The Cyclic Codes over A_k

Yasemin Cengellenmis, Trakya University, Turkey
Steven Dougherty, University of Scranton, USA

ACCT
Pomorie,Bulgaria
June 15-21, 2012

Table of Contents

History

- $\mathbb{F}_q$: finite field
- $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/ < x^n - 1 >$
- $C \subset \mathbb{F}_q^n \iff \pi(C) \subset \mathbb{F}_q[x]/ < x^n - 1 >$
- A subset C of $\mathbb{F}_q^n$ is called a cyclic code of length n if C satisfies the following conditions:
  *C is a subspace of $\mathbb{F}_q^n$ and
  *If every $c = (c_0, \ldots, c_{n-1}) \in C$ then
  $\sigma(c) = (c_{n-1}, c_0 \ldots, c_{n-2}) \in C$
  (E.Prange,1957)

History

- $\mathbb{Z}_4$
  (1994) A.Hammons,P.V.Kumar,A.R.Calderbank, N.J.A Calderbank,P.Sole
  (1996) V.Pless,Z.Qian
  (1997) V.Pless,P.Sole,Z.Qian
  (2001) J.Wolfmann
  (2003)T.Abualrub,Oehmke
  (2006) S.Dougherty,S.Ling
  (2003) T.Blackford
  (2010) X.Kai,S.Zhu
- $\mathbb{Z}_{p^m}$
  (1995)A.R.Calderbank, N.J.A Sloane
  (2002)S.Ling,T.Blackford
  (1997)P.Kanwar,S.R.Lopez Permouth
  (2007)S.Dougherty,Y.H.Park

History

- $\mathbb{F}_2[u]/ < u^2 >, u^2 = 0$
  (1998) A.Bonnecaze,P.Udaya
- Galois Ring
  (1999) Wan
  (2008) H.M.Kiah,K.H.Leung,S.Ling
  (2009)R.Sobrani,M.Esmaeili
- Finite Chain Ring
  (2000)G.Norton,A.Salagean
  (2004)H.Dihn,S.Lopez-Permouth
  (2008)J.Qian,W.Ma,X.Wang
- $\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$
  (2004)J.F.Qian,L.N.Zhang,Z.X.Zhu
  (2011)M.Han,Y.Ye,S.Zhu,C.Xu,B.Dou
- $\mathbb{Z}_2 + u\mathbb{Z}_2, \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$
  (2007)T.Abualrub,I.Siap
- $\mathbb{F}_2[u]/ < u^2 - 1 >, u^2 = 1$
  (2009) I.Siap,T.Abualrub

History

- $\mathbb{Z}_2 + \ldots + u^{k-1}\mathbb{Z}_2$
  (2010)M.Al-Ashker,M.Hammoudeh
- $\mathbb{F}_2[v]/ < v^2 - v >, v^2 = v$
  (2010)S.Zhu,Y.Wang,M.Shi
- $\mathbb{F}_2[u,v]/ < u^2, v^2, uv - vu >, u^2 = 0, v^2 = 0, uv = vu$
  (2010)B.Yildiz,S.Karadeniz
- $\mathbb{F}_2[u_1, u_2, \ldots, u_n]/ < u_i^2, u_iu_j - u_ju_i >, u_i^2 = 0, u_iu_j = u_ju_i$
  (2011)S.Dougherty,B.Yildiz,S.Karadeniz
- $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$
  (2011)X.U.Xiaofang,L.Xiusheng
- Formal Power Series
  (2011) S.Dougherty,L.Hongwei
- $M_2(\mathbb{F}_2)$
  (2012)A.Alamadhi,H.Sboui,P.Sole,O.Yemen

History

(2010)S.Zhu,Y.Wang,M.Shi

- $R = \mathbb{F}_2[v]/ < v^2 - v >, v^2 = v$
- $\pi : R \to \mathbb{F}_2^2$
  $(a + vb) \mapsto (a, a + b)$
- $C_1 = \{x \in \mathbb{F}_2^n | x, y \in \mathbb{F}_2^n | x + vy \in C\}$
  $C_2 = \{x + y \in \mathbb{F}_2^n | y \in \mathbb{F}_2^n | x + vy \in C\}$
- $C = (1 + v)C_1 \oplus vC_2$
  C cyclic $\iff$? $\quad C_1, C_2$
  $C^\perp = ?$
  C cyclic $\Rightarrow C =?$ $\quad g_1(x), g_2(x)$

Theorem

For any cyclic code C over R, there is a unique polynomial $g(x)$ such that $C =< g(x) >$ and $g(x) | x^n - 1$ where $g(x) = (1 + v)g_1(x) + g_2(x)$.

