}\}^\perp = \{M^t : M \in \mathcal{C}^\perp\}$. In particular, up to a transposition of the matrices, the assumption $k \leq m$ is not restrictive.

We start by recalling the MacWilliams identities for linear codes endowed with the rank weight (see [10] or Example 39).

Theorem 55. Let $\mathcal{C} \subseteq \text{Mat}$ be a linear code. The rank-distributions of \mathcal{C} and \mathcal{C}^\perp satisfy

$$W_j(\mathcal{C}^\perp, \omega_{\text{rk}}) = \frac{1}{|\mathcal{C}|} \sum_{i=0}^k W_i(\mathcal{C}, \omega_{\text{rk}}) \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}$$

for all $0 \leq j \leq k$. In particular, they determine each other.

The first enumerative technique that we present is based on the following simple observation. If $f : \text{Mat} \rightarrow \mathbb{F}_q$ is a non-zero \mathbb{F}_q -linear function, then $\ker(f)^\perp$ is a linear code generated by one matrix. Any two generating matrices have the same rank, say R_f . Thus the rank distribution of the linear code $\mathcal{C} := \ker(f)^\perp$ is

$$W_i(\mathcal{C}, \omega_{\text{rk}}) = \begin{cases} 1 & \text{if } i = 0 \\ q-1 & \text{if } i = R_f \\ 0 & \text{otherwise.} \end{cases}$$

Applying Theorem 55 to $\mathcal{C} := \ker(f)^\perp$ one can now explicitly compute the number of matrices of rank j in $\ker(f) = \mathcal{C}^\perp$ for all $0 \leq j \leq k$. More precisely, the following hold.

Corollary 56. Let $f : \text{Mat} \rightarrow \mathbb{F}_q$ be a non-zero linear map, and let R_f be the rank of any matrix that generates $\ker(f)^\perp$. For all $0 \leq j \leq k$ the number of rank j matrices in $\ker(f)$ is

$$\frac{1}{q} \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \left(\begin{bmatrix} k \\ s \end{bmatrix} + (q-1) \begin{bmatrix} k-R_f \\ s \end{bmatrix} \right).$$

Let e.g. $f : \text{Mat} \rightarrow \mathbb{F}_q$ be the linear map that sends a matrix to the sum of its entries. The orthogonal code of $\ker(f)$ is generated by the matrix whose entries are all ones, which has rank one. By Corollary 56, for all $0 \leq j \leq k$ the number of rank j matrices over \mathbb{F}_q of size $k \times m$ whose entries sum to zero is

$$\frac{1}{q} \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \left(\begin{bmatrix} k \\ s \end{bmatrix} + (q-1) \begin{bmatrix} k-1 \\ s \end{bmatrix} \right).$$

Generalizing the previous argument one obtains the following.

Corollary 57. Let $I \subseteq [k] \times [m]$ be a non-zero set of indices. For all $0 \leq j \leq k$ the number of $k \times m$ rank j matrices M over \mathbb{F}_q such that $\sum_{(s,t) \in I} M_{st} = 0$ is

$$\frac{1}{q} \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \left(\begin{bmatrix} k \\ s \end{bmatrix} + (q-1) \begin{bmatrix} k - \text{rk}(M(I)) \\ s \end{bmatrix} \right),$$

where $M(I)$ denotes the $k \times m$ matrix defined, for all $(s, t) \in [k] \times [m]$, by $M(I)_{st} := 1$ if $(s, t) \in I$, and $M(I)_{st} := 0$ otherwise.

The computation of the number of matrices over \mathbb{F}_q with given size, rank and zero entries in a prescribed region is an active research area in combinatorics and combinatorial statistics (see, among others [16], [20], [23], [32] and the references therein). Such matrices can be regarded as q -analogues of permutations with restricted positions. It turns out that some instances of this type of enumeration problems can be investigated using MacWilliams identities for the rank support, as we now show.

Let us first fix a convenient notation. The complement of a set $I \subseteq [k] \times [m]$ is denoted by I^c . For $I \subseteq [k] \times [m]$ define $\text{Mat}[I] := \{M \in \text{Mat} : M_{st} = 0 \text{ for all } (s, t) \in I^c\}$. Clearly, $\text{Mat}[I]$ is an \mathbb{F}_q -subspace of Mat of dimension $|I|$.

Remark 58. For any subset $I \subseteq [k] \times [m]$ we have $\text{Mat}[I]^\perp = \text{Mat}[I^c]$. Therefore by Theorem 55 the rank distributions of $\text{Mat}[I]$ and $\text{Mat}[I^c]$ determine each other.

