Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 7, Number 3 (2011), pp. 319-324

http://www.ripublication.com/gjpam.htm

On MDS Q-ary Images Codes Over GF(q)

Christophe Mouaha and Sélestin Ndjeya

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

Abstract

Maximum distance separable (MDS) codes have properties that give them excellent error correcting capabilities. In this paper we give an upper bound of the minimum (Hamming) distance of the q-ary images of a linear code over an extension field of a Galois field. This new bound is, in some cases, better than the one of P. Rabizzoni [5], [6]. Using this bound we show that, there are only up to equivalence of linear codes, two MDS codes over GF(3) which are ternary images of linear codes over GF(9).

Index Terms: Linear code, q-ary image, MDS code, Hamming distance, matrix representation.

Introduction

Let n and k be positive integers. Let C be an (n,k,d) linear code over GF(q), where $d = \min\{d_H(x,y): x,y \in C, x \neq y\}$, and $d_H(x,y)$ denotes the Hamming distance between x and y. The minimal distance always satisfies the Singleton bound, $d \leq n-k+1$. Linear codes C with minimal distance $d= n-k+1$ are called maximum distance separable (MDS) codes and these codes are systematic ones and are of great interest for the reason that they have the greatest error correcting capability.

The use of matrix representations of $GF(q^m)$ in the study of q-ary images has been intensively developed in [2]. This matrix description will be of great help in the study of MDS codes which are q-ary images.

In this paper we investigate the question when a q-ary image of a linear code is an MDS code. This question is a bit related to matrix representation of $GF(q^m)$. We prove that, up to equivalence of linear codes, there are only two MDS codes over GF(3) which are ternary images of linear codes over GF(9). The plan of this paper is as follows Section 2 gives some preliminaries in q-ary images and matrix representations of finite fields. Section 3 gives an upper bound of parameters of a linear code to have MDS q-ary image.

Preliminaries

Let m be an integer, m≥2, and let B = (b_0, b_1,...,b_{m-1}) be a basis of K = GF(q^m) over F = GF(q). Let n be another integer such that n≥2 and £$_B$ be the map from K^n to F^{nm} defined by

$$£_B((x_1,...,x_n)) = (..., x_{i0}, ..., x_{im-1}, ...),$$

where for all 1≤ i≤ n, $x_i = x_{ij}b_j$, for some $x_{ij} \in F$, 1≤i≤n, 0≤j≤ m-1. Clearly £$_B$ is an isomorphism of F-vector spaces [1], [2], [4]. If C is an (n,k) linear code over K then £$_B$(C) is an (nm,mk) linear code over F and this code is called the q-ary image of C with respect to B. Let a∈K and μ_a be the F- endomorphism of K defined by $\mu_a(x) = ax$. Let M_a be the matrix of μ_a with respect to B. In [2], it is shown that the F-algebras K, and are isomorphic, and is called the matrix representation of K over F with respect to the basis B. This matrix representation is very useful in the q-ary image theory [2].

Proposition 2.1. Let C be an (n,k) linear code over K = GF(q^m) and let B = (b_0, b_1,...,b_{m-1}) be a basis of K over F .The following statements are equivalent:

1. G =(g_{ij}) is a generator matrix of C over K
2. G'=(Mg_{ij}) is a generator matrix of £$_B$(C) over F, where for all 0 ≤ i≤m-1, Mg_{ij} is the matrix of μ_{gij} with respect to B.

The following result is a direct consequence of Proposition 2.1.

Corollary. 2.1. Let C be an (n,k) linear code over K = GF(q^m) and let B = (b_0, b_1,...,b_{m-1}) be a basis of K over F .The following statements are equivalent:

1. C is a systematic code
2. £$_B$(C) is a systematic code.

Proof. The result follows from the fact that if C has a generator matrix [I_k A], then £$_B$(C) has as generator matrix [I_{mk} A'], where A =(a_{ij}) and A'=(Ma_{ij}) with Ma_{ij} the matrix of μa_{ij} with respect to B, for all 0 ≤ i≤m-1.

