International Journal of Algebra, Vol. 7, 2013, no. 17, 803 - 807
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2013.310100

Skew Cyclic and Quasi-Cyclic Codes of Arbitrary Length over Galois Rings

Mingzhong Wu

Department of Mathematics, China West Normal University
Nanchong, Sichuan 637002, P.R. China

Copyright © 2013 Mingzhong Wu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

We mainly investigate the structures of skew cyclic and skew quasi-cyclic codes of arbitrary length over Galois rings. Similar to [5], our results show that the skew cyclic codes are equivalent to either cyclic and quasi-cyclic codes over Galois rings. Moreover, we give a necessary and sufficient condition for skew cyclic codes over Galois rings to be free. A sufficient condition for 1-generator skew quasi-cyclic codes to be free is also determined.

Keywords: Skew cyclic codes, Skew quasi-cyclic codes, 1-Generator skew quasi-cyclic codes, Galois rings

1 Preliminaries

Let $q = p^r$, p a prime number and r a positive integer. Let $f(x)$ be a basic irreducible polynomial of degree m over Z_q . The Galois ring of degree m over Z_q is the residue class ring $Z_q[x]/(f(x))$, denoted as $\mathcal{R} = GR(q, m)$. $\mathcal{R}$ is a local ring with maximum ideal $\langle p\rangle$ and the residue field F_{p^m}. Each element of $\mathcal{R}$ can be uniquely expressed as $a = a_0 + a_1\xi + \ldots + a_{m-1}\xi^{m-1}$, where $a_i \in Z_q$, $\quad i = 1, 2, \ldots , m - 1$. The set $\mathcal{T} = \{0, 1, \xi, \ldots , \xi^{p^m-2}\}$ is called the Teichmuller set of $\mathcal{R}$. The Frobenius automorphism ϕ of $\mathcal{R}$ over Z_q is defined by $\phi(a) = a_0 + a_1\xi^p + \ldots + a_{m-1}\xi^{(m-1)p}$. The group of automorphism of $\mathcal{R}$ is a cyclic group with order m and is generated by ϕ.

Let θ be an automorphism of $\mathcal{R}$. The skew polynomial ring $\mathcal{R}[x; \theta]$ is the set of polynomials over $\mathcal{R}$, where the addition is defined as the usual addition of polynomial and the multiplication is defined by the basic rule $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}, \quad a, b \in \mathcal{R}$.

Let θ be an automorphism with order t and let $Z(\mathcal{R}[x;\theta])$ be the center of $\mathcal{R}[x;\theta]$. Then it is easy to deduce that the center of $\mathcal{R}[x;\theta]$ is $\mathcal{R}_\infty[x^t]$, where $\mathcal{R}_\infty = GR(q, m/t)$. Let $f, g \in \mathcal{R}[x;\theta]$. Then g is called a right divisor of f if there exists $q \in \mathcal{R}[x;\theta]$ such that $f = qg$. A right divisor of a center polynomial is also its left divisor. In particular if t divides n, then $x^n - 1 \in Z(\mathcal{R}[x;\theta])$ and hence a right divisor of $x^n - 1$ is also its left divisor. This result has a big impact on the structure of elements in $\mathcal{R}[x;\theta]/(x^n - 1)$. If we remove this restriction, then we can define skew cyclic codes of any length n. However, if t is not a divisor of n, then $\mathcal{R}[x;\theta]/(x^n - 1)$ is not a ring anymore. It is only a left $\mathcal{R}[x;\theta]$-module.

2 Skew cyclic codes

Let θ be an automorphism of the Galois ring $\mathcal{R}$. A linear code $\mathcal{C}$ of length n over $\mathcal{R}$ is called skew cyclic if and only if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in \mathcal{C}$. As traditional study of cyclic codes, we can identify each codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ by a polynomial $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ in $\mathcal{R}[x;\theta]/(x^n - 1)$.

Proposition 2.1 *Let $\mathcal{C}$ be a skew cyclic code of length n and let θ be an automorphism of $\mathcal{R}$ with order t. If $gcd(t, n) = 1$ then $\mathcal{C}$ is a cyclic code of length n.*

Proof Since $gcd(t, n) = 1$, it follows that there exist integers a, b such that $at + bn = 1$. Therefore, $at = 1 - bn = 1 + ln$, where $l > 0$. Let $c(x) = c_0 + c_1(x) + \ldots + c_{n-1}x^{n-1}$ be a codeword in $\mathcal{C}$. Note that $x^{at}c(x) = \theta^{at}(c_0)x^{1+ln} + \theta^{at}(c_1)x^{2+ln} + \ldots + \theta^{at}(c_{n-1})x^{n+ln} = c_{n-1} + c_0x + \ldots + c_{n-2}x^{n-2} \in \mathcal{C}$. Thus $\mathcal{C}$ is a cyclic code of length n. □

