Geometric approach to the MacWilliams Extension Theorem for codes over modules

Serhii Dyshko *

Institut de mathématiques de Toulon, Université de Toulon, France

Abstract

The MacWilliams Extension Theorem states that each linear Hamming isometry of a linear code extends to a monomial map. In this paper an analogue of the extension theorem for linear codes over a module alphabet is observed. A geometric approach to the extendability of isometries is described. For a matrix module alphabet we found the minimum length of a code for which an unextendable Hamming isometry exists. We also proved an extension theorem for MDS codes over a module alphabet.

1 Introduction

The famous MacWilliams Extension Theorem states that each linear isometry of a linear code extends to a monomial map. The result was originally proved in the MacWilliams' Ph.D. thesis, see [8]. Later, the result was generalized for codes over modules. A summary is given below.

Let R be a ring with identity and let A be a finite left R-module. Consider a module A^n with the Hamming metrics and a code $C \subseteq A^n$ that is a left R-submodule. For two R-modules A and B let $\mathrm{Hom}_R(A, B)$ denote the set of R-module homomorphism from A to B. Call a map $f \in \mathrm{Hom}_R(A^n, A^n)$ *monomial*, if there exist a permutation $\pi \in S_n$ and automorphisms $g_1, \dots, g_n \in \mathrm{Aut}_R(A)$, such that, for any $a \in A^n$,

$$f\big((a_1, \dots, a_n)\big) = \left(g_1(a_{\pi(1)}), \dots, g_n(a_{\pi(n)})\right) .$$

Note that a monomial map preserves the Hamming distance. It can be easily shown, that each isometry $f \in \mathrm{Hom}_R(A^n, A^n)$ is monomial. We say that an alphabet A has the *extension property* if for any positive integer n, for any code $C \subseteq A^n$ each Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$ extends to a monomial map.

Classical linear codes correspond to the case when $R = \mathbb{F}_q$ and $A = R$, where $\mathbb{F}_q$ is a finite field. As we mentioned before, the MacWilliams Extension Theorem states that the alphabet $A = R = \mathbb{F}_q$ has the extension property.

Apparently, not every module alphabet satisfies the extension property. Recall the definition of a pseudo-injective module. A left R-module A is called *pseudo-injective*, if for each left R-submodule $B \subseteq A$ and for each two embeddings $\phi, \psi \in \mathrm{Hom}_R(B, A)$ there exists an automorphism $h \in \mathrm{Aut}_R(A)$ such that $\psi = h\phi$. In other words, A is pseudo-injective if and only if any R-linear isomorphism between its submodules extends to an R-linear automorphism of A. Not all the R-modules are pseudo-injective.

*Electronic address: dyshko@univ-tln.fr

$$\begin{tikzcd}
A^n \arrow[dr, "h"] & \\
C \arrow[u, hook, "\iota"] \arrow[r, "f"'] & A^n
\end{tikzcd}$$

Figure 1: Extension property.

$$\begin{tikzcd}
B \arrow[r, hook, "\psi"] \arrow[dr, hook, "\phi"'] & A \\
& A \arrow[u, "h"']
\end{tikzcd}$$

Figure 2: Pseudo-injectivity of a module A.

Example 1. Consider a $\mathbb{Z}$-module $A = \mathbb{Z}_2 \oplus \mathbb{Z}_4$. Let $M = \langle(0,2)\rangle$ and $N = \langle(1,0)\rangle$. Obviously, $M \cong N$, with isomorphism $\psi : (0,2) \to (1,0)$, but there is no isomorphism $\phi : A \to A$ such that $\phi = \psi$ on M. So, A is not pseudo-injective.

Recall the *socle* of A is a submodule $\operatorname{soc}(A) \subseteq A$ that is equal to the sum of all simple submodules of A. A module is called *simple* (or irreducible) if it does not contain any other submodules except zero and itself. In [9] the author proved a general extension theorem for a pseudo-injective module alphabet with a cyclic socle and showed that these conditions are maximal.

