

POLYCYCLIC CODES AND THEIR STRUCTURE

Thesis Report - I

Sümeýra Bedir

Thesis Supervisor: Prof. Dr. İrfan Şiap

Yıldız Technical University

15 May 2016

Polycyclic codes over finite fields, first introduced as pseudo-cyclic codes [Peterson and Weldon, 1972], are shown to be useful in terms of constructing long-length and optimal linear codes directly [Alahamdi et al., preprint, Bedir and Şiap, 2015, Lopez-Permouth, 2009]. Even though it is proven that polycyclic codes correspond to shortened cyclic codes over finite fields, these codes are linear codes different from cyclic or consta-cyclic codes and they enjoy an algebraic structure. This algebraic structure gives a hand to explore this family of linear codes.

Our recent work "Polycyclic codes over finite chain rings" deals with the structure of these codes in the most general way and has been presented in the Proceedings of The International Conference on Coding Theory and Cryptography (ICCC2015).

Cyclic Codes

Let F be a finite field. A linear code C over F with length n , is a subspace of the vector space F^n . Linear codes, simply denoted with $[n, k, d]$, are identified with their parameters; length(n), dimension(k) and the minimum Hamming distance (d), which is defined as the minimum number of different coordinates between any two codewords of C . C is called a cyclic linear code if whenever $(c_0, c_1, \dots, c_{n-1})$ is in C , so is its cyclic shift $(c_{n-1}, c_0, \dots, c_{n-2})$. So cyclic codes are invariant subspaces of F^n under the transformation which applies cyclic shift to a vector. Each codeword $(c_0, c_1, \dots, c_{n-1})$ is associated to a polynomial $c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ in $F[x]$ and every cyclic code corresponds to an ideal of $F[x]/(x^n - 1)$. The representation matrix for the cyclic shift transformation, denoted by T , is precisely the companion matrix of $x^n - 1$, and any divisor of this polynomial generates a cyclic code over F .

Constacyclic Codes

For $\alpha \in F$, α -constacyclic codes correspond to ideals in $F[x]/(x^n - \alpha)$. As a generalization of cyclic codes, constacyclic codes are invariant under the constacyclic shift; if whenever $(c_0, c_1, \dots, c_{n-1})$ is in C , so is its α -constacyclic shift $(\alpha c_{n-1}, c_0, \dots, c_{n-2})$. The transformation for α -constacyclic shift of a vector is represented by the companion matrix of $x^n - \alpha$, which we denote by T_α . Any divisor $g(x)$ of the polynomial $x^n - \alpha$, generates an α -constacyclic code over F .

Polycyclic Codes

Polycyclicity is the most general case in terms of cyclicity of linear codes. Some authors have called these type of codes as "pseudo-cyclic codes" [Peterson and Weldon, 1972], some as "generalized cyclic codes (GCC)" [Liu and Lin, 2000] and some as "polycyclic codes" [Lopez-Permouth, 2009]. There have been many studies on the properties of polycyclic codes [Alahamdi et al., preprint, Bedir and Şiap, 2015, Lopez-Permouth, 2009]. Polycyclic codes correspond to ideals in $F[x]/(f(x))$, for any monic polynomial $f = x^n - v(x)$ with a nonzero constant term. In this case, the companion matrix of f represents the transformation that corresponds to the polycyclic shift with respect to v , and we denote it by T_v . A polycyclic code generated by a divisor g of f is invariant under T_v , has a generator matrix $g(T_v^{tr})$ and a parity check matrix $h(T_v)$ [Bedir and Şiap, 2015].

Polycyclic Codes

Definition

A linear code C with length n over a finite field F is called right *polycyclic* with respect to $v = (v_0, v_1, \dots, v_{n-1}) \in F^n$ (with the usual correspondence to $v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}$) if, whenever $c = (c_0, c_1, \dots, c_{n-1})$ is in C , so is its v -polycyclic shift $(v_0c_{n-1}, c_0 + v_1c_{n-1}, \dots, c_{n-2} + v_{n-1}c_{n-1})$.

- Any cyclic code is *polycyclic* with respect to $v = (1, 0, \dots, 0)$. ($v(x) = 1$)

Polycyclic Codes

Definition

A linear code C with length n over a finite field F is called right *polycyclic* with respect to $v = (v_0, v_1, \dots, v_{n-1}) \in F^n$ (with the usual correspondence to $v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}$) if, whenever $c = (c_0, c_1, \dots, c_{n-1})$ is in C , so is its v -polycyclic shift $(v_0c_{n-1}, c_0 + v_1c_{n-1}, \dots, c_{n-2} + v_{n-1}c_{n-1})$.

