On Quasi-Abelian Complementary Dual Codes

Somphong Jitman[1], Herbert S. Palines [2], and Romar B. dela Cruz [3]

5th International Castle Meeting on Coding Theory and Applications
Vihula, Estonia

August 28-31, 2017

[1]Silpakorn University, Thailand
[2]University of the Philippines Los Baños
[3]University of the Philippines Diliman

Table of contents

Introduction

Let G be a finite abelian group, written additively, $|G| = n$ and $H \leq G$.
Let $G := \{g_1, g_2, \ldots g_n\}$.

- $\mathbb{F}_q[G] := \{\sum_{i=1}^{n} u_{g_i} Y^{g_i} : u_{g_i} \in \mathbb{F}_q\}$
- $\mathbb{F}_q^n := \{(u_{g_1}, u_{g_2}, \ldots, u_{g_n}) : u_{g_i} \in \mathbb{F}_q\}$
- Let $h \in H$ and $u := (u_{g_1}, u_{g_2}, \ldots, u_{g_n})$,

$$h(c) := (u_{g_1+h}, u_{g_2+h}, \ldots, u_{g_n+h})$$

- Suppose B is a linear code in $\mathbb{F}_q^n$.

$$h(B) := \{h(u) : u \in B\}$$

Introduction

Let G be a finite abelian group, written additively, $|G| = n$ and $H \leq G$.

- $C \subseteq \mathbb{F}_q[G]$ is a quasi-abelian code if C is an $\mathbb{F}_q[H]$-module of $\mathbb{F}_q[G]$
- B is a $G - H$ code if $h(B) = B$ for all $h \in H$
- quasi-abelian codes $C \leftrightarrow G - H$ codes B (Wasan, 1977)
- Let $h \in H$. $h(B) := \{h(u) = (u_{g_1+h}, u_{g_2+h}, \ldots, u_{g_n+h}) : u \in B\}$

  $H = G$ is cyclic $\implies$ Cyclic codes

  $H = G$ is non-cyclic $\implies$ Abelian codes

  $H \neq G$ is cyclic $\implies$ QC codes
- C is a Linear Complementary Dual (LCD) code if $C \cap C^{\perp}$

Motivations

- Bazzi and Mitter, "Some randomized code constructions from group actions" (2006)
- Jitman and Ling "Quasi-abelian codes" (2015)
- Yang and Massey, "The condition for a cyclic code to have a complementary dual" (1994)
- Esmaeili and Yari, "On complementary-dual quasi-cylic codes" (2009)
- Guneri, Ozkaya and Solé, "Quasi-cylic complementary dual codes" (2016)
- Carlet, and Guilley, "Complementary dual codes for countermeasures to side-channel attacks" (2015)

Motivations

"We aim to extend the investigation of LCD codes in the class of quasi-abelian codes."

Characterization

Decompositions

Let $H \leq G$, $[G : H] = l$, and $R := \mathbb{F}_q[H]$. Let $e_1, e_2, \ldots e_t$ be the primitive idempotents of R. Then

$$\mathbb{F}_q[G] \cong R^l \cong \bigoplus_{i=1}^{t} (Re_i)^l.$$

$$C \leftrightarrow \Phi(C) \leftrightarrow \prod_{i=1}^{t} C_i$$

QA codes $\leftrightarrow$ linear codes $\leftrightarrow$ cross product of linear codes

Characterization

Decompositions

Let $H \leq G$, $[G : H] = l$, and $R := \mathbb{F}_q[H]$. Let $e_1, e_2, \ldots e_t$ be the primitive idempotents of R.

- primitive idempotents $\leftrightarrow$ q-cylclotomic classes of H (Ding, Kohel, and Ling, 2000)

- $\gcd(q, |H|) = 1$, $h \in H$,

$$S_q(h) := \{q^i \cdot h \mid i = 0, 1, \ldots\} = \{q^i \cdot h \mid 0 \leq i < \nu_h\}$$

  - $q^i \cdot h := h + h + \ldots + h$ in H
  - ν_h: smallest positive integer such that $q^{\nu_h} \equiv 1 (\text{mod } \text{ord}(h))$
  - $\text{ord}(h)$: order of h in H

- q-cyclotomic classes of $H \implies$ decomposition of C

Characterization

Decompositions: types of q-cyclotomic classes

Euclidean Case (Jitman, Ling, Liu, and Xie, 2013)

