Journal of Mathematics Research; Vol. 12, No. 2; April 2020
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

On the Hyper-Kloosterman Codes Over Galois Rings

Etienne TANEDJEU ASSONGMO[1] & Christophe MOUAHA[2]

[1] Department of mathematics, Faculty of Sciences, University of Yaounde 1, Cameroon

[2] Department of mathematics, Higher Teachers Training College of Yaounde, University of Yaounde 1, Cameroon; P.O. Box 47 Yaounde, Cameroon

Correspondence: Etienne TANEDJEU ASSONGMO, Department of mathematics, University of Yaounde 1, Cameroon. E-mail: assongmoetienne@yahoo.fr

Received: November 3, 2019 Accepted: February 10, 2020 Online Published: February 19, 2020

doi:10.5539/jmr.v12n2p12 URL: https://doi.org/10.5539/jmr.v12n2p12

Abstract

The Hyper-Kloosterman code was first defined over finite fields by Chinen-Hiramatsu, see (Chinen, & Hiramatsu, 2001). In the present paper we define the Hyper-Kloosterman codes over Galois rings $R(p^e, m)$. We show that this code is the trace of linear code over $R(p^e, m)$. By the Hyper-Kloostermann sums over Galois rings, we determine the Hamming weight of any codeword of this code over Galois rings.

Keywords: characters sums, Hyper-Kloosterman sums, Hyper-Kloosterman codes, trace codes, Galois rings

1. Introduction

It all starts with a paper by Kloosterman in 1926 (Kloosterman, 1926), in his study of certain positive definite integral quadratic forms. In his paper, Kloosterman, introduced certain exponential sum (since then known as the Kloosterman sum). Since then Kloosterman sums have enjoyed much attention of the finite fields. Some of this interest is due to their applications in cryptography and coding theory; see for example: the search for the number of solution of certain equations over finite fields, the distribution of values of Kloosterman sums, the divisibility properties of classical binary Kloosterman sums , see (Pascale, Helleseth , & Victor, 2009) , the search for the weight of certain codes, called the Kloosterman code, see (Jacques,1989), (Gilles, 1989) and (Chinen, & Hiramatsu, 2001). The hyper-Kloosterman code was first defined over finite fields by Chinen-Hiramatsu, (Chinen, & Hiramatsu, 2001). In the present paper we define the Hyper-Kloosterman codes over Galois rings $R(p^e, m)$. We show that this code is the trace of linear code over $R(p^e, m)$. By the Hyper-Kloostermann sums over Galois rings, we determine the Hamming weight of any codeword of this code over Galois rings.

2. Preliminaries

Some preliminaries on Galois rings are given below. For more details, the reader is referred to (Shuqin, & Han, 2004). Let $e \geq 1$ be a fixed integer, p a prime number. A monic polynomial $h(x) \in \mathbb{Z}_{p^e}[x]$ is said to be a basic irreducible polynomial of degree m if $(h(x) \bmod p) \in \mathbb{Z}_p[x]$ is a monic irreducible polynomial of degree m. Galois ring $R_{e,m} = GR(p^e, m)$ is the unique unramified extension of degree m over $\mathbb{Z}_{p^e}$ and can be written as

$$R_{e,m} = GR(p^e, m) = \mathbb{Z}_{p^e}[X]/(h(X))$$

where $h(x)$ is a basic irreducible polynomial of degree m over $\mathbb{Z}_{p^e}$. The ring $R_{e,m}$ is a local ring with unique maximal ideal $pR_{e,m}$. The unit set $R^*_{e,m} = R_{e,m} \backslash pR_{e,m}$ in $R_{e,m}$ is a multiplicative group of order