- Any cyclic code is *polycyclic* with respect to $v = (1, 0, \dots, 0)$. ($v(x) = 1$)
- Any constacyclic code with respect to α , is *polycyclic* with respect to $v = (\alpha, 0, \dots, 0)$. ($v(x) = \alpha$)

Consider the following transformation

$$\begin{aligned} \tau_v: F^n &\rightarrow F^n \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto (v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \dots, c_{n-2} + v_{n-1} c_{n-1}) \end{aligned}$$

- It has the following representation matrix as $\tau_v(c) = T_v c$, and T_v is exactly the companion matrix for $f(x) = x^n - v(x)$.

$$T_v = \begin{bmatrix} 0 & \cdots & \cdots & 0 & v_0 \\ 1 & 0 & \cdots & 0 & v_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & v_{n-1} \end{bmatrix}_{n \times n}$$

Consider the following transformation

$$\begin{aligned} \tau_v: F^n &\rightarrow F^n \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto (v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \dots, c_{n-2} + v_{n-1} c_{n-1}) \end{aligned}$$

- It has the following representation matrix as $\tau_v(c) = T_v c$, and T_v is exactly the companion matrix for $f(x) = x^n - v(x)$.

$$T_v = \begin{bmatrix} 0 & \cdots & \cdots & 0 & v_0 \\ 1 & 0 & \cdots & 0 & v_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & v_{n-1} \end{bmatrix}_{n \times n}$$

- A polycyclic code with respect to v is invariant under τ_v .

- The following type of matrices, called " v -based vector circulant matrix of c " (Jitman, 2013), generate polycyclic codes;

$$G = \begin{bmatrix} c_0 & \cdots & c_{n-1} \\ - & T_v \vec{c} & - \\ - & T_v^2 \vec{c} & - \\ & \vdots & \\ - & T_v^{n-1} \vec{c} & - \end{bmatrix}_{n \times n}$$

Polycyclic Codes Over Finite Chain Rings

An associative finite ring with unity is called a **chain ring** if its ideals are linearly ordered under inclusion. Finite chain rings are **principal ideal rings**; every ideal of these rings is generated by a single element. They are also **local rings**; they have unique maximal ideals.

While constructing linear codes over finite chain rings, we are going to be dealing with **factorization of polynomials** and we also need a **Euclidean type algorithm**, therefore we make use of the corresponding definitions and theorems [Lopez et al., 2013].

Let $K = R/M$ be the residue field of a finite chain ring R . A polynomial f in $R[x]$ is called **basic irreducible** if its image μf under the natural projection $\mu : R[x] \longrightarrow K[x]$, is irreducible over $K[x]$. A *primary* polynomial is defined to be a polynomial which generates a primary ideal; an ideal $I \neq R$, for which $xy \in I$ implies $x \in I$ or $y^n \in I$ for some $n \in \mathbb{Z}^+$. A polynomial f in $R[x]$ is called **regular**, if it is not a zero divisor. We have the following equivalent conditions for regular polynomials.

Theorem (Theorem XIII.11 [McDonald, 1974])

Let f be a regular polynomial in $R[x]$. Then, $f = \delta g_1 \cdots g_n$ where δ is a unit and g_1, \dots, g_n are pairwise coprime regular primary polynomials. If $f = \beta h_1 \cdots h_m$ is another factorization of f where β is a unit and h_1, \dots, h_m are pairwise coprime regular primary polynomials, then $m = n$ and $g_i = h_i$ up to reordering.

As a consequence of this fact, for a **square-free, monic, regular** polynomial f , this factorization into pairwise coprime monic basic irreducible factors is unique up to associates and reordering.

A Euclidean type algorithm also holds as follows:

Theorem ([McDonald, 1974])

Let f and g be polynomials in $R[x]$ such that g is regular. Then, there exist polynomials $q, r \in R[x]$ with $f = qg + r$ and $\deg(r) < \deg(g)$.