- Type I_{E}: $a = -a$, i.e., $S_q(a) = S_q(-a))$
- Type II_{E}: $S_q(a) = S_q(-a)$ and $a \neq -a$
- Type III_{E}: $S_q(a) \neq S_q(-a)$

Hermitian Case, $q = q_0^2$ (Jitman, Ling, and Solé, 2014)

- Type I_{H}: $S_q(a) = S_q(-q_0 \cdot a)$
- Type II_{H}: $S_q(a) \neq S_q(-q_0 \cdot a$

$$-q_0 \cdot a = (-a) + (-a) + \ldots + (-a) \in H$$

Characterization

Decompositions

Euclidean Case (Jitman, Ling, Liu, and Xie, 2013)

$$\mathbb{F}_q[G] \cong R^l \cong \bigoplus_{i=1}^{t} (Re_i)^l$$

$$\cong \left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} \mathbb{F}_q^l \right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} \mathbb{F}_{q^{s_j}}^l \right) \times \left(\prod_{r=1}^{r_{III_{\mathrm{E}}}} \left(\mathbb{F}_{q^{t_r}}^l \times \mathbb{F}_{q^{t_r'}}^l \right) \right)$$

Hermitian Case, $q = q_0^2$ (Jitman, Ling, and Solé, 2014)

$$\mathbb{F}_q[G] \cong R^l \cong \bigoplus_{i=1}^{t} (Re_i)^l$$

$$\cong \left(\prod_{i=1}^{r_{I_{\mathrm{H}}}} \mathbb{F}_{q^{s_i}}^l \right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{H}}}} (\mathbb{F}_{t_j}^l \times \mathbb{F}_{t_j'}^l) \right)$$

Characterization

Decompositions

Euclidean Case

$$\mathbb{F}_q[G] \cong \left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} \mathbb{F}_q^l\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} \mathbb{F}_{q^{s_j}}^l\right) \times \left(\prod_{r=1}^{r_{III_{\mathrm{E}}}} \left(\mathbb{F}_{q^{t_r}}^l \times \mathbb{F}_{q^{t'_r}}^l\right)\right)$$

Complete set of representatives of q-cyclotomic classes of H:

$$\{a_1, a_2, \ldots, a_t\}$$

$$\begin{array}{ccc} e_1, e_2, \ldots, e_{r_{I_{\mathrm{E}}}} & \leftrightarrow & a_1, a_2, \ldots, a_{r_{I_{\mathrm{E}}}} \\ e_{r_{I_{\mathrm{E}}}+1}, e_{r_{I_{\mathrm{E}}}+2}, \ldots, e_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}} & \leftrightarrow & a_{r_{I_{\mathrm{E}}}+1}, a_{r_{I_{\mathrm{E}}}+2}, \ldots, a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}} \\ \left(e_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r}, e_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r_{III_{\mathrm{E}}}+r}\right) & \leftrightarrow & \left(a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r}, a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r_{III_{\mathrm{E}}}+r}\right) \end{array}$$

$a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r_{III_{\mathrm{E}}}+r} = -a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r}$, $r = 1, 2, \ldots r_{III_{\mathrm{E}}}$

$t = r_{I_{\mathrm{E}}} + r_{II_{\mathrm{E}}} + 2r_{III_{\mathrm{E}}}$

$s_j := |S_q(a_{r_{I_{\mathrm{E}}}+j})|$; $t_r := |S_q(a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r})| = |S_q(-a_{r_{I_{\mathrm{E}}}+r_{II_{\mathrm{E}}}+r})| =: t'_r$

Characterization

Decompositions

Euclidean Case

$$\mathbb{F}_q[G] \cong \left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} \mathbb{F}_q^l\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} \mathbb{F}_{q^{s_j}}^l\right) \times \left(\prod_{r=1}^{r_{III_{\mathrm{E}}}} \left(\mathbb{F}_{q^{t_r}}^l \times \mathbb{F}_{q^{t_r'}}^l\right)\right)$$

$$C \cong \left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} B_i\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} C_j\right) \times \left(\prod_{r=1}^{r_{III_{\mathrm{E}}}} (D_r \times D_r')\right)$$

Hermitian Case, $q = q_0^2$

$$\mathbb{F}_q[G] \cong \left(\prod_{i=1}^{r_{I_{\mathrm{H}}}} \mathbb{F}_{q^{s_i}}^l\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{H}}}} (\mathbb{F}_{t_j}^l \times \mathbb{F}_{t_j'}^l)\right)$$

$$C \cong \left(\prod_{i=1}^{r_{I_{\mathrm{H}}}} C_i\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{H}}}} (D_j \times D_j')\right)$$

