k-Galois Hull of Constacyclic Codes

HABIBUL ISLAM

School of Computer Science
University of St Gallen

Coding Theory and Cryptography - A conference in honor of Joachim Rosenthal's 60th birthday

Basic definitions and results

- Jointly with I. Debnath and O. Prakash (IIT Patna)
- **Linear code:** A non-empty subset C of $\mathbb{F}_q^n$ is said to be a linear code of length n over $\mathbb{F}_q$ if it is a subspace of $\mathbb{F}_q^n$.
- Let $q = p^e$, p be a prime and e, a positive integer. $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$, $\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_q^n$ and each integer k with $0 \leq k < e$, k-**Galois inner product** [Fan and Zhang, 2017] is defined by

$$[\boldsymbol{x}, \boldsymbol{y}]_k = \sum_{i=0}^{n-1} x_i y_i^{p^k}.$$

- It is the Euclidean inner product for $\boldsymbol{k = 0}$, and Hermitian inner product when e is even and $\boldsymbol{k = \frac{e}{2}}$.

Basic definitions and results

- The k-**Galois dual** code of a linear code C defined as

$$C^{\perp_k} = \{\boldsymbol{x} \in \mathbb{F}_q^n \mid [\boldsymbol{c}, \boldsymbol{x}]_k = 0, \ \forall \ \boldsymbol{c} \in C\}.$$

- The k-**Galois hull** of C over $\mathbb{F}_q$ is defined as

$$hull_k(C) = C \cap C^{\perp_k}.$$

- Liu and Pan (2018) studied Galois hull of linear codes; Ding and Lu (2020) studied Galois hull of cyclic codes.
- **Constacyclic code:** A linear code C is said to be a λ-constacyclic code, for $\lambda \in \mathbb{F}_q \setminus \{0\}$, if $(a_0, a_1, \ldots, a_{n-1}) \in C$ implies that $(\lambda a_{n-1}, a_0, \ldots, a_{n-2}) \in C$.
- Every λ-constacyclic code C is a principally generated ideal of $\mathbb{F}_q[x]/\langle x^n - \lambda \rangle$, i.e., $C = \langle g(x) \rangle$, where $g(x)$ is a factor of $x^n - \lambda$.

Basic definitions and results

Lemma [Liu et al. 2018]

Let C be a λ-constacyclic code over $\mathbb{F}_q$ of length n and dimension m. Let $h(x) = \sum_{i=0}^{m} h_i x^i$ be the parity-check polynomial of C. Then $C^{\perp_k}$ is a $\lambda^{-p^{e-k}}$-constacyclic code generated by the polynomial

$$h^{\#}(x) := \sum_{i=0}^{m} h_0^{-p^{e-k}} h_i^{p^{e-k}} x^{m-i} \quad \textbf{(Hash Polynomial)}$$

- Let $C = \langle g(x) \rangle$ be a λ-constacyclic code and $\lambda^{1+p^{e-k}} = 1$. Then the k-Galois $hull_k(C)$ is a λ-constacyclic code generated by $\mathrm{lcm}(g(x), h^{\#}(x))$.

Factorization of $x^n - \lambda$

- Pick up $g(x)$, calculate $h^{\#}(x)$, $hull_k(C) = \langle \text{lcm}(g(x), h^{\#}(x)) \rangle$
- Let $n = n'p^{\nu}$, with $\gcd(p, n') = 1$. [Sangwisut et al., 2017]

$$x^n - \lambda = \left\{ \prod_{j \in A} \gcd(Q_j(x), x^{n'} - \alpha^{n'}) \right\}^{p^{\nu}} \tag{1}$$

$A := \{j \in \mathbb{N} \mid \gcd(j, q) = 1,\ j \text{ divides } n'r \text{ and } \gcd(\frac{n'r}{j}, r) = 1\}$,
$\text{ord}(\lambda) = r$,
$Q_j(x)$:= jth cyclotomic polynomial over $\mathbb{F}_q$,
α:= primitive $(n'r)$-th root of unity in $\mathbb{F}_{q^s}$ where s is the smallest positive integer such that $n'r \mid (q^s - 1)$.

