Global Journal of Mathematical Sciences: Theory and Practical.
ISSN 0974-3200 Volume 4, Number 2 (2012), pp. 159-164

http://www.irphouse.com

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_pm 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 intensevely 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_pm 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_pm and a one-to-one map of Z_pm 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 Z_pm and GF (p^m).

Let p be a prime natural number and let m an integer such that m≥2. Let γ be a one-to-one map of the Galois ring Z_pm onto the Galois field K= GF (p^m) of order p^m such that γ (0) =0.

The following theorem extended the definition of homogeneous distance to Z_pm. in general

Theorem 1.1 Let ψ 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 ∇_L of Z_pm x Z_pm onto the set ℕ of natural numbers defined by ∇_L (u, v) = d_H (ψ (γ (u)) , ψ (γ (v))) is a distance on Z_pm.

Proof. Let ϕ be the map of Z_pm x Z_pm onto GF (p^m) x GF (p^m) defined by ϕ (u, v) = (ψ (γ (u)) , ψ (γ (v))). Then $d_H O\phi$ is a distance on Z_pm.

Definition 1.2. The distance defined in Theorem 1.1. is called a homogeneous distance on Z_pm.

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

Theorem 1.2. Let Δ_L be the map of KxK onto the set ℕ of natural numbers defined by Δ_L (u, v) = ∇_L (γ^{-1} (u) , γ^{-1} (v)).Then:

1. Δ_L is a distance on K
2. γ is an isometry of Z_pm onto K.

Proof.

1. Δ_L is obviously a distance on K.
2. Let u and v be two elements of Z_pm. Then Δ_L (γ (u) , γ (v)) = ∇_L (γ^{-1} (γ (u)) , γ^{-1} (γ (v))) = ∇_L (u, v).

Definition 1.2. The distance Δ_L defined above is called the homogeneous distance on GF (p^m) with respect to γ.

As we know, ∇_L can be extended in $(Z_pm)^n$, and we can also extend Δ_L on K^n by the following obvious proposition.

Proposition 1.1. Let n≥2. The map Π_L of $K^n x K^n$ onto ℕ defined by

Π_L ((u_0, u_1, …, u_{n-1}) , (v_0, v_1, …, v_{n-1})) = $\sum_{0 \le i \le n-1} \Delta_L$ (u_i, v_i) is a distance on K^n.

Definition 1.2. (K^n, Π_L) is then called a homogeneous metric space.

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

Proposition 1.2. Let n be a natural number, n≥2. Then the map ψ of K^n onto F^{mn} defined by ψ ((u_0, u_1, …, u_{n-1})) = (φ (u_0) , φ (u_1) , …., φ (u_{n-1})) is an isometry of

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

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

Example 1.1. p=3, m=2, GF (9) =GF (3) (α) with $\alpha^2=1+2\alpha$. Let γ be the one-to-one of Z_9 onto GF (9) defined γ (u_0+3u_1) = $u_0+u_1\alpha^2$, For all u_i in GF (3) , $0 \leq i \leq 1$. B= (1, α) is a basis of the GF (3) -algebra GF (9). The map φ_B of GF (9) onto GF (3) ^{2} defined by φ_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 φ_B ($u_0\alpha+u_1\alpha^2$).

Example 1.2. GF (4) = GF (2) (α) , B= (1, α) is a basis of the GF (2) -algebra GF (4). The map φ_B of GF (4) onto GF (2) ^{2} defined by φ_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 ψ_B of GF (4) ^{n} onto GF (2) ^{2n} defined by ψ_B (u_0, u_1, …, u_{n-1}) = (φ_B (u_0) , φ_B (u_1) , …., φ_B (u_{n-1})) is an isometry of (GF (4) ^{n}, Π_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 φ a linear GF (p) -isometry of (GF (p^m) , Δ_L) onto the Hamming metric space GF (p) ^{m}. Let ψ be the GF (p) - linear map of (GF (p^m) ^{n}, Π_L) onto the Hamming metric space GF (p) ^{mn} defined by ψ ((u_0, u_1, …, u_{n-1})) = (φ (u_0) , φ (u_1) , …., φ (u_{n-1})). Then C and ψ (C) have the same weight distribution with respect to Π_L and the Hamming distance respectively.

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

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

Proof. Assume that ψ_B ($C^\perp$) = ψ_B (C) $^\perp$. Then C as a homogeneous metric space and ψ_B (C) as a Hamming metric space have the same weight distribution. In the same manner, $C^\perp$ as a Lee metric space and ψ_B ($C^\perp$) as a Hamming metric space have the same weight distribution. The result follows that the MacWilliams identity holds for ψ_B (C) and ψ_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 ψ_B ($C^\perp$) = ψ_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) ^{n}, Π_L) verifies d'≤ m (d-1) +1.

Proof. The result follows by Theorem 2.2., since the Hamming minimum distance d' of ψ_B (C) verifies d'≤ m (d-1) +1.

