Finite Quasi-Frobenius Modules and Linear Codes

Marcus Greferath, Alexandr Nechaev*, and Robert Wisbauer

August 12, 2003

Abstract

The theory of linear codes over finite fields has been extended by A. Nechaev to codes over quasi-Frobenius modules over commutative rings, and by J. Wood to codes over (not necessarily commutative) finite Frobenius rings. In the present paper we subsume these results by studying linear codes over quasi-Frobenius and Frobenius modules over any finite ring. Using the character module of the ring as alphabet we show that fundamental results like MacWilliams' theorems on weight enumerators and code isometry can be obtained in this general setting.

Introduction

The foundations of classical algebraic coding theory over finite fields involve notions and results like *dual code*, *MacWilliams identity* and *extension theorem*. In the papers [21, 22, 23, 15], Kuzmin, Kurakin, Markov, Mikhalev, and Nechaev developed a theory of linear codes over finite modules over commutative rings. It was shown that for such rings the basic results mentioned above may be suitably generalized to codes over *quasi-Frobenius modules*. Moreover, it turns out that the quasi-Frobenius module of a commutative ring is unique up to isomorphism.

The present article is a further contribution in this direction, based on the observation that every finite (noncommutative) ring A possesses a quasi-Frobenius bimodule ${}_AQ_A$. Even more, it can be shown that this module is unique up to (left and right) isomorphism, if we claim its socle to be cyclic, in which case we call it the *Frobenius module* of A. We show the the theory of linear codes over commutative rings can be extended to suchmodules to a far extent. The results of Wood [31] cover exactly the case where the given ring A is a Frobenius ring, i.e., where it is isomorphic to Q as a left (and as a right) module. We feel that, in general, coding theory over a finite ring A should involve the Frobenius module of A as alphabet rather than the ring A itself.

This article is organized as follows. Section 1 contains preliminaries and useful results concerning injectivity and cogenerator properties of modules; Section 2 recalls the notions of quasi-Frobenius and Frobenius bimodules and derives existence and uniqueness theorems about Frobenius bimodules over finite rings. In Section 3 we introduce linear codes over modules and observe the equality of the Hamming distance of a code and that of its socle (for the commutative case see [22]). As a consequence, the Hamming distance of any linear code can be expressed by the Hamming distances of linear codes over modules over simple rings. We provide an appropriate notion of the dual code and generalize MacWilliams' theorem (concerning the relationship between the weight enumerators

*The author thanks DFG and the University of Düsseldorf for support and hospitality.

of mutually dual codes) to linear codes over finite modules. Section 4 deals with the equivalence of linear codes over Frobenius modules. After studying homogeneous functions on finite modules (initiated in [4, 10, 12, 8]) we will prove that every homogeneous isometry and every Hamming isometry between linear codes over the Frobenius module extends to a monomial transformation of the ambient space.

1 Preliminaries from Module Theory

Let A be an associative ring with identitiy and denote by ${}_A\mathbf{M}$ and $\mathbf{M}_A$ the categories of unital left and right A-modules, respectively. For $M, M' \in {}_A\mathbf{M}$ and $N, N' \in \mathbf{M}_A$ we write $\mathrm{Hom}({}_AM, {}_AM')$ and $\mathrm{Hom}(N_A, N'_A)$ for the set of homomorphisms between these modules, and $\mathrm{End}({}_AM)$ and $\mathrm{End}(N_A)$ for the corresponding endomorphism rings; suffixes (e.g., in ${}_AM$) are deleted if the context is clear. We let morphisms of left modules act from the right side, and morphisms of right modules act from the left; thus any $M \in {}_A\mathbf{M}$ with $B = \mathrm{End}({}_AM)$ is an (A,B)-bimodule.

Given any (A,B)-bimodule ${}_AM_B$, there is a canonical ring homomorphism $\phi : A \to \mathrm{End}(M_B)$ and we call M *left balanced* provided ϕ is an isomorphism. Similariy *right balanced* bimodules are defined and a bimodule is called *balanced* if it is left and right balanced.

$\mathfrak{J}(A)$ denotes the *Jacobson radical* of A. If A is left or right artinian $\mathfrak{J}(A)$ is a nilpotent ideal and $\overline{A} = A/\mathfrak{J}(A)$ is a classical semisimple ring; that is, a finite direct sum of matrix rings over division rings. If A is finite then all these division rings are fields (Wedderburn).

For any A-module M, the *socle* $\mathfrak{S}({}_AM)$ is the sum of all minimal submodules of M; clearly $\mathfrak{S}({}_AM)$ is annihilated by $\mathfrak{J}(A)$ and hence can be considered as module over $\overline{A} = A/\mathfrak{J}(A)$. For artinian rings A, the socle of M is an essential submodule and is equal to the annihilator of the radical,

$$\mathfrak{S}({}_AM) = \{m \in M \mid \mathfrak{J}(A)m = 0\}.$$

Let $M, N \in {}_A\mathbf{M}$. The module N is called *(finitely) M-generated* if N is a homomorphis image of a (finite) direct sum of copies of M. The full subcategory of ${}_A\mathbf{M}$ whose objects are submodules of M-generated modules is denoted by $\sigma[{}_AM]$. It is a basic fact that $\sigma[{}_AM] = {}_A\mathbf{M}$ provided M is a faithful A-module which is finitely generated as $\mathrm{End}({}_AM)$-module (see [30, 15.4]). In particular, for any finite faithful left A-module M we have $\sigma[{}_AM] = {}_A\mathbf{M}$ and the ring A is finite.

Definition 1.1 Annihilators. For a module ${}_AM$ and the ring $B = \mathrm{End}({}_AM)$ we consider the following *annihilators*. For subsets $I \subseteq A$, $J \subseteq B$ and $K \subseteq M$ define

$$\begin{aligned}
\rho_M(I) &:= \{m \in M \mid Im = 0\} \leq M_B,\\
\lambda_M(J) &:= \{m \in M \mid mJ = 0\} \leq {}_AM,\\
\rho_B(K) &:= \{b \in B \mid Kb = 0\} \leq B_B, \text{ and}\\
\lambda_A(K) &:= \{a \in A \mid aK = 0\} \leq {}_AA.
\end{aligned}$$

For particular subsets we have natural identifications

$$\begin{aligned}
\rho_M(I) &= \mathrm{Hom}(A/I, {}_AM), && \text{for left ideals } I \leq A,\\
\lambda_M(J) &= \mathrm{Hom}(B/J, M_B), && \text{for right ideals } J \leq B,\\
\rho_B(K) &= \mathrm{Hom}(M/K, {}_AM), && \text{for } A\text{-submodules } K \leq M,\\
\lambda_A(K) &= \mathrm{Hom}(M/K, M_B), && \text{for } B\text{-submodules } K \leq M, \text{ provided } M \text{ is left balanced.}
\end{aligned}$$

For A artinian, $\mathfrak{S}({}_AM) = \rho_M(\mathfrak{J}(A)) = \mathrm{Hom}(\overline{A}, {}_AM)$.

Injective modules. Let $M, N \in {}_A\mathbf{M}$. M is called *N-injective* if for any submodule $K \leq N$ any homomorphism $K \to M$ can be extended to a homomorphism $N \to M$. If M is M-injective then M is called *self-injective* (also *quasi-injective*).

Proposition 1.2 *Let ${}_AM$ be self-injective with finitely generated essential socle. Then for any submodule $K \subset M$, monomorphisms $f : K \to M$ can be extended to automorphisms of M.*

Proof: Denote by $\widehat{K} \subset M$ a maximal essential extension of K in M. Then f can be extended to a monomorphism $\hat{f} : \widehat{K} \to M$. Furthermore $\widehat{K}$ is a direct summand (by [30, 17.7]) and hence is M-injective and so is $\hat{f}(\widehat{K})$, i.e.,

$$M = \widehat{K} \oplus U = \hat{f}(\widehat{K}) \oplus V \cong \widehat{K} \oplus V,$$

for suitable submodules $U, V \subset M$. By [30, 22.1], $\mathrm{End}(U)$ is semiperfect and hence by the cancellation property (cf. [16, 20.11]) there is an isomorphism $g : U \to V$. Now

$$\hat{f} \oplus g : M = \widehat{K} \oplus U \to \hat{f}(\widehat{K}) \oplus V = M$$

is an automorphism of M extending f. □

Given $M, N \in {}_A\mathbf{M}$, the module M is said to be *min-N-injective* if for any simple submodule $K \leq {}_AN$ any homomorphism ${}_AK \to {}_AM$ can be extended to a homomorphism ${}_AN \to {}_AM$. We call M *min-self-injective* provided it is min-M-injective.

Proposition 1.3 *Let $M, N \in {}_A\mathbf{M}$ and $B = \mathrm{End}({}_AM)$.*

(a) *The following are equivalent:*

- **(i)** *M is min-self-injective;*
- **(ii)** *for any simple A-module K, $\mathrm{Hom}(K, M)$ is either zero or a simple B-module.*
- **(iii)** *for every maximal left ideal $I \leq A$, $\rho_M(I)$ is either zero or a simple B-module.*

(b) *If ${}_AM$ is faithful and min-self-injective then it is also min-A-injective.*

(c) *Let M be min-self-injective and $U \leq V \leq N$ submodules with V/U simple. Then the B-module $\mathrm{Hom}(N/V, M)$ can naturally be considered as submodule of $\mathrm{Hom}(N/U, M)$ and the quotient module*

$$\mathrm{Hom}(N/U, M)/\mathrm{Hom}(N/V, M)$$

is either zero or a simple right B-module.

Proof: **(a)** $(i) \Leftrightarrow (ii)$ Let M be min-self-injective and K a simple A-module. Then for any two morphisms $f, g : K \to M$ we have two isomorphic minimal submodules $f(K)$ and $g(K)$ of

the module ${}_AM$. The definition of min-self-injective module imply that there exists $h \in B$ with $h \circ g = f$. Hence $f \in gB$. So any non-zero element $g \in \mathrm{Hom}(K, M)$ is a generating element of $\mathrm{Hom}(K, M)_B$. The converse conclusion is seen similarly.

The equivalence $(ii) \Leftrightarrow (iii)$ follows from the equality $\rho_M(I) = \mathrm{Hom}(A/I, {}_AM)$.

(b) As a faithful A-module, M cogenerates A. Hence for any simple left ideal $i : K \to A$ there is a morphism $h : A \to M$ with $h \circ i \neq 0$. Given any morphism $f : K \to M$ there is a $g : M \to M$ such that $f = g \circ (h \circ i) = (g \circ h) \circ i$ showing that M is min-A-injective.

(c) Since the functor $\mathrm{Hom}(-, M)$ is left exact the exact sequence of A-modules $0 \to V/U \to N/U \to N/V \to 0$ yields the exact sequence of B-modules

$$0 \to \mathrm{Hom}(N/V, M) \to \mathrm{Hom}(N/U, M) \to \mathrm{Hom}(V/U, M),$$

and the assertion follows from the fact that the last module is either simple or zero. □

Cogenerator properties. We say that an A-module K is *(finitely) cogenerated* by an A-module M if there exists a monomorphism $K \to M^\Lambda$, for some (finite) set Λ. M is called a *self-cogenerator* if every factor module of M is cogenerated by M. The next proposition shows that cogenerator properties correspond to annihilator conditions (see [30, 28.1]).

