NEW METRICS ON LINEAR CODES OVER $\mathbb{F}_q[u]/(u^t)$

Ricardo Alfaro[1]

December, 2007

Abstract

We define new metrics for linear codes over the ring $\mathbb{F}_q[u]/(u^t)$ via an $\mathbb{F}_q$-module monomorphism on linear codes over $\mathbb{F}_q$. The construction generalizes the Gray map, Gray weight, and Lee weight; and the technique allows us to find some new optimal linear codes and their weight enumerator polynomial.

Keywords: *Linear Codes, Gray map, Codes over Rings.*

1. *Department of Mathematics, University of Michigan-Flint, USA.*

The study of linear codes over rings, rather than the field of q elements $\mathbb{F}_q$, has proven to be very important, getting some insight into optimal nonlinear codes. In particular, the ring $\mathbb{F}_2 + u\mathbb{F}_2$ has been extensively studied. Bachoc, in [1] has studied self-dual codes over $\mathbb{F}_3 + u\mathbb{F}_3$, and, Gulliver and Harada [2] found good examples of ternary codes over $\mathbb{F}_q3$ using a particular type of *Gray map.* Siap and Ray-Chaudhuri in [3] established a relation between codes over $\mathbb{F}_u/(u^2 - a)$ and codes over $\mathbb{F}_q$, which was used to obtained new codes over $\mathbb{F}_q3$ and $\mathbb{F}_q5$. In this paper we present a generalization of the method used in [2] and [3], defining a family of metrics for linear codes over $\mathbb{F}_q[u]/(u^t)$ and obtaining as particular examples the *Gray map,* the *Gray weight,* the *Lee weight* and some other optimal q-ary codes.

Codes over $\mathbb{F}_q[u]/(u^t)$

A linear q-ary $[n,k]$-code C is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of C are called codewords and their *Hamming weight* $w_H(x)$ is the number of nonzero components of x. The *Hamming distance* $d(x,y)$ between two codewords is the Hamming weight of their difference, $d(x,y) = w_H(x-y)$. The minimum Hamming distance d of the code C is the minimum of all distances between distinct codewords. A linear q-ary $[n,k,d]$-code C is an $[n,k]$-code with minimum Hamming distance d. The Hamming weight enumerator is the polynomial $\sum_{x\in C} y^{w_H(x)}$.

We consider the commutative ring $R(q,t) := \mathbb{F}_q[u]/(u^t)$, which q^t elements can be represented as polynomials in the indeterminate u of degree less or equal to $(t-1)$ with coefficients in $\mathbb{F}_q$, and use the notation $R(q,t) = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q + \cdots + u^{t-1}\mathbb{F}_q$. We also use the u-ary coefficient representation of the finite ring $R(q,t)$ as an $\mathbb{F}_q$-vector space. A *linear code C* over $R(q,t)$ of length n is a left $R(q,t)$-submodule of $R(q,t)^n$.

Let $B \in M_t(\mathbb{F}_q)$ be an invertible $t \times t$ matrix, and let $\alpha_B : R(q,t) \to \mathbb{F}_q^t$ act as the right multiplication by B on $R(q,t)$ (seen as $\mathbb{F}_q$-vector space.) Thus, α_B is an $\mathbb{F}_q$-module isomorphism.

We extend the map α_B linearly to the $\mathbb{F}_q$-module $(R(q,t))^n$, by concatenation of the images: $\phi_B : (R(q,t))^n \rightarrow (\mathbb{F}_q)^{tn}$ is given by

$$\phi_B(x_1, x_2, \ldots, x_n) \quad = \quad (\alpha_B(x_1), \alpha_B(x_2), \ldots, \alpha_B(x_n))$$

and it follows that ϕ_B is an $\mathbb{F}_q$-module monomorphism. An easy counting argument proves that ϕ_B is an isomorphism and:

Lemma 1 *If C is a linear code over $R(q,t)$ of length n, then $\phi_B(C)$ is a linear q-ary code of length tn.*