Polycyclic Codes as Invariant Submodules

Let f be a square-free, monic regular polynomial in $R[x]$. And let $f(x) = x^n - v(x) = f_1 \cdot f_2 \dots f_t$ be the unique factorization of f into pairwise coprime, monic, basic irreducible polynomials over the finite chain ring R . Consider the submodules $f_i(T_v)x = 0$, where $x \in R^n$. Denoting $U_i = \text{Ker } f_i(\tau_v)$, we give a generalization of the results in [Radkova and Van Zanten, 2009] and [Wu, 2013] to the polycyclic case as follows:

Lemma

- (1) Each U_i is a free τ_v -invariant submodule of R^n .
- (2) If W is a τ_v -invariant submodule of R^n and $W_i = W \cap U_i$ for $i = 1, 2, \dots, t$, then W_i is τ_v -invariant and $W = \bigoplus_{i=1}^t W_i$.
- (3) $R^n = \bigoplus_{i=1}^t U_i$
- (4) $\text{rank}(U_i) = \deg(f_i)$
- (5) The minimal polynomial of τ_v over U_i is $f_i(x)$
- (6) U_i is a free minimal τ_v -invariant submodule of R^n
- (7) If U is a free τ_v -invariant submodule of R^n , then U is a direct sum of some minimal free τ_v -invariant submodules U_i of R^n .

Theorem

Let C be a linear polycyclic code of length n over R . Then the following facts hold

(1) $C = \bigoplus_{j=1}^s U_{i_j}$ for some minimal τ_v -invariant submodules of R^n and

$\text{rank}(C) = \sum_{j=1}^s k_{i_j}$ where k_{i_j} is the rank of U_{i_j}

(2) $h(x) = f_{i_1}(x) \cdot f_{i_2}(x) \cdot \dots \cdot f_{i_s}(x)$ is the minimal polynomial of τ_v over C

(3) $\text{rank}(h(T_v)) = n - \text{rank}(C)$

(4) $c \in C$ if and only if $h(T_v)c = 0$.

- If $g(x) = f(x)/h(x)$ is the generating polynomial of a polycyclic code C , then $H = h(T_v)$ is a parity check matrix for C and $G = g(T_v^{tr})$ is a generator matrix for C which gives the vector-circulant matrix of $c = (g_0, g_1, \dots, g_{n-1})$ with respect to v .

Example

Let $R = GR(2^2, 3)$ be the Galois ring obtained from the quotient ring $\mathbb{Z}_4[x]/(p(x))$ where $p(x)$ is a basic irreducible polynomial of degree 3 with ξ as a primitive root. And let $f(x) = x^7 + 3x^6 + x^4 + 3x^3 + x + 3$. So we have $v(x) = x^6 + 3x^4 + x^3 + 3x + 1$ $v = (1, 3, 0, 1, 3, 0, 1)$ and $f(x)$ has a unique factorization into basic irreducible polynomials g_1, g_2, g_3, g_4 over R as

$$\begin{aligned} f(x) &= g_1(x)g_2(x)g_3(x)g_4(x) \\ g_1(x) &= (x + 3), \\ g_2(x) &= (x^2 + 3\xi x + 1), \\ g_3(x) &= (x^2 + (3\xi^2 + 2)x + 1), \\ g_4(x) &= (x^2 + (\xi^2 + \xi + 1)x + 1). \end{aligned}$$

Example (contd.)

We have

$$T_v = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Let C be the right polycyclic code generated by $g_3(x)g_4(x), 2g_3(x)$. We obtain a generator matrix by evaluating $[g_3g_4 + 2g_3](T_v^{tr})$. In standard form we get;

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & \zeta + 1 & \zeta^2 + 1 & 2\zeta^2 + \zeta \\ 0 & 0 & 1 & \zeta & \zeta^2 + 1 & 2\zeta^2 + \zeta & 3 \\ 0 & 0 & 0 & 2 & 0 & 2\zeta^2 + 2\zeta + 2 & 2\zeta^2 \\ 0 & 0 & 0 & 0 & 2 & 2\zeta^2 & 2 \end{bmatrix} \text{ and } C \text{ is a } (7, 4^9 2^6)$$

linear code over R .

Example

We have searched over quaternary codes of length up to 29 and found many new codes most of which have better parameters than the known ones [Asamov and Aydın, 2007]. Some of them are stated in the related presentation [Bedir and Şiap, 2015].

Applications to DNA

The interest on DNA computing originally was initiated by Adleman where DNA property was used to solve an NP-complete problem [Adleman et al., 1994]. It is also well-known that DNA whenever it reproduces errors may occur and DNA due to its structural properties it can detect such errors and control them.

Reproduction and similar activities in DNA take places in a huge amount and this error control capability of the DNA has attracted many researchers in coding theory. In this direction algebraic codes that resemble the DNA structure so called DNA codes are constructed in many aspects and have been studied intensively.