$$\sharp R^*_{e,m} = (p^m - 1)p^{m(e-1)} = p^{me} - p^{m(e-1)}.$$

The set $R^*_{e,m}$ always contains a cyclic group of order $p^m - 1$. In analogy with finite fields, we will call an element a primitive element of the Galois ring $R_{e,m}$ if it is a generator for this cyclic group. Let $\gamma_{e,m}$ denote a primitive element in $R_{e,m}$. Let $\mathcal{T}^* = \{1, \gamma_{e,m}, \gamma^2_{e,m}, ..., \gamma^{p^m-2}_{e,m}\}$. The set $\mathcal{T}^*$ is called Teichmuller system. Let $\mathcal{T} = \mathcal{T}^* \bigcup \{0\} = \{0, 1, \gamma_{e,m}, \gamma^2_{e,m}, ..., \gamma^{p^m-2}_{e,m}\}$. For any element $z \in R_{e,m}$ the p-adic expansion has giving by:

$$z = z_0 + pz_1 + ... + p^{e-1}z_{e-1}$$

where $z_i \in \mathcal{T}$.

Let τ the Frobenius map of $R_{e,m}$ over $\mathbb{Z}_{p^e}$ given by

$$\tau(z) = z_0^p + pz_1^p + ... + p^{e-1}z_{e-1}^p$$

where $z = \sum_{i=0}^{e-1} p^i z_i \in R_{e,m}$ and $z_i \in \mathcal{T}$. As we know τ is the generator of Galois group of $R_{e,m}/\mathbb{Z}_{p^e}$ which is a cyclic group of order m. The trace mapping $tr_{e,m} : R_{e,m} \to \mathbb{Z}_{p^e}$ is defined via

$$tr_{e,m}(x) = x + \tau(x) + ... + \tau^{m-1}(x)$$

for $x \in R_{e,m}$

3. Hyper-Kloosterman Codes

Definition 3.1 In a similar way to the Hyper-Kloosterman codes over Galois fields defined for the first time by Chinen-Hiramatsu , we define the hyper-Kloosterman code $C_l(p^e, m)$ of degree $l-1$, ($l \geq 2$, l is an integer), over Galois ring, by the image of the map:

$$\begin{array}{rccc} \varphi_l : & R_{e,m}^l & \to & \mathbb{Z}_{p^e}^{(p^{me}-p^{m(e-1)})^{l-1}} \\ & a & \mapsto & \varphi_l(a) = \{Tr(a,x)\}_{x \in (R_{e,m}^*)^{l-1}} \end{array}$$

Where

$$Tr(a,x) = tr_{e,m}(a_1x_1 + a_2x_2 + ... + a_{l-1}x_{l-1} + a_l(x_1...x_{l-1})^{-1})$$

$a = (a_1, ..., a_l) \in R_{e,m}^l$, $x = (x_1, ..., x_{l-1}) \in (R_{e,m}^*)^{l-1}$ and $tr_{e,m} = trace_{R_{e,m}/\mathbb{Z}_{p^e}}$

The symbol $\{\quad\}_{x \in (R_{e,m}^*)^{l-1}}$ represents a vector obtained by letting x run through the set $(R_{e,m}^*)^{l-1}$ (such a notation is often used in the literature on the trace codes). The code $C_l(p^e, m)$ is a generalization, over Galois ring, of the hyper-Kloosterman code. The Hyper-Kloosterman code over Galois fields has been investigated by many authors. See for example: (Chinen, & Hiramatsu, 2001), (Chinen, 2003) and (Moisio, 2008).

Remark 3.1 The length of a code $C_l(p^e, m)$ is a power of the order of the group of invertible elements, $R_{e,m}^*$.

$$(p^{me} - p^{m(e-1)})^{l-1} = (\sharp R_{e,m}^*)^{l-1}$$

Proposition 3.1 The code $C_l(p^e, m)$ is a linear code over $\mathbb{Z}_{p^e}$.

Proof

φ_l is a module homomorphism and so his image is a sub-module of $\mathbb{Z}_{p^e}^{(p^{me}-p^{m(e-1)})^{l-1}}$. Therefore $C_l(p^e, m)$ is a linear code.