An upper minimum bound of q-ary images codes

In this section, we give a new bound on the minimum (Hamming distance) of a q-ary image of a linear code over an extension of a Galois field.

Now, for a basis B= (b_0, b_1, …, b_{m-1}) of IL= GF(q^m) over IMI= GF(q), we define the map h_B of IL^n into IMI^{nm} by $h_B(\underline{c}_0b_0+\underline{c}_1b_1+…+\underline{c}_{m-1}b_{m-1}) = (\underline{c}_0, \underline{c}_1,…, \underline{c}_{m-1})$, where for all 0 ≤ i≤m-1, $\underline{c}_i \in IMI^n$. The fundamental properties of h_B are studied in [3]. If C is a linear code over IL, £$_B$(C and h_B(C) are equivalent codes in the sense that there is an nm by nm monomial matrix over MI transforming h_B(C) to £$_B$(C).

Theorem 3.1. Let C be a linear code over with minimum (Hamming) distance d. Let B=(b_0,b_1,…,b_{m-1}) be a basis of GF(q^m) over GF(q). Then the minimum distance d' of

$£_B(C)$ verifies

$$d' \leq m(d-1)+1.$$

Proof. There is a codeword u of C with minimum (Hamming) distance d. Let ω be a nonzero component of u. Then $W_H(£_B(b_0\omega^{-1}u)) \leq m(d-1)+1$.

Corollary 3.1. Let C be a linear code over $GF(q^m)$, having a minimum (Hamming) distance d. Let e and e' be correction capabilities of C and $£_B(C)$ respectively. Then

$$e \leq e' \leq \lfloor \rfloor$$

Proof. The result follows by Theorem 3.1. and the fact that d≤ d', where is the minimum weight of $£_B(C)$.

Theorem 3.2.(Rabizzoni, 1988). Let C be an (n, k) linear code over $GF(q^m)$, with minimum (Hamming) distance d, and d' the minimum (Hamming) distance of the q-ary image of C with respect to a basis $B=(b_0, b_1,\ldots,b_{m-1})$ of $GF(q^m)$ over GF(q). Then

$$d' \leq \lfloor \rfloor.$$

Proof [5].

Theorem 3.3. Let m, d and q be positive integers. Then

$$m(d-1)+1 - \leq 0 \Leftrightarrow d \leq$$

Proof. We have

$$m(d-1)+1 - = md\ () - (m-1)$$

$$= md - (m-1) \text{ . Therefore}$$

$$md - (m-1) \leq 0 \Leftrightarrow d \leq$$

Corollary 3.2. The bound of Theorem 3.1. is better than the Rabizzoni's one if and only if

$$d \leq \lfloor \rfloor.$$

Proposition 3.1. Let C be an (n, k, d) linear code over $GF(q^m)$ and B a basis of $GF(q^m)$ over GF(q). If $h_B(C)$ is an MDS code then C is also an MDS code.

Proof. Assume that C is not an MDS code. Then by Singleton bound d< n-k+1. Therefore by Theorem 3.1. d' < m(n-k)+1, which shows that $h_B(C)$ is not an MDS code.

Proposition 3.2. Let C be an (n, k) linear code over $GF(q^m)$, m≥2, such that $£_B(C)$ is a MDS code, for some basis B of $GF(q^m)$ over GF(q). Let u be a codeword u of C of weight n-k+1. Then the number r of non-zero components of u that are GF(q)-

multiples of elements of B verifies $r \in \{0,1\}$.

Proof. Since $£_B(C)$ is a MDS code then by Proposition 3.1. C is also MDS. Now assume that there is a codeword u of C of weight n-k+1 having r non-zero components that are GF(q)-multiples of elements of B. By Theorem 3.1 we obtain $m(n-k)+1 \leq r+ m(n-k+1-r)$ .Therefore $r(m-1) \leq m-1$. The result follows from the fact that $m \geq 2$.