For some sets I , the rank distribution of $\text{Mat}[I]$ can be explicitly computed. In these cases Theorem 55 gives a formula for the number of matrices in Mat of any rank and zero entries on I .

Corollary 59. Let $1 \leq k' \leq k$ and $1 \leq m' \leq m$ be integers. For all $0 \leq j \leq k$ the number of $k \times m$ rank j matrices M over \mathbb{F}_q such that $M_{st} = 0$ for all $(s, t) \in [k'] \times [m']$ is

$$q^{-k'm'} \sum_{i=0}^{\min\{k', m'\}} \begin{bmatrix} m' \\ i \end{bmatrix} \prod_{u=0}^{i-1} (q^{k'} - q^u) \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}.$$

Proof. Let $I := [k'] \times [m']$. The code $\mathcal{C} := \text{Mat}[I]$ is the set of matrices whose entries are contained in the rectangular region described by I . As a consequence, for all $0 \leq i \leq \min\{k', m'\}$, $W_i(\mathcal{C}, \omega_{\text{rk}})$ is the number of $k' \times m'$ matrices over \mathbb{F}_q with rank i , i.e.,

$$W_i(\mathcal{C}, \omega_{\text{rk}}) = \begin{bmatrix} m' \\ i \end{bmatrix} \prod_{u=0}^{i-1} (q^{k'} - q^u) \quad \text{for } 0 \leq i \leq \min\{k', m'\}.$$

For $\min\{k', m'\} < i \leq k'$ we have $W_i(\mathcal{C}, \omega_{\text{rk}}) = 0$. The result immediately follows from Remark 58 and Theorem 55. \square

Up to a permutation of rows and columns, the matrices of Corollary 59 have all their non-zero entries contained in a Ferrers board. Matrices with this property have been widely studied in the literature (see [16] among others).

Again concerning matrices with prescribed zero entries, a question of R. Stanley asks for the number of invertible matrices over \mathbb{F}_q having zero diagonal entries (see the Introduction of [23]). The question was answered in [23, Proposition 2.2], where the authors provide a formula for the number of $k \times m$ full-rank matrices over \mathbb{F}_q with zero diagonal entries. Notice that for diagonal entries of a rectangular matrix M we mean the entries of the form M_{ss} for $1 \leq s \leq k$.

The following corollary generalizes Proposition 2.2 of [23] with a simple proof based on MacWilliams identities.

Corollary 60. Let $I \subseteq \{(s, t) \in [k] \times [m] : s = t\}$ be a set of diagonal entries. For all $0 \leq j \leq k$ the number of $k \times m$ matrices M over \mathbb{F}_q having rank j and $M_{st} = 0$ for all $(s, t) \in I$ is

$$q^{-|I|} \sum_{i=0}^{|I|} \binom{|I|}{i} (q-1)^i \sum_{s=0}^k (-1)^{j-s} q^{ms + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}.$$

Proof. Define $\mathcal{C} := \text{Mat}[I]$. For $|I| < i \leq k$ we have $W_i(\mathcal{C}, \omega_{\text{rk}}) = 0$, and for $0 \leq i \leq |I|$ we have

$$W_i(\mathcal{C}, \omega_{\text{rk}}) = \binom{|I|}{i} (q-1)^i.$$

Therefore the formula follows from Remark 58 and Theorem 55. \square

We conclude this section mentioning a very concise method to compute the number of symmetric and skew-symmetric $k \times k$ matrices of given rank over \mathbb{F}_q . Different formulæ for the same numbers were given by Carlitz in [6] and [7] and by MacWilliams in [26] using quite involved recursive arguments. Our technique employs the Möbius inversion formula and the regularity of the lattice of subspaces of \mathbb{F}_q^k , which we denote by \mathcal{L} in the sequel (see Example 39).

Recall that a $k \times k$ matrix M is **symmetric** if $M_{ij} = M_{ji}$ for all $1 \leq i, j \leq k$ and **skew-symmetric** if $M_{ii} = 0$ and $M_{ij} = -M_{ji}$ for all $1 \leq i, j \leq k$. We denote by Sym and s-Sym the spaces of $k \times k$ symmetric and skew-symmetric matrices over \mathbb{F}_q , respectively.

Lemma 61. Let $S \subseteq \mathbb{F}_q^k$ be any s -dimensional subspace. Then $\{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq S\}$ has dimension $s(s+1)/2$ over \mathbb{F}_q .