Theorem 1. *If A is an alphabet that is pseudo-injective and* $\operatorname{soc}(A)$ *cyclic, then A has the extension property.*

In the case, when $A = R$, in [2, 6, 9] the authors proved the extension theorem for Frobenius rings and showed the maximality of the condition.

Theorem 2. *Let R be a Frobenius ring. Then the alphabet $A = R$ has the extension property.*

In [1, 2] the extension problem for arbitrary ring and alphabet was partially translated to the case of matrix rings and matrix modules. There the authors proved the existence of a general counterexample for codes over a matrix module alphabet. An explicit construction appeared in [9].

Theorem 3 (see [9])**.** *Let $R = \mathrm{M}_m(\mathbb{F}_q)$ be a ring of all $m \times m$ matrices over a finite field $\mathbb{F}_q$ and let $A = \mathrm{M}_{m\times k}(\mathbb{F}_q)$ be a left R-module of all $m \times k$ matrices over $\mathbb{F}_q$.*

If $k \leq m$, then the alphabet A has the extension property.

If $k > m$, there exist a linear code $C \subset A^K$, $K = \prod_{i=1}^{k-1}(1+q^i)$, and a map $f \in \operatorname{Hom}_R(C, A^K)$ that is a Hamming isometry, but there is no monomial map extending f.

Note that the theorem does not say if the given counterexample has minimum possible code length. In this paper we improve Theorem 3. More precisely, in the context of matrix modules, we found the minimum code length for which an example of a code with unextendable isometry exists. It appear that such a code with minimal code length is similar to the code from Theorem 3, described in [9]. In our previous work [3] we found the precise bound for the case $m = 1$, which corresponds to linear codes over a vector space alphabet.

Our main idea is to use a geometric approach. In Proposition 1 we describe an unextendable isometries in terms of nontrivial solution of the isometry equation (1), which is an equation of indicator functions of modules. In [3] we observed basic properties of this equation for the case of vector spaces and here, in Proposition 2 we describe some properties of the equation for matrix modules.

In Theorem 5 we prove that the extension property holds for MDS codes over a module alphabet, when the dimension of a code does not equal 2. Despite the general result of Theorem 1, for MDS codes the extension theorem holds for arbitrary finite R-module alphabet.

2 Extension criterium

Let W be a left R-module isomorphic to C. Let $\lambda \in \mathrm{Hom}_R(W, A^n)$ be a map such that $\lambda(W) = C$. Present the map λ in the form $\lambda = (\lambda_1, \dots, \lambda_n)$, where $\lambda_i \in \mathrm{Hom}_R(W, A)$ is a projection on the ith coordinate, for $i \in \{1, \dots, n\}$. Consider the following modules, for $i \in \{1, \dots, n\}$,

$$V_i = \mathrm{Ker}\, \lambda_i \subseteq W\ .$$

Let $f : C \to A^n$ be a homomorphism of left R-modules. Define $\mu = f\lambda \in \mathrm{Hom}_R(W, A^n)$ and denote

$$U_i = \mathrm{Ker}\, \mu_i \subseteq W\ .$$

$$\begin{tikzcd}
W \arrow[r, "\lambda"] \arrow[dr, "\mu"'] & C \arrow[d, "f"] \\
 & A^n
\end{tikzcd}$$

Figure 3: The maps λ and μ.

Denote the tuples of modules $\mathcal{V} = (V_1, \dots, V_n)$ and $\mathcal{U} = (U_1, \dots, U_n)$. We say that $\mathcal{V} = \mathcal{U}$ if they represent the same multiset of modules. In other words, $\mathcal{V} = \mathcal{U}$ if and only if there exists $\pi \in S_n$ such that for each $i \in \{1, \dots, n\}$, $U_i = V_{\pi(i)}$. Recall the indicator function of a subset Y of a set X is a map $\mathbb{1}_Y : X \to \{0, 1\}$, such that $\mathbb{1}_Y(x) = 1$ if $x \in Y$ and $\mathbb{1}_Y(x) = 0$ otherwise.