- C cyclic $\Rightarrow C^\perp = ?$

The Ring A_k and the Gray Map on A_k

For integers $k \geq 1$, $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i, v_i v_j - v_j v_i \rangle$
where $v_i^2 = v_i, v_i v_j = v_j v_i, i = 1, \ldots, k, j = 1, \ldots, k$.
$A_k = \{\sum_{B \in \mathcal{P}_k} \alpha_B v_B \mid \alpha_B \in \mathbb{F}_2, v_B = \prod_{i \in B} v_i, B \subseteq \{1, 2, \ldots, k\}\}$

The Ring A_k and the Gray Map on A_k

For integers $k \geq 1$, $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i, v_i v_j - v_j v_i \rangle$ where $v_i^2 = v_i, v_i v_j = v_j v_i, i = 1, \ldots, k, j = 1, \ldots, k$.
$A_k = \{\sum_{B \in \mathcal{P}_k} \alpha_B v_B \mid \alpha_B \in \mathbb{F}_2, v_B = \prod_{i \in B} v_i, B \subseteq \{1, 2, \ldots, k\}\}$

Example

For $k = 1$, $A_1 = \mathbb{F}_2[v_1]/\langle v_1^2 - v_1 \rangle$ *where* $v_1^2 = v_1$.
For $k = 2$, $A_2 = \mathbb{F}_2[v_1, v_2]/\langle v_1^2 - v_1, v_2^2 - v_2, v_1 v_2 - v_2 v_1 \rangle$ *where* $v_1^2 = v_1, v_2^2 = v_2, v_1 v_2 = v_2 v_1$.

The Ring A_k and the Gray Map on A_k

For integers $k \geq 1$, $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i, v_i v_j - v_j v_i \rangle$ where $v_i^2 = v_i, v_i v_j = v_j v_i, i = 1, \ldots, k, j = 1, \ldots, k$.
$A_k = \{\sum_{B \in \mathcal{P}_k} \alpha_B v_B \mid \alpha_B \in \mathbb{F}_2, v_B = \prod_{i \in B} v_i, B \subseteq \{1, 2, \ldots, k\}\}$

Example

For $k = 1$, $A_1 = \mathbb{F}_2[v_1]/\langle v_1^2 - v_1 \rangle$ where $v_1^2 = v_1$.
For $k = 2$, $A_2 = \mathbb{F}_2[v_1, v_2]/\langle v_1^2 - v_1, v_2^2 - v_2, v_1 v_2 - v_2 v_1 \rangle$ where $v_1^2 = v_1, v_2^2 = v_2, v_1 v_2 = v_2 v_1$.

Lemma

The ring A_k has characteristic 2 and cardinality 2^{2^k}.

Lemma

The only unit in the ring A_k is 1.

The Ring A_k and the Gray Map on A_k

Theorem

The ideal $\langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{v_i, 1 + v_i\}$ for each $i = 1, 2, \ldots, k$, is a maximal ideal of cardinality $2^{2^k - 1}$.

Lemma

Let $\mathfrak{m}_i$ be a maximal ideal as above. Then there are 2^k such ideals and $\mathfrak{m}_i^e = \mathfrak{m}_i$ for all i and $e \geq 1$.

Theorem

The ring A_k is isomorphic via the Chinese Remainder Theorem to $\mathbb{F}_2^{2^k}$. Consequently, the ring A_k is a principal ideal ring.

The Ring A_k and the Gray Map on A_k

- $\phi_1 : A_1 \to \mathbb{F}_2^2$
  $$a + bv_1 \mapsto \phi_1(a + bv_1) = (a, a + b)$$
- For $k \geq 2$,
  $$\phi_k : A_k \to A_{k-1}^2$$
  $$\alpha + \beta v_k \mapsto \phi_k(\alpha + \beta v_k) = (\alpha, \alpha + \beta)$$
- $\Phi_k : A_k \to \mathbb{F}_2^{2^k}$
  $$\Phi_k(\gamma) = \phi_1(\phi_2(\ldots(\phi_{k-2}(\phi_{k-1}(\phi_k(\gamma)))))$$

The Linear Codes over A_k

A linear code C over A_k of length n is a submodule of A_k^n

The Linear Codes over A_k

A linear code C over A_k of length n is a submodule of A_k^n

- $C = (m_1)C_1 \oplus \ldots \oplus (m_{2^k})C_{2^k}$
- $C^\perp = (m_1)C_1^\perp \oplus \ldots \oplus (m_{2^k})C_{2^k}^\perp$

The Cyclic codes over A_k

Definition

A subset C of A_k^n is called a cyclic code of length n if C satisfies the following conditions:
* C is a submodule of A_k^n
*   If every $c = (c_0, \ldots, c_{n-1}) \in C$ then
$\sigma(c) = (c_{n-1}, c_0 \ldots, c_{n-2}) \in C$

The Cyclic codes over A_k

Definition

A subset C of A_k^n is called a cyclic code of length n if C satisfies the following conditions:

* C is a submodule of A_k^n

* If every $c = (c_0, \ldots, c_{n-1}) \in C$ then

$\sigma(c) = (c_{n-1}, c_0 \ldots, c_{n-2}) \in C$

Theorem

Let C be a code over A_k and let C_i be the binary codes given before. The code C is cyclic if and only if C_i is a cyclic code for all i.

