Codes over Infinite Family of Algebras

Irwansyah
Intan Muchtadi
Ahmad Muchlis
Aleams Barra
Djoko Supriyanto

Department of Mathematics
Institut Teknologi Bandung, Indonesia

Lens, June 9, 2015

Introductions

- Corresponding ring is $B_k = \mathbb{F}_p[v_1, \ldots, v_k]$, where $v_i^2 = v_i$ for all $i = 1, \ldots, k$.

Introductions

- Corresponding ring is $B_k = \mathbb{F}_p[v_1, \ldots, v_k]$, where $v_i^2 = v_i$ for all $i = 1, \ldots, k$.
- A code over B_k is a subset of B_k^n.

Introductions

- Corresponding ring is $B_k = \mathbb{F}_p[v_1, \ldots, v_k]$, where $v_i^2 = v_i$ for all $i = 1, \ldots, k$.
- A code over B_k is a subset of B_k^n.
- A linear codes over B_k is a B_k-submodule of B_k^n.

- B_k is a commutative algebra over $\mathbb{F}_p$.

- B_k is a commutative algebra over $\mathbb{F}_p$.
- In [Cengellenmis and Dougherty, 2012], there are many nice properties of codes over B_k, with $p = 2$, including Gray maps, MacWiliams relations, relation to complex lattices, *etc*.

- B_k is a commutative algebra over $\mathbb{F}_p$.
- In [Cengellenmis and Dougherty, 2012], there are many nice properties of codes over B_k, with $p = 2$, including Gray maps, MacWiliams relations, relation to complex lattices, *etc*.
- In [Abualrub *et al*, 2012], structures of skew-cyclic codes over B_1, with $p = 2$, have been studied via skew-polynomial ring

- B_k is a commutative algebra over $\mathbb{F}_p$.
- In [Cengellenmis and Dougherty, 2012], there are many nice properties of codes over B_k, with $p = 2$, including Gray maps, MacWiliams relations, relation to complex lattices, *etc*.
- In [Abualrub *et al*, 2012], structures of skew-cyclic codes over B_1, with $p = 2$, have been studied via skew-polynomial ring and they find some optimal Euclidean self-dual codes.

- B_k is a commutative algebra over $\mathbb{F}_p$.
- In [Cengellenmis and Dougherty, 2012], there are many nice properties of codes over B_k, with $p = 2$, including Gray maps, MacWiliams relations, relation to complex lattices, *etc*.
- In [Abualrub *et al*, 2012], structures of skew-cyclic codes over B_1, with $p = 2$, have been studied via skew-polynomial ring and they find some optimal Euclidean self-dual codes.
- Others then insterested to study skew-cyclic codes over this ring in general.

Properties of the ring B_k

Lemma

Properties of the ring B_k

Lemma

- The ring B_k can be viewed as an $\mathbb{F}_p$-vector space with dimension 2^k and basis consists of elements of the form $\beta^{|B|}\prod_{i\in B} w_i$, for some $\beta \in B_k^{\times}$, where $B \subseteq \{1,\ldots,k\}$ and $w_i \in \{v_i, 1-v_i\}$, and 1.

Properties of the ring B_k

Lemma

- The ring B_k can be viewed as an $\mathbb{F}_p$-vector space with dimension 2^k and basis consists of elements of the form $\beta^{|B|}\prod_{i\in B} w_i$, for some $\beta \in B_k^{\times}$, where $B \subseteq \{1,\ldots,k\}$ and $w_i \in \{v_i, 1-v_i\}$, and 1.
- The ring B_k has characteristic p and cardinality $(p)^{2^k}$.

Properties of the ring B_k

Lemma

- The ring B_k can be viewed as an $\mathbb{F}_p$-vector space with dimension 2^k and basis consists of elements of the form $\beta^{|B|}\prod_{i\in B} w_i$, for some $\beta \in B_k^{\times}$, where $B \subseteq \{1,\ldots,k\}$ and $w_i \in \{v_i, 1-v_i\}$, and 1.
- The ring B_k has characteristic p and cardinality $(p)^{2^k}$.
- $\omega \in B_k$ is a zero divisor if and only if $\omega \in \langle w_1, w_2, \ldots, w_k\rangle$, where $w_i \in \{\beta v_i, \beta(1-v_i)\}$ for all $i = 1, 2, \ldots, k$, for some unit β.

Prop.

An ideal I in B_k is maximal if and only if

Prop.

An ideal I in B_k is maximal if and only if $I = \langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{\beta v_i, \beta(1 - v_i)\}$ for all $i = 1, 2, \ldots, k$, for some unit β.

Prop.

An ideal I in B_k is maximal if and only if $I = \langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{\beta v_i, \beta(1 - v_i)\}$ for all $i = 1, 2, \ldots, k$, for some unit β.

Prop. 2

Let θ be an endomorphism in B_k. Then, θ is an automorphism if and only if

Prop.