Definition 3.2 For a code C over $R_{e,m}$, we denote the trace code of C (over $\mathbb{Z}_{p^e}$) by $tr_{e,m}C$:

$$tr_{e,m}C := (tr_{e,m}c_1, ..., tr_{e,m}c_n) | (c_1, ..., c_n) \in C$$

Proposition 3.2 The code $C_l(p^e, m)$ is a trace code over Galois ring.

Proof Let α_l the map defined by:

$$\begin{array}{rccc} \alpha_l : & R_{e,m}^l & \to & R_{e,m}^{(p^{me}-p^{m(e-1)})^{l-1}} \\ & a & \mapsto & \alpha_l(a) = \{(a,x)\}_{x \in (R_{e,m}^*)^{l-1}} \end{array}$$

Where

$l \geq 2$, (l is an integer), $(a,x) = a_1x_1 + a_2x_2 + ... + a_{l-1}x_{l-1} + a_l(x_1...x_{l-1})^{-1}$, $a = (a_1, ..., a_l) \in R_{e,m}^l$ and $x = (x_1, ..., x_{l-1}) \in (R_{e,m}^*)^{l-1}$. We see easily α_l is a module homomorphism , and so his image is a sub-module. Let $\overline{C_l}(p^e, m) = Im(\alpha_l)$, the image of α_l. $\overline{C_l}(p^e, m)$ is a linear code over Galois ring $R_{e,m}$. By definition of α_l, we obtained $C_l(p^e, m) = tr_{e,m}(\overline{C_l}(p^e, m))$.

In the following, $\overline{C_l}(p^e, m)$ denote the code defined in the previous proof. That is to say:

$$C_l(p^e, m) = tr_{e,m}(\overline{C_l}(p^e, m))$$

Construction of the generator matrix $\overline{G_l}(p^e, m)$ of $\overline{C_l}(p^e, m)$. where $C_l(p^e, m) = tr_{e,m}(\overline{C_l}(p^e, m))$.

Let $f_1, f_2, ..., f_{(p^{me}-p^{m(e-1)})^{l-1}}$ be a fixed ordering of the elements of.

$$(R_{e,m}^*)^{l-1} = \{f_1, ..., f_{(p^{me}-p^{m(e-1)})^{l-1}}\}$$

Let $f_j \in (R_{e,m}^*)^{l-1}$, so

$$f_j = (f_{1,j}, f_{2,j}, ..., f_{(l-1)j})$$

Moreover we define $I(x)$ for $x = (x_1, x_2..., x_{l-1}) \in (R^*_{e,m})^{l-1}$ by:

$$I(x) = (x_1 x_2 ... x_{l-1})^{-1}$$

Let f_j^T the transpose of the vector f_j.

Then we form the matrix as follows:

$$\overline{G_l}(p^e, m) = \begin{pmatrix} f_1^T & f_2^T & ... & f^T_{(p^{me}-p^{m(e-1)})^{l-1}} \\ I(f_1) & I(f_2) & ... & I(f_{(p^{me}-p^{m(e-1)})^{l-1}}) \end{pmatrix}$$

Proposition 3.3 The matrix $\overline{G_l}(p^e, m) = \begin{pmatrix} f_1^T & f_2^T & ... & f^T_{(p^{me}-p^{m(e-1)})^{l-1}} \\ I(f_1) & I(f_2) & ... & I(f_{(p^{me}-p^{m(e-1)})^{l-1}}) \end{pmatrix}$ is a generator matrix of the code $\overline{C_l}(p^e, m)$