Remark 3.1. If C is a linear code over $GF(q^m)$, we can observe that:

i. In the case of m=2, the bound of Corollary 3.2. becomes d ≤;
ii. if $h_B(C)$ is an MDS code over GF(q), then the bound of Theorem 3.1. is attained;
iii. For all non zero element σ of $GF(q^m)$, $h_B(C) = h_{\sigma B}(C)$.

The following result follows from Theorem 3.2. and Proposition 3.1.

Proposition 3.3. Let C be an (n, k) MDS code over $GF(q^m)$ such tat its q-ary image with respect to a basis B of $GF(q^m)$ over GF(q) is an MDS code. Then

n-k+1 ≤.

Proof. Since a q-ary image of C is an MDS code, then by Rabizzoni's bound

m(n-k)+1 ≤. Then we obtain

n-k+1 ≤.

Remark 3.2. The only linear code over $GF(q^m)$ with a generator matrix over GF(q) and having a q-ary image MDS is the whole space. Therefore if C is an (n, k) linear code over $GF(q^m)$ with k≤n-1, then

2 ≤ n-k+1 ≤.

The following result is a direct consequence of Proposition 3.1.

Corollary 3.3. Let C be an (n, k) MDS code over $GF(q^2)$ such tat its q-ary image with respect to a basis B of $GF(q^2)$ over GF(q) is an MDS code, and k≤n-1. Then

2 ≤ n-k+1 ≤.

Remark 3.3. If C be an (n, k) MDS code over GF(9) such tat its ternary image with respect to a basis B of GF(9) over GF(3) is an MDS code, and k≤n-1. Then n=k+1.

The following result gives an upper bound on the dimension of linear code having a q-ary image MDS.

Proposition 3.4. Let C be an (n, k) linear code over $GF(q^m)$ with k≤ n-1 and having a q-ary image MDS. Then

$k \leq -m$.

Proof. Since C has a q-ary image MDS with respect to a basis B of $GF(q^m)$ over GF(q), then C itself is MDS. Therefore C has a generator systematic matrix, $[I_k\ A]$. Let's define on the set of nonzero elements of $GF(q^m)$ the equivalence relation"x is related to y if and only if there is $\lambda \in GF(q)$ such that $y=\lambda x$". The number of equivalence classes modulo the relation defined above is. Since B is a basis of $GF(q^m)$ over GF(q), two different elements of B are not related through the relation defined above. If two elements of the same line or the same column of A are related to each other then there is a 2x2 submatrix of A which is not invertible. If $k \geq -m+1$, there is a coefficient of A say γ which is related to an element of B. Now let us consider the automorphism μ_γ of the GF(q) vector $GF(q^m)$ defined by $\mu_\gamma(x)=\gamma x$. Therefore the matrix of μ_γ with respect to B has at least one zero component. So the q-ary image of C with respect to B is not an MDS code.

We have the following proposition.

Proposition 3.5. Let λ and γ be two elements of $GF(q^2)$ such that $B=(1,\lambda)$ and $B'=(1,\gamma)$ are GF(q) basis of $GF(q^2)$. Let C and C' be linear codes over $GF(q^2)$ generated by $=(1,\lambda)$ and $(1,\gamma)$ respectively. Then $£_{B'}(C)$ MDS if and only $£_B(C')$ MDS.

Proof. There are $\lambda_0,\lambda_1,\gamma_0,\gamma_1$ in GF(q) such that $\lambda=\lambda_0+\lambda_1\gamma$ and $\lambda\gamma=\gamma_0+\gamma_1\gamma$. Consider now the matrix M_λ of μ_λ with respect to B'. Since a generator matrix of $£_{B'}(C)$ is $[I_2\ M_\lambda]$, then $£_{B'}(C)$ is MDS if and only if $\lambda_0,\lambda_1,\gamma_0,\gamma_1$ and $\lambda_0\gamma_1-\lambda_1\gamma_0$ are nonzero elements of $GF(q^2)$. In that case, we also obtain $\gamma=\lambda_1^{-1}(-\lambda_0+\lambda)$ and $\lambda\gamma=\lambda_1^{-1}(\lambda_1\gamma_0-\gamma_1\lambda_0+\gamma_1\lambda)$. Consider the matrix N_γ of μ_γ with respect to B. Then a generator matrix of $£_B(C')$ is $[I_2\ N_\gamma]$. The result follows from the fact that $\lambda_0,\lambda_1,\gamma_0,\gamma_1$ and $\lambda_0\gamma_1-\lambda_1\gamma_0$ are nonzero elements of $GF(q^2)$.