An ideal I in B_k is maximal if and only if $I = \langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{\beta v_i, \beta(1 - v_i)\}$ for all $i = 1, 2, \ldots, k$, for some unit β.

Prop. 2

Let θ be an endomorphism in B_k. Then, θ is an automorphism if and only if $\theta(w_i) = \beta w_j$, for every $i \in \{1, \ldots, k\}$, where β is a unit in B_k, and $\theta(a) = a$, for every $a \in \mathbb{F}_p$.

Gray map

Gray map

$$\begin{array}{rcccl} \varphi & : & B_k & \to & \mathbb{F}_p^{2^k} \\ & & a = \sum_{i=1}^{\lambda} \alpha_{S_i} w_{S_i} & \mapsto & (\alpha_{S_1}, \sum_{B \subseteq S_2} \alpha_B, \ldots, \sum_{B \subseteq S_\lambda} \alpha_B) \end{array}$$

Gray map

$$\begin{array}{rcccl} \varphi & : & B_k & \to & \mathbb{F}_p^{2^k} \\ & & a = \sum_{i=1}^{\lambda} \alpha_{S_i} w_{S_i} & \mapsto & (\alpha_{S_1}, \sum_{B \subseteq S_2} \alpha_B, \ldots, \sum_{B \subseteq S_\lambda} \alpha_B) \end{array}$$

where $w_{S_i} = \prod_{i \in S_i} w_i$ and $S_i \subseteq \{1, \ldots, k\}$.

Gray map

$$\begin{array}{rcccl} \varphi & : & B_k & \to & \mathbb{F}_p^{2^k} \\ & & a = \sum_{i=1}^{\lambda} \alpha_{S_i} w_{S_i} & \mapsto & (\alpha_{S_1}, \sum_{B \subseteq S_2} \alpha_B, \ldots, \sum_{B \subseteq S_\lambda} \alpha_B) \end{array}$$

where $w_{S_i} = \prod_{i \in S_i} w_i$ and $S_i \subseteq \{1, \ldots, k\}$.

Remark

- There is one-on-one correspondence between φ and automorphism in B_k up to lexicographic order.
- This map should be a permutation of similar map in [Cengellenmis and Dougherty, 2012]

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if there exist linear codes, $C_1, \ldots, C_\lambda$, over $\mathbb{F}_p$ such that

$$C = \varphi^{-1}(C_1, \ldots, C_{2^k}).$$

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if there exist linear codes, $C_1, \ldots, C_\lambda$, over $\mathbb{F}_p$ such that

$$C = \varphi^{-1}(C_1, \ldots, C_{2^k}).$$

Equivalence

Two codes C and C' over B_k are equivalent

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if there exist linear codes, $C_1, \ldots, C_\lambda$, over $\mathbb{F}_p$ such that

$$C = \varphi^{-1}(C_1, \ldots, C_{2^k}).$$

Equivalence

Two codes C and C' over B_k are equivalent if either they are permutation-equivalent or

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if there exist linear codes, $C_1, \ldots, C_\lambda$, over $\mathbb{F}_p$ such that

$$C = \varphi^{-1}(C_1, \ldots, C_{2^k}).$$

Equivalence

Two codes C and C' over B_k are equivalent if either they are permutation-equivalent or C is permutation equivalent to the code $\theta(C')$ for some automorphism θ in A_k, *i.e.* the code $\theta(C')$ obtained from C' by changing c' with $\theta(c')$ in all coordinates.

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if there exist linear codes, $C_1, \ldots, C_\lambda$, over $\mathbb{F}_p$ such that

$$C = \varphi^{-1}(C_1, \ldots, C_{2^k}).$$

Equivalence

Two codes C and C' over B_k are equivalent if either they are permutation-equivalent or C is permutation equivalent to the code $\theta(C')$ for some automorphism θ in A_k, *i.e.* the code $\theta(C')$ obtained from C' by changing c' with $\theta(c')$ in all coordinates.

Characterization

C and C' are equivalent if and only if

Characterization for codes over B_k

C is a B_k-linear code with length n if and only if there exist linear codes, $C_1, \ldots, C_\lambda$, over $\mathbb{F}_p$ such that

$$C = \varphi^{-1}(C_1, \ldots, C_{2^k}).$$

Equivalence

Two codes C and C' over B_k are equivalent if either they are permutation-equivalent or C is permutation equivalent to the code $\theta(C')$ for some automorphism θ in A_k, *i.e.* the code $\theta(C')$ obtained from C' by changing c' with $\theta(c')$ in all coordinates.

Characterization

C and C' are equivalent if and only if there exists a permutation which sends $(C_1, \ldots, C_s)$ to $(C'_1, \ldots, C'_s)$ or to $(C'_1, C'_{\lambda_1}, C'_2, \ldots, C'_{\lambda_1-1}, \ldots, C'_{\lambda_t}, \ldots, C'_{\lambda_t-1}, C'_s)$.

Other Properties

Euclidean self-dual codes

Let $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$.