Proposition 1.4 *For an A-module M with $B = \mathrm{End}({}_AM)$, the following are equivalent:*

- **(a)** *M is a self-cogenerator;*
- **(b)** *for any submodule $K \leq {}_AM$, $K = \mathrm{Ke}\,\mathrm{Hom}(M/K, M) = \bigcap \{\mathrm{Ke}\ f \mid f \in \mathrm{Hom}(M/K, M)\}$;*
- **(c)** *for any submodule $K \leq {}_AM$, $K = \lambda_M(\rho_B(K))$.*

Under finiteness conditions min-injectivity can imply injectivity.

Proposition 1.5 *For an A-module M of finite length, the following are equivalent:*

- **(a)** *M is an injective cogenerator in $\sigma[M]$;*
- **(b)** *M is a self-injective self-cogenerator;*
- **(c)** *M is a min-self-injective self-cogenerator.*

Proof: (**a**) $\Leftrightarrow$ (**b**) follows by [30, 16.5, 16.3]; (**b**) $\Rightarrow$ (**c**) is obvious.

(**c**) $\Rightarrow$ (**b**) It is to show that for any submodule $K \subset M$, morphisms $K \to M$ can be extended to endomorphisms. This can be proved by induction on the composition length of K. □

2 Quasi-Frobenius and Frobenius modules

A bimodule ${}_AM_B$ is called *quasi-Frobenius bimodule (QF-bimodule)[1]*, or *duality context* [7], if for every maximal left ideal $I \leq {}_AA$ its (right annihilator $\rho_M(I) = \{\beta \in M \mid I\beta = 0\}$ in M is zero or an irreducible B-module, and for every maximal right ideal $J \leq B_B$ its left annihilator $\lambda_M(J) = \{\alpha \in M \mid \alpha J = 0\}$ in M is zero or an irreducible A-module.

A left A-module M is called *quasi-Frobenius module*, or *QF-module* for short (see [9, 30]), if for any $n \in \mathbb{N}$ and finitely generated submodules $U \leq {}_AM^n$,

(i) the factor module M^n/U is cogenerated by M,

(ii) the canonical map $\mathrm{Hom}(M^n, M) \to \mathrm{Hom}(U, M)$ is surjective.

An interesting property of such modules is that for a QF-module ${}_AM$ with $B = \mathrm{End}({}_AM)$, the module M_B is also a QF-module and A is dense in the biendomorphism ring $\mathrm{End}(M_B)$ of ${}_AM$ (see [30, 48.2]).

Clearly a noetherian module $M \in {}_A\mathbf{M}$ is QF if and only if M is a self-injective self-cogenerator (injective cogenerator in $\sigma[{}_AM]$, see [30, 16.5]). Notice that ${}_AM$ noetherian does not imply M_B noetherian in general. However, if ${}_AM$ is finite and faithful then we have a priori finiteness conditions on both sides and we have complete left-right symmetry for QF-modules.

2.1 Characterization of finite QF-modules.

Theorem 2.1 *For a finite faithful left A-module M with $B = {}_A\mathrm{End}(M)$, the following conditions are equivalent:*

(a) ${}_AM_B$ *is a QF-bimodule;*

(b) ${}_AM$ *is a QF-module;*

(c) ${}_AM$ *is an injective cogenerator in* ${}_A\mathbf{M}$*;*

(d) ${}_AM$ *and* M_B *are cogenerators in* ${}_A\mathbf{M}$ *and* $\mathbf{M}_B$*, respectively;*

(e) M *is a balanced (A, B)-bimodule and any of the following equivalent conditions holds:*

(i) ${}_AM$ *and* M_B *are self-cogenerators;*

(ii) *for any submodules* $K \leq {}_AM$ *and* $N \leq M_B$,

$$K = \lambda_M(\rho_B(K)) \quad \text{and} \quad N = \rho_M(\lambda_A(N)); \tag{2.1}$$

(iii) M_B *is an injective cogenerator in* $\mathbf{M}_B$*;*

(iv) ${}_AM$ *and* M_B *are (min-)self-injective;*

(v) $\mathfrak{S}(M_B) = \mathfrak{S}({}_AM) =: \mathfrak{S}$ *and for* $\overline{A} = A/\mathfrak{J}(A)$, $\overline{B} = B/\mathfrak{J}(B)$, *the bimodule* ${}_{\overline{A}}\mathfrak{S}_{\overline{B}}$ *is quasi-Frobenius;*

(vi) $\mathfrak{S}(M_B) \subset \mathfrak{S}({}_AM)$ *and for every semisimple submodule* $K \leq {}_AM$, *any homomorphism* $\varphi : K \to M$ *extends to an endomorphism of* M.

If the above conditions are satisfied, then for left ideals $I \leq {}_AA$ *and right ideals* $J \leq B_B$,

$$\lambda_A(\rho_M(I)) = I \quad \text{and} \quad \rho_B(\lambda_M(J)) = J. \tag{2.2}$$

Proof: (**b**) $\Leftrightarrow$ (**c**) is clear since $\sigma[{}_AM] = {}_A\mathbf{M}$; (**c**) $\Leftrightarrow$ (**d**) $\Leftrightarrow$ (**e.iii**) follow from [30, 48.2]; (**d**) $\Rightarrow$ (**e.i**) is a consequence of the density theorem; (**e.i**) $\Leftrightarrow$ (**e.ii**) is pointed out in 1.4; (**b**) $\Rightarrow$ (**e.iv**) is clear from the implications mentioned before.

(**e.i**) $\Rightarrow$ (**e.iv**) (min) Since every factor module of ${}_AM$ is cogenerated by M it follows from the proof of [30, 47.7] that $\mathrm{Hom}_B(-, M)$ is exact on exact sequences $0 \to L \to M$ in $\mathbf{M}_B$, where L is cyclic. This implies that M_B is min-self-injective. Symmetrically ${}_AM$ is also min-self-injective.

(**e.iv**) $\Rightarrow$ (**e.ii**) For this an argument from the theory of noetherian QF-rings can be adapted (compare [17, Theorem 16.2]).

(**e.i**) $\Rightarrow$ (**c**) Since we know that (**e.i**) implies (**e.iv**) (min) we can apply Proposition 1.5 to prove our assertion. This also yields self-injectivity in (**e.iv**).

(**e.iv**) $\Rightarrow$ (**e.v**) The properties of $A/\mathfrak{J}(A)$ and $B/\mathfrak{J}(B)$ are just the characterisations of the endomorphism rings of self-injective modules with essential socles, e.g., $\mathrm{End}(\mathfrak{S}({}_AM)) \cong B/\mathfrak{J}(B)$ (see [30, 22.1]). Then the coincidence of the socles follow from the fact that every finitely generated semisimple module is semisimple as module over its endomorphism ring.

(**e.v**) $\Rightarrow$ (**e.vi**) Since $\mathfrak{S}(M_B) \subseteq \mathfrak{S}({}_AM)$, every semisimple submodule $N \leq {}_AM$ is a submodule $N \leq {}_{\overline{A}}\mathfrak{S}({}_AM)$, any homomorphism $\varphi : {}_AN \to {}_AM$ is a homomorphism $\varphi : {}_{\overline{A}}N \to {}_{\overline{A}}\mathfrak{S}$ and hence there exists some $b \in B$ such that for all $x \in N$, $\varphi(x) = x\overline{b} = xb$, proving our assertion.

(**b**) $\Leftrightarrow$ (**e.vi**) is shown in [1, Proposition 3].

The annihilator conditions (2.2) follow from the cogenerator property of ${}_AM$ and M_B.

Finally note that in view of Proposition 1.3 (**a**) $\Leftrightarrow$ (**e.iv**), so (**a**) $\Leftrightarrow$ (**b**). $\square$

Note that characterization (**e.v**) was announced in [24] without proof.

Note also that for any bimodule ${}_AM_B$ and two-sided ideal I of A, the annihilator $\rho_M(I)$ is a subbimodule of ${}_AM_B$, and $J = \rho_B(\rho_M(I))$ is a two-sided ideal of B. So $\rho_M(I)$ is a left and right faithful $(\tilde{A}, \tilde{B})$-bimodule for $\tilde{A} = A/I$, $\tilde{B} = B/J$. Moreover (see e.g. [7, 23.17(c)]):

Proposition 2.2 *Let M be a finite QF-module and refer to the notation above. Then for any two-sided ideal I of A the module ${}_{\tilde{A}}(\rho_M(I))_{\tilde{B}}$ is a QF-bimodule.*

2.2 A QF-module for a given finite coefficient ring.

It is well known (cf. [7]) that for every commutative finite (artinian) ring A there exists a unique (up to isomorphism) QF-module ${}_AQ$ and it satisfies the condition $\mathrm{End}({}_AQ) = A$. This fact has been the basis for the results in [22, 15]. The following facts about character groups will help to generalize this existence theorem to finite not necessarily commutative rings.

Proposition 2.3 *For a left A-module ${}_AM$, $M^\flat = \mathrm{Hom}({}_\mathbb{Z}M, \mathbb{Q}/\mathbb{Z})$ is is a right A-module, and for a right A-module M_A, $M^\flat$ is a left A-module. In particular, $A^\flat = \mathrm{Hom}({}_\mathbb{Z}A, \mathbb{Q}/\mathbb{Z})$ is a left and right A-module and is an injective cogenerator in ${}_A\mathbf{M}$ and $\mathbf{M}_A$ (e.g., [30, 16.8]).*
If the module M is finite, then $(M^\flat, +) \cong (M, +)$, and there is a natural module isomorphism

$$M \cong M^{\flat\flat}, \quad m \mapsto [\omega \mapsto \omega(m)].$$

Summarizing these observations we have:

Theorem 2.4 *For any finite ring A, the character module ${}_AA^\flat$ is a finite QF-module with ${}_A\mathrm{End}(A^\flat) \cong A$, i.e., ${}_AA^\flat_A$ is a QF-bimodule.*

This result can be writen in slightly different form referring to properties of character modules. For this consider a finite group $(M, +)$. For subgroups $N \leq M$ and $W \leq M^\flat$ define *annihilators* by

$$\begin{aligned} N^\perp &:= \{\omega \in M^\flat \mid \omega(x) = 0 \text{ for all } x \in N\} \simeq \mathrm{Hom}(M/N, \mathbb{Q}/\mathbb{Z}), \\ W^\perp &:= \{x \in M \mid \omega(x) = 0 \text{ for all } \omega \in W\} = \mathrm{Ke}\, W. \end{aligned}$$

Then $W^{\perp} \leq {}_{\mathbb{Z}}M$, $N^{\perp} \leq {}_{\mathbb{Z}}M^{\flat}$ and we have the equalities

$$N^{\perp\perp} = N \quad \text{and} \quad W^{\perp\perp} = W.$$

Applied to finite A-modules these notions yield:

Lemma 2.5 *Let ${}_AM$ be a finite module. Then:*

(i) *For every submodule $N \leq {}_AM$, the annihilator $N^{\perp}$ is a submodule of $M^{\flat}_A$.*

(ii) *For every submodule $W \leq M^{\flat}_A$, the annihilator $W^{\perp}$ is a submodule of ${}_AM$.*

Moreover, in this case $N^{\perp} \cong (M/N)^{\flat}$ is an isomorphism of right modules.