Proposition 2.2 *A code $\mathcal{C}$ of length n over $\mathcal{R}$ is a skew cyclic code if and only if $\mathcal{C}$ is a left $\mathcal{R}[x;\theta]$-submodule of the left $\mathcal{R}[x;\theta]$-module $\mathcal{R}[x;\theta]/(x^n - 1)$.*

Proof Let $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ be a codeword in $\mathcal{C}$. Since $\mathcal{C}$ is cyclic, it follows that $xc(x), x^2c(x), \ldots, x^ic(x)$ are all elements in $\mathcal{C}$, where all the indices are taken modulo n. Therefore, $r(x)c(x) \in \mathcal{C}$ for any $r(x) \in \mathcal{R}[x;\theta]$. Thus $\mathcal{C}$ is an $\mathcal{R}[x;\theta]$-submodule of $\mathcal{R}[x;\theta]/(x^n - 1)$.

Conversely, suppose $\mathcal{C}$ is a left $\mathcal{R}[x;\theta]$-submodule of the left $\mathcal{R}[x;\theta]$-module $\mathcal{R}[x;\theta]/(x^n - 1)$. Then for any codeword $c(x) \in \mathcal{C}$, $xc(x) \in \mathcal{C}$. Therefore, $\mathcal{C}$ is skew cyclic. □

Note that not all left $\mathcal{R}[x;\theta]$-submodules are $\mathcal{R}$-free, but in following we will focus on those submodules. Similar to the case that the order of θ divides

n, the following proposition gives a well-defined properties of free skew cyclic codes for any length n.

Proposition 2.3 *A skew cyclic code $\mathcal{C}$ of length n over $\mathcal{R}$ is free if and only if it is generated by a monic right divisor $g(x)$ of $x^n - 1$ with degree k. The set $\{g(x), xg(x), \dots, x^{n-k-1}g(x)\}$ forms a basis of $\mathcal{C}$ and the rank of $\mathcal{C}$ is $n-k$.*

3 Skew quasi-cyclic codes

Let θ be an automorphism of $\mathcal{R}$ and $n = ls$. A linear code $\mathcal{C}$ over $\mathcal{R}$ is called skew quasi-cyclic with index l if and only if $(c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, c_{1,1}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}) \in \mathcal{C} \Rightarrow (\theta(c_{s-1,0}), \theta(c_{s-1,1}), \dots, \theta(c_{s-1,l-1}), \theta(c_{0,0}), \theta(c_{0,1}), \dots, \theta(c_{0,l-1}), \dots, \theta(c_{s-2,0}), \theta(c_{s-2,1}), \dots, \theta(c_{s-2,l-1})) \in \mathcal{C}$. If θ is the identity map, we call $\mathcal{C}$ a quasi-cyclic code over $\mathcal{R}$.

In the following, we illustrate the relationship between skew cyclic codes and quasi-cyclic codes over $\mathcal{R}$.

Proposition 3.1 *Let $\mathcal{C}$ be a skew cyclic code of length n over $\mathcal{R}$ and let θ be an automorphism with order t. If $gcd(t, n) = l$, then $\mathcal{C}$ is equivalent to a quasi-cyclic code of length n with index l over $\mathcal{R}$.*

Proof Let $n = sl$ and $(c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, c_{1,1}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}) \in \mathcal{C}$. Since $gcd(t, n) = d$, there exist integers a, b such that $at + bn = d$. Therefore, $at = d - bn = d + gn$, where g is a nonnegative integer. Note that $\theta^{d+gn}(c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, c_{1,1}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1})$ $= (c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}, c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, \dots, c_{s-2,0}, c_{s-2,1}, \dots, c_{s-2,l-1}) \in \mathcal{C}$. Thus, $\mathcal{C}$ is equivalent a quasi-cyclic code of length n with index l over $\mathcal{R}$.

From Proposition 3.1, we have the following corollary directly.

