On Weight Distributions of Homogeneous Metric Spaces Over GF (p^m) and MacWilliams Identity

Christophe Mouaha and Sélestin Ndjeya

E.N.S. – Département de Mathématiques
B.P. 47 Yaoundé – Cameroun

Abstract

We introduce in this paper the notion homogeneous metric space on the Galois field GF (p^m), where p is a prime natural number. We show that homogeneous weight enumerators of some linear codes over GF (p^m) are Hamming weight enumerators of some of their p-ary images. It is also proved that in some cases, the MacWilliams Identity holds for homogeneous metric spaces.

Keywords: Homogeneous distance, Hamming distance, isometry, p-ary image, MacWilliams Identity.

Introduction

A code of length on a Galois ring Z_p^m or a Galois field GF (p^m) can give a code with longer length nm. Constructing such p-ary images of longer length over GF (p) from codes over GF (p^m) has been intensely studied in [5, 6, 7, 8, 9, 10, 12] among others. The importance of p-ary images in burst-correction and in multilevel communication has also been shown.

In this paper, an upper bound on the Hamming minimum distance of such a code is given. It is also shown that some homogeneous metric spaces over Z_p^m and GF (p^m) have the same weight distributions as their Hamming space p-ary image over GF (p). Consequently the MacWilliams identity holds for some Lee metric spaces.

The plan of this paper is as follows. Section I introduces a homogeneous metric on GF (p^m) from a homogeneous distance on Z_p^m and a one-to-one map of Z_p^m onto GF (p^m). The homogeneous distance defined on GF (p^m) is extended to GF (p^m)^n. Section II gives some properties on Lee weight distributions of some linear codes over GF (p^m) in connection with some of their p-ary images.
Homogeneous metric spaces over $\mathbb{Z}_p^m$ and $GF (p^m)$.

Let $p$ be a prime natural number and let $m$ an integer such that $m \geq 2$. Let $\gamma$ be a one-to-one map of the Galois ring $\mathbb{Z}_p^m$ onto the Galois field $K = GF (p^m)$ of order $p^m$ such that $\gamma (0) = 0$.

The following theorem extended the definition of homogeneous distance to $\mathbb{Z}_p^m$ in general.

**Theorem 1.1** Let $\psi$ be a $GF (p)$ - isomorphism of vectors spaces $GF (p^m)$ onto $GF (p)^m$. If $d_H$ denotes the Hamming distance on $GF (p)^m$ then be the map $\nabla_L$ of $\mathbb{Z}_p^m \times \mathbb{Z}_p^m$ onto the set $\mathbb{N}$ of natural numbers defined by $\nabla_L (u, v) = d_H (\psi (\gamma (u)) , \psi (\gamma (v)))$ is a distance on $\mathbb{Z}_p^m$.

**Proof.** Let $\phi$ be the map of $\mathbb{Z}_p^m \times \mathbb{Z}_p^m$ onto $GF (p^m) \times GF (p^m)$ defined by $\phi (u, v) = (\psi (\gamma (u)) , \psi (\gamma (v)))$. Then $d_H \circ \phi$ is a distance on $\mathbb{Z}_p^m$.

**Definition 1.2.** The distance defined in Theorem 1.1. is called a homogeneous distance on $\mathbb{Z}_p^m$.

The following result defines a homogeneous metric in an extension of a Galois field.

**Theorem 1.2.** Let $\Delta_L$ be the map of $K \times K$ onto the set $\mathbb{N}$ of natural numbers defined by $\Delta_L (u, v) = \nabla_L (\gamma^{-1} (u) , \gamma^{-1} (v))$. Then:

1. $\Delta_L$ is a distance on $K$.
2. $\gamma$ is an isometry of $\mathbb{Z}_p^m$ onto $K$.

**Proof.**

1. $\Delta_L$ is obviously a distance on $K$.
2. Let $u$ and $v$ be two elements of $\mathbb{Z}_p^m$. Then $\Delta_L (\gamma (u) , \gamma (v)) = \nabla_L (\gamma^{-1} (\gamma (u)) , \gamma^{-1} (\gamma (v))) = \nabla_L (u, v)$.

**Definition 1.2.** The distance $\Delta_L$ defined above is called the homogeneous distance on $GF (p^m)$ with respect to $\gamma$.

As we know, $\nabla_L$ can be extended in $(\mathbb{Z}_p^m)^n$, and we can also extend $\Delta_L$ on $K^n$ by the following obvious proposition.

**Proposition 1.1.** Let $n \geq 2$. The map $\Pi_L$ of $K^n \times K^n$ onto $\mathbb{N}$ defined by $\Pi_L ((u_0, u_1, \ldots, u_{n-1}), (v_0, v_1, \ldots, v_{n-1})) = \sum_{0 \leq i \leq n-1} \Delta_L (u_i, v_i)$ is a distance on $K^n$.

**Definition 1.2.** $(K^n, \Pi_L)$ is then called a homogeneous metric space.

Now, set $F = GF (p)$. Let $\varphi$ be an isometry of the homogeneous metric space $(K, \Delta_L)$ onto the Hamming metric space $(F^m, d_H)$.