Other Properties

Euclidean self-dual codes

Let $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$. C is a self-dual code over B_k if and only if

Other Properties

Euclidean self-dual codes

Let $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$. C is a self-dual code over B_k if and only if $C_1, \ldots, C_\lambda$ are also self-dual codes over $\mathbb{F}_p$ and $C_1 = C_2 = \cdots = C_{2^k}$.

Other Properties

Euclidean self-dual codes

Let $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$. C is a self-dual code over B_k if and only if $C_1, \ldots, C_\lambda$ are also self-dual codes over $\mathbb{F}_p$ and $C_1 = C_2 = \cdots = C_{2^k}$.

Minimum Hamming distance

If $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$, for some codes $C_1, \ldots, C_{2^k}$ over $\mathbb{F}_p$,

Other Properties

Euclidean self-dual codes

Let $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$. C is a self-dual code over B_k if and only if $C_1, \ldots, C_\lambda$ are also self-dual codes over $\mathbb{F}_p$ and $C_1 = C_2 = \cdots = C_{2^k}$.

Minimum Hamming distance

If $C = \overline{\varphi}^{-1}(C_1, \ldots, C_{2^k})$, for some codes $C_1, \ldots, C_{2^k}$ over $\mathbb{F}_p$, then $d_H(C) = \min_{1 \leq i \leq 2^k} d_H(C_i)$.

MacWiliams Relation

MacWiliams Relation

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p^{2^k} - 1)Y, X - Y)$$

Group Action

MacWiliams Relation

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p^{2^k} - 1)Y, X - Y)$$

Group Action

- $\langle T, D \rangle$,

MacWiliams Relation

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p^{2^k} - 1)Y, X - Y)$$

Group Action

- $\langle T, D \rangle$,
- $T = \begin{pmatrix} \frac{1}{p^{2^{k-1}}} & \frac{p^{2^k}-1}{p^{2^{k-1}}} \\ \frac{1}{p^{2^{k-1}}} & \frac{-1}{p^{2^{k-1}}} \end{pmatrix}$ and

MacWiliams Relation

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p^{2^k} - 1)Y, X - Y)$$

Group Action

- $\langle T, D \rangle$,
- $T = \begin{pmatrix} \frac{1}{p^{2^k-1}} & \frac{p^{2^k}-1}{p^{2^k-1}} \\ \frac{1}{p^{2^k-1}} & \frac{-1}{p^{2^k-1}} \end{pmatrix}$ and $D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

MacWiliams Relation

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p^{2^k} - 1)Y, X - Y)$$

Group Action

- $\langle T, D \rangle$,
- $T = \begin{pmatrix} \frac{1}{p^{2^k-1}} & \frac{p^{2^k}-1}{p^{2^k-1}} \\ \frac{1}{p^{2^k-1}} & \frac{-1}{p^{2^k-1}} \end{pmatrix}$ and $D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Lemma

If $W_C(X,Y)$ is a Hamming weight enumerator for a self-dual code C over B_k,

MacWiliams Relation

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X + (p^{2^k} - 1)Y, X - Y)$$

Group Action

- $\langle T, D \rangle$,
- $T = \begin{pmatrix} \frac{1}{p^{2^k-1}} & \frac{p^{2^k}-1}{p^{2^k-1}} \\ \frac{1}{p^{2^k-1}} & \frac{-1}{p^{2^k-1}} \end{pmatrix}$ and $D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Lemma

If $W_C(X,Y)$ is a Hamming weight enumerator for a self-dual code C over B_k, then $W_C(X,Y)$ is invariant under the action of G.

Invariant ring

Invariant ring of G is generated by $W_{C_0}(x,y) = x^2 + (p^{2^k} - 1)y^2$ and $\tilde{f}(x,y) = \frac{1}{4}\left(\frac{2p^{2^{k-1}}+2}{p^{2^k}}x^2 + \frac{4\left(p^{2^k}-1\right)}{p^{2^{k-1}}}xy + \frac{2(p^{2^k}-1)^2}{p^{2^{k-1}}}y^2\right)$.

Invariant ring

Invariant ring of G is generated by $W_{C_0}(x,y) = x^2 + (p^{2^k} - 1)y^2$ and $\tilde{f}(x,y) = \frac{1}{4}\left(\frac{2p^{2^{k-1}}+2}{p^{2^k}}x^2 + \frac{4\left(p^{2^k}-1\right)}{p^{2^{k-1}}}xy + \frac{2(p^{2^k}-1)^2}{p^{2^{k-1}}}y^2\right)$.

Remark

$W_{C_0}(x,y) = x^2 + (p^{2^k} - 1)y^2$ is the Hamming weight enumerator for repetition code.

Remarks

- The result can be generalized to the ring $\mathbb{F}_{p^r}[v_1, \ldots, v_k]$, where $v_i^2 = v_i$.
- It is interesting to study skew-cyclic codes over B_k, since it has a connection to skew-cyclic codes over finite field which gives optimal Euclidean self-dual skew-cyclic codes, see [Boucher and Ulmer, 2009].

Thank You