Proposition 1. *The map $f \in \mathrm{Hom}_R(C, A^n)$ is a Hamming isometry if and only if the following equality holds,*

$$\sum_{i=1}^{n} \mathbb{1}_{V_i} = \sum_{i=1}^{n} \mathbb{1}_{U_i}\ . \tag{1}$$

If f extends to a monomial map, then $\mathcal{V} = \mathcal{U}$. If A is pseudo-injective and $\mathcal{V} = \mathcal{U}$, then f extends to a monomial map.

Proof. Prove the first part. By definition, the map f is a Hamming isometry if for each $a \in C$, $\mathrm{wt}(f(a)) = \mathrm{wt}(a)$, or, equivalently, f is an isometry if and only if for each $w \in W$, $\mathrm{wt}(\lambda(w)) = \mathrm{wt}(\mu(w))$. Note that for any $w \in W$, $n - \mathrm{wt}(\lambda(w)) = \sum_{i=1}^{n}(1 - \mathrm{wt}(\lambda_i(w))) = \sum_{i=1}^{n} \mathbb{1}_{\mathrm{Ker}\,\lambda_i}(w)$ and the same for the map μ. Hence eq. (1) holds.

Prove the second part. Consider any two maps $\sigma, \tau \in \mathrm{Hom}_R(W, A)$. If there exists $g \in \mathrm{Aut}_R(A)$ such that $\sigma = g\tau$ then $\mathrm{Ker}\,\sigma = \mathrm{Ker}\,\tau$.

Let $\mathrm{Ker}\,\sigma = \mathrm{Ker}\,\tau = N \subseteq W$ and let A be pseudo-injective. The corresponding homomorphisms defined on the quotient module $\bar{\sigma}, \bar{\tau} : W/N \to A$ are injective. Using the property of A, there exists $h \in \mathrm{Aut}_R(A)$ such that $\bar{\sigma} = h\bar{\tau}$. It is easy to check that $\sigma = h\tau$. □

Let a pair of tuples of modules $(\mathcal{U}, \mathcal{V})$ be a solution of eq. (1). If $\mathcal{U} = \mathcal{V}$ then we call the solution *trivial*. Proposition 1 gives a relation between trivial solutions of eq. (1) and extendable isometries.

Remark 1. As it was noted in [2] and [9], the property of pseudo-injectivity is necessary in the statement. Assuming that the alphabet is not pseudo-injective means that the extension property fails even if the length of a code is 1.

3 General extension theorem

In this section we show how to use the approach from the previous section to prove Theorem 1. Recall that a left R-module M is called *cyclic* if there exists a generator element $x \in M$, such that $M = Rx = \{rx \mid r \in R\}$.

Lemma 1. *An R-module M is not cyclic if and only if there exist submodules $\{0\} \subset E_1, \dots, E_r \subset M$ such that $M = \bigcup_{i=1}^{r} E_i$.*

Proof. Assume that there exists such a covering $M = \bigcup_{i=1}^{r} E_i$ of M by submodules and let M be cyclic. For a generator $x \in M$ there exists $i \in \{1, \dots, r\}$ such that $x \in E_i$ and thus $M = Rx \subseteq E_i \subset M$ that leads to a contradiction.

If M is not cyclic, then for any $x \in M \setminus \{0\}$, $\{0\} \subset Rx \subset M$ and therefore $M = \bigcup_{x \in M \setminus \{0\}} Rx$. □

Lemma 2. *For each non-cyclic module M there exists a nontrivial solution of eq. (1) with at least one module equals M. A solution of the equation*

$$\sum_{i=1}^{s} a_i \mathbb{1}_{V_i} = \sum_{i=1}^{t} b_i \mathbb{1}_{U_i} \ ,$$

with only cyclic modules is trivial, where all the coefficients are in $\mathbb{C}$.

Proof. Prove the first part. Let $M = \bigcup_{i=1}^{r} E_i$ be a nontrivial covering of M by submodules. Denote $M_I = \bigcap_{i \in I} E_i$, where $I \subseteq \{1, \dots, r\}$ and define $M_\emptyset = M$. Use the inclusion-exclusion formula,

$$\sum_{|I| \text{ is even}} \mathbb{1}_{M_I} = \sum_{|I| \text{ is odd}} \mathbb{1}_{M_I} \ ,$$

where the summation is over all subsets $I \subseteq \{1, \dots, r\}$. It is easy to see that the resulting equation is nontrivial, for example, the module M appears only from the left side. The number of terms on each side is the same and equals 2^{r-1}.