The following result gives all linear codes over GF(9) with MDS images in GF(3).

Theorem 3.4. Let $GF(9) = GF(3)(\alpha)$, $\alpha^2=1+2\alpha$. The only non trivial linear (n, k) MDS code over GF(9) with ternary MDS image with respect to a basis B of GF(9) over GF(3) are the following C_i codes, $1 \leq i \leq 4$, generated respectively by $(1,\alpha^2)$,$(1,\alpha)$, $(1,\alpha^3)$ and $(1,\alpha^2)$ with to $B_1=(1,\alpha)$, $B_2=(1,\alpha^2)$, $B_3=(1,\alpha^2)$ and $B_4=(1,\alpha^3)$.respectively.

Proof. Let a and b be two elements of $\{\alpha,\alpha^2,\alpha^3\}$, and let M_a and M_b be matrix representations of a and b respectively with respect to a basis B of GF(9) over GF(3), where B is an element $\{(1,\alpha),(1,\alpha^2),(1,\alpha^3)\}$. Let C be a (3,2,2) linear code over GF(9) with generator matrix $[I_2\ A]$, Where $A=(a;b)$. Then the matrix $(M_a;M_b)$ has either a zero coefficient or one can extract from it a 2x2 submatrix which is not invertible. This shows that there is no (3,2,2) linear code over GF(9) with ternary MDS image.

By Theorem 3.4., we have the following result.

Corollary.3.4. There are only , up to equivalence of linear codes, two MDS codes over GF(3) which are ternary images of linear codes over GF(9).

Proof. The ternary images of linear codes C_1, C_2 and C_3 generated respectively $(1,\alpha^2)$, $(1,\alpha)$ and $(1,\alpha^3)$ with respect to $B_1=(1,\alpha)$, $B_2=(1,\alpha^2)$ and $B_3=(1, \alpha^2)$ respectively are equivalent codes. The ternary image of the linear code C_4 generated by $(1,\alpha^2)$ with respect to $B_4=(1, \alpha^3)$ is not equivalent to the MDS ternary images of codes mentioned above.

We know by [1] that a $£_B$ –q-ary image of a linear code C over $GF(q^2)$ is cyclic if and only if C is cyclic. The following result is immediate by Corollary 3.4.

Corollary 3.5. There is no cyclic $£_B$ –ternary MDS image of a linear code over GF(9).

Conclusion

In this correspondence we have given bounds on parameters of a linear code to have an MDS q-ary image. We have also determine all MDS ternary images of linear codes over GF(9). But the complete problem is still unsolved and that problem is the characterization and the determination of the number of MDS q-ary images over GF(q) of MDS codes over $GF(q^m)$.

References

[1] C. Mouaha,"On cyclic codes which are q-ary images of linear codes", AAECC2, Springer-Verlag, pp.163-170 (1992).

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

[3] Christophe Mouaha,"A description of q-ary images of quasi-cyclic codes", African Journal of Pures and Applied Mathematics, vol.2, N°1,pp.37-61 (1998).

[4] Christophe Mouaha and Gerhard Schiffels,"All q^m-ary cyclic codes with cyclic q-ary image are known", Designs, Codes and Cryptography, vol. 23, pp. 81 – 98, May 2001.

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

[6] Patrick Solé and Virgilio Sison,"Bounds on the minimum homogeneous distance of the p^r-ary image of linear block codes over the Galois ring $GR(p^r,m)$, IEEE Transactions on Information Theory, IT-53, pp. 2270-2274 (2007).