Characterization

Euclidean Case

$$C \cong \left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} B_i\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} C_j\right) \times \left(\prod_{r=1}^{r_{III_{\mathrm{E}}}} (D_r \times D'_r)\right)$$

$$C^{\perp_{\mathrm{E}}} \cong \left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} B_i^{\perp_{\mathrm{e}}}\right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} C_j^{\perp_{\mathrm{h}}}\right) \times \left(\prod_{r=1}^{r_{III_{\mathrm{E}}}} \left((D'_r)^{\perp_{\mathrm{e}}} \times D_r^{\perp_{\mathrm{e}}}\right)\right)$$

Proposition

A quasi-abelian code C of index I is an H-QAECD code if and only if the following conditions hold:

(*i*) B_i is an ECD code, for each $i = 1, 2, \ldots r_{I_{\mathrm{E}}}$,

(*ii*) C_j is an HCD code, for each $j = 1, 2, \ldots r_{II_{\mathrm{E}}}$, and

(*iii*) $D_r \oplus (D'_r)^{\perp_{\mathrm{e}}} = \mathbb{F}_{q^{t_r}}^{I}$ for each $r = 1, 2, \ldots, r_{III_{\mathrm{E}}}$.

Characterization

Proposition

A quasi-abelian code C of index l is an H-QAECD code if and only if the following conditions hold:

(*i*) B_i is an ECD code, for each $i = 1, 2, \ldots r_{I_{\mathrm{E}}}$,

(*ii*) C_j is an HCD code, for each $j = 1, 2, \ldots r_{II_{\mathrm{E}}}$, and

(*iii*) $D_r \oplus (D'_r)^{\perp_{\mathrm{e}}} = \mathbb{F}^l_{q^{tr}}$ for each $r = 1, 2, \ldots, r_{III_{\mathrm{E}}}$.

Proof outline: C is a QAECD code is equivalent to the following based on the decompositions above:

$$B_i \cap B_i^{\perp_{\mathrm{e}}} = \{0\}$$

$$C_j \cap C_j^{\perp_{\mathrm{h}}} = \{0\}$$

$$D'_r \cap D_r^{\perp_{\mathrm{e}}} = \{0\} \leftrightarrow D_r \oplus (D'_r)^{\perp_{\mathrm{e}}} = \mathbb{F}^l_{q^{tr}}.$$

Characterization

Hermitian Case ($q = q_0^2$)

$$C \cong \left(\prod_{i=1}^{r_{I_{\mathrm{H}}}} C_i \right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{H}}}} (D_j \times D_j') \right)$$

$$C^{\perp_{\mathrm{H}}} \cong \left(\prod_{i=1}^{r_{I_{\mathrm{H}}}} C_i^{\perp_{\mathrm{h}}} \right) \times \left(\prod_{j=1}^{r_{II_{\mathrm{H}}}} \left((D_j')^{\perp_{\mathrm{e}}} \times D_j^{\perp_{\mathrm{e}}} \right) \right)$$

Proposition

A quasi-abelian code C of index I is an H-QAHCD code if and only if the following conditions hold:

(*i*) C_i is an HCD code, for each $i = 1, 2, \ldots r_{I_{\mathrm{H}}}$, and

(*ii*) $D_j \oplus (D_j')^{\perp_{\mathrm{e}}} = \mathbb{F}_{q^{t_j}}^{I}$ for each $j = 1, 2, \ldots, r_{II_{\mathrm{H}}}$.

Enumeration

Proposition (Euclidean Case)

The the number of H-QAECD codes C is given by

$$\left(\prod_{i=1}^{r_{I_{\mathrm{E}}}} N_{ECD}(q,l)\right)\left(\prod_{j=1}^{r_{II_{\mathrm{E}}}} N_{HCD}(q^{s_j},l)\right)\left(\prod_{r=1}^{r_{III_{\mathrm{E}}}}\left(2+\sum_{k=1}^{l-1}\left(\begin{bmatrix} l \\ k \end{bmatrix}_{q^{t_r}} \cdot N_{\oplus}(q^{t_r},k,l)\right)\right)\right).$$