It is worth noting that in case $M = A$ the foregoing statement can be applied to ${}_AA$ as well as A_A, and hence the annihilator of a left (right) ideal of A is a right (left) submodule of $A^{\flat}$. But even more is true, as the following statement shows which are easily proved.

Proposition 2.6 *For any submodules $I \leq {}_AA$ and $J \leq A_A$,*

$$\rho_{A^{\flat}}(I) \; = \; I^{\perp}, \quad \lambda_{A^{\flat}}(I) = J^{\perp}.$$

Symmetrically, for submodules $L \leq {}_AA^{\flat}$ and $N \leq A^{\flat}_A$,

$$\rho_A(L) = L^{\perp}, \quad \lambda_A(N) = N^{\perp}.$$

Note that Theorem 2.4 can also be deduced from the last proposition, the double annihilator properties mentioned before Lemma 2.5, and characterizations of QF-modules in Theorem 2.1.

Remark 2.7 The preceding results may be obtained partially from [31, Th. 3.2] where instead of $M^{\flat}$ the module $\widehat{M}$ of all complex characters $\xi : (M, +) \longrightarrow (\mathbb{C}^{\times}, \cdot)$ is considered. In that paper the action of elements $a \in A$ is defined by the rule $\xi^a(x) := \xi(ax)$, if M is a left A-module, and ${}^a\xi(x) = \xi(xa)$, if M is a right A-module. It is evident, that $M^{\flat}_A \cong \widehat{M}_A$ where the isomorphism comes from the natural embedding

$$(\mathbb{Q}/\mathbb{Z}, +) \longrightarrow (\mathbb{C}^{\times}, \cdot), \quad z \mapsto \exp(2\pi i z).$$

Now, the result [31, Th. 3.2] states that for every finite ring A the functor $M \mapsto \widehat{M}$ is a duality functor between the category ${}_A\mathcal{F}$ of all finite left A-modules and the category $\mathcal{F}_{\mathcal{A}}$ of all finite right A-modules.

2.3 Finite Frobenius and symmetric rings.

As noted above (cf. [7]), if A is commutative, then any two QF-modules over A are isomorphic. For non-commutative rings this is no longer true, even if A is a finite *quasi-Frobenius ring*, i.e. if ${}_AA_A$ is a QF-bimodule. In this case QF-bimodules ${}_AA_A$ and ${}_AA^{\flat}_A$ are not necessarily isomorphic. In order to derive a uniqueness result, we need further conditions.

It is known (see e.g. [13, Th. 13.4.2]) that a finite ring A is a QF-ring if and only if $\mathfrak{S}({}_AA) = \mathfrak{S}(A_A)$ and for any primitive idempotent f of the ring A, the ideals $f\mathfrak{S}(A)$ and $\mathfrak{S}(A)f$ are irreducible (right resp. left) modules.

Classically a *Frobenius ring* is defined as a QF-ring A for which ${}_A(A/\mathfrak{J}(A)) \cong {}_A\mathfrak{S}({}_AA)$ and $(A/\mathfrak{J}(A))_A \cong \mathfrak{S}({}_AA)_A$. In the finite context this can be simplified. It has been shown in [11] that if the left socle of a finite ring is a left principal ideal then it is also a right principal ideal and coincides with the right-socle, moreover we have from [11]:

Theorem 2.8 *A finite ring A is a Frobenius ring if and only if $\mathfrak{S}({}_AA)$ is a principal left ideal.*

We call a character $\varepsilon \in A^\flat$ *left generating*[1] if $A\varepsilon = A^\flat$. The last equality is equivalent to the condition $\lambda_A(\varepsilon) = 0$ which means that $\varepsilon(xr)$ is a nonzero character for any $r \in A \setminus 0$, i.e., the kernel $\varepsilon^\perp$ of ε does not contain a nonzero left ideal (the definition of left distinguished character). A character that is left and right generating is called a *generating* character. From [31, Th.3.10, Th.4.3] and partly [18, sec. 3.2, Lemma 1] we have useful characterizations of finite Frobenius rings.

Proposition 2.9 *For a finite ring A every left (or right) generating character is generating, and the following statements are equivalent:*

- **(a)** *A is a Frobenius ring.*
- **(b)** *A has a (left) generating character ε.*
- **(c)** *There exists an isomorphism $\varphi : {}_AA \to {}_AA^\flat$.*
- **(d)** *There exists an isomorphism $\psi : A_A \to A^\flat_A$.*

Under the condition **(b)** of 2.9 the isomorphisms in **(c)** and **(d)** can be chosen in the form

$$\varphi(a) = a\varepsilon \quad \text{and} \quad \psi(a) = \varepsilon a, \text{ for } a \in A.$$

For a quasi-Frobenius ring A there are at least two QF-bimodules, ${}_AA_A$ and ${}_AA^\flat_A$. However, even in this case we cannot show that ${}_AA_A$ and ${}_AA^\flat_A$ are isomorphic as bimodules since the isomorphisms φ and ψ may be different.

Definition 2.10 A finite ring A is called *symmetric* if ${}_AA_A \cong {}_AA^\flat_A$ as bimodules.

Of course any symmetric ring is Frobenius (by 2.9). In order to obtain an internal characterization of a symmetric ring A let $K(A)$ be the subgroup generated by all commutators in A, i.e.,

$$K(A) := {}_{\mathbb{Z}}\langle ab - ba \mid a, b \in A\rangle.$$

Proposition 2.11 *A finite ring A is symmetric if and only if it has a generating character $\varepsilon \in A^\flat$ such that $\varepsilon(K(A)) = 0$.*

Proof: Let ε be a generating character with the desired property. In order to prove the above bimodule isomorphy it is sufficient to prove that the isomorphisms φ and ψ coincide. Indeed for any $a \in A$ we have $\psi(a) = a\varepsilon \in A^\flat$, $\psi(a)(x) = \varepsilon(xa)$. Since $\varepsilon(K(A)) = 0$ we have

$$\varepsilon(xa) = \varepsilon(xa + (ax - xa)) = \varepsilon(ax) = (\varepsilon a)(x) = \varphi(a)(x).$$

Therefore $\psi = \varphi$ and our claim is true.

[1] These characters are called (left) distinguished character in [22], and (left) admissible character in [2].

Conversely, let $\varphi : A \to A^\flat$ be an isomorphism of bimodules and let $\varepsilon := \varphi(1)$. Then ε is a generating character, and we have $a\varepsilon = \varphi(a) = \varepsilon a$ for all $a \in A$. Now $\varepsilon(ba - ab) = (a\varepsilon)(b) - (\varepsilon a)(b) = 0$ for all $a, b \in A$ and hence $K(A) \subseteq \mathrm{Ker}(\varepsilon)$. □

Corollary 2.12 *If A is a symmetric ring then $K(A)$ does not contain any nonzero left or right ideals of A.*

The converse of the latter statement is an open question.

Examples 2.13 The following rings are symmetric: Finite commutative Frobenius rings, ring-direct products of symmetric rings, full matrix rings over symmetric rings A with generating character ε (consider the trace composed with ε), finite group rings over symmetric rings (see [31]).

Finally note that there exist finite Frobenius non-symmetric rings.

Example 2.14 For a non-prime suitable $q \in \mathbb{N}$ consider the field $\mathbb{F}_q$ and the non-trivial automorphism σ of $\mathbb{F}_q$. Let $\mathbb{F}_q[x;\sigma]$ be an Ore polynomial ring with multiplication defined for $a \in \mathbb{F}_q$ by $xa = \sigma(a)x$. Then $A = \mathbb{F}_q[x;\sigma]/(x^2)$ is a finite local principal ideal (hence Frobenius) ring consisting of elements $\alpha = a_0 + a_1 z$, $a_0, a_1 \in \mathbb{F}_q$, $z = x + (x^2)$ [26]. The unique proper ideal of A is $\mathfrak{J}(A) = Az = \mathbb{F}_q z$. For a pair of elements $\alpha \in A$ and $\beta = b_0 + b_1 z \in A$ we have

$$\alpha\beta - \beta\alpha = (a_1(\sigma(b_0) - b_0) + b_1(\sigma(a_0) - a_0))z.$$

Now it is evident that the set of all such differences is $\mathbb{F}_q z = Az$, and $K(A) = \mathfrak{J}(A)$ is a nonzero ideal. So A is not a symmetric ring.

2.4 Finite Frobenius modules.

We now concentrate on uniqueness conditions for QF-modules. For our main definition we need the following observations.

Proposition 2.15 *For every finite ring A, $\mathfrak{S}({}_A A^\flat) = \mathfrak{S}(A^\flat_A) =: \mathfrak{S}(A^\flat)$, and for $\overline{A} = A/\mathfrak{J}(A)$, there is an isomorphism of bimodules*

$$\overline{A}\overline{A}_{\overline{A}} \cong \overline{A}\,\mathfrak{S}(A^\flat)_{\overline{A}}.$$

Furthermore ${}_{\overline{A}}\mathfrak{S}(A^\flat)$ and $\mathfrak{S}(A^\flat)_{\overline{A}}$ are cyclic modules and there exists a common generator ω of these modules such that $\overline{r}\omega = \omega\overline{r}$ for all $\overline{r} \in \overline{A}$.

Proof: According to Lemma 2.5 we have

$$\mathfrak{S}({}_A A^\flat) = \rho_{A^\flat}(\mathfrak{J}(A)) = \mathfrak{J}(A)^\perp \text{ and } \mathfrak{S}(A^\flat_A) = \lambda_{A^\flat}(\mathfrak{J}(A)) = \mathfrak{J}(A)^\perp.$$

This implies the identity of left and right socle, as required.