EXAMPLE 1 Consider ternary codes $q = 3$, and $t = 2$, the ring $R(3,2) = \mathbb{F}_q 3 + u\mathbb{F}_q 3$ with $u^2 = 0$. This ring was considered by Bachoc [1]. Choosing $B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ which is invertible over $\mathbb{F}_q 3$ we obtained the *Gray map* $\phi_B : (\mathbb{F}_q 3 + u\mathbb{F}_q 3)^n \rightarrow \mathbb{F}_q 3^{2n}$ with

$$\alpha_B(a + ub) = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b & a+b \end{pmatrix}.$$

Which is the Gray map used by Gulliver and Harada in [2].

The lemma above gives the relation between the lengths of the codes C (over $R(q,t)$) and the code $\phi_B(C)$ (over $\mathbb{F}_q$.) We use the matrix B to define a new metric in the code C and analyze what is the relation between the minimum distances of these codes.

Definition 1 *Let C be a linear code over $R(q,t)$. Let B be an invertible matrix in $M_t(\mathbb{F}_q)$, and let ϕ_B be the corresponding map. The B-weight of an element $x \in R(q,t)$, $w_B(x)$, is defined as the Hamming weight of $\alpha(x)$ in $(\mathbb{F}_q)^t$. Also, the B-weight of a codeword $(x_1, \cdots, x_n) \in C$ is defined as:*

$$w_B(x_1, \cdots, x_n) \quad = \quad \sum_{i=1}^{n} w_B(x_i)$$

Similarly, the B-distance between two codewords in C is defined as the B-weight of their difference, and the B-distance, d_B of the code C is defined as the minimal B-distance between any two distinct codewords.

Example 2 Following the example above, the corresponding *B-weight* of an element of $\mathbb{F}_q3 + u\mathbb{F}_q3$ is given by:

$$w_B(x) = w_B(a+ub) = w_B(\alpha(a+ub)) = w_H(b, a+b) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x = 1, 2, 2+u, 1+2u \\ 2 & \text{otherwise} \end{cases}$$

which coincide with the *Gray weight* given in [2].

Example 3 Consider the matrix $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, the corresponding *B-weight* of an element of $\mathbb{F}_2 + u\mathbb{F}_2$ is given by:

$$w_B(x) = w_B(a+ub) = w_H(\alpha(a+ub)) = w_H(a+b, b) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x = 1, 1+u \\ 2 & \text{if } x = u \end{cases}$$

The *B-weight* coincides with the known *Lee weight* w_L for codes over $\mathbb{F}_2 + u\mathbb{F}_2$.

As a direct consequence of the definition, the map ϕ_B preserves weights and distances:

Lemma 2 *Let C be a linear code over R(q, t), let B be an invertible matrix over $M_t(\mathbb{F}_q)$. The corresponding map ϕ_B preserves weights and distances between codewords.*

Proof. It follows as a direct consequence of ϕ_B being an $\mathbb{F}_q$-module homomorphism. We have:

$$w_B(x) = \sum_{i=1}^{n} w_H(\alpha(x_i)) = w_H(\alpha(x_1), \alpha(x_2), \cdots, \alpha(x_n)) = w_H(\phi_B(x))$$

and

$$d_B(x,y) = w_B(x-y) = w_H(\phi_B(x-y)) = w_H(\phi_B(x) - \phi_B(x)) = d(\phi_B(x), \phi_B(y)).$$

■

For linear codes the minimum weight of a code coincide with the minimum distance of the code. By the above Lemma we have that the *B-distance* of a code coincides with the minimum *B-weight* of the code. We can now establish the correspondence between the parameters of the codes.