Proof

$$\text{Let } a = (a_1, ..., a_l) \in R^l_{e,m}$$

$$\begin{aligned} a\overline{G_l}(p^e, m) &= (a_1, ..., a_l) \begin{pmatrix} f_1^T & f_2^T & ... & f^T_{(p^{me}-p^{m(e-1)})^{l-1}} \\ I(f_1) & I(f_2) & ... & I(f_{(p^{me}-p^{m(e-1)})^{l-1}}) \end{pmatrix} \\ &= (a_1, ..., a_l) \begin{pmatrix} f_{1,1} & ... & f_{1,(p^{me}-p^{m(e-1)})^{l-1}} \\ f_{2,1} & ... & f_{2,(p^{me}-p^{m(e-1)})^{l-1}} \\ \vdots & & \vdots \\ f_{(l-1),1} & ... & f_{(l-1),(p^{me}-p^{m(e-1)})^{l-1}} \\ (f_{1,1}...f_{(l-1),1})^{-1} & ... & (f_{1,(p^{me}-p^{m(e-1)})^{l-1}}...f_{(l-1),(p^{me}-p^{m(e-1)})^{l-1}})^{-1} \end{pmatrix}. \\ &= [a_1 f_{1,1} + ... + a_{l-1} f_{(l-1),1} + ... + a_l (f_{1,1}...f_{(l-1),1})^{-1}; ...; a_1 f_{1,(p^{me}-p^{m(e-1)})^{l-1}} + ... + \\ &\quad a_{l-1} f_{(l-1),(p^{me}-p^{m(e-1)})^{l-1}} + a_l (f_{1,(p^{me}-p^{m(e-1)})^{l-1}}...f_{(l-1),(p^{me}-p^{m(e-1)})^{l-1}})^{-1}]. \end{aligned}$$

Which is a codeword of the code $\overline{C_l}(p^e, m)$.

Therefore, the matrix $\overline{G_l}(p^e, m)$ is a generator matrix of the code $\overline{C_l}(p^e, m)$.

Remark 3.2 The matrix $\overline{G_l}(p^e, m)$ is the type $(l, (p^{me} - p^{m(e-1)})^{l-1})$; l-lengths and $(p^{me} - p^{m(e-1)})^{l-1}$-columns.

4. Hamming Weights of the Codewords of $C_l(p^e, m)$

Definition 4.1 Let C a code of length n. $x = x_1 x_2 \dots x_n$ and $y = y_1 y_2 \dots y_n$ two codewords on code C. The Hamming distance of x and y, is given by

$d(x, y) = \sharp\{i : x_i \neq y_i\}$.

The Hamming weight W_H of a codeword $x = x_1 x_2 \dots x_n$ of C is the number of non-zero x_i for $1 \leq i \leq n$.

$W_H(x) = \sharp\{i : x_i \neq 0\}$

Definition 4.2 Additive characters over Galois rings.

An additive character of $R_{e;m}$ is a homomorphism from the additive group of $R_{e;m}$ to $\mathbb{C}^*$; the multiplicative group of complex field. We Define $\psi(a) = \mathbf{exp}(2\pi i t r_{e,m}(a)/p^e)$ for any given element a in $R_{e;m}$ and " **exp**" denote the exponential function : It is easily seen that ψ is an additive character of $R_{e;m}$; called the canonical additive character. For $b \in R_{e;m}$; define $\psi_b(a) = \psi(ba)$: $a \in R_{e;m}$. ψ is also an additive character. In fact, we have:

Proposition 4.1 $\{\psi_b\}_{b \in R_{e;m}}$ consists of all the additive characters of $R_{e;m}$.

We present a well-known result, sometimes called the orthogonality of characters, as a proposition for later reference.

Proposition 4.2 Let $b \in R_{e;m}$; ψ be the canonical additive character of $R_{e;m}$. Then:

$$\sum_{b \in R_{e,m}} \psi_b(a) = \begin{cases} p^{me} \text{ if } a = 0 \\ 0 \text{ if } a \neq 0 \end{cases}.$$

Definition 4.3 For $l \geq 2$ and any $a \in R^l_{e,m}$ the hyper-Kloosterman sums of degree $l - 1$ are defined by

$$K_{e,m}(a, p) = \sum_{x \in (R^\star_{e,m})^{l-1}} \mathbf{exp}(\frac{2\pi i}{p^e} Tr(a, x))$$

where $Tr(a,x) = tr_{e,m}(a_1x_1 + a_2x_2 + ... + a_{l-1}x_{l-1} + a_l(x_1x_2...x_{l-1})^{-1})$ for $a = (a_1, a_2, ..., a_l)$ and $x = (x_1, x_2, ..., x_{l-1})$, and $tr_{e,m} = traceR_{e,m}/\mathbb{Z}_{p^e}$

The Kloosterman sums have been used by several authors to evaluate the Hamming weights of a certain linear code C(q), called the Kloosterman code (see for example (Gilles, 1989) and (Jacques, 1989)).