The isomorphism in Lemma 2.5, $\mathfrak{J}(A)^\perp \to \overline{A}^\flat$, is an isomorphism of bimodules ${}_{\overline{A}}\mathfrak{J}(A)^\perp_{\overline{A}} \cong {}_{\overline{A}}\overline{A}^\flat_{\overline{A}}$, that is, we have

$$\overline{A}\,\mathfrak{S}(A^\flat)_{\overline{A}} \cong {}_{\overline{A}}\overline{A}^\flat_{\overline{A}}.$$

Since $\overline{A}$ is semisimple and hence symmetric (cf. Examples 2.13), there exists an isomorphism of bimodules ${}_{\overline{A}}\overline{A}^{\flat}_{\overline{A}} \cong {}_{\overline{A}}\overline{A}_{\overline{A}}$. Together with the foregoing observation this implies the required isomorphy. For the remaining statement choose $\omega \in \mathfrak{S}(A^{\flat})$ as the character corresponding to $\overline{1} \in \overline{A}$ under this isomorphism. □

Definition 2.16 We call a finite QF-bimodule ${}_AQ_A$ (QF-module ${}_AQ$) a *Frobenius bimodule* (*Frobenius module*), if ($\mathrm{End}({}_AQ) = A$ and) there are module isomorphisms

$$ {}_{\overline{A}}\overline{A} \cong {}_{\overline{A}}\mathfrak{S}(Q), \quad \text{and} \quad \overline{A}_{\overline{A}} \cong \mathfrak{S}(Q)_{\overline{A}}; $$

and we call Q a *symmetric Frobenius bimodule* if, in addition,

$$ {}_{\overline{A}}\overline{A}_{\overline{A}} \cong {}_{\overline{A}}\mathfrak{S}(Q)_{\overline{A}} \quad \text{as bimodules.} $$

From Proposition 2.15 we see that $A^{\flat}$ is indeed not only Frobenius but even a symmetric Frobenius bimodule for every finite ring A. Note also that the bimodule ${}_AA_A$ from Example 2.14 does not satisfy the above bimodule isomorphy, so it is a Frobenius but not a symmetric Frobenius bimodule.

Our final theorem will now show that the Frobenius module of a finite ring A is unique up to left and right A-linear isomorphism.

Proposition 2.17 *For a QF-module ${}_AQ$ with $A = \mathrm{End}({}_AQ)$ and $\overline{A} = A/\mathfrak{J}(A)$, the following conditions are equivalent:*

- **(a)** *${}_AQ_A$ is a Frobenius bimodule.*
- **(b)** *${}_{\overline{A}}\mathfrak{S}(Q)_{\overline{A}}$ is a Frobenius bimodule.*
- **(c)** *$\mathfrak{S}(Q)$ is a left and right cyclic A-module.*
- **(d)** *${}_AQ \cong {}_AA^{\flat}$ and $Q_A \cong A^{\flat}_A$.*

Proof: (**a**) $\Rightarrow$ (**b**) $\Rightarrow$ (**c**) follow immediately from Definition 2.16.

(**c**) $\Rightarrow$ (**d**) Let $\mathfrak{S} = \mathfrak{S}(Q) = A\omega$ for some $\omega \in \mathfrak{S}$. Then $\mathfrak{S} = \overline{A}\omega$ and we have an epimorphism of left $\overline{A}$-modules

$$ \varphi : {}_{\overline{A}}\overline{A} \longrightarrow {}_{\overline{A}}\mathfrak{S}, \quad \overline{r} \mapsto \overline{r}\omega. $$

We show $I = \mathrm{Ker}\,\varphi = 0$. Since ${}_{\overline{A}}\mathfrak{S}_{\overline{A}}$ is a QF-bimodule it is faithful, hence $\lambda_{\overline{A}}(\omega) = \lambda_{\overline{A}}(\mathfrak{S}) = 0$. But $\omega \in \rho_{\mathfrak{S}}(I)$, thus $\lambda_{\overline{A}}(\rho_{\mathfrak{S}}(I)) = 0$. Since ${}_{\overline{A}}\mathfrak{S}_{\overline{A}}$ is a QF-bimodule we have $\rho_{\mathfrak{S}}(I) = \rho_{\mathfrak{S}}(\lambda_{\overline{A}}(\rho_{\mathfrak{S}}(I))) = \rho_{\mathfrak{S}}(0) = \mathfrak{S}$ thus $I = 0$. It remains to note that an isomorphism of modules ${}_A\mathfrak{S}({}_AQ) \cong {}_A\overline{A}$ can be extended to an isomorphism of the injective hulls ${}_AQ \cong {}_AA^{\flat}$.

(**d**) $\Rightarrow$ (**a**) By (**d**), ${}_{\overline{A}}\mathfrak{S} \cong {}_{\overline{A}}\mathfrak{S}(A^{\flat})$ and $\mathfrak{S}_{\overline{A}} \cong \mathfrak{S}(A^{\flat})_{\overline{A}}$. Now (**a**) follows from 2.15. □

3 Linear codes over modules

Let A be a finite (not necessarily commutative) ring with identity $1 = 1_A$, and let ${}_AM$ be a finite faithful module. A submodule $\mathcal{K} \leq {}_AM^n$ is called a *linear n-code* over ${}_AM$. As usual the *Hamming weight* of a word $\vec{\alpha} \in M^n$ is the number $w_H(\vec{\alpha})$ of its nonzero coordinates, and the *Hamming distance* $d(\mathcal{K})$ of a code $\mathcal{K} \leq {}_AM^n$ is

$$ d(\mathcal{K}) \;:=\; \min\{w_H(\vec{\alpha} - \vec{\beta}) \mid \vec{\alpha}, \vec{\beta} \in \mathcal{K}, \vec{\alpha} \neq \vec{\beta}\} \;=\; \min\{w_H(\vec{\alpha}) \mid \vec{\alpha} \in \mathcal{K} \setminus \vec{0}\}. $$

We suggest some simplification for the computation of $d(\mathcal{K})$.

For any left A-module M the socle $\mathfrak{S}(M)$ is a module over the semisimple ring $\overline{A}$. Let $\overline{A} = A_1 \oplus \cdot \oplus A_n$ be a composition into simple rings (matrix rings over fields) A_i and let ε_i be identity of the component A_i. Then $\varepsilon_1 + ... + \varepsilon_t = 1_{\overline{A}}$ and $\mathfrak{S}(M)$ has a fully invariant decomposition into homogeneous components

$$\mathfrak{S}(M) \ = \ \mathfrak{S}_1 \oplus \ldots \oplus \mathfrak{S}_t,$$

where each $\mathfrak{S}_i = \varepsilon_i \mathfrak{S},\ i \in \{1, \cdots, t\},$ is a module over A_i.

For the computation of the distance $d(\mathcal{K})$ of a code $\mathcal{K}$ the following observation is useful.

Proposition 3.1 *Let M be a left A-module and $\mathcal{K} \leq M^n$ be a linear code, $n \in \mathbb{N}$.*

(i) *The socle $\mathfrak{S}(\mathcal{K})$ is a linear code over the socle of the base module $\mathfrak{S}(M)$,*

$$\mathfrak{S}(\mathcal{K}) = \mathcal{K} \cap (\mathfrak{S}(M))^n \leq {}_{\overline{A}}\mathfrak{S}(M)^n.$$

(ii) *For the Hamming distance of $\mathcal{K}$ we have the equality*

$$d(\mathcal{K}) = d(\mathfrak{S}(\mathcal{K})).$$

(iii) *If $\mathfrak{S}(\mathcal{K}) = \mathcal{L}_1 \oplus \ldots \oplus \mathcal{L}_t$ is a fully invariant decomposition into homogeneous components $\mathcal{L}_i = \varepsilon_i \mathcal{L}$, then $\mathcal{L}_i$ is a linear n-code over a module ${}_{A_i}\mathfrak{S}_i$ and*

$$d(\mathcal{K}) = \min\{d(\mathcal{L}_1), \ldots, d(\mathcal{L}_t)\}.$$

Proof: **(i)** is clear by general properties of the socle.

For **(ii)** we first note that $d(\mathcal{K}) \leq d(\mathfrak{S}(\mathcal{K}))$ since $\mathfrak{S}(\mathcal{K}) \subseteq \mathcal{K}$. Now consider any $\vec{\alpha} \in \mathcal{K}$ with $w_H(\vec{\alpha}) = d(\mathcal{K})$. Since $\mathfrak{S}(\mathcal{K})$ is essential in $\mathcal{K}$ there exists $a \in A$ with $0 \neq a\vec{\alpha} \in \mathfrak{S}(\mathcal{K})$. This implies $d(\mathfrak{S}(\mathcal{K})) \leq w_H(a\vec{\alpha}) \leq w_H(\vec{\alpha}) = d(\mathcal{K})$ proving our assertion.

Finally we observe that **(iii)** is a consequence of **(ii)**. □

So the computation of the Hamming distance of any linear code over an arbitrary finite module reduces to the same problem for codes over modules with simple coefficient rings A_i.

Let us remark that 3.1 extends results of [22, Prop. 5,6] for commutative rings A.

For the following consideration we need a notion of *dual codes*. There is more than one way to define this. We will follow the line in P. Delsarte [6].

3.1 Duality defined via the character module

Let M be a finite abelian group. Any subgroup $\mathcal{K} \leq M^n$ is called an *additive n-code* over M. We define the code dual to $\mathcal{K}$ as additive n-code over the group $M^\flat$.

Consider any row $\vec{\varphi} = (\varphi_1, \ldots, \varphi_n) \in (M^\flat)^n$ as element of $(M^n)^\flat$, acting on elements $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in M^n$ by the rule

$$\vec{\varphi}(\vec{\alpha}) \ := \ \varphi_1(\alpha_1) + \ldots + \varphi_n(\alpha_n) \in \mathbb{Q}/\mathbb{Z}.$$

Then $(M^\flat)^n = (M^n)^\flat$.

For every additive code $\mathcal{K} \leq M^n$ we define its *dual code in Delsarte form* by

$$\mathcal{K}^\perp := \{\vec{\varphi} \in (M^\flat)^n \mid \vec{\varphi}(\vec{\alpha}) = 0 \text{ for all } \vec{\alpha} \in \mathcal{K}\}.$$

Then of course $\mathcal{K} \subseteq \mathcal{K}^{\perp\perp}$ for all $\mathcal{K} \leq M^n$ and referring to [20, 6] we observe the following facts. As we have seen earlier, if ${}_AM$ is a finite module and $\mathcal{K}$ is a linear code over ${}_AM$, then $\mathcal{K}^\perp$ is a submodule of $(M^\flat)^n_A$, that is, a right linear code over $M^\flat_A$.

Proposition 3.2 *For any additive code $\mathcal{K} \leq M^n$, we have the equality $\mathcal{K}^{\perp\perp} = \mathcal{K}$ and a group isomorphism $\mathcal{K}^\perp \cong M^n/\mathcal{K}$. In particular, $|\mathcal{K}^\perp| \cdot |\mathcal{K}| = |M|^n$.*

Similar to codes over rings generator matrices are defined for codes over modules.

Definition 3.3 Let $\mathcal{K}$ be a linear code of length n over the finite module ${}_AM$. A $(k \times n)$-matrix G with entries in M, whose rows form a generating set of the module ${}_A\mathcal{K}$, is called a *generator matrix* of $\mathcal{K}$. A generator matrix of the code $\mathcal{K}^\perp$ over $M^\flat$ is called a *check matrix* for $\mathcal{K}$.