Theorem 1 *Let B be an invertible matrix over $M_t(\mathbb{F}_q)$, let C be a linear code over $R(q,t)$ of length n with $|C| = (q^t)^k$ and B-distance d_B, and let ϕ_B be the corresponding map. Then $\phi_B(C)$ is a linear $[tn, tk, d_B]$-code over $\mathbb{F}_q$.*

Proof. Proposition 1 indicates that $\phi_B(C)$ is a linear code over $\mathbb{F}_q$. By the remark above that same proposition, the number of codewords in both codes are the same, and a basis for $\phi_B(C)$ can be obtain form a set of generators for C, in the following way: let $y_1, y_2, \cdots, y_k$ be a set of generators for the linear code C over $R(q,t)$. Then the set $\{u^i y_j / i = 0..(t-1), j = 1..k\}$ form a set of generators for C as an $\mathbb{F}_q$-submodule. Since B is invertible, it follows that $\{\phi_B(u^i y_j)/i = 0..(t-1), j = 1..k\}$ are linearly independent vectors over $\mathbb{F}_q$ and form a basis for the linear code $\phi_B(C)$. Hence the dimension of the code $\phi_B(C)$ is tk. Finally, from lemma 2, the minimum Hamming distance for the code $\phi_B(C)$ is equal to the minimum *B-distance* d_B. ■

In matrix form, we can construct a generator matrix for the linear code $\phi_B(C)$ from a generator matrix G of the code C as follows. For each row $(x_1, x_2, \cdots, x_n)$ of G consider the matrix representation $(X_1, X_2, \cdots, X_n)$, of the elements of $R(q,t)$ given by:

$$X_i = f(a_0 + a_1 u + a_2 u^2 + \cdots + a_{t-1} u^{t-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{t-1} \\ 0 & a_0 & a_1 & \cdots & a_{t-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_0 \end{pmatrix}.$$

Then the rows of the matrix $(X_1 B, X_2 B, \cdots, X_n B)$ form t generators for the linear code $\phi_B(C)$. Repeating this process for each row of G we will obtain the

tk generators for $\phi_B(C)$. We denote this matrix by $\phi_B(G)$. It is then easy to see that both codes will share the same weight enumerator polynomial (they share distances and weights), and the map ϕ_B preserves quasi-cyclic codes.

Corollary 1 *The Hamming weight enumerator polynomial of the linear code $\phi_B(C)$ over $\mathbb{F}_q$ is the same as the B-weight enumerator polynomial of the code C over $R(q,t)$.*

Some examples of optimal codes have been obtain by looking at *quasi-cyclic (QC)* codes over $\mathbb{F}_q$. This construction allows to obtain such codes from cyclic codes over $R(q,t)$ as indicated by the following (easy to show) corollary.

Corollary 2 *Let C be a QC-code over $R(q,t)$, and let B and ϕ_B as in the previous theorem. Then $\phi_B(C)$ is a QC-code over $\mathbb{F}_q$.*

We present first a ternary code with optimal distance for the given parameters.

Example 4 Consider a linear code C over $\mathbb{F}_3 + u\mathbb{F}_3$ of length 9 with generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 5 & 4 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 3 & 5 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 3 & 5 & 4 \\ 0 & 0 & 0 & 1 & 4 & 1 & 0 & 3 & 5 \end{pmatrix}$$

For notation purposes, we have identified each element of $\mathbb{F}_q + u\mathbb{F}_q$ with its decimal numeral replacing $u = q$.

Let $B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. The *B-weight* enumerator polynomial is given by the following matrix

$$\begin{pmatrix} 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 98 & 206 & 412 & 780 & 1032 & 1308 & 1224 & 828 & 462 & 166 & 40 & 4 \end{pmatrix}$$

where the numbers in the first row indicate the *B-weight* (exponents) and the corresponding numbers in the second row are the number of codewords with that particular *B-weight* (coefficients).

By corollary 1 the Hamming weight enumerator polynomial of the code $\phi_B(C)$ has the same coefficients. The linear ternary code $\phi_B(C)$ is an $[18, 8, 7]$-code, which has the optimal minimum distance (7) for a ternary code of length 18 and dimension 8.