Proof. Define $V := \{x \in \mathbb{F}_q^k : x_i = 0 \text{ for } i > s\} \subseteq \mathbb{F}_q^k$. There exists an \mathbb{F}_q -isomorphism $g : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^k$ such that $g(S) = V$. Let $G \in \text{GL}_k(\mathbb{F}_q)$ be the matrix associated to g with respect to the canonical basis $\{e_1, \dots, e_k\}$ of \mathbb{F}_q^k . Since G is invertible, the map $M \mapsto GMG^t$ is an \mathbb{F}_q -linear isomorphism $\{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq S\} \rightarrow \{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq V\}$. The lemma now follows from the fact that $\dim(\{M \in \text{Sym} : \sigma_{\text{rk}}(M) \subseteq V\}) = s(s+1)/2$. \square

We can now compute the number of symmetric $k \times k$ matrices over \mathbb{F}_q of rank i as follows. For any subspace $T \subseteq \mathbb{F}_q^k$ define $f(T) := |\{M \in \text{Sym} : \sigma_{\text{rk}}(M) = T\}|$ and $g(T) := \sum_{S \subseteq T} f(S)$. By Lemma 61, for all $S \subseteq \mathbb{F}_q^k$ we have $g(S) = q^{s(s+1)/2}$, where $s := \dim(S)$. Therefore applying the Möbius inversion formula ([31], Proposition 3.7.1) to the functions f and g we obtain, for any given i -dimensional subspace $T \subseteq \mathbb{F}_q^k$,

$$f(T) = \sum_{S \subseteq T} g(S) \mu_{\mathcal{L}}(S, T) = \sum_{s=0}^k \sum_{\substack{S \subseteq T \\ \dim(S)=s}} q^{s(s+1)/2} \mu_{\mathcal{L}}(s, i) = \sum_{s=0}^k q^{\binom{s+1}{2}} \begin{bmatrix} i \\ s \end{bmatrix} (-1)^{i-s} q^{\binom{i-s}{2}}.$$

The expected result is now derived summing over all the i -dimensional subspaces $T \subseteq \mathbb{F}_q^k$. A similar argument applies to skew-symmetric matrices. The final result is the following.

Proposition 62. The number of symmetric and skew-symmetric $k \times k$ matrices over \mathbb{F}_q of rank i is, respectively,

$$\begin{bmatrix} k \\ i \end{bmatrix} \sum_{s=0}^k (-1)^{i-s} q^{\binom{s+1}{2} + \binom{i-s}{2}} \begin{bmatrix} i \\ s \end{bmatrix}, \quad \begin{bmatrix} k \\ i \end{bmatrix} \sum_{s=0}^k (-1)^{i-s} q^{\binom{s}{2} + \binom{i-s}{2}} \begin{bmatrix} i \\ s \end{bmatrix}.$$

One can also observe that the spaces of $k \times k$ symmetric and skew-symmetric matrices over \mathbb{F}_q are orthogonal to each other. Therefore the rank distributions of symmetric and skew-symmetric matrices are related by a MacWilliams transformation. More precisely, the following hold.

Corollary 63. For all integers $0 \leq j \leq k$ we have

$$W_j(\text{Sym}, \omega_{\text{rk}}) = q^{-\binom{k}{2}} \sum_{i=0}^k W_i(\text{s-Sym}, \omega_{\text{rk}}) \sum_{s=0}^k (-1)^{j-s} q^{ks + \binom{j-s}{2}} \begin{bmatrix} k-s \\ k-j \end{bmatrix} \begin{bmatrix} k-i \\ s \end{bmatrix}.$$

Acknowledgement

The author is grateful to Elisa Gorla, Frank R. Kschischang, and the Referees of this paper for help in improving Section 6 and the presentation of this work.