Let $\vec{\varphi}_i = (\varphi_{i1}, \ldots, \varphi_{in}) \in (M^\flat)^n$, $i \in \{1, \cdots, l\}$, be a generating system of the module ${}_A\mathcal{K}^\perp$. Then $\Phi = (\varphi_{ij})_{l \times n}$ is a check matrix of the code $\mathcal{K}$. We consider Φ as a group homomorphism $\Phi : M^n \to (\mathbb{Q}/\mathbb{Z})^l$ into the group of all l-columns over $\mathbb{Q}/\mathbb{Z}$, acting on $\vec{\alpha} \in M^n$ by the rule $\Phi(\vec{\alpha}) = (\vec{\varphi}_1(\vec{\alpha}), \ldots, \vec{\varphi}_l(\vec{\alpha}))^T$. As in the classical case we have (in analogy to [22]):

Proposition 3.4 $\mathcal{K} = \operatorname{Ker} \Phi$.

As for linear codes over a field we can characterize the Hamming minimum distance of a code $\mathcal{K} \leq {}_AM^n$ by inspecting a check matrix Φ for $\mathcal{K}$. Any column Φ_j, $j \in \{1, \cdots, n\}$, of the matrix Φ is a homomorphism $\Phi_j : M \to (\mathbb{Q}/\mathbb{Z})^l$. We say that a system $\Phi_{j_1}, \ldots, \Phi_{j_k}$ of k columns of Φ is *linearly independent* over M, if $\Phi_{j_1}(\alpha_1) + \ldots + \Phi_{j_k}(\alpha_k) \neq 0$ for any $(\alpha_1, \ldots, \alpha_k) \in M^k \setminus \{\vec{0}\}$.
We define the *guaranteed rank $\varkappa_M(\Phi)$ of the matrix Φ relative to M* as maximal $k \in \mathbb{N}$ such that any system $\Phi_{j_1}, \ldots, \Phi_{j_k}$ of k columns of Φ is linearly independent over M. Then (as in [22]) we have the following generalization of a well known classical result.

Proposition 3.5 *Let $\mathcal{K} \leq {}_AM^n$ be a linear code with check matrix Φ. Then $d(\mathcal{K}) = \varkappa_M(\Phi) + 1$.*

Finally note that any linear code over a QF-bimodule ${}_AQ_A$ has a check matrix over A, and certainly the foregoing results hold for these codes. For the commutative case this has been observed in [22] and for further references see [15].
Let ${}_AM$ be a finite module of m elements and let $\mathcal{K}$ be a linear code of length n over ${}_AM$. For a vector $\mathbf{x} = (x_s : s \in M)$ of m indeterminates we define the *complete weight enumerator* of $\mathcal{K}$ as

$$W_\mathcal{K}(\mathbf{x}) := \sum_{\vec{\alpha} \in \mathcal{K}} \prod_{s \in M} x_s^{\sigma_s(\vec{\alpha})} \in \mathbb{Z}[\mathbf{x}], \qquad \text{where} \quad \sigma_s(\vec{\alpha}) = \#\{i \in \overline{1,n} \mid \alpha_i = s\}.$$

Similarly for a linear code $\mathcal{L} \leq (M^\flat)^n_A$ over the module $M^\flat_A$ (of same cardinality m), and for a vector $\mathbf{y} = (y_\tau : \tau \in M^\flat)$ of m indeterminates we have the complete weight enumerator

$$W_\mathcal{L}(\mathbf{y}) := \sum_{\vec{\omega} \in \mathcal{L}} \prod_{\tau \in M^\flat} y_\tau^{\sigma_\tau(\vec{\omega})} \in \mathbb{Z}[\mathbf{y}], \qquad \text{where} \quad \sigma_\tau(\vec{\omega}) = \#\{i \in \overline{1,n} \mid \omega_i = \tau\}.$$

With this preparation we can show that one of the major formulas for linear codes holds in our more general situation.

Theorem 3.6 *(MacWilliams' identity) Let ${}_AM$ be a finite module with m elements and let $\mathcal{K} \leq {}_AM^n$ be a linear code with complete weight enumerator $W_{\mathcal{K}}(\mathbf{x})$. Then the complete weight enumerator of $\mathcal{K}^\perp$ is given by*

$$W_{\mathcal{K}^\perp}(\mathbf{y}) \;=\; \frac{1}{|\mathcal{K}|} W_{\mathcal{K}}(\mathbf{y}\mathcal{A}),$$

where $\mathcal{A} = (a_{\tau s})$ is the square $(m \times m)$-matrix with $a_{\tau s} := \exp(2\pi i\, \tau(s))$ for all $s \in M$ and $\tau \in M^\flat$.

Proof: We can essentially follow the proofs in [20] and [22] (for commutative rings). First we have

$$W_{\mathcal{K}^\perp}(\mathbf{y}) \;=\; \sum_{\vec{\omega} \in \mathcal{K}^\perp} f(\vec{\omega}), \quad \text{where } f(\vec{\omega}) \;:=\; \prod_{\tau \in M^\flat} y_\tau^{\sigma_\tau(\vec{\omega})} \quad \text{for all } \vec{\omega} \in (M^\flat)^n.$$

Let us consider the Fourier transform $\widehat{f}$ of the function f defined as

$$\widehat{f}(\mathbf{v}) \;=\; \sum_{\vec{\omega} \in (M^\flat)^n} \exp\left[2\pi i\, \vec{\omega}(\mathbf{v})\right] f(\vec{\omega}) \quad \text{for all } \mathbf{v} \in M^n,$$

where $\vec{\omega}(\mathbf{v}) = \sum_{i \in \overline{1,n}} \omega_i(v_i)$, and show that

$$W_{\mathcal{K}^\perp}(\mathbf{y}) \;=\; \frac{1}{|\mathcal{K}|} \sum_{\vec{\alpha} \in \mathcal{K}} \widehat{f}(\vec{\alpha}). \tag{3.1}$$

We obtain

$$\sum_{\vec{\alpha} \in \mathcal{K}} \widehat{f}(\vec{\alpha}) \;=\; \sum_{\vec{\omega} \in (M^\flat)^n} \Delta(\vec{\omega}) f(\vec{\omega}), \quad \text{where} \quad \Delta(\vec{\omega}) \;=\; \sum_{\vec{\alpha} \in \mathcal{K}} \exp\left[2\pi i\, \vec{\omega}(\vec{\alpha})\right].$$

If $\vec{\omega} \in \mathcal{K}^\perp$ then clearly $\Delta(\vec{\omega}) = |\mathcal{K}|$, and otherwise $\Delta(\vec{\omega}) = 0$ since $K := \{\vec{\omega}(\vec{\alpha}) \mid \vec{\alpha} \in \mathcal{K}\}$ is a non-trivial subgroup of $\mathbb{Q}/\mathbb{Z}$ with $\exp(2\pi i\, K) \neq 1$. From this we obtain (3.1).
Now we expand $\widehat{f}(\vec{\alpha})$ in a different way, namely

$$\begin{aligned}
\widehat{f}(\vec{\alpha}) \;&=\; \sum_{\vec{\omega} \in (M^\flat)^n} \exp\Big[2\pi i \sum_{j=1}^n \omega_j(\alpha_j)\Big] f(\vec{\omega}) \;=\; \sum_{\vec{\omega} \in (M^\flat)^n} \prod_{j=1}^n \exp\left[2\pi i\, \omega_j(\alpha_j)\right] \prod_{\tau \in M^\flat} y_\tau^{\sigma_\tau(\vec{\omega})} \\
&=\; \sum_{\vec{\omega} \in (M^\flat)^n} \prod_{j=1}^n \exp\left[2\pi i\, \omega_j(\alpha_j)\right] y_{\omega_j} \;=\; \prod_{j=1}^n \sum_{\tau \in M^\flat} \exp[2\pi i\, \tau(\alpha_j)] y_\tau \\
&=\; \prod_{s \in M} \Big[\sum_{\tau \in M^\flat} \exp[2\pi i\, \tau(s)] y_\tau \Big]^{\sigma_s(\vec{\alpha})} \;=\; \prod_{s \in M} \Big[(\mathbf{y}\mathcal{A})_s\Big]^{\sigma_s(\vec{\alpha})},
\end{aligned}$$

where $(\mathbf{y}\mathcal{A})_s$ is the s-th coordinate of the row $(\mathbf{y}\mathcal{A})$. Together with (3.1) this finally leads to

$$W_{\mathcal{K}^\perp}(\mathbf{y}) \;=\; \frac{1}{|\mathcal{K}|} \sum_{\vec{\alpha} \in \mathcal{K}} \prod_{s \in M} \Big[(\mathbf{y}\mathcal{A})_s\Big]^{\sigma_s(\vec{\alpha})} \;=\; \frac{1}{|\mathcal{K}|} W_{\mathcal{K}}(\mathbf{y}\mathcal{A}),$$

as was our claim. □

The *Hamming weight enumerator* of a linear code $\mathcal{K} \leq {}_AM^n$ is defined as

$$W_{\mathcal{K}}^H(x,y) := \sum_{\vec{\alpha}\in\mathcal{K}} x^{n-w_H(\vec{\alpha})} y^{w_H(\vec{\alpha})}$$

and satisfies the equality

$$W_{\mathcal{K}}^H(x,y) = W_{\mathcal{K}}(x, \underbrace{y,\ldots,y}_{\text{m-1 times}}).$$

This enables us to obtain the following result from [6] as a consequence.

Corollary 3.7 *Let ${}_AM$ be a finite module with m elements, and let $\mathcal{K} \leq {}_AM^n$ be a linear code with Hamming weight enumerator $W_{\mathcal{K}}^H$. Then the Hamming weight enumerator of $\mathcal{K}^\perp$ is given by*

$$W_{\mathcal{K}^\perp}^H(x,y) = \frac{1}{|\mathcal{K}|} W_{\mathcal{K}}^H(x+(m-1)y, x-y).$$

These results are generalizations of previous results in [22] (for A a commutative ring) and results in [31] (for $M = A$ a Frobenius ring).