- $N_{ECD}(q,l)$: no. of ECD codes in $\mathbb{F}_q^l$
- $N_{HCD}(q^{s_j},l)$: no. of HCD codes in $\mathbb{F}_{q^{s_j}}^l$
- $\begin{bmatrix} l \\ k \end{bmatrix}_{q^{t_r}}$: no. of k-dimensional subspaces of $\mathbb{F}_{q^{t_r}}^l$
- $N_{\oplus}(q^{t_r},k,l)$: no. of codes D_r' such that $D_r \oplus (D_r')^{\perp_{\mathrm{e}}} = \mathbb{F}_{q^{t_r}}^l$, for a fixed D_r of dimension k

Enumeration

Proposition (Hermitian Case)

The the number of H-QAHCD codes C is given by

$$\left(\prod_{i=1}^{r_{I_{\mathrm{H}}}} N_{HCD}(q^{s_i}, l)\right)\left(\prod_{j=1}^{r_{II_{\mathrm{H}}}}\left(2+\sum_{k=1}^{l-1}\left(\begin{bmatrix} l \\ k \end{bmatrix}_{q^{t_j}} \cdot N_{\oplus}(q^{t_j}, k, l)\right)\right)\right).$$

Enumeration

$N_{ECD}(q, l) = ?$ $N_{HCD}(q, l) = ?$ $N_{\oplus}(q, k, l) = (q^k)^{l-k}$

Lemma (Index 2 case)

Let q be a prime power. Then

(*i*)

$$N_{ECD}(q, 2) = \begin{cases} q+2 & \text{if } q \text{ is even,} \\ q+1 & \text{if } q \equiv 1 \pmod 4 \\ q+3 & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

(*ii*) if $q = q_0^2$,

$$N_{HCD}(q, 2) = q - q_0 + 2.$$

Enumeration

Proof outline:

(i)

- Count the number of generators of ECD codes in $\mathbb{F}_q^n$ of dimensions 0,1,2.
- dimension 1: $(\alpha, 0)$, $(0, \alpha)$, $(1, \alpha)$, $\alpha \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.
- Count the no. of α such that $1 + \alpha^2 \neq 0$
- $O := \{\alpha \in \mathbb{F}_q^* : \alpha^2 = -1\}$
- $f : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$ s.t. $f(x) = x^2$
- If q is even, f is bijective $\implies$ there is only one solution for $\alpha^2 = -1$, i.e., $|O| = 1$
- $N_{ECD}(q, 2) = 2 + 2 + (q - 1 - 1) = q + 2$
- If q is odd, -1 is a square if and only if $q \equiv 1 (\mathrm{mod} 4)$

(ii) Note: $q = q_0^2$. Use $Nrm : \mathbb{F}_q^* \longrightarrow \mathbb{F}_{q_0}^*$ defined by $Nrm(\alpha) = \alpha\overline{\alpha}$; $\overline{\alpha} := \alpha^{q_0}$.

- $O' = \{\alpha \in \mathbb{F}_q^* : \alpha\overline{\alpha}\} = -1$
- $Nrm^{-1}(-1) = \frac{|\mathbb{F}_q^*|}{|\mathbb{F}_{q_0}^*|} = \frac{q_0^2 - 1}{q_0 - 1} = q_0 + 1 \implies |O'| = q_0 + 1$
- $N_{HCD} = 2 + 2 + (q - 1 - |O'|) = 4 + q - 1 - q_0 - 1 = q - q_0 + 2$

□

Asymptotically Good Binary QAECD Codes

(Huffman and Pless, 2003)

We say that a family of codes is asymptotically good provided that there exists an infinite subset of $[n_i, k_i, d_i]$ codes from this family with $\lim_{i\to\infty} n_i = \infty$ such that both $\liminf_{i\to\infty} k_i/n_i > 0$ and $\liminf_{i\to\infty} d_i/n_i > 0$.

(Huffman and Pless, 2003)

"In a family of codes, we want an infinite subfamily where both the code rates and relative distances are bounded away from 0."

Asymptotically Good Binary QAECD Codes

Recall

Let $H \leq G$, $[G : H] = l$, and $R := \mathbb{F}_q[H]$. Let $e_1, e_2, \ldots e_t$ be the primitive idempotents of R. Then

$$\mathbb{F}_q[G] \cong R^l \cong \bigoplus_{i=1}^{t} (Re_i)^l.$$

$$C \leftrightarrow \Phi(C) \leftrightarrow \prod_{i=1}^{t} C_i$$

QA codes $\leftrightarrow$ linear codes (over rings) $\leftrightarrow$ cross product of linear codes

Asymptotically Good Binary QAECD Codes

Focus: Linear codes in R^l where $R := \mathbb{F}_2[H]$ and $l = 2, 3$.