The Cyclic codes over A_k

Definition

A subset C of A_k^n is called a cyclic code of length n if C satisfies the following conditions:

* C is a submodule of A_k^n

* If every $c = (c_0, \dots, c_{n-1}) \in C$ then $\sigma(c) = (c_{n-1}, c_0 \dots, c_{n-2}) \in C$

Theorem

Let C be a code over A_k and let C_i be the binary codes given before. The code C is cyclic if and only if C_i is a cyclic code for all i.

Corollary

If a code C over A_k is cyclic then $C^\perp$ is cyclic.

The Cyclic codes over A_k

$$C = (m_1)C_1 \oplus \ldots \oplus (m_{2^k})C_{2^k}$$

The Cyclic codes over A_k

$$C = (m_1)C_1 \oplus \ldots \oplus (m_{2^k})C_{2^k}$$

Theorem

Let C be a cyclic code over A_k then there exist a polynomial $g(x)$ in $A_k[x]$ that divides $x^n - 1$ that generates the code.

The Cyclic codes over A_k

For a polynomial, $p(x) = a_0 + \ldots + a_k x^k$ define $\overline{p(x)} = a_k + a_{k-1}x + \ldots + a_0 x^k$

The Cyclic codes over A_k

For a polynomial, $p(x) = a_0 + \ldots + a_k x^k$ define $\overline{p(x)}$=$a_k + a_{k-1}x + \ldots + a_0 x^k$

Lemma

If C is a cyclic code over A_k generated by $g(x)$ then $C^\perp$ is a cyclic code generated by $\overline{(x^n - 1/g(x))}$.

The Gray image of the Self Dual Cyclic Codes over A_k

Definition

Let $\mathbf{a} \in \mathbb{F}_2^{2^k n}$ *with* $\mathbf{a} = (a_0, \ldots, a_{2^k n-1}) = (a^{(0)}|a^{(1)}| \ldots |a^{(2^k-1)})$, $a^{(i)} \in \mathbb{F}_2^n$ *for* $i = 0, 1, \ldots, 2^k - 1$. *Let* $\sigma^{\otimes 2^k}$ *be the map from* $\mathbb{F}_2^{2^k n}$ *to* $\mathbb{F}_2^{2^k n}$ *given by* $\sigma^{\otimes 2^k}(\mathbf{a}) = (\sigma(a^{(0)})| \ldots |\sigma(a^{(2^k-1)}))$ *where* σ *is the usual shift* $(c_0, \ldots, c_{n-1}) \mapsto (c_{n-1}, c_0, \ldots, c_{n-2})$ *on* $\mathbb{F}_2^n$.
A code C *of length* $2^k n$ *over* $\mathbb{F}_2$ *is said to be quasi-cyclic of index* 2^k *if* $\sigma^{\otimes 2^k}(C) = C$.

The Gray image of the Self Dual Cyclic Codes over A_k

Definition

Let $\mathbf{a} \in \mathbb{F}_2^{2^k n}$ with $\mathbf{a} = (a_0, \ldots, a_{2^k n-1}) = (a^{(0)}|a^{(1)}|\ldots|a^{(2^k-1)})$, $a^{(i)} \in \mathbb{F}_2^n$ for $i = 0, 1, \ldots, 2^k - 1$. Let $\sigma^{\otimes 2^k}$ be the map from $\mathbb{F}_2^{2^k n}$ to $\mathbb{F}_2^{2^k n}$ given by $\sigma^{\otimes 2^k}(\mathbf{a}) = (\sigma(a^{(0)})|\ldots|\sigma(a^{(2^k-1)}))$ where σ is the usual shift $(c_0, \ldots, c_{n-1}) \mapsto (c_{n-1}, c_0, \ldots, c_{n-2})$ on $\mathbb{F}_2^n$.
A code C of length $2^k n$ over $\mathbb{F}_2$ is said to be quasi-cyclic of index 2^k if $\sigma^{\otimes 2^k}(C) = C$.

Corollary

The image of a cyclic self dual code of length n over A_k is a length $2^k n$ self dual quasi-cyclic code of index 2^k.

Bibliography

- C. Bachoc,Application of Coding Theory to the Construction of Modular Lattices,J.Combin Theory Ser.A78,92-119,1997
- Y.Cengellenmis,A.Dertli,S.Dougherty,Cyclic and Skew Cyclic Codes over an Infinite Family of Rings with Gray Map,in submission
- Y.Cengellenmis,On the Cylic codes over $\mathbb{F}_3 + v\mathbb{F}_3$,International Journal of Algebra,4,no 6,253-259,2010
- N.J.A Sloane,J.G.Thompson, Cyclic Self Dual Codes,IEEE Trans.Information Theory,IT-29,364-366,1983
- S.Zhu,Y.Wang,M.J.Shi,Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$,ISIT,Korea,2009

Thank you for your attention...