3.2 Duality defined via the Reciprocal Module

An alternative, but equivalent notion of a *dual code* is based on the following idea. For a faithful module ${}_AM$ let $M^\times = \mathrm{Hom}({}_AM, {}_AA^\flat)$. As $A^\flat$ is also a right A-module we again obtain a right A-module structure on $M^\times$ where the product $\mu r \in M^\times$ of $\mu \in M^\times$ and $r \in A$ is defined by $(\mu r)(\alpha) = \mu(\alpha)r$, for all $\alpha \in M$. So by definition, $(\mu r)(\alpha) \in A^\flat$ is a function on A of the form

$$(\mu r)(\alpha)(x) = \mu(\alpha)(rx), \text{ for } x \in A.$$

We call $M_A^\times$ the *reciprocal module to* ${}_AM$ (in [7] it is called the *Morita-dual*) and observe that there is a natural module isomorphism (see [30, Prop. 16.8])

$$\tau : M_A^\times \to M_A^\flat, \quad \mu \mapsto [m \mapsto \mu(m)(1_A)].$$

As a corollary of this isomorphism and (2.3) we have

$$(M^\times, +) \cong (M, +), \quad |M^\times| = |M|.$$

Let us define a product of $\alpha \in M$ and $\mu \in M^\times$ as $\alpha\times\mu = \mu(\alpha) \in A^\flat$. Then for a fixed $\alpha \in M$, the correspondence $\mu \to \alpha\times\mu$ induces a homomorphism ${}_AM^\times \to A^\flat$ belonging to the left A-module $M^{\times\times} = \mathrm{Hom}_A(M^\times, A^\flat)$. We can identify this homomorphism with α. Then we have the equality ${}_AM^{\times\times} = {}_AM$. Note that by our definition we have

$$(\alpha\times\mu r)(x) = (\alpha\times\mu)(rx) \text{ and } (r\alpha\times\mu)(x) = (\alpha\times\mu)(xr) \quad \text{for all } r \in A. \tag{3.2}$$

Now, as in section 3.1 we consider any element of $(M^n)^\times = \mathrm{Hom}_A(M^n, A^\flat)$ as row

$$\vec{\psi} = (\psi_1, \ldots, \psi_n) \in (M^\times)^n = \mathrm{Hom}_A(M, A^\flat)^n,$$

acting on elements $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in M^n$ by the rule

$$\vec{\psi}(\vec{\alpha}) \;:=\; \vec{\alpha} \times \vec{\psi} = \alpha_1 \times \psi_1 + \ldots + \alpha_n \times \psi_n \in A^\flat. \tag{3.3}$$

So we have a natural identification $(M^n)^\times = (M^\times)^n$. For a linear code $\mathcal{K} \leq {}_AM^n$ we then define the *dual code* (over the reciprocal module) as right linear code $\mathcal{K}^\otimes \leq (M_A^\times)^n$ over the module $M_A^\times$ of the form

$$\mathcal{K}^\otimes = \rho_{(M^\times)^n}(\mathcal{K}) = \{\vec{\psi} \in (M^\times)^n \mid \mathcal{K} \times \vec{\psi} = 0\}. \tag{3.4}$$

These conventions give rise to the inclusions $\mathcal{K}^{\otimes\otimes} < (M^n)^{\times\times} = M^n$, $\mathcal{K} \subseteq \mathcal{K}^{\otimes\otimes}$. However note that the latter inclusion, unlike the inclusion $\mathcal{K} \subseteq \mathcal{K}^{\perp\perp}$, is strict if $\mathcal{K}$ is only a subgroup but not an A-submodule of M. Indeed, from the definitions (3.4), (3.3) and properties (3.2) it follows that $\mathcal{K}^\otimes$ is a submodule of $(M_A^\times)^n$ (and correspondingly $\mathcal{K}^{\otimes\otimes}$ is a submodule of ${}_AM^n$) for any subset $\mathcal{K} \subseteq M^n$. However for linear codes over ${}_AM$ we have

Proposition 3.8 *For any linear code $\mathcal{K} \leq {}_AM^n$ the coordinatewise extension*

$$\tau^n : (M^\times)_A^n \to (M^\flat)_A^n$$

of the isomorphism τ is induced by restricting the isomorphism $\sigma : \mathcal{K}_A^\otimes \to \mathcal{K}_A^\perp$, $\sigma = \tau^n | \mathcal{K}^\otimes$.

This result together with Proposition 3.2 implies the following statement.

Proposition 3.9 *For every linear code $\mathcal{K} \leq {}_AM^n$, there is a group isomorphism*

$$\mathcal{K}^\otimes \cong M^n/\mathcal{K},$$

and hence $|\mathcal{K}^\otimes| \cdot |\mathcal{K}| = |M|^n$, $\mathcal{K}^{\otimes\otimes} = \mathcal{K}$.

For the reciprocal dual we now have the following fundamental formula.

Theorem 3.10 *(MacWilliams' duality) Let ${}_AM$ be a finite module with m elements and $\mathcal{K} \leq {}_AM^n$ a linear code with complete weight enumerator $W_\mathcal{K}(\mathbf{x})$. Then the complete weight enumerator of $\mathcal{K}^\otimes$ is given by*

$$W_{\mathcal{K}^\otimes}(\mathbf{y}) \;=\; \frac{1}{|\mathcal{K}|} W_\mathcal{K}(\mathbf{y}\mathcal{B}),$$

where $\mathcal{B} = (b_{\tau s})_{m \times m}$ is the $(m \times m)$-matrix with $b_{\tau s} := \exp(2\pi i\, \tau(s)(1))$ for all $s \in M$, $\tau \in M^\times$.

Proof: For the proof of this theorem we may repeat the proof of 3.6 with the following modifications. Instead of the vector $\vec{\omega} \in (M^\flat)^n$ and the functions

$$f(\vec{\omega}) = \prod_{\tau \in M^\flat} y_\tau^{\sigma_\tau(\vec{\omega})}, \quad \widehat{f}(\vec{\alpha}) \;=\; \sum_{\vec{\omega} \in (M^\flat)^n} \exp\left[2\pi i\, \vec{\omega}(\vec{\alpha})\right] f(\vec{\omega}), \quad \Delta(\vec{\omega}) \;= \sum_{\vec{\alpha} \in \mathcal{K}} \exp\left[2\pi i\, \vec{\omega}(\mathbf{v})\right],$$

we consider the vector $\vec{\psi} \in (M^\times)^n$ and the functions

$$\begin{aligned} f(\vec{\psi}) \;=\; \prod_{\tau \in M^\times} y_\tau^{\sigma_\tau(\vec{\psi})}, \qquad \widehat{f}(\vec{\alpha}) \;&=\; \sum_{\vec{\psi} \in (M^\times)^n} \exp\left[2\pi i\, \vec{\psi}(\vec{\alpha})(1_A)\right] f(\vec{\psi}), \\ \Delta(\vec{\psi}) \;&=\; \sum_{\vec{\alpha} \in \mathcal{K}} \exp\left[2\pi i\, \vec{\psi}(\vec{\alpha})(1_A)\right]. \end{aligned}$$

Then the equality $\Delta(\vec{\psi}) = 0$ for $\vec{\psi} \in (M^\times)^n \backslash \mathcal{K}^\otimes$ is proved in the following way. Since $\vec{\alpha} \times \vec{\psi} \neq 0$ for some $\alpha \in \mathcal{K}$, we have $(\vec{\alpha} \times \vec{\psi})(r) \neq 0$ for the same α and some $r \in A$. But then $((r\vec{\alpha}) \times \psi)(1_A) \neq 0$ and $r\alpha \in \mathcal{K}$ because $\mathcal{K} \leq {}_AM^n$. Therefore $K = \{(\vec{\alpha} \times \psi)(1_A) \mid \vec{\alpha} \in \mathcal{K}\}$ is a nonzero subgroup of $\mathbb{Q}/\mathbb{Z}$. Now continue as in the proof of 3.6. □

4 Equivalence of Linear Codes

The classical notion of code equivalence is based on a theorem by F. J. MacWilliams [19] who proved that Hamming isometries between linear codes over finite fields can be extended to monomial transformations of the ambient vector space. This theorem is the basis of the equivalence notion for classical algebraic coding theory and has been extended to the ring-linear context in different ways (cf. [5, 31, 32, 33, 14]). The article by M. Greferath and S. E. Schmidt [8] combines these results and gives monomial representations of homogeneous and Hamming isometries between linear codes over finite Frobenius rings. The preparation in the foregoing section allows us to generalize these results to linear codes over Frobenius modules.

4.1 Homogeneous functions on finite Modules

The notion of homogeneous weight has first been established on integer residue rings by Heise and Constantinescu [3, 4] and was generalized in two different ways. On the one hand the approach in Honold-Nechaev [12] introduced a weight on what they call a *weighted module*. This is a module with a cyclic socle satisfying further conditions that make the resulting weight strictly positive and let it satisfy the triangle inequality. On the other hand the approach in Greferath-Schmidt [8] defines a more liberal notion of homogeneous weight on every finite ring regardless of the structure of its socle and also dropping postulates like positivity and triangle inequality. The preferred notion in the present article will adopt features of both of these approaches. We will call these mappings homogeneous *functions* rather than *weights*, and most of the following results are proved in the same way as their counterparts in [12, 8].

Definition 4.1 A real-valued function w on the finite module ${}_AM$ is called (left) *homogeneous*, if $w(0) = 0$ and the following is true:

(H1) If $Ax = Ay$ then $w(x) = w(y)$ for all $x, y \in M$.

(H2) There exists a real number γ such that

$$\sum_{y \in Ax} w(y) \;=\; \gamma\,|Ax| \qquad \text{for all } x \in M \setminus \{0\}\,.$$

Remark 4.2 In [12] the definition of homogeneous function instead of (**H2**) involves the condition

(H2') $\sum_{y \in U} w(y) \;=\; \gamma\,|U|$ for all nonzero $U \leq {}_AM$.

The number γ may be called the average of w on one-generated submodules of M. Note that homogeneous functions (in the sense of 4.1) exist on *every* finite module. If we exchange condition **(H2)** by **(H2')** the existence of these functions depends on further conditions. Of course homogeneous functions in sense of [12] with property $w(0) = 0$ are homogeneous in the sense of Definition 4.1.

In order to derive an existence result and characterization for homogeneous functions we will use the following theorem by Bass (see e.g. [16, Th. 20.9]). Let A^* denote the set of units of A.

Theorem 4.3 *For all $x, y \in {}_AM$ the equality $Ax = Ay$ is equivalent to the equality $A^*x = A^*y$.*

Recall also briefly the Möbius inversion on a finite *partially ordered set*[2] $(P, \leq)$ as discussed in detail in [29], [27],[28, ch. 3.6]. For a finite poset $(P, \leq)$ the Möbius function $\mu : P \times P \longrightarrow \mathbb{Q}$ is implicitly defined by $\mu(x, x) = 1$, $\mu(x, y) = 0$ if $x \not\leq y$,and

$$\sum_{y \leq t \leq x} \mu(t, x) \;=\; 0 \text{ if } y < x.$$

This function induces for arbitrary pairs of real-valued functions f, g on P the following equivalence, referred to as *Möbius inversion*:

$$\forall x \in P: \;\; g(x) \;=\; \sum_{y \leq x} f(y) \quad \Longleftrightarrow \quad \forall y \in P: \;\; f(y) \;=\; \sum_{x \leq y} g(x)\, \mu(x, y).$$

Let now ${}_AM$ be a finite module and (unless stated otherwise) μ be the Möbius function on the set $P = \{Ax \mid x \in M\}$ of its cyclic submodules (partially ordered by set inclusion). The Möbius inversion allows the following statement.