Involution on R: $* : R \longrightarrow R$ such that
$\left(\sum_{h\in H} \alpha_h Y^h\right)^* = \sum_{h\in H} \alpha_h Y^{-h} = \sum_{h\in H} \alpha_{-h} Y^h$

Lemma

Consider a linear code $C_{(a,b)} := \{(fa, fb) : f \in R\}$ in R^2. Then, $C_{(a,b)}$ is an LCD code if $aa* + bb*$ is a unit in R.

Lemma (Jitman and Ling, 2015)

A linear code $C_{(a,b)}$ in R^2 is self-dual if and only if aa^* and bb^* are units and $aa^* + bb^* = 0$.

Corollary

An LCD code $C_{(a,b,1)} := \{(fa, fb, f) : f \in R\}$ in R^3 can be constructed from a self-dual code $C_{(a,b)}$.

Asymptotically Good Binary QAECD Codes

Proposition

Let (H_{m_k}) be a sequence of abelian groups of odd order m_k, where (m_k) is a strictly increasing sequence (and satisfy all other conditions from Theorem 7.1 (Jitman and Ling, 2015). Let $A_k = H_{m_k} \oplus \mathbb{Z}_4$, $R_k = \mathbb{F}_2[A_k]$ and

$$\Omega = \{(a, b) \in \mathcal{U}(R_k) \times \mathcal{U}(R_k) \mid \mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \pmod 4\}.$$

For each k, assume that $(a, b) \in \Omega$ is chosen as random and let $C^{(k)}_{(a,b)} := \{(fa, fb) \mid f \in R_k\}$. Define a sequence of codes given by $\left(C^{(k)}_{(a,b,1)}\right)$ where $C^{(k)}_{(a,b,1)} := \{(fa, fb, f) \mid f \in R_k\}$. Then

(*i*) $C^{(k)}_{(a,b,1)}$ is a QAECD code for each k,

(*ii*) the codes $C^{(k)}_{(a,b,1)}$ have relative minimum distances $\frac{\mathrm{d}\left(C^{(k)}_{(a,b,1)}\right)}{12m_k} > 0$, and have a positive constant relative rates.

Asymptotically Good Binary QAECD Codes

Proof outline:

(i) Clear from the previous corollary.

(ii) $\frac{\mathrm{d}\left(C^{(k)}_{(a,b,1)}\right)}{12m_k} \geq \frac{\mathrm{d}\left(C^{(k)}_{(a,b)}\right)}{3(4m_k)} = \frac{8}{12} \cdot \frac{\mathrm{d}\left(C^{(k)}_{(a,b)}\right)}{8m_k} \geq \frac{2}{3} \cdot \delta > 0$, for some $\delta > 0$ and for k large enough.

It can be shown that $C^{(k)}_{(a,b,1)} \cong R_k$. Then

$$\dim_{\mathbb{F}_2}(C_{(a,b,1)}) = |R_k| = m_k \implies \frac{\dim_{\mathbb{F}_2}(C_{(a,b,1)})}{12m_k} = \frac{1}{12} > 0$$

□

Summary

Characterization of *QACD* codes (decomposition of semi-simple Group Algebra $\gcd(q, |H|) = 1$)

Enumeration of *QACD* codes

Constructed asymptotically good binary *QAECD* codes

Future works

Construction of "good" *QACD* codes

Distance properties of *QACD* codes (rank distance, bounds, etc.)

Thank you!

References I

- Bazzi, L. M. J. and Mitter, S. K.: Some randomized code constructions from group actions. IEEE Trans. Inf. Theory **52**, 3210–3219 (2006).
- Bosma, W., Cannon, J., and Playoust, C.: The Magma algebra system I: The user language. J. Symb. Comput. **24**, 235–265 (1997).
- Carlet, C. and Guilley, S.: Complementary dual codes for countermeasures to side-channel attacks. Coding Theory and Applications **3** 97–105 (2015).
- Carlet, C., Daif, A., Danger, J.L., Guilley, S., Najm, Z., Ngo, X.T., Portebouef, T. and Tavernier, C.: Optimized linear complementary codes implementation for hardware trojan prevention. In: Proceedings of European Conference on Circuit Theory and Design, 2015 August 24-26; Trondheim, Norway. Piscataway, USA: IEEE (2015).