Corollary 3.2 *Let $\mathcal{C}$ be a skew quasi-cyclic code of length n with index l over $\mathcal{R}$ and let θ be an automorphism with order t. If $gcd(t, n) = k$, then $\mathcal{C}$ is equivalent to a quasi-cyclic code of length n with index lk over $\mathcal{R}$.*

Let $\mathcal{C}$ be an skew qusi-cyclic codes of length n with index l over $\mathcal{R}$. As traditional study of quasi-cyclic codes , we can identity an element $(c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, c_{1,1}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}) \in \mathcal{C}$ with the polynomial $(c_0(x), c_1(x), \dots, c_{l-1}(x)) \in (\mathcal{R}[x;\theta]/(x^s - 1))^l$, where $c_j(x) = \sum_{i=0}^{s-1} c_{i,j} x^i \in \mathcal{R}[x;\theta]/(x^s - 1)$, $\quad j = 0, 1, \dots, l-1$. Then, like in the case of skew cyclic codes in section 2, it is easy to see that skew quasi-cyclic code of length n with index l over $\mathcal{R}$ is a left $\mathcal{R}[x;\theta]$-submodule of $(\mathcal{R}[x;\theta]/(x^s - 1))^l$; and conversely, a left $\mathcal{R}[x;\theta]$-submodule of $(\mathcal{R}[x;\theta]/(x^s - 1))^l$ is a skew quasi-cyclic code of length n with index l over $\mathcal{R}$. It can lead us to compute the number of distinct skew cyclic and quasi-cyclic codes over R.

A 1-generator skew quasi-cyclic code $\mathcal{C}$ defined as $\mathcal{C}$ generated by an element $(g_1(x), g_2(x), \ldots, g_l(x)) \in (\mathcal{R}[x;\theta]/(x^n-1))^l$. For 1-generator skew quasi-cyclic codes, we have the following property.

Proposition 3.3 *Let $\mathcal{C}$ be an 1-generator skew quasi-cyclic code over $\mathcal{R}$, which generated by $(g_1(x), g_2(x), \ldots, g_l(x)) \in (\mathcal{R}[x;\theta]/(x^s-1))^l$. For each $i = 1, 2, \ldots, l$, if $g_i(x)$ generates an $\mathcal{R}$-free skew cyclic code over $\mathcal{R}$, then $\mathcal{C}$ is $\mathcal{R}$-free with rank $s - degg(x)$, where $g(x) = gcld(g_1(x), g_2(x), \ldots, g_l(x), x^s - 1)$.*

4 Examples

Example 4.1 *Let $\mathcal{R} = GR(4,2)$, θ be a Frobenius automorphism. Let $g(x) = x^3 + 2x^2 + x + 3$, which is a right divisor of $x^7 - 1$. Since $gcd(2,7) = 1$, by Proposition 2.1 and Proposition 2.3, skew cyclic code $\mathcal{C} = \langle g(x) \rangle$ is a free cyclic code with rank $7 - 3 = 4$ over $\mathcal{R}$. In fact, it is an $[7,4,3]$ cyclic code.*

Example 4.2 *Let $\mathcal{R} = GR(9,2)$, θ be a Frobenius automorphism. Let $g(x) = x + \alpha^2$ is a right divisor of $x^4 - 1$, where α is a primitive element in $\mathcal{R}$. This polynomial generates a MDS skew cyclic code with parameters $[4,3,2]$ over $\mathcal{R}$. Since $gcd(2,4) = 2$, this code is equivalent to a quasi-cyclic code of length 4 with index 2 generated by $g_1(x) = 1$ and $g_2(x) = \alpha^2 x$ over $\mathcal{R}$.*

Example 4.3 *Let $\mathcal{R} = GR(9,2)$, θ be a Frobenius automorphism. Let $g(x) = x + \alpha^2$ is a right divisor of $x^4 - 1$, where α is a primitive element in $\mathcal{R}$. Let $\mathcal{C} = (g(x), g(x), g(x))$ be a 1-generator skew quasi-cyclic code of length 12 with index 3 over $\mathcal{R}$. Then by Corollary 3.2 and Proposition 3.3, $\mathcal{C}$ is an R-free quasi-cyclic code of length 12 with index $2 \times 3 = 6$ over $\mathcal{R}$. In fact, it is an $[12,3,6]$ code over $\mathcal{R}$.*

References

[1] T. Abualrub, A. Ghrayeb, N. Aydim and I. Siap, On the construction of skew quasi-cyclic codes,*IEEE. Trans. Inform. Theory*, **56**(2010), 2081-2090.

[2] D. Boucher, F. Ulmer, Coding with skew polynoial rings, *Journal of Symbolic Computation,* **44**(2009), 1644-1656.

[3] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes, *AAECC*, **18**(2007), 379-389.

[4] M. Bhaintwal, Skew quasi-cyclic codes over Galois rings,*Designs, Codes and Cryptography*, **62**(2012), 85-101.

[5] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, Skew cyclic codes of arbitrary length, *Int. J. Inf. Coding Theory*, **2**(2011), 10-20.

Received: October 15, 2013