Theorem 4.4 *A real-valued function w on the finite module ${}_AM$ is homogeneous if and only if the following holds:*

(H) *There exists a real number γ such that $w(x) \;=\; \gamma\,(1 - \frac{\mu(0,Ax)}{|A^*x|})$ for all $x \in M$.*

Proof: The proof repeats the proof of [8, Theorem 1.3] (see also [12, Proposition 5]). First of all we observe that by Möbius inversion we have

$$|A^*x| \;=\; \sum_{Ay \leq Ax} |Ay|\, \mu(Ay, Ax),$$

for all $x, y \in M$. For a given weight w let us always assume **(H1)** from definition 4.1 because this condition results from **(H)** by use of the initial observation. If now **(H2)** or **(H)** holds with respect to a positive real number γ, then the expression $f(Ax) := (\gamma - w(x))\, |A^*x|$ is well-defined for all $x \in M$, and it follows $f(0) = 0$ as well as

$$\sum_{Ay \subseteq Ax} f(Ay) \;=\; \sum_{y \in Ax} (\gamma - w(y))$$

for all $x \in M$. Now **(H2)** is equivalent to $\sum_{Ay \subseteq Ax} f(Ay) = 0$ for all $x \in M \setminus \{0\}$ which by Möbius inversion is seen to be equivalent to $f(Ax) = \gamma\, \mu(0, Ax)$ for all $x \in M$. The latter is finally equivalent to **(H)**. □

Below we use the following result of [12, Prop.4, Prop.5] (see also [8, Lemma 1.5] for the case $M = A$), which gives a criteria of the equivalence of the conditions **(H2)** and **(H2')**.

[2] These are also called *posets*.

Proposition 4.5 *For a finite module* ${}_AM$ *and a homogeneous function* w *on* M *of average value* γ *the following are equivalent:*

(a) $\mathfrak{S}({}_AM)$ *is cyclic.*

(b) *For all nonzero* $U \leq {}_AM$ *there holds* $\sum_{y\in U} w(y) = \gamma\,|U|$.

In [12] a module ${}_AM$ with $\mathfrak{S}({}_AM)$ cyclic is called a *friendly* module.

4.2 Monomial Representation of Homogeneous Isometries

In this section we will make use of the existence of a Frobenius module ${}_AM$ for every finite ring A, as we have discussed in Section 2.

As a general preparation let us fix the homogeneous function on a finite module ${}_AM$ as:

$$w_{\hom} : M \longrightarrow \mathbb{P}, \quad w_{\hom}(x) = 1 - \frac{\mu(0, Ax)}{|A^*x|}.$$

As common in coding theory, we tacitly extend $w_{\hom}$ additively to a function on M^n . Furthermore let π_i denote the projection of M^n onto its i-th coordinate.

As a direct consequence of Proposition 4.5 we state:

Lemma 4.6 *If* ${}_AM$ *is a finite module with a cyclic socle then for every* A*-linear code* $\mathcal{K}$ *over* M *there holds*

$$\frac{1}{|\mathcal{K}|}\sum_{\vec{c}\in\mathcal{K}} w_{\hom}(\vec{c}) \;=\; |\{i \mid \pi_i(\mathcal{K}) \neq 0\}|.$$

Proof : Let $\mathcal{K}$ be a linear code of length n over ${}_AM$. By an application of Proposition 4.5 we obtain $|\mathcal{K} \cap \mathrm{Ker}(\pi_i)| \sum_{x\in\pi_i(\mathcal{K})} w_{\hom}(x) \;=\; |\mathcal{K}|$ provided $\pi_i(\mathcal{K}) \neq 0$, and it follows

$$\sum_{\vec{c}\in\mathcal{K}} w_{\hom}(\vec{c}) = \sum_{i=1}^{n}\sum_{\vec{c}\in\mathcal{K}} w_{\hom}(\pi_i(\vec{c})) = \sum_{i=1}^{n} |\mathcal{K} \cap \mathrm{Ker}(\pi_i)| \sum_{x\in\pi_i(\mathcal{K})} w_{\hom}(x) = |\mathcal{K}| \cdot |\{i \mid \pi_i(\mathcal{K}) \neq 0\}|.$$

□

Definition 4.7 Let $\mathcal{K}$ be a linear code of length n over ${}_AM$. A linear mapping $\mathcal{K} \xrightarrow{\varphi} M^n$ is called *homogeneous isometry* if $w_{\hom}(\varphi(\vec{c})) = w_{\hom}(\vec{c})$ for all $\vec{c} \in \mathcal{K}$.

We will now prove the *Nullspaltenlemma* from [5] which will be a basic ingredient of the proof of Theorem 4.10.

Lemma 4.8 *Let* ${}_AM$ *be a finite module with cyclic socle and let* $\mathcal{K}$ *be a linear code of length* n *over* ${}_AM$ *. Then for every linear homogeneous isometry* $\mathcal{K} \xrightarrow{\varphi} M^n$ *,*

$$|\{i \mid \pi_i(\mathcal{K}) = 0\}| \;=\; |\{i \mid \pi_i\varphi(\mathcal{K}) = 0\}|.$$

Proof : By $|\mathcal{K}| = |\varphi(\mathcal{K})| \cdot |\mathrm{Ker}(\varphi)|$ we obtain

$$\frac{1}{|\mathcal{K}|}\sum_{\vec{c}\in\mathcal{K}} w_{\hom}(\vec{c}) \;=\; \frac{1}{|\varphi(\mathcal{K})|}\sum_{\vec{d}\in\varphi(\mathcal{K})} w_{\hom}(\vec{d}),$$

which yields our claim by Lemma 4.6. □

Definition 4.9 For an A-module M with endomorphism ring B and $n \in \mathbb{N}$, a linear mapping of the form

$$T : {}_AM^n \longrightarrow {}_AM^n, \quad (x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}b_1, \ldots, x_{\sigma(n)}b_n),$$

where σ is a permutation on $\overline{1,n}$ and $b_i \in B^*$, for all $i \in \overline{1,n}$, is called a *monomial transformation of* ${}_AM^n$.

Note that according to Proposition 1.2, if ${}_AM_B$ is a QF-bimodule then every embedding in ${}_AM$ is the restriction of a monomial transformation of ${}_AM$ and this will be crucial for the inductive proof of the subsequent theorem.

Theorem 4.10 *Let ${}_AM_A$ be a Frobenius bimodule, and let $\mathcal{K}$ be a left A-linear code of length n over M and $\mathcal{K} \xrightarrow{\varphi} {}_AM^n$ be an A-linear embedding. Then the following are equivalent:*

(a) *φ is a homogeneous isometry.*

(b) *φ is the restriction of a monomial transformation of ${}_AM^n$.*

Proof: First observe that monomial transformations T preserve the homogeneous function w_{hom} on ${}_AM$ since for any $x \in M$ and $u \in A^*$ there exists a natural isomorphism of A-modules $Ax \cong Axu$ and therefore $\mu(0, Ax) = \mu(0, Axu)$, $|A^*x| = |A^*xu|$ and $w_{\text{hom}}(x) = w_{\text{hom}}(xu)$.

Conversely, let $\mathcal{K} \xrightarrow{\varphi} {}_AM^n$ be a linear injective homogeneous isometry. If $n = 1$ then there is nothing to show because of Proposition 1.2. For general $n \geq 2$ we may assume, by Lemma 4.8, that $\mathcal{K}$ and $\mathcal{L} := \varphi(\mathcal{K})$ do not possess zero coordinates. We now choose a coordinate $i \in \overline{1,n}$, for which $\pi_i(\mathcal{K})$ is of minimal cardinality and set $\mathcal{K}_i := \mathcal{K} \cap \text{Ker}(\pi_i)$. Again by Lemma 4.8, the code $\varphi(\mathcal{K}_i) \subseteq \mathcal{L}$ has (at least) one zero coordinate, say j, and we obviously have $\varphi(\mathcal{K}_i) \subseteq \mathcal{L}_j$. The latter containment is even an equality, because otherwise $\mathcal{K}_i$ would be a proper subcode of $\varphi^{-1}(\mathcal{L}_j)$ which has again (at least) one zero coordinate (by Lemma 4.8). This however would contradict our minimality assumption on the cardinality of $\pi_i(\mathcal{K})$. So $\varphi(\mathcal{K}_i) = \mathcal{L}_j$ and we have

$$\pi_i(\mathcal{K}) \;\cong\; \mathcal{K}/\mathcal{K}_i \;\overset{\varphi}{\cong}\; \mathcal{L}/\mathcal{L}_j \;\cong\; \pi_j(\mathcal{L}),$$

and hence, by Proposition 1.2, we obtain a unit $u \in A = \text{End}({}_AM)$ with

$$(\varphi(\vec{c}))_j = \pi_j\varphi(\vec{c}) = \pi_i(\vec{c})u = c_iu \text{ for all } \vec{c} \in \mathcal{K}.$$

We now consider the projections $\pi^i(\mathcal{K})$ and $\pi^j(\mathcal{L})$ of $\mathcal{K}$ and $\mathcal{L}$ onto the coordinates different from i and j respectively. Our goal is to show that φ induces a homogeneous isometry $\varphi' : \pi^i(\mathcal{K}) \longrightarrow \pi^j(\mathcal{L})$. As these codes are of smaller length, our claim will then follow by induction on the code length n.

All we have to do is to show that $\varphi(\mathcal{K}^i) \subseteq \mathcal{L}^j$ where we have defined π^i to be the projection onto the coordinates different from i and $\mathcal{K}^i := \mathcal{K} \cap \text{Ker}(\pi^i)$ (accordingly $\mathcal{L}^j := \mathcal{L} \cap \text{Ker}(\pi^j)$). It is clear again by Lemma 4.8 that there exists $k \in \{1, \ldots, n\}$ with $\mathcal{K}^i \subseteq \mathcal{L}^k$. In case $k = j$ we are done, otherwise we have $\mathcal{L}^k \subseteq \mathcal{L}_j$ and hence $\mathcal{L}^k = 0$. But then $\mathcal{K}^i = 0$ which shows that we have $\varphi(\mathcal{K}^i) \subseteq \mathcal{L}^j$ nevertheless. □

4.3 Monomial Extension of Hamming Isometries

We first recall (following to [8]) the inversion principle for functions on unital modules with values in some fixed subfield $\mathbb{P}$ of the complex number field $\mathbb{C}$. Following the proofs in [8] will allow us to derive the equivalence theorem for Hamming isometries stated in Theorem 4.15.

For a given finite module ${}_AM$ consider the vector space over $\mathbb{P}$

$$F({}_AM, \mathbb{P}) = \{f : M \longrightarrow \mathbb{P} \mid \forall x, y \in M \ (Ax = Ay) \Rightarrow (f(x) = f(y))\}.$$

It is evident that the homogeneous function $w_{\hom}$ and the Hamming function w_H belong to $F({}_AM, \mathbb{P})$. Moreover it is easy to see that these functions are connected by the equality

$$w_H(x) \ = \ \Sigma w_{\hom}(x),$$

where Σ is endomorphism of the space $F({}_AM, \mathbb{P})$ defined by

$$(\Sigma f)(x) \ := \ \frac{1}{|Ax|} \sum_{y \in Ax} f(y).$$

Note first of all that in fact Σ is an automorphism of $F({}_AM, \mathbb{P})$. We shall call *kernel* a function $K : M \times M \longrightarrow \mathbb{P}$ defined via

$$K(x, y) \ := \ \frac{|Ax|}{|A^{\times}x|} \cdot \frac{|Ay|}{|A^*y|} \cdot \mu(Ax, Ay)$$

where again μ denotes the Möbius function on the set $\{Ax \mid x \in M\}$. As in [8] we have the following statement.