Prove the second part. Assume that there exists a nontrivial solution of the equation. Without loss of generality, we can assume that the equation is simplified by eliminating equal terms and making a reindexing. Hence, $a_i, b_j \neq 0$ for $i \in \{1, \ldots, s\}$, $j \in \{1, \ldots, t\}$ and all V_i, U_i are different. Since the solution is nontrivial, $s, t > 0$. Among the modules choose the maximal with respect to the inclusion, suppose it is V_1. Then $V_1 = \bigcup_{i=1}^{t} (V_1 \cap U_i)$, where $\{0\} \subset V_1 \cap U_i \subset V_1$, $i \in \{1, \ldots, t\}$. From Lemma 1, the module V_1 is therefore non-cyclic, which contradicts to our assumption. □

Characters and Fourier transform. Denote by $\hat{A} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^*)$ the set of characters of A. The set $\hat{A}$ has a natural structure of a right R-module. Let A, W be two left R-modules. For a map $\sigma \in \mathrm{Hom}_R(W, A)$ define a map $\hat{\sigma} : \hat{A} \to \hat{W}$, $\chi \mapsto \chi\sigma$. Note that $\hat{\sigma} \in \mathrm{Hom}_R(\hat{A}_R, \hat{W}_R)$. It is known that $\wedge$ is an exact contravariant functor on the category of left(right) R-modules, see [9].

Let M be a left R-module. The Fourier transform of a map $f : M \to \mathbb{C}$ is a map $\mathcal{F}(f) : \hat{M} \to \mathbb{C}$, defined as

$$\mathcal{F}(f)(\chi) = \sum_{m \in M} f(m)\chi(m) \ .$$

It can be easily proved that for a submodule $V \subseteq M$, $\mathcal{F}(\mathbb{1}_V) = |V| \mathbb{1}_{V^\perp}$, where an orthogonal module is defined as $V^\perp = \{\chi \in \hat{M} \mid \forall v \in V, \chi(v) = 1\} \subseteq \hat{M}$. Note that the Fourier transform is invertible, $V^{\perp\perp} \cong V$ and for any $V, U \subseteq W$, $(V \cap U)^\perp = V^\perp + U^\perp$.

For any $\sigma \in \mathrm{Hom}_R(W, A)$, $\mathrm{Ker}\,\sigma = \{w \in W \mid \sigma(w) = 0\} = \{w \in W \mid \forall \chi \in \hat{A}, \chi(\sigma(w)) = 1\} = (\mathrm{Im}\,\hat{\sigma})^\perp$, and thus $(\mathrm{Ker}\,\sigma)^\perp = \mathrm{Im}\,\hat{\sigma}$.

Theorem 4. *If $\hat{A}$ is a cyclic right R-module and A is pseudo-injective, then A has the extension property.*

Proof. Let $C \subset A^n$ be a code and let $f \in \mathrm{Hom}_R(C, A^n)$ be an isometry. By Proposition 1, f is extendable if and only if the solution $(\mathcal{U}, \mathcal{V})$ of eq. (1) is trivial. Due to the properties of the Fourier transform, eq. (1) is equivalent to the following equality of functions defined on $\hat{W}$,

$$\sum_{i=1}^{n} |V_i| \mathbb{1}_{V_i^\perp} = \sum_{i=1}^{n} |U_i| \mathbb{1}_{U_i^\perp} \tag{2}$$

and the solution of eq. (1) is trivial if and only if the corresponding orthogonal solution is trivial. The statement of the theorem is a direct consequence of Lemma 2 and the fact that the modules $V_i^\perp = \mathrm{Im}\,\hat{\lambda}_i$, $U_i^\perp = \mathrm{Im}\,\hat{\mu}_i$, $i \in \{1, \ldots, n\}$, are all cyclic, since so is $\hat{A}$. □