Theorem 2.3. Let A be a code of length n over Z_pm and γ be a one-to-one map of Z_pm onto GF (p^m) such that γ (0) =0. If γ (A) is a linear code over GF (p^m) with minimum Hamming distance d, then the homogeneous minimum distance d' of A verifies d'≤ m (d-1) +1.

Proof. Let Δ_L be the map of GF (p^m) x GF (p^m) onto the set $\mathbb{N}$ of natural numbers defined by Δ_L (u, v) = δ_L (γ^{-1} (u) , γ^{-1} (v)). Then Δ_L is a homogeneous metric on GF (p^m) and is an isometry of (Z_pm) ^{n} onto the Hamming metric space GF (p^m) ^{n}. Since there is a linear GF (p) -isometry φ of the homogeneous space GF (p^m) onto the Hamming metric space GF (p) ^{m}, let us define the map ψ of GF (p^m) ^{n} onto GF (p) ^{mn} defined by ψ (u_0, u_1, …, u_{n-1}) = (φ (u_0) , φ (u_1) , …., φ (u_{n-1})) is an isometry of (GF (p^m) ^{n}, Π_L) onto the Hamming metric space F^{mn}. Hence the Hamming minimum weight d' of ψ (γ (A)) verifies d'≤ m (d-1) +1. The result follows by Corollary 2.1. and the fact that γ (A) as a homogeneous metric space and ψ (γ (A) as a Hamming metric space have the same minimum distance.

The following example illustrates Theorems 2.2 and 2.3.

Example 3.1. GF (4) = GF (2) (α) , B= (1, α) is a basis of the GF (2) -algebra GF (4). The map φ_B of GF (4) onto GF (2) ^{2} defined by φ_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 ψ_B of GF (4) ^{4} onto GF (2) ^{8} by ψ_B (u_0, u_1, …, u_7) = (φ_B (u_0) , φ_B (u_1) , …., φ_B (u_7)). Then ψ_B is an isometry of (GF (4) ^{n}, Π_L) onto the Hamming metric space GF (2) ^{8}. Let RS^e be the extended (4, 2, 3) self-dual Reed-Solomon code over GF (4). Then ψ_B (RS^e) is the binary (8, 4, 4) self-dual code with all its Hamming weights multiple of 4. Therefore RS^e has also its Lee weights all multiple by 4. Now let η be the one-to-one map of Z_4 onto GF (4) defined by η (0) =0, η (1) = α, η (2) = α^2 and η (3) =1. So η^{-1} (RS^e) is a non linear code over Z_4 with all its homogeneous weights multiple of 4.

Conclusion

We have shown in this paper that a homogeneous metric on Z_pm can give rise to a homogeneous metric over GF (p^m) that can be extended on GF $(p^m)^{\ n}$. 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

[1] Astola J., "An Elias-type bound for Lee codes over large alphabets and its application to perfect codes", Information Theory, IEEE Transactions on, Vol. 28, Issue:1 pp.111- 113, (1982)..

[2] Bonnecaze A. and Solé P., "Quaternary constructions of formally self-dual binary codes and unimodular lattices ", Lecture Notes in Computer Science, Vol.781, pp.194-205, (1993)

[3] Byrne, E. " Decoding a class of Lee metric codes over a Galois ring", Information Theory, IEEE Transactions on, Volume 48, Issue 4, pp:966 – 975 (2002).

[4] Galand, F. « On the Minimum Distance of Some Families of ℤ2k-Linear Codes », Lecture Notes in Computer Science, Vol. 2643, pp. 603 (2003).

[5] Mouaha C., “ On q-ary images of self-dual codes”, AAECC3, Springer-Verlag, N°4, pp;311-319 (1992).

[6] Mouaha C. and Schiffels G., “ All qm-ary cyclic codes with cyclic q-ary image are known”, Designs, Codes and Cryptography, vol. 23, pp. 81 – 98, May 2001

[7] Patrice Rabizzoni, “Relation between the minimum weight of a linear code over GF (qm) and its q-ary image over GF (q) ”, Springer Lect. Notes in Comp. Sc. Vol.388, pp. 209-212 (1988).

[8] Rabizzoni P. “Relation between the minimum weight of a linear code over GF (qm) and its q-ary image over GF (q) ”, Springer Lect. Notes in Comp. Sc. Vol.388, pp. 209-212 (1988).

[9] Solé P. and Sison V., “ Bounds on the minimum homogeneous distance of the pr-ary image of linear block codes over the Galois ring GR (pr, m) , IEEE Transactions on Information Theory, IT-53, pp. 2270-2274 (2007).

[10] Wolfmann J., "Binary Images of Cyclic Codes over Z4", IEEE Trans. Inform. Theory, vol. 47, pp. 1773-1779, 2001.

[11] Wolfmann J., "Difference Sets in (Z4) m and (F2) 2m ", Designs, Codes and Cryptography, 20, 73-88, 2000.

[12] Wolfmann J., "Negacyclic and Cyclic Codes over Z4", IEEE Trans. Inform. Theory, vol.45, n°5, pp. 2527-2532, 1999.