The researchers have focused on codes with specific properties (reversible, reversible-complement) and studied their structures

([Abulraub et al., 2006, Bayram et al., 2015, Öztaş and Şiap, 2013, Öztaş and Şiap, 2015, Şiap et al., 2009, Yildiz and Şiap, 2012]).

In [Abulraub et al., 2006], by considering additive codes, especially codes over F_4 (a finite field with four elements) where a very natural one to one correspondence between DNA single bases (Adenine(A), Guanine(G), Cytosine(C), Thymine(T)) and the elements of F_4 are studied. Later, in

[Öztaş and Şiap, 2013, Öztaş and Şiap, 2015], elements of F_{16} and $F_{4^{2k}}$ are matched to DNA 2-bases and DNA $2k$ -bases respectively and codes over these fields with specific properties are studied.

The following definition and result are the straight forward generalizations of the concepts in [Öztaş and Şiap, 2013, Öztaş and Şiap, 2015];

Definition

Let $g(x)$ be a polynomial over $F_{4^{2k}}$. $g(x)$ is called a polynomial of 4^k -lifted form, if $g(x)$ have the term $a^j x^i$ and $a^j 4^k x^{\deg(g(x))-i}$ for all $i \in \{0, 1, \dots, \lceil \deg(g(x))/2 \rceil\}$.

Theorem

Let $g(x)$ be a polynomial of 4^k -lifted form over $F_{4^{2k}}$ with $\deg g(x) = t$. For an arbitrary length n , the spanning set

$$S_{g(x)} = \{g(x), xg(x), \dots, x^{n-t-1}g(x)\}$$

generates a polycyclic code C . Then $\Theta(C)$ is a reversible DNA code of length $2kn$. And, the code generated by the spanning set

$$S_{g(x)} = \{g(x), xg(x), \dots, x^{n-t-1}g(x), r(x)\}$$

where $r(x) = 1 + x + \dots + x^{n-1}$, corresponds to a reversible complement DNA code of length $2kn$.

Example

Consider the polynomial $g(x) = 1 + \omega^{14}x + \omega^{11}x^2 + x^3$ over F_{16} , where ω is a root of an irreducible polynomial of degree 4 over the prime field F_2 .

$g(x)$ generates a $[7,4,4]$ optimal polycyclic code which satisfies the Griesmer bound over F_{16} . It is also an MDS code. This code corresponds to a reversible DNA code. The generator matrix is as follows:

$$\begin{pmatrix} 1 & \omega^{14} & \omega^{11} & 1 & 0 & 0 & 0 \\ 0 & 1 & \omega^{14} & \omega^{11} & 1 & 0 & 0 \\ 0 & 0 & 1 & \omega^{14} & \omega^{11} & 1 & 0 \\ 0 & 0 & 0 & 1 & \omega^{14} & \omega^{11} & 1 \end{pmatrix}$$









...

Future Work

Vector circulant matrices have various applications in different areas of coding theory. Some of these applications, which we are examining as a continuing work are

- Constructing Recursive MDS Matrices [Augot and Finiasz, 2015]
- Constructing linear codes over Rank Metric and Term Rank Metric Spaces [Gritsenko and Maevskiy, 2014]

Another further research objective is to examine the structure of polycyclic codes over some noncommutative rings.

-  T. Abulraub, A. Ghrayeb and X. Nian Zeng, Construction of cyclic codes over $GF(4)$ for DNA computing, J. Franklin Inst., 343 (2006), 448–457.
-  L. Adleman, Molecular computation of solutions to combinatorial problems, Science, New Series, 266 (1994), 1021–1024.
-  A. Alahamdi, S. Dougherty, A. Leroy, and P. Sole, On the duality and the direction of polycyclic codes, preprint.
-  A. Asamov, N. Aydın, The database for \mathbb{Z}_4 codes, <http://www.asamov.com/Z4Codes/>, (2007). accessed at June, 2015.
-  Augot D., Finiasz M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes, Lecture Notes in Computer Science, vol. 8540, Springer, Berlin (2015).
-  A. Bayram, E.S. Oztas and I. Siap, Codes over $F_4 + vF_4$ and some DNA applications, Designs, Codes and Cryptography, (2015).
-  S. Bedir and I. Siap, Polycyclic Quaternary Codes, Proceedings of The International Conference on Coding Theory and Cryptography (ICCC2015), Algeria.
-  V. V. Gritsenko and A. E. Maevskiy, On a construction of optimal codes in term rank metric via $p(x)$ -circulants, 14th International Workshop on Algebraic and

Thank you for your attention..