Factorization of $x^n - \lambda$

- Let $f(x) = \sum_{i=0}^{m} f_i x^i \in \mathbb{F}_q[x]$.
- Successively we define $f^{i\#}(x) = (f^{(i-1)\#}(x))^{\#}$, where $f^{0\#}(x) = f(x)$, we get

$$f^{i\#}(x) = \begin{cases} \sum_{j=0}^{m} f_0^{-p^{i(e-k)}} f_j^{p^{j(e-k)}} x^{m-j} & \text{if } i \text{ is odd} \\ \sum_{j=0}^{m} f_m^{-p^{i(e-k)}} f_j^{p^{i(e-k)}} x^{j} & \text{if } i \text{ is even} \end{cases}$$

Remark

Let l' be the least positive multiple of $\mathrm{lcm}(e, e-k)$ such that $l = \frac{l'}{e-k}$ is even and $l' = el''$ for some positive integer l''. Then $\boldsymbol{f^{l\#}(x) = uf(x)}$ for some unit $u \in \mathbb{F}_q$.

Factorization of $x^n - \lambda$

$B_1 = \{j \in \mathbb{N} \mid$ there exist a non-negative integer l_1 for which $j \mid (p^{el_1} + p^{e-k})\}$
and for $i > 1$,
$B_i = \{j \in \mathbb{N} \setminus \cup_{t=1}^{i-1} B_t \mid$ there exist a non-negative integer l_1 for which $j \mid (p^{el_1} + (-1)^{i-1} p^{i(e-k)})\}$.

Lemma

1. $B_i \cap B_j = \phi$ for $i \neq j$.
2. $A \subseteq \bigcup_{i=1}^{l} B_i = \mathbb{N}$.
3. If i is not a divisor of l, then $A \cap B_i = \phi$, for $2 \leq i \leq l-1$.
4. $$A = \bigcup_{i=1}^{s} (A \cap B_{a_i})$$
   where $a_1, a_2, \ldots, a_s$ is the complete list of distinct factors of l.

Factorization of $x^n - \lambda$

Lemma

Let j be a positive integer such that $\gcd(j, q) = 1$. Then

1. The jth cyclotomic polynomial $Q_j(x)$ factors into a product of $\frac{\phi(j)}{m}$ number of distinct monic irreducible polynomials over $\mathbb{F}_q$ and each one of them have the same degree $m = \mathrm{ord}_j(q)$ where ϕ is the Euler's Totient function.
2. If $j \in A \cap B_{a_i}$, then all irreducible factors of $Q_j(x)$ can be partitioned into sets of the form

$$S_f = \{f(x), f^{\#}(x), f^{2\#}(x), \ldots, f^{(a_i-1)\#}(x)\}.$$

Factorization of $x^n - \lambda$

We denote $D_i = A \cap B_{a_i}$ for $1 \leq i \leq s$. We can arrange irreducible factors of $x^n - \lambda$

$$x^n - \lambda = \left\{ \prod_{j \in A} \gcd(Q_j(x), x^{n'} - \alpha^{n'}) \right\}^{p^\nu}$$

$$= \prod_{t=1}^{s} \prod_{j \in D_t} \prod_{i=1}^{\beta_t(j)} \{ f_{ij}(x) \cdot f_{ij}^{\#}(x) \cdots f_{ij}^{(a_t-1)\#}(x) \}^{p^\nu}, \qquad (2)$$

where $\beta_t(j) = \frac{\phi(j)}{a_t \cdot \phi(r) \cdot \mathrm{ord}_j(q)}$ for all $j \in D_t$ and $t = 1, 2, \ldots, s$.

Generator Polynomial

Following equation (2), we the form of generator polynomial of a λ-constacyclic code as

$$g(x) = \prod_{t=1}^{s} \prod_{j \in D_t} \prod_{i=1}^{\beta_t(j)} \{(f_{ij}(x))^{u_{tij,0}} \cdot (f_{ij}^{\#}(x))^{u_{tij,1}} \cdots (f_{ij}^{(a_t-1)\#}(x))^{u_{tij,a_t-1}}\} \quad (3)$$

where $0 \leq u_{tij,m} \leq p^{\nu}$ for $0 \leq m \leq a_t - 1$.