Theorem 4.1 For any codeword $\varphi_l(a) \in C_l(p^e, m)$, the weight of $\varphi_l(a)$ is given by:

$$W_H(\varphi_l(a)) = (p^{me} - p^{m(e-1)})^{l-1} - \frac{1}{p^e}\sum_{\lambda=0}^{p^e-1} K_{e,m}(\lambda a, p)$$

Proof.

Let "**exp**" denote the exponential function. For all $a \in R_{e,m}^l$ and all $x \in (R_{e,m}^*)^{l-1}$, $\mathbf{exp}(Tr(a,x))$ is a p^e-th root of unity, and is equal to 1 or not according to $Tr(a,x) = 0$ or not. So we have:

$$\sum_{\lambda=0}^{p^e-1} e^{(\lambda Tr(a,x))} = \begin{cases} p^e \text{ if } Tr(a,x) = 0 \\ 0 \text{ if } Tr(a,x) \neq 0 \end{cases}.$$

Therefore

$$\begin{aligned} \sharp\{x \in (R_{e,m}^*)^{l-1}; Tr(a,x) = 0\} &= \frac{1}{p^e}\sum_{x\in(R_{e,m}^\star)^{l-1}}\sum_{\lambda=0}^{p^e-1}\mathbf{exp}(\lambda Tr(a,x)) \\ &= \frac{1}{p^e}\sum_{\lambda=0}^{p^e-1}\sum_{x\in(R_{e,m}^\star)^{l-1}}\mathbf{exp}(\lambda Tr(a,x)) \\ &= \frac{1}{p^e}\sum_{\lambda=0}^{p^e-1} K_{e,m}(\lambda a, p). \end{aligned}$$

We know that, the unit set $R_{e,m}^* = R_{e,m}\backslash pR_{e,m}$ in $R_{e,m}$ is a multiplicative group of order

$$\sharp R_{e,m}^* = (p^m - 1)p^{m(e-1)} = p^{me} - p^{m(e-1)}$$

So the weight $W_H(\varphi_l(a))$ for any codeword $\varphi_l(a)$ it is obtened by :

$$\begin{aligned} W_H(\varphi_l(a)) &= \sharp(R_{e,m}^*)^{l-1} - \sharp\{x \in (R_{e,m}^*)^{l-1}; Tr(a,x) = 0\} \\ &= (p^{me} - p^{m(e-1)})^{l-1} - \frac{1}{p^e}\sum_{\lambda=0}^{p^e-1} K_{e,m}(\lambda a, p). \end{aligned}$$

Example 4.1 For $l = 2$, $p = 2$, $e = 2$ and $m = 1$ we obtained $R_{e,m} = \mathbb{Z}_4$ and the trace map $t_{e,m}$ become identity map from $\mathbb{Z}_4$. $\mathbb{Z}_4^* = \mathbb{Z}_4\backslash 2\mathbb{Z}_4 = \{1, 3\}$. Without harming the generality, let's $x_1 = 1$ and $x_2 = 3$ So $x_1^{-1} = x_1 = 1$ and $x_2^{-1} = x_2 = 3$.