References

- [1] G. E. Andrews, *The Theory of Partitions*. Encyclopedia of Mathematics and its Applications, vol. 2, G.C. Rota Editor. Addison-Wesley, 1976.
- [2] P.G. Bonneau, *Weight Distributions of Translates of MDS Codes*, *Combinatorica*, 10 (1), 103–105, 1990.
- [3] E. Byrne, *On the weight distribution of codes over finite rings*. *Advances in Mathematics of Communications*, 5 (2011), pp. 395 – 406.
- [4] E. Byrne, M. Greferath, M. E. O’Sullivan, *The linear programming bound for codes over finite Frobenius rings*. *Designs, Codes and Cryptography*, 42 (2007), pp. 289 – 301.
- [5] P. Camion, *Codes and association schemes*. In V. S. Pless and W. C. Huffman (editors), *Handbook of Coding Theory*, Vol. II, pp. 1441 – 1566. Elsevier (1998).
- [6] L. Carlitz, *Representations by quadratic forms in a finite field*. *Duke Mathematical Journal*, 21 (1954), pp. 123 – 137.
- [7] L. Carlitz, *Representations by skew forms in a finite field*. *Archiv der Mathematik*, 5 (1954), pp. 19 – 31.
- [8] I. Constantinescu, W. Heise, *A metric for codes over residue class rings*. *Problems on Information Transmission*, 33 (1997), pp. 208 – 213.
- [9] P. Delsarte, *Association schemes and t -designs in regular semilattices*. *Journal of Combinatorial Theory, Series A*, 2 (1976), 2, pp. 230 – 243.
- [10] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*. *Journal of Combinatorial Theory, Series A*, 25 (1978), 3, pp. 226 – 241.
- [11] P. Delsarte, *An algebraic approach to the association schemes of coding theory*. Philips Research Report, Supplement, 10 (1973).
- [12] G. D. Forney, Jr, *Transforms and groups*. In A. Vardy (ed.), *Codes, Curves and Signals: Common Threads in Communications*, pp. 79 – 97. Kluwer, 1998.
- [13] H. Gluesing-Luerssen, *Fourier-reflexive partitions and MacWilliams identities for additive codes*. *Designs, Codes and Cryptography*, 75 (2015), pp. 543 – 563.
- [14] H. Gluesing-Luerssen, *Partitions of Frobenius rings induced by the homogeneous weight*. *Advances in Mathematics of Communications*, 8 (2014), pp. 191 – 207.

- [15] M. Greferath, S. Schmidt, *Finite ring combinatorics and MacWilliams' Equivalence Theorem*. Journal of Combinatorial Theory, 92A (2000), pp. 17 – 28.
- [16] J. Haglund, *q-rook polynomials and matrices over finite fields*. Advances in Applied Mathematics, 20 (1998), 4, pp. 450 – 487.
- [17] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes*. IEEE Transactions on Information Theory, 40 (1994), pp. 301 – 319.
- [18] T. Honold, I. Landjev, *MacWilliams identities for linear codes over finite Frobenius rings*. In D. Jungnickel and H. Niederreiter, editors, *Proceedings of The Fifth International Conference on Finite Fields and Applications Fq5*, Augsburg, 1999, pp. 276 – 292. Springer 2001.
- [19] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press (2003).
- [20] A. J. Klein, J. B. Lewis, A. H. Morales, *Counting matrices over finite fields with support on skew Young diagrams and complements of Rothe diagrams*. Journal of Algebraic Combinatorics, 39 (2014), 2, pp. 429 – 456.
- [21] T. Y. Lam, *Lectures on Modules and Rings*. Graduate Text in Mathematics, vol. 189. Springer 1999.
- [22] C. Lee, *Some properties of nonbinary error-correcting codes*. IRE Transactions on Information Theory, 4 (1958), 2, pp. 77 – 82.
- [23] J. B. Lewis, R. Liu, G. Panova, A. H. Morales, S. V. Sam, Y. X. Zhang, *Matrices with restricted entries and q-analogues of permutations*. Journal of Combinatorics, 2 (2012), 3, pp. 355 – 396.
- [24] J. H. van Lint, *Introduction to Coding Theory*, third edition. Springer (1999).
- [25] F. J. MacWilliams, *A Theorem on the Distribution of Weights in a Systematic Code*. Bell System Technical Journal, 42 (1963), 1, pp. 79 – 94.
- [26] F. J. MacWilliams, *Orthogonal matrices over finite fields*. American Mathematical Monthly, 76 (1969), pp. 152 – 164.
- [27] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Mathematical Library (1977).
- [28] A. Ravagnani, *Rank-metric codes and their duality theory*. Designs, Codes and Cryptography, 80 (2016), 1, pp. 197 – 216.
- [29] D. Silva, F. R. Kschischang, *On metrics for error correction in network coding*. IEEE Transactions on Information Theory, 55 (2009), 12, pp. 5479 – 5490.
- [30] E. Spiegel, C. J. O'Donnell, *Incidence algebras*. CRC Press (1997).
- [31] P. Stanley, *Enumerative Combinatorics*, vol. 1, second ed., Cambridge Stud. Adv. Math., vol. 49, Cambridge University Press, Cambridge (2012).
- [32] J. R. Stembridge, *Counting points on varieties over finite fields related to a conjecture of Kontsevich*. Annals of Combinatorics, 2 (1998), 4, pp. 365 – 385.

- [33] V. A. Zinoviev, T. Ericson, *On Fourier invariant partitions of finite abelian groups and the MacWilliams identity for group codes*. Problems of Information Transmission, 32 (1996), pp. 117 – 122.
- [34] V. A. Zinoviev, T. Ericson, *Fourier invariant pairs of partitions of finite abelian groups and association schemes*. Problems of Information Transmission, 45 (2009), pp. 221 – 231.