Remark 2. Theorem 4 is an analogue of Theorem 1, where instead of the cyclic socle condition we use the cyclic character module condition. Prove that these two conditions are equivalent. In [9] it was proven that $\mathrm{soc}(A)$ is cyclic if and only if A can be embedded into ${}_R\hat{R}$. This means there exists an injective homomorphism of left R-modules $\phi : A \to_R \hat{R}$. Since $\wedge$ is an exact functor, the last is equivalent to the fact that the map $\hat{\phi} : \hat{\hat{R}}_R \cong R_R \to \hat{A}_R$ is a projective homomorphism of right R-modules that is a characterization of cyclicity of $\hat{A}_R$.

4 Extension theorem for matrix alphabets

An R-module A is called *semisimple* (or completely reducible) if A is a direct sum of simple submodules.

Lemma 3. *If a left R-module A is semisimple, then A is pseudo-injective.*

Proof. Let $N, M \subseteq A$ be two submodules and let $\psi : N \to M$ be an isomorphism. Since A is semisimple, there exist $N', M' \subseteq A$ such that $A = N \oplus N' = M \oplus M'$. Since $N \cong M$, there is an isomorphism $\phi : N' \to M'$. Then ψ extends to the automorphism $\psi \times \phi : A = N \oplus N' \to M \oplus M' = A$. □

It is proved in [7, p. 656] that each module M over the ring $R = \mathrm{M}_m(\mathbb{F}_q)$ is semisimple and is isomorphic to $\mathrm{M}_{m\times k}(\mathbb{F}_q)$ for some k. Call k the dimension of M and denote $\dim M = k$. We need the following lemmas to prove an extension theorem for R-linear codes over M.

Lemma 4. *The following equalities hold,*

$$\sum_{i=0}^{t-1}(-1)^i q^{\binom{i}{2}}\binom{t}{i}_q = (-1)^{t-1}q^{\binom{t}{2}}\ ,$$

$$\sum_{i=0}^{t} q^{\binom{i}{2}}\binom{t}{i}_q = \prod_{i=0}^{t-1}(1+q^i)\ .$$

Proof. Use a well-known Cauchy binomial theorem,

$$\prod_{i=0}^{t-1}(1+xq^i) = \sum_{i=0}^{t} q^{\binom{i}{2}}\binom{t}{i}_q x^i\ .$$

To get the equalities in the statement, put $x = -1$ and $x = 1$. □

Lemma 5. *Let R be a matrix module over $\mathbb{F}_q$, let M be a t-dimensional R-module and let X be a p-dimensional submodule of M. For each $i \in \{p, \dots, t\}$ we have,*

$$|\{V \subseteq M \mid X \subseteq V, \dim V = i\}| = \binom{t-p}{i-p}_q$$

Proof. It is a well known fact that for any $k \in \{0, \dots, t\}$ there are $\binom{t}{k}_q$ submodules of M of dimension i. The number of such submodules, that contain X is equal to the number of submodules of dimension $i-\dim X$ in M/X that contain $\{0\}$, which is always the case. In other words, $|\{V \subseteq M \mid X \subseteq V, \dim V = i\}| = |\{V \subseteq M/X \mid \dim V = i-p\}| = \binom{\dim M/X}{i-p}_q = \binom{t-p}{i-p}_q$. □

The next proposition is an improvement of Theorem 3. Note that the code length K in Theorem 3 depends on k (the alphabet parameter) whereas in the following proposition the code length N depends on m (the ring parameter) and N is not greater than K. In our proof this improvement is easily obtained from the author's construction in [9], however it does not appear in the original statement of the author.

Proposition 2. *Let $R = \mathrm{M}_m(\mathbb{F}_q)$ and let $A = \mathrm{M}_{m\times k}(\mathbb{F}_q)$ be a left R-module.*

If $k \leq m$, then the alphabet A has the extension property.

If $k > m$, there exist a linear code $C \subset A^N$, $N = \prod_{i=1}^{m}(1+q^i)$, and a map $f \in \mathrm{Hom}_R(C, A^N)$ that is a Hamming isometry, but there is no monomial transformation extending f.