$C_2(4, 1)$ it is the image of the map:

$$\begin{array}{rccc} \varphi_2: & \mathbb{Z}_4^2 & \to & \mathbb{Z}_4^2 \\ & a = (a_1, a_2) & \mapsto & \varphi_2(a) = (a_1x_1 + a_2x_1^{-1}, a_1x_2 + a_2x_2^{-1}) = (a_1 + a_2, 3a_1 + 3a_2) \end{array}$$

We have:

$$\begin{aligned} \varphi_2(0,0) &= (0,0) \\ \varphi_2(0,1) &= (1,3) \\ \varphi_2(0,2) &= (2,2) \\ \varphi_2(0,3) &= (3,1) \end{aligned}$$

$$\begin{aligned}\varphi_2(1,3) &= (0,0)\\ \varphi_2(1,2) &= (3,1)\\ \varphi_2(1,1) &= (2,2)\\ \varphi_2(1,0) &= (1,3)\end{aligned}$$

... etc

We obtened

$$C_2(4,1) = \{(0,0);(2,2);(1,3);(3,1)\}$$

5. Conclusion and Perspectives

We have generalized the hyper-Klosterman codes over Galois rings. This code is seen as a trace of a linear code over galois rings. We get the Hamming weight of a codeword by the hyper-kloosterman sums. The first trivial example gives the 1-quasi-cyclic or cyclic codes. We can therefore continue to study the properties of this code, quasy-cyclic properties and others.

References

Abhijit, G. S., & Vijay, P. K. (1998). An Upper Bound for the Extended Kloosterman Sums over Galois Rings. *Finite fields and their Applications*, *4*(3), 218-238. https://doi.org/10.1006/ffta.1998.0211

Chinen, K. (2003). On Some Properties of the Hyper-Kloosterman Codes. *TOKYO J. MATH*, *26*(1), 55-65. https://doi.org/10.3836/tjm/1244208682

Chinen, K., & Hiramatsu, T. (2001). Hyper-Kloosterman Sums and their Applications to the Coding Theory. *AAECC*, *12*(5), 381-390. https://doi.org/10.1007/s002000100080

Gilles, L. (1989). Distribution of the weights of the dual of the Melas codes. *Discrete Mathematics*, *79*(1), 103-106. https://doi.org/10.1016/0012-365x(90)90059-q

Honold, T. L. (2000). Linear codes over finite chain rings. *Electron. J. Combinat.*, *7*(1). https://doi.org/10.37236/1489

Jacques WOLFMAN. (1989). The weights of the dual code of the Melas Code over GF(3). *Discrete Mathematics*, *74*, 327-329. https://doi.org/10.1016/0012-365x(89)90145-3

KLOOSTERMAN, H. D. (1926). On the representations of a number in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, *49*, 407-464. https://doi.org/10.1112/plms/s2-25.1.143

Martinez-Moro, E., Nicolas, A. P., & Rua, I. F. (2013). On trace codes and Galois invariance over finite commutative chain rings. *Finite Fields and Their Applications*, *22*, 114-121. https://doi.org/10.1016/j.ffa.2013.03.004

MOISIO, M. (2008). On the duals of binary Hyper-Kloosterman codes. *SIAM J. DISCRETE MATH.*, *22*(1), 273-287. https://doi.org/10.1137/060668900

Norton, G. H., & Salagean, A. (2000). On the structure of linear and cyclic codes over a finite chain ring. *Appl. Algebra Engrg. Comm. Comput.*, *10*(6), 489-506. https://doi.org/10.1007/pl00012382

NORTON, G. H., & SALAGEAN, A. (2000). On the Hamming distance of linear codes over a finite chain ring. *IEEE transactions on information theory*, *46*(3), 1060-1067. https://doi.org/10.1109/18.841186

Pascale, C., Helleseth, T., & Victor, Z. (2009). Divisibility properties of classical binary Kloosterman sums. *Discrete Mathematics*, *309*, 3975-3984. https://doi.org/10.1016/j.disc.2008.11.010

Shuqin, F., & Han, W. (2004). Character sums over Galois rings and primitive polynomials over finite fields. *Finite Fields and Their Applications*, *10*, 36-52. https://doi.org/10.1016/s1071-5797(03)00041-8

Copyrights