**Proposition 1.2.** Let $n$ be a natural number, $n \geq 2$. Then the map $\psi$ of $K^n$ onto $F^{mn}$ defined by $\psi ( (u_0, u_1, \ldots, u_{n-1}) ) = (\varphi (u_0) , \varphi (u_1) , \ldots, \varphi (u_{n-1}))$ is an isometry of
On Weight Distributions of Homogeneous Metric Spaces Over $GF(p^m)$

(K^n, $\Pi_L$) onto the Hamming metric space $F^{mn}$.

**Proof.** Since the Hamming weight of $\psi((u_0, u_1, \ldots, u_{n-1}))$ is the sum of the Hamming weights of $\phi(u_i), 0 \leq i \leq m-1$, the result follows from the fact $\phi$ is an isometry of the homogeneous metric space $(K, \Delta_L)$ onto the Hamming metric space $(F^{mn}, d_H)$.

**Example 1.1.** $p=3, m=2$, $GF(9) = GF(3)(\alpha)$ with $\alpha^2 = 1 + 2\alpha$. Let $\gamma$ be the one-to-one of $Z_9$ onto $GF(9)$ defined $\gamma(u_0 + 3u_1) = u_0 + u_1\alpha^2$. For all $u_i$ in $GF(3), 0 \leq i \leq 1$. $B = (1, \alpha)$ is a basis of the $GF(3)$ -algebra $GF(9)$. The map $\phi_B$ of $GF(9)$ onto $GF(3)^2$ defined by $\phi_B(x_0 + x_1\alpha^2) = (x_0 + x_1, 2x_1)$ is an isometry of a Lee metric space $GF(9)$ onto the Hamming metric space $GF(3)^2$, where the homogeneous weight of $u_0 + u_1\alpha^2$ is defined to be the Hamming weight of $\phi_B(u_0\alpha + u_1\alpha^2)$.

**Example 1.2.** $GF(4) = GF(2)(\alpha)$, $B = (1, \alpha)$ is a basis of the $GF(2)$ -algebra $GF(4)$. The map $\phi_B$ of $GF(4)$ onto $GF(2)^2$ defined by $\phi_B(x_0 + x_1\alpha) = (x_0, x_1)$ is an isometry of a homogeneous metric space $GF(4)$ onto the Hamming metric space $GF(2)^2$. Now define the map of $\psi_B$ of $GF(4)^n$ onto $GF(2)^{2n}$ defined by $\psi_B(u_0, u_1, \ldots, u_{n-1}) = (\phi_B(u_0), \phi_B(u_1), \ldots, \phi_B(u_{n-1}))$ is an isometry of $(GF(4)^n, \Pi_L)$ onto the Hamming metric space $GF(2)^{2n}$.

**Homogeneous weight distributions of some linear codes over $GF(p^m)$**

In this paragraph we are going to give an upper bound on the minimum distance of a homogeneous subspace over $GF(p^m)$, and in some cases we describe the weight distribution of such space.

We have the following theorem.

**Theorem 2.1.** Let $C$ be an $(n, k)$ linear code over $GF(p^m)$ and $\phi$ a linear $GF(p)$ -isometry of $(GF(p^m), \Delta_L)$ onto the Hamming metric space $GF(p)^m$. Let $\psi$ be the $GF(p)$ - linear map of $(GF(p^m)^n, \Pi_L)$ onto the Hamming metric space $GF(p)^{mn}$ defined by $\psi((u_0, u_1, \ldots, u_{n-1})) = (\phi(u_0), \phi(u_1), \ldots, \phi(u_{n-1}))$. Then $C$ and $\psi(C)$ have the same weight distribution with respect to $\Pi_L$ and the Hamming distance respectively.

**Proof.** Since $\phi$ is a $GF(p)$ -linear map, it is sufficient to prove that $\psi$ is an isometry of $(GF(p^m)^n, \Pi_L)$ onto the Hamming metric space $GF(p)^{mn}$. Let $u = (u_0, u_1, \ldots, u_{n-1})$ be an element of $GF(p^m)^n$. Then the result follows from the fact the homogeneous weight $\psi(u)$ is equal to the sum of Hamming weights of $\phi(u_i), 0 \leq i \leq m-1$.

**Theorem 2.2.** Let $B$ be a $GF(p)$ -basis of $GF(p^m)$ and $\phi_B$ a $GF(p)$ - isomorphism of $GF(p^m)$ onto $GF(p)^m$. Let $\psi_B$ be the map of $GF(p^m)^n$ onto $GF(p)^{mn}$ defined by $\psi_B(u_0, u_1, \ldots, u_{n-1}) = (\phi_B(u_0), \phi_B(u_1), \ldots, \phi_B(u_{n-1}))$. Assume that $\phi_B$ is an isometry of $(GF(p^m), \Delta_L)$ onto the Hamming metric space $GF(p)^m$. Let $C$ be an $(n, k)$ linear
code over GF ($p^m$). If $\psi_B(C^\perp) = \psi_B(C)^\perp$, then the MacWilliams Identity holds for weight enumerator polynomials of homogeneous metric spaces $C$ and $C^\perp$.