For any $n < N$, each Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$ is extendable.

Proof. For any k, since A is semisimple, by Lemma 3, A is pseudo-injective. If $k \leq m$, the right R-module $\hat{A}$ is cyclic, since $\dim \hat{A} = \dim A = k \leq m$. From Theorem 4, A has the extension property.

To construct a code of the length N we do the following. Let C' be the code over the alphabet $B = M_{m\times m+1}(\mathbb{F}_q)$ and let $f \in \mathrm{Hom}_R(C', B^N)$ be the unextendable isometry from Theorem 3. Choosing this alphabet, we have $K = N$. Since $k > m$, in A there exists a submodule isomorphic to B, so C' can be considered as a code in A^N and $f \in \mathrm{Hom}_R(C', A^N)$. Due to the construction of the author in [9], the code C' has all zero column and $f(C')$ does not. Therefore f is unextendable.

Let $k > m$. Let n' be the minimum value of the code length for which there exists and unextendable isometry $f \in \mathrm{Hom}_R(C, A^{n'})$. By Proposition 1, there exists a non-trivial solution of eq. (1). Hence, the minimum length n of a nontrivial solution of eq. (1) is not greater than n'. Consider a solution of the length n which have the minimum value $\max\{\dim V_i, \dim U_i \mid i \in \{1,\dots,n\}\}$, and denote this value by r. From Lemma 2, $r > m$. Without loss of generality, let $\dim V_1 = r$.

Introduce a new notation. Denote $I_j = \{i \mid \dim V_i < r - j\}$, $J_j = \{i \mid \dim U_i < r - j\}$ and

$$\Sigma_j = \sum_{\dim V = r-j} \mathbb{1}_V \ ,$$

for $j \in \{0,\dots,r\}$, where the summation is over all the submodules in V_1 of the given dimension. Calculate the restriction of eq. (1) on the module V_1,

$$a\Sigma_0 = \sum_{i\in J_0} \mathbb{1}_{U_i \cap V_1} - \sum_{i \in I_0} \mathbb{1}_{V_i\cap V_1} \ ,$$

where by $a \geq 1$ we denote the number of modules V_1 in the left part of eq. (1). This is a nontrivial solution of the length n and the maximum dimension r. Evidently, since the length n is the minimal, $U_i \cap V_1 \subset V_1$ for all $i \in J_0$ and $V_i \cap V_1 \subset V_1$ for all $i \in I_0$, so, without loss of generality, let $U_i, V_i \subseteq V_1$, for $i \in \{1,\dots,n\}$.

Say that on the t-step, $0 \leq t < r$, we have proved that eq. (1) is of the form,

$$a\sum_{i=0}^{t}(-1)^i q^{\binom{i}{2}} \Sigma_i = \sum_{i\in J_t} \mathbb{1}_{U_i} - \sum_{i\in I_t} \mathbb{1}_{V_i} \ .$$

For $t = 0$ this is true. Let $X \subset V_1$ be of dimension $r - t - 1$. Restrict the equation on X,

$$a\sum_{i=0}^{t}(-1)^i q^{\binom{i}{2}} \sum_{\dim V = r-i} \mathbb{1}_{V\cap X} = \sum_{i\in J_t} \mathbb{1}_{U_i\cap X} - \sum_{i\in I_t} \mathbb{1}_{V_i \cap X} \ .$$

The dimension of X is smaller than r, so the restricted solution is trivial. Calculate the number of $\mathbb{1}_X$ terms from the left and from the right. Denote $b = |\{i \in J_t \mid X = U_i\}|$ and $c = |\{i \in I_t \mid X = V_i\}|$. Note that either $b = 0$ or $c = 0$. Using Lemma 5 and Lemma 4,

$$a\sum_{i=0}^{t}(-1)^i q^{\binom{i}{2}}\binom{t+1}{i}_q = a(-1)^t q^{\binom{t+1}{2}}\binom{t+1}{i}_q = b - c\,,$$

and therefore $c = 0$ if t is even and $b = 0$ if t is odd.