- Now we calculate dim $hull_k(C)$
- **LCD:** dim $hull_k(C) = 0$
- **Self-orthogonal:** dim $hull_k(C) =$ dim C

Hull dimension

Theorem

Let λ be a unit in $\mathbb{F}_q$ such that $\mathrm{ord}(\lambda) = r$, $r \mid (1 + p^{e-k})$ and $\gcd(n', r) = 1$. If $C = \langle g(x) \rangle$ is a λ-constacyclic code of length $n = n'p^\nu$ over $\mathbb{F}_q$, then the dimension of k-Galois hull of C is of the form

$$\sum_{t=1}^{s} \sum_{j \in D_t} \mathrm{ord}_j(q) \cdot b_{tj}$$

where $b_{tj} = \sum_{i=1}^{\beta_t(j)} b_{tij}$, $b_{tij} = a_t p^\nu - [\max\{u_{tij,0}, p^\nu - u_{tij,a_t-1}\} + \max\{u_{tij,1}, p^\nu - u_{tij,0}\} + \cdots + \max\{u_{tij,a_t-1}, p^\nu - u_{tij,a_t-2}\}]$ and $0 \leq b_{tj} \leq \beta_t(j) \cdot \lfloor \frac{a_t p^\nu}{2} \rfloor$ for $1 \leq t \leq s$.

Hull dimension

Corollary

If we consider $a_1 = 1$, then the dimension of the k-Galois hull of is

$$\sum_{t=2}^{s} \sum_{j \in D_t} \mathrm{ord}_j(q) \cdot b_{tj}$$

where $0 \leq b_{tj} \leq \beta_t(j) \cdot \lfloor \frac{a_t p^\nu}{2} \rfloor$ for $1 \leq t \leq s$. Moreover,

$$0 \leq \sum_{t=1}^{s} \sum_{j \in D_t} \mathrm{ord}_j(q) \cdot b_{tj} \leq \frac{n}{2}$$

.

Example

Let $\mathbb{F}_{25}^* = \langle \alpha \rangle$, where α is a root of the polynomial $x^2 + 2x + 3$. Let $\lambda = \alpha^8$. Then $r = \text{ord}(\lambda) = 3$. Now,

$$x^7 - \alpha^8 = (x + \alpha^{20})(x^3 + \alpha^9 x^2 + \alpha^9 x + 4)(x^3 + \alpha^{13} x^2 + \alpha^5 x + 4).$$

- $C = \langle x^3 + \alpha^9 x^2 + \alpha^9 x + 4 \rangle$ is an α^8-constacyclic code of length 7.
- We calculate the dimension of the 1-Galois hull of C.
- Here, $q = 25$, $p^\nu = 1$, $e = 2$, $k = 1$, $l = 2$, $a_1 = 1$, $a_2 = 2$. $A = \{3, 21\}$, $D_1 = A \cap B_1 = \{3, 21\}$, $D_2 = A \cap B_2 = \phi$ and $\text{ord}_3(25) = 1, \text{ord}_{21}(25) = 3$.

Example

- Then $\beta_1(3) = 1, \beta_1(21) = 2$ and

$$b_{1,1,3} = 1 - \max\{0, 1 - 0\} = 0$$
$$b_{1,1,21} = 1 - \max\{1, 1 - 1\} = 0$$
$$b_{1,2,21} = 1 - \max\{0, 1 - 0\} = 0$$

- $b_{1,3} = b_{1,1,3} = 0, b_{1,21} = b_{1,1,21} + b_{1,2,21} = 0.$
- Thus, the dimension of the 1-Galois hull of C is 0 and C is a 1-**Galois LCD** code.

Number of constacyclic codes

- When $e \mid 4(e-k)$ but $e \nmid 2(e-k)$, we calculate the number of constacyclic codes having hull dimension L.
- We get two numbers for two cases: q is even, and q is odd.*

*I. Debnath, O. Prakash and H. Islam: Galois hulls of constacyclic codes over finite fields. Cryptogr. Commun. (2022). https://doi.org/10.1007/s12095-022-00591-6

Number of constacyclic codes

- When $e \mid 4(e-k)$ but $e \nmid 2(e-k)$, we calculate the number of constacyclic codes having hull dimension L.
- We get two numbers for two cases: q is even, and q is odd.*

*I. Debnath, O. Prakash and H. Islam: Galois hulls of constacyclic codes over finite fields. Cryptogr. Commun. (2022). https://doi.org/10.1007/s12095-022-00591-6