Theorem 4.11 *The endomorphism Σ is inverse to the endomorphism Δ of $F({}_AM, \mathbb{P})$ defined by*

$$(\Delta g)(x) \ := \ \frac{1}{|Ax|} \sum_{y \in Ax} f(y) \, K(y, x).$$

Proof: According to the definition the condition $g = \Sigma f$ means

$$g(x) \ = \ \frac{1}{|Ax|} \sum_{Ay \leq Ax} |A^*y| f(y) \ \text{ for all } x \in M.$$

Now Möbius inversion for the function $|Ax|g(x)$ gives

$$|A^*x| f(x) \ = \ \sum_{Ay \leq Ax} |Ay| g(y) \mu(Ay, Ax).$$

This relation implies the equality

$$f(x) \ = \ \frac{1}{|A^*x|} \sum_{y \in Ax} \frac{|Ay|}{|A^*y|} g(y) \mu(Ay, Ax) \ = \ (\Delta g)(x)$$

and hence proves our claim. □

We are now able to clarify the connection between homogeneous functions and Hamming weight, and later on the connection between homogeneous isometries and Hamming isometries. To avoid confusion in the following statement we denote by $f^{(n)}$ the additive extension of $f \in F({}_AM, \mathbb{P})$ to M^n, i.e., we set

$$f^{(n)}(\vec{x}) := f(x_1) + \ldots + f(x_n) \quad \text{for all } \vec{x} \in M^n .$$

Proposition 4.12 *For all $f \in F({}_AM, \mathbb{P})$ and all $n \in \mathbb{N}$,*

$$(\Sigma f)^{(n)} = \Sigma f^{(n)} \quad \textit{and} \quad (\Delta f)^{(n)} = \Delta f^{(n)}.$$

In particular we have $\Sigma w_{\mathrm{hom}}^{(n)} = w_H^{(n)}$ and $\Delta w_H^{(n)} = w_{\mathrm{hom}}^{(n)}$.

Proof: The proof of the first equality works like this:

$$\begin{aligned}
(\Sigma f^{(n)})(\vec{x}) &= \frac{1}{|A\vec{x}|} \sum_{\vec{y} \in A\vec{x}} f^{(n)}(\vec{y}) = \frac{1}{|A\vec{x}|} \sum_{\vec{y} \in A\vec{x}} \sum_{i=1}^{n} f(y_i) \\
&= \frac{1}{|A\vec{x}|} \sum_{i=1}^{n} \sum_{\vec{y} \in A\vec{x}} f(y_i) = \frac{1}{|A\vec{x}|} \sum_{i=1}^{n} \frac{|A\vec{x}|}{|Ax_i|} \sum_{y_i \in Ax_i} f(y_i) \\
&= \sum_{i=1}^{n} \frac{1}{|Ax_i|} \sum_{y_i \in Ax_i} f(y_i) = \sum_{i=1}^{n} (\Sigma f)(x_i) = (\Sigma f)^{(n)}(\vec{x}).
\end{aligned}$$

The remaining parts follow in a similar way using the preceding theorem. □

Definition 4.13 Let $\mathcal{K}$ be a linear code of length n over ${}_AM$ and $f \in F({}_AM, \mathbb{P})$. An A-linear injective mapping $\mathcal{K} \xrightarrow{\varphi} M^n$ is called an *f-isometry* if $f(\varphi(\vec{c})) = f(\vec{c})$ for all $\vec{c} \in \mathcal{K}$, i.e., if the functions $f\varphi$ and f coincide on $\mathcal{K}$.

Proposition 4.14 *Let $\mathcal{K} \leq {}_AM^n$ and $f \in F({}_AM, \mathbb{P})$. A linear injective mapping $\mathcal{K} \xrightarrow{\varphi} M^n$ is an f-isometry if and only if it is a (Σf)-isometry.*

Proof: Since φ is a linear and injective map we have $A\varphi(\vec{c}) = \varphi(A\vec{c})$ and $|A\varphi(\vec{c})| = |A\vec{c}|$, for all $\vec{c} \in \mathcal{K}$. Now for any $\vec{c} \in \mathcal{K}$ we have

$$\begin{aligned}
(\Sigma f)\varphi(\vec{c}) &= \frac{1}{|A\varphi(\vec{c})|} \sum_{\vec{d} \in A\varphi(\vec{c})} f(\vec{d}) = \frac{1}{|A\vec{c}|} \sum_{\vec{d} \in \varphi(A\vec{c})} f(\vec{d}) \\
&= \frac{1}{|A\vec{c}|} \sum_{\vec{a} \in A\vec{c}} f(\varphi(\vec{a})) = \Sigma(f\varphi)(\vec{c}).
\end{aligned}$$

So if $f\varphi$ and f coincide on $\mathcal{K}$ then the same is true for $(\Sigma f)\varphi$ and Σf. The converse assertion follows from Theorem 4.11. □

The foregoing statement together with Proposition 4.12 shows in particular that a linear mapping is a homogeneous isometry if and only if it is a Hamming isometry. Since Hamming isometries are trivially injective, we obtain by combination of Theorem 4.10 with Propositions 4.12 and 4.14 a monomial extension of Hamming isometries.

Theorem 4.15 *Let ${}_AM_A$ be a Frobenius bimodule. Then for an left A-linear code $\mathcal{K}$ of length n over M and an A-linear mapping $\mathcal{K} \xrightarrow{\varphi} {}_AM^n$ the following are equivalent:*

(a) *φ is a Hamming isometry;*

(b) *φ is the restriction of a monomial transformation of ${}_AM^n$.*

References

[1] G. Azumaya, *A duality theory for injective modules (Theory of quasi-Frobenius modules)*, *Amer. J. Math.*, **81**(1) (1959), 249-278.

[2] H. L. Claasen, R. W. A. Goldbach, *A field-like property of finite rings*, Indag. Math. **3** (1992), 11-26.

[3] I. Constantinescu, *Lineare Codes über Restklassenringen ganzer Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik*, Ph.D. thesis, Technische Universität München, 1995.

[4] I. Constantinescu, W. Heise, *A metric for codes over residue class rings of integers*, Problemy Peredachi Informatsii **33**(3) (1997), 22-28.

[5] I. Constantinescu, W. Heise, T. Honold, *Monomial extensions of isometries between codes over $\mathbb{Z}_m$*, Proceedings of the 5th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 1996), Unicorn Shumen, 98-104.

[6] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips research, Rep. Suppl. **10**, 1973.

[7] C. Faith, *Algebra II. Ring Theory*, Springer. Berlin, 1976.

[8] M. Greferath, S.E. Schmidt, *Finite-ring combinatorics and MacWilliams' equivalence Theorem*, J. Combin. Theory, Ser A **92**(1) (2000), 17-28.

[9] G. Hauger, W. Zimmermann, *Quasi-Frobenius-Moduln*, Arch.Math. 24 (1975), 379-386.

[10] W. Heise, T. Honold, A. A. Nechaev, *Weighted modules and representations of codes*, Proceedings of the ACCT 6 (Pskov, Russia, 1998), 123-129.

[11] T. Honold, *Characterization of Finite Frobenius rings*, Arch. Math. (Basel) **76**(6) (2001), 406-415.

[12] T. Honold, A. A. Nechaev, *Weighted modules and linear representations of codes*, Problems Inform. Transmission, **35**(3) (1999), 205-223.

[13] F. Kasch, *Moduln und Ringe*, B.G. Teubner, Stuttgart, 1977.

[14] I. Kheifetc, *The extension Theorem for isometries of linear codes over QF-modules*, Fundamentalnaja i prikladnaja matematika. CNIT Moscow St. Univ. 7(4) (2001), 1227-1236 (in Russian).

[15] A.S. Kuzmin, V.L. Kurakin, V.T. Markov, A.V. Mikhalev, A. A. Nechaev, *Linear codes and polylinear recurrences over finite rings and modules (Survey)*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proc. of the 13-th. Int Symp. AAECC-13. LNCS, Springer, 1999.

[16] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, **131**, Springer-Verlag (1991).

[17] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, **189**, Springer-Verlag (1999).

[18] E. Lamprecht, *Über I-reguläre Ringe, reguläre Ideale und Erklärungsmoduln* I, Math. Nachricht. **10** (1953), 353-382.

[19] F. J. MacWilliams, *Combinatorial properties of elementary abelian groups*, Ph.D. thesis, Radcliffe College, Cambridge MA, 1962.

[20] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Co., 1977.

[21] A.A. Nechaev, *Linear codes and polylinear recurrences over finite rings and quasi-Frobenius modules*, Dokl. Akad. Nauk. **345**(1) (1995), 229-254 (in Russian).

[22] ———, *Linear codes over modules and over spaces. MacWilliams identity*, Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl., Victoria B. C., Canada (1996), 35-38.

[23] A.A. Nechaev, A.S. Kuzmin, V.T. Markov, *Linear codes over finite rings and modules*, Fundamentalnaja i prikladnaja matematika, **2**(3) (1996), 195-254 (in Russian). English translation: CNIT of Mosc. State Univ. preprint N 1995-6-1, http://www.math.msu.su/~markov.

[24] A. A. Nechaev, V. N. Tzypyshev, *Artinian bimodule with quasi-Frobenius canonical bimodule*, Proc. Int. Workshop devoted to 70-th anniversary of scientific algebraic workshop of Moscow State University (2000), 39-40 (in Russian).

[25] W.K. Nicholson, M.F. Yousif, *Mininjective Rings*, J. Algebra **187** (1997), 548-578.

[26] R. Raghavendran, *Finite associative rings*, Compos. Math. **21**(2) (1969), 195-220.

[27] G.-C. Rota, *On the foundations of combinatorial theory. I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **2** (1964), 340-368.

[28] R. P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Univ. Press, 1997.

[29] R. Wiegandt, *On the general theory of Möbius inversion formula and Möbius product*, Acta Sci. Math. Szeged **20** (1959), 164-180.

[30] R. Wisbauer, *Grundlagen der Modul- und Ringtheorie*, Reinhard Fischer, München 1988; *Foundations of Module and Ring Theory*, Gordon and Breach, Reading 1991.

[31] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121**(3), 555-575, 1999.

[32] ———, *Extension theorems for linear codes over finite rings*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (T. Mora and H. Mattson, eds.), Springer Verlag (1997), 329-340.

[33] ———, *Weight functions and the extension Theorem for linear codes over finite rings*, in *Finite fields: theory, applications, and algorithms* (Waterloo, ON, 1997), 231-243, Contemp. Math., 225, Amer. Math. Soc., Providence, RI, 1999.