All the submodules of V_1 of dimension $r - t - 1$ are presented from the left or from the right side of eq. (1), depending on the parity of t, with the same multiplicity. Considering this fact, we rewrite eq. (1) in the form,

$$a\sum_{i=0}^{t+1}(-1)^i q^{\binom{i}{2}}\Sigma_i = \sum_{i\in J_{t+1}}\mathbb{1}_{U_i} - \sum_{i\in I_{t+1}}\mathbb{1}_{V_i}\ .$$

On the output of $t = r - 1$ step we get,

$$a\sum_{i=0}^{r}(-1)^i q^{\binom{i}{2}}\Sigma_i = \sum_{i\in J_r}\mathbb{1}_{U_i} - \sum_{i\in I_r}\mathbb{1}_{V_i} \equiv 0\ .$$

The length of the equation is $\frac{1}{2}a\sum_{i=0}^{r} q^{\binom{i}{2}}\binom{r}{i}_q$. Since the equation has the minimal length, $a = 1$ and $r = m + 1$. From Lemma 4, $n = \frac{1}{2}\prod_{i=0}^{m}(1 + q^i) = \prod_{i=1}^{m}(1 + q^i) = N$. Therefore $n' \geq n = N$. □

5 Extension theorem for MDS codes

There is a famous Singleton bound, that states that for a code $C \subseteq A^n$, $|C| \leq |A|^{n-d+1}$, where d is the minimum distance of C. When a code C attains the bound, it is called an MDS code. The value $k = n - d + 1$ is called a dimension C and the code is said to be an $(n, k)_A$ MDS code.

An alternative definition is the following. A code $C \subseteq A^n$ is MDS if and only if a restriction of C on any k columns is isomorphic to A^k. In other words, any k columns of C can be taken as an information set of the code. We interpret this definition in terms of modules $\mathcal{V} = (V_1, \ldots, V_n)$.

Lemma 6. *Let C be an $(n, k)_A$ MDS code. For each subset $I \subseteq \{1, \ldots, n\}$ of size k, $\sum_{i\in I} V_i^{\perp} = \hat{W}_R$. Moreover, $|V_i^{\perp}| = |A|$ for all $i \in \{1, \ldots, n\}$.*

Proof. Let $I \subseteq \{1, \ldots, n\}$ be a subset with k elements. Let C' be a code obtained from C by keeping only coordinates from I. The map $\lambda' = (\lambda_i)_{i\in I}$, $\lambda' : W \to A^k$ is a parametrization of C'. Since C is MDS, λ' is injective, which implies $\bigcap_{i\in I} V_i = \{0\}$. Calculating the orthogonal, we get $\sum_{i\in I} V_i^{\perp} = \hat{W}_R$.

We know that all the modules W, C, C' are isomorphic to A^k. Thus there is an isomorphism of right R-modules $\hat{W} \cong \hat{A}^k$. Also, $|V_i^{\perp}| \leq |A| = |\hat{A}_R|$ and for any $i, j \in \{1, \ldots, n\}$, $|V_i^{\perp} + V_j^{\perp}| = |V_i^{\perp}||V_j^{\perp}|/|V_i^{\perp} \cap V_j^{\perp}|$. Combining all the facts, we get $|V_i^{\perp}| = |A|$. □

The next lemma shows that the condition of pseudo-injectivity in Proposition 1 can be omitted if a code is MDS.

Lemma 7. *Let C be an $(n, k)_A$ MDS code and let $f \in \mathrm{Hom}_R(C, A^n)$. If $\mathcal{V} = \mathcal{U}$, then f extends to a monomial map.*

Proof. The proof is almost identical to the second part of the proof of Proposition 1. Let $\sigma, \tau \in \mathrm{Hom}_R(W, A)$ be two maps that parametrize a column in C and a column in $f(C)$ correspondingly. Since C is an MDS code, from Lemma 6, $\mathrm{Im}\,\sigma = A$, because $|\mathrm{Im}\,\sigma| = |(\mathrm{Ker}\,\sigma)^{\perp}| = |A|$.