References II

- Dey, B.K.: On existence of good self-dual quasi-cyclic codes. IEEE Trans. Inform. Theory **50**, 1794–1798 (2004) .
- Dey, B. K. and Rajan, B. S.: Codes closed under arbitrary abelian group of permutations. SIAM J. Discrete Math. **18** 1–18 (2004).
- Ding, C., Kohel, D. R. and Ling, S.: Split group codes. IEEE Trans. Inform. Theory **46** 485–495 (2000).
- Esmaeili, M. and Yari, S.: On complementary-dual quasi-cylic codes. Finite Fields and Their Applications **15** 375–386 (2009).
- Etesami, J., Hu, F. and Henkel, W.: LCD codes and iterative decoding by projections, a first step towards an intuitive description of iterative decoding. In: Proceedings of IEEE Globecom, 2011 December 5-9 ; Texas, USA. Piscataway, USA: IEEE (2011).

References III

- Fan, Y. and Lin, L.: Thresholds of random quasi-abelian codes. IEEE Trans. Inform. Theory **61** 82–90 (2015).
- Guneri, C., Ozkaya, B., Solé, P.: Quasi-cylic complementary dual codes. Finite Fields and Their Applications **42** 67–80 (2016).
- Ishai, Y., Sahai, A. and Wagner, D.: Private circuits: securing hardware against probing attacks. In: *CRYPTO*, vol. 2729 of Lecture Notes in Computer Science, pages 463-481. Springer, August 1721 2003. Santa Barbara, CA, USA.
- Jitman, S., Ling, S., Liu, H. and Xie, X., Abelian codes in principal ideal group algebras, *IEEE Transactions on Information Theory* **59** 3046–3058 (2013).
- Jitman, S., Ling, S.: Quasi-abelian codes. Designs, Codes and Cryptography **74** 511–531 (2015).

References IV

- Jitman, S., Ling, S. , Solé, P.: Hermitian self-dual abelian codes. IEEE Transactions on Information Theory **60** 1496 –1507 (2014).
- Lally, K. and Fitzpatrick, P.: Algebraic structure of quasicyclic codes. Discrete Appl. Math. **111** 157–175 (2001).
- Ling, S. and Solé, P.: On the algebraic structure of quasi-cyclic codes I: Finite fields. IEEE Trans. Inform. Theory **47** 2751–2760 (2001).
- Ling, S. and Solé, P.: Good self-dual quasi-cyclic codes exist. IEEE Trans. Inform. Theory **49** 1052–1053 (2003).
- Ling, S. and Solé, P.: On the algebraic structure of quasi-cyclic codes III: Generator theory. IEEE Trans. Inform. Theory **51**, 2692–2700 (2005).
- Ling, S. and Xing, C.: Coding theory, A first course. Cambridge University Press, New York (2004).

References V

- Massey, J.L.: Linear codes with complementary duals. Discrete Mathematics **106/107** 337–342 (1992).
- Ngo, X.T., Guilley, S., Bhasin, S., Danger, J.L. and Najm, Z.: Encoding the state of integrated circuits: a proactive and reactive protection against hardware trojans horses. In: Proceedings of WESS '14, 2014 October 12-17; New Delhi, India. New York, ACM (2014).
- Ngo, X.T., Bhasin, S., Danger, J.L., Guilley, S., and Najm, Z.: Linear complementary dual code improvement to strengthen encoded cirucit against Hardware Trojan Horses. In: Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust (HOST): 2015 May 2015; Washington DC Metropolitan Area, USA. Piscataway, USA: IEEE (2015).
- Pei, J. and Zhang, X.: 1-generator quasi-cyclic codes. J. Syst. Sci. Complex. **20** 554–561 (2007).

References VI

- Rajan, B. S. and Siddiqi, M. U.: Transform domain characterization of abelian codes. IEEE Trans. Inform. Theory **38** 1817–1821 (1992).
- Séguin, G.: A class of 1-generator quasi-cyclic codes. IEEE Trans. Inform. Theory **50** 1745–1753 (2004).
- Sendrier, N.: Linear codes with complementary duals meet the Gilber-Varshamov bound. Discrete Math **285** 345–347 (2004).
- Yang, X. and Massey, J.L.: The condition for a cyclic code to have a complementary dual. Discrete Mathematics **126** 391–393 (1994).
- Wan, Z.X.: Finite fields and Galois rings. World Scientific Pub. Co. Pte. Ltd., Singapore (2012).
- Wasan, S. K.: Quasi abelian codes. Publ. Inst. Math. **35** 201–206 (1977).