Notice that if we take $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ we get the following *B-weight* enumerator coefficients:

$$\begin{pmatrix} 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 8 & 22 & 24 & 58 & 152 & 386 & 720 & 1206 & 1302 & 1180 & 842 & 474 & 140 & 46 \end{pmatrix}$$

which forms also the Hamming enumerator polynomial for a linear ternary code of length 18, dimension 8, but now, with minimal distance 4. Changing the matrix B will produce linear codes with same length and dimension, but different minimum weight.

Question. For each set of parameters n, k is there a matrix B for which we can always obtain a code with optimal minimum distance?

Question. Do codes over $R(q, t)$ satisffied the same inequalities as of codes over $\mathbb{F}_q$? If so, how does this help in improving the minimal distances inequalities for codes over $\mathbb{F}_q$?

Question. How does the choice of B afects the minimal distance for a code?

Example 5 Consider a linear code C over $\mathbb{F}_q5 + u\mathbb{F}_q5$ of length 5 with generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 10 & 18 & 4 \\ 0 & 1 & 4 & 10 & 18 \end{pmatrix}$$

Let $B = \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix}$. The *B-weight* enumerator polynomial is given by the following matrix:

$$\begin{pmatrix} 6 & 7 & 8 & 9 & 10 \\ 84 & 144 & 144 & 184 & 68 \end{pmatrix}$$

The linear $\mathbb{F}_q5$-code $\phi_B(C)$ is an $[10, 4, 6]$-code, which is the optimal minimum distance for these parameters $[10, 4]$. This method gives a new technique to find new codes. We can generate several codes of given length and dimension using less information. The generator matrix for the code obtained by the above mentioned method is given by:

$$\phi_B(G) \quad = \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 3 & 2 & 2 & 0 & 3 \\ 0 & 1 & 0 & 0 & 2 & 3 & 3 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 3 & 2 & 3 & 2 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 3 & 3 & 1 \end{pmatrix}$$

Example 6 Consider a linear code C over $R(5,3) = \mathbb{F}_q5 + u\mathbb{F}_q5 + u^2\mathbb{F}_q5$ of length 14 with generator matrix obtained by cyclic shifts of the first 5 components and cyclic shift of the last 9 components of the vector:

$$(1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 5 \quad 18 \quad 22 \quad 20 \quad 0 \quad 4 \quad 28 \quad 32 \quad 30)$$

Let $B = \begin{pmatrix} 0 & 3 & 3 \\ 0 & 0 & 4 \\ 3 & 3 & 2 \end{pmatrix}$. The *B-weight* enumerator polynomial is given by the following matrix:

$$\begin{pmatrix} 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 32 & 80 & 150 & 158 & 140 & 82 & 44 & 14 & 4 \end{pmatrix}$$

The linear $\mathbb{F}_q5$-code $\phi_B(C)$ is an $[42, 15, 16]$-code over $\mathbb{F}_q5$, which has the optimal maximum distance known.

References

[1] C. Bachoc, *Applications of coding theory to the construction of modular lattices.* J. Combin. Theory Ser. A, (1997),**78**, pp. 92–119.

[2] A. Gulliver and M. Harada, *Codes over $F_3 + uF_3$ and Improvements to the bounds on ternary linear codes.* Design, Codes and Cryptography, (2001), **22**, pp. 89–96.

[3] I. Siap and D. Ray-Chaudhuri, *New Linear Codes over F_3 and F_5 and Improvements on Bounds.* Design, Codes and Cryptography, (2000), **21**, pp. 223–233.

Resumen

Definimos una nueva métrica para códigos lineales sobre el anillo $Fq[u]/\ (ut)$ a través de un monomorfismo módulo Fq en códigos lineales sobre Fq. La construcción generaliza la aplicación Gray, el peso Gray y el peso Lee. La técnica nos permite conocer algunos de los nuevos códigos lineales óptimos y su polinomio enumerador de peso.

Palabras Clave: Códigos Lineales, Aplicación Gray, Códigos sobre Anillos.

Ricardo Alfaro
Department of Mathematics,
University of Michigan-Flint,
Flint, MI 48502, USA
ralfaro@umflint.edu