Let $\mathrm{Ker}\,\sigma = \mathrm{Ker}\,\tau = N \subseteq W$. This implies $\mathrm{Im}\,\tau = \mathrm{Im}\,\sigma = A$. Consider the canonical isomorphisms $\bar{\sigma}, \bar{\tau} : W/N \to A$. The map $h \in \mathrm{Aut}_R(A)$, defined as $h = \bar{\tau}\bar{\sigma}^{-1}$, satisfies the equality $h\sigma = \tau$. □

Theorem 5. *Let R be a ring with identity and let A be a finite left R-module. Let C be an $(n, k)_A$ MDS code, $k \neq 2$. Each Hamming isometry $f \in \mathrm{Hom}_R(C, A^n)$ extends to a monomial map.*

Proof. Assume that there exists an unextendable isometry $f \in \mathrm{Hom}_R(C, A^n)$. From Proposition 1 and Lemma 7, there exists a nontrivial solution of eq. (1), or equivalently, there exists a nontrivial solution of the orthogonal equation (2). It is clear that $f(C)$ is also an MDS code.

The proof is obvious for the case $k = 1$, so let $k \geq 3$. This means, from Lemma 6, for any different $i, j, k \in \{1, \dots, n\}$, $V_i^{\perp} \cap (V_j^{\perp} + V_k^{\perp}) = \{0\}$. Without loss of generality, assume that $U_1^{\perp}$ is covered nontrivially by modules $V_1^{\perp}, \dots, V_t^{\perp}$, $t > 1$, i.e. $U_1^{\perp} = \bigcup_{i=1}^{t} V_i^{\perp}$, $\{0\} \subset V_i^{\perp} \subset U_1^{\perp}$, for $i \in \{1, \dots, t\}$ and no module is contained in another.

Take a nonzero element $a \in U_1^{\perp} \cap V_1^{\perp}$ and a nonzero element $b \in U_1^{\perp} \cap V_2^{\perp}$. Obviously, since $V_1^{\perp} \cap V_2^{\perp} = \{0\}$, $a + b \notin V_1^{\perp} \cup V_2^{\perp}$. But $a + b \in U_1^{\perp}$ and hence $t > 2$. There exists an index i, let it be 3, such that $a + b \in U_1^{\perp} \cap V_3^{\perp}$. Then $a + b \in (V_1^{\perp} + V_2^{\perp}) \cap V_3^{\perp} \neq \{0\}$, which gives a contradiction. □

The case of MDS codes of dimension 2 is observed in [4], where R is a finite field and the alphabet A is a vector space. Note that the statement is true for all abelian groups as $\mathbb{Z}$-modules. In [5] the author proved that there exists only $(n, 1)_G$ and $(n, n)_G$ MDS codes over a nonabelian group G. It is not difficult to show that an analogue of the extension property holds for these two families of trivial codes.

References

[1] H. Q. Dinh and S. R. López-Permouth, On the equivalence of codes over rings and modules, *Finite Fields and Their Applications*, **10** (2004), 615–625.

[2] H. Q. Dinh and S. R. López-Permouth, On the equivalence of codes over finite rings, *Appl. Algebra Eng., Commun. Comput.*, **15**, 1 (2004), 37–50.

[3] S. Dyshko, On extendibility of additive code isomorphisms, arXiv:1406.1714, (2014).

[4] S. Dyshko, MacWilliams Extension Theorem for MDS additive codes, arXiv:1504.01355, (2015).

[5] G. D. Forney, On the Hamming distance properties of group codes, *IEEE Transactions on Information Theory*, **38**, 6 (1992), 1797–1801.

[6] M. Greferath, A. Nechaev and R. Wisbauer, Finite quasi-frobenius modules and linear codes, *Journal of Algebra and Its Applications*, **3** (2004), 247–272.

[7] S. Lang, *Algebra*. Addison-Wesley series in mathematics. Addison-Wesley Publishing Company, Advanced Book Program, 1984.

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

[9] J. A. Wood, Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities, in *Codes over rings* (Ed. Patrick Sóle), World Scientific Pub. Co. Inc., (2009), 124–190.