**Proof.** Assume that $\psi_B(C^\perp) = \psi_B(C)^\perp$. Then $C$ as a homogeneous metric space and $\psi_B(C)$ as a Hamming metric space have the same weight distribution. In the same manner, $C^\perp$ as a Lee metric space and $\psi_B(C^\perp)$ as a Hamming metric space have the same weight distribution. The result follows that the MacWilliams identity holds for $\psi_B(C)$ and $\psi_B(C)^\perp$.

**Remark 2.1.** If $C$ is an $(n, k)$ linear code over GF ($p^m$) with no generator matrix over GF ($p$) then the assumption $\psi_B(C^\perp) = \psi_B(C)^\perp$ occurs when $B$ is such that the matrix representation of GF ($p^m$) with respect to $B$ is a symmetric one [5].

**Corollary 2.1.** Let $C$ be a linear code over GF ($p^m$) with minimum Hamming weight $d$. Then the minimum distance $d'$ of the Lee metric subspace $C$ of ($GF(p^m), \Pi_L$) verifies $d' \leq m(d-1)+1$.

**Proof.** The result follows by Theorem 2.2., since the Hamming minimum distance $d'$ of $\psi_B(C)$ verifies $d' \leq m(d-1)+1$.

**Theorem 2.3.** Let $A$ be a code of length $n$ over $Z_{pm}$ and $\gamma$ be a one-to-one map of $Z_{pm}$ onto $GF(p^m)$ such that $\gamma(0) = 0$. If $\gamma(A)$ is a linear code over GF ($p^m$) with minimum Hamming distance $d$, then the homogeneous minimum distance $d'$ of $A$ verifies $d' \leq m(d-1)+1$.

**Proof.** Let $\Delta_L$ be the map of GF ($p^m$) x GF ($p^m$) onto the set $\mathbb{N}$ of natural numbers defined by $\Delta_L(u, v) = \delta_L(\gamma^{-1}(u), \gamma^{-1}(v))$. Then $\Delta_L$ is a homogeneous metric on GF ($p^m$) and is an isometry of ($Z_{pm}, \Pi$) onto the Hamming metric space GF ($p^m$) $n$. Since there is a linear GF ($p$) -isometry $\varphi$ of the homogeneous space GF ($p^m$) onto the Hamming metric space GF ($p^m$) $\mathbb{N}$, let us define the map $\psi$ of GF ($p^m$) $n$ onto GF ($p^m$) $\mathbb{N}$ defined by $\psi(u_0, u_1, \ldots, u_{n-1}) = (\varphi(u_0), \varphi(u_1), \ldots, \varphi(u_{n-1}))$ is an isometry of ($GF(p^m)^n, \Pi_L$) onto the Hamming metric space $F^m$. Hence the Hamming minimum weight $d'$ of $\psi(\gamma(A))$ verifies $d' \leq m(d-1)+1$. The result follows by Corollary 2.1.

The following example illustrates Theorems 2.2 and 2.3.

**Example 3.1.** $GF(4) = GF(2)(\alpha)$, $B= (1, \alpha)$ is a basis of the GF (2) -algebra GF (4). The map $\varphi_B$ of GF (4) onto GF (2) $^2$ defined by $\varphi_B(x_0+x_1\alpha) = (x_0, x_1)$ is an isometry of a homogeneous metric space GF (4) onto the Hamming metric space GF (2) $^2$. Now define the map of $\psi_B$ of GF (4) $^4$ onto GF (2) $^8$ by $\psi_B(u_0, u_1, \ldots, u_7) = (\varphi_B(u_0), \varphi_B(u_1), \ldots, \varphi_B(u_7))$. Then $\psi_B$ is an isometry of (GF (4) $^n, \Pi_L$) onto the Hamming metric space GF (2) $^8$. Let RS$^5$ be the extended (4, 2, 3) self-dual Reed-Solomon code
over GF(4). Then $\psi_B(RS^6)$ is the binary $(8, 4, 4)$ self-dual code with all its Hamming weights multiple of 4. Therefore $RS^6$ has also its Lee weights all multiple by 4. Now let $\eta$ be the one-to-one map of $\mathbb{Z}_4$ onto GF(4) defined by $\eta(0)=0$, $\eta(1)=\alpha$, $\eta(2)=\alpha^2$ and $\eta(3)=1$. So $\eta^{-1}(RS^6)$ is a non-linear code over $\mathbb{Z}_4$ with all its homogeneous weights multiple of 4.

**Conclusion**

We have shown in this paper that a homogeneous metric on $\mathbb{Z}_{p^m}$ can give rise to a homogeneous metric over GF($p^m$) that can be extended on GF($p^m$). With the materials developed in this paper, we know that, in some cases, a homogeneous weight enumerator of a linear code over GF($p^m$) is exactly the Hamming weight enumerator of one of its $p$-ary image.

**References**


