A Gröbner approach to dual containing cyclic left module (θ, δ)-codes $Rg/Rf \subset R/Rf$ over finite commutative frobenius rings

Hedongliang Liu[1], Cornelia Ott[2] and Felix Ulmer[3]

Technical University of Munich[1], Ulm University[2], Université de Rennes 1[3]

August 28, 2023

Our setting:

- A is a finite commutative frobenius ring
- θ is a unitary endomorphism of A
- δ is a θ-derivation $\delta : A \to A$ such that, for all $a, b \in A$
  - $\delta(a+b) = \delta(a) + \delta(b)$,
  - $\delta(a \cdot b) = \delta(a) \cdot b + \theta(a) \cdot \delta(b)$.
- Exponential notation: $\theta(a) = a^\theta$ and $\delta(a) = a^\delta$
- $R = A[X; \theta, \delta] := \left\{\sum_{i=0}^{n} a_i X^i | a_i \in A, n \in \mathbb{N}\right\}$ is a skew polynomial ring (multiplication is defined using the rule $Xa = a^\theta X + a^\delta$ which is extended using associativity and distributivity)
- $\mathcal{C} = Rg/Rf \subset R/Rf$ is a cyclic left module (θ, δ)-code with $f, g \in R$, f monic, $f = hg$ with $\deg(f) = n$ and $\deg(g) = n - k$
- $\mathcal{C}^\perp = \{\boldsymbol{v} \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0,\ \forall \boldsymbol{c} \in \mathcal{C}\}$, dual containing means $\mathcal{C}^\perp \subset \mathcal{C}$

Consider a monic polynomial $f = hg$ in $R = A[X;\theta,\delta]$ of degree 4 with $g = g_1X + g_0$, $h = \sum_{i=0}^{3} h_i X^i$. The code $\mathcal{C} = Rg/Rf \subset R/Rf$ is a $[4,3]_A$ code whose generating matrix is

$$G = \begin{pmatrix} g_0 & g_1 & 0 & 0 \\ g_0^{\delta} & g_1^{\delta} + g_0^{\theta} & g_1^{\theta} & 0 \\ g_0^{\delta^2} & g_0^{\delta\theta} + g_0^{\theta\delta} + g_1^{\delta^2} & g_0^{\theta^2} + g_1^{\delta\theta} + g_1^{\theta\delta} & g_1^{\theta^2} \end{pmatrix}.$$

The existence of the parity check matrix as a generator matrix of $C^{\perp}$ for our setting was already shown in

- Mhammed Boulagouaz and Abdulaziz Deajim. Characterizations and Properties of Principal (f, σ, δ) -Codes over Rings. arXiv preprint arXiv:1809.10409 (2018).
- Mhammed Boulagouaz and Abdulaziz Deajim. "Matrix-Product Codes over Commutative Rings and Constructions Arising from (σ, δ)-Codes." Journal of Mathematics 2021 (2021): 1-10.

Additional assumption we need: $\exists \hbar \in R$: $f = hg = g\hbar$.
We give a proof within the setting of skew polynomial rings

Parity Check Matrix Construction

- A word $w \in R$ of degree $< n$ is a code word of $\mathcal{C}$ if and only if $w \cdot \hbar = 0$ in R/Rf.
- Let M be an $n \times n$ matrix defined as

$$\boldsymbol{M} = \begin{pmatrix} \mathrm{coeffs}(\hbar) & \mod f \\ \mathrm{coeffs}(X\hbar) & \mod f \\ \vdots & \\ \mathrm{coeffs}(X^{n-1}\hbar) & \mod f \end{pmatrix}$$

then $C = \{\vec{w} \in A^n \mid \vec{w}\boldsymbol{M} = \vec{0}\}$, i.e. $C = \mathrm{lker}(\boldsymbol{M})$ is a left kernel of $\boldsymbol{M}$.

Parity Check Matrix Example

$n = 3, k = 1$, $f = X^3 + \sum_{i=0}^{2} f_i X^i \in R$, $g = X^2 + g_1 X + g_0$ and $\hbar = \hbar_1 X + \hbar_0$. $w = c_0 + c_1 X + c_2 X^2 \in \mathcal{C}$.

$$
\begin{aligned}
w\hbar \mod f = & \left(c_2(\hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2) + c_1 \hbar_1^{\theta} \right) X^2 \\
& + \left(c_2(\hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1) + c_1(\hbar_1^{\delta} + \hbar_0^{\theta}) + c_0 \hbar_1 \right) X \\
& + c_2(\hbar_0^{\delta^2} - \hbar_1^{\theta^2} f_0) + c_1 \hbar_0^{\delta} + c_0 \hbar_0
\end{aligned}
$$

We obtain the condition $\boldsymbol{w} \in \mathcal{C} \Leftrightarrow \boldsymbol{w} \cdot \boldsymbol{M} = \boldsymbol{0}$ where $\boldsymbol{w} = (c_0, c_1, c_2)$ and

$$
\boldsymbol{M} = \begin{pmatrix}
\hbar_0 & \hbar_1 & 0 \\
\hbar_0^{\delta} & \hbar_1^{\delta} + \hbar_0^{\theta} & \hbar_1^{\theta} \\
\hbar_0^{\delta^2} - \hbar_1^{\theta^2} f_0 & \hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1 & \hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2
\end{pmatrix}.
$$

$n=3, k=1$, $f=X^3+\sum_{i=0}^{2} f_i X^i \in R$, $g=X^2+g_1X+g_0$ and $\hbar=\hbar_1 X+\hbar_0$. $w=c_0+c_1X+c_2X^2 \in \mathcal{C}$.

$$\begin{aligned} w\hbar \mod f = &\left(c_2(\hbar_1^{\theta\delta}+\hbar_1^{\delta\theta}+\hbar_0^{\theta^2}-\hbar_1^{\theta^2} f_2)+c_1\hbar_1^{\theta}\right)X^2 \\ &+\left(c_2(\hbar_1^{\delta^2}+\hbar_0^{\theta\delta}+\hbar_0^{\delta\theta}-\hbar_1^{\theta^2} f_1)+c_1(\hbar_1^{\delta}+\hbar_0^{\theta})+c_0\hbar_1\right)X \\ &+c_2(\hbar_0^{\delta^2}-\hbar_1^{\theta^2} f_0)+c_1\hbar_0^{\delta}+c_0\hbar_0 \end{aligned}$$

We obtain the condition $\boldsymbol{w} \in \mathcal{C} \Leftrightarrow \boldsymbol{w}\cdot\boldsymbol{M}=\boldsymbol{0}$ where $\boldsymbol{w}=(c_0,c_1,c_2)$ and

$$\boldsymbol{M} = \begin{pmatrix} \hbar_0 & \hbar_1 & 0 \\ \hbar_0^{\delta} & \hbar_1^{\delta}+\hbar_0^{\theta} & \hbar_1^{\theta} \\ \hbar_0^{\delta^2}-\hbar_1^{\theta^2} f_0 & \hbar_1^{\delta^2}+\hbar_0^{\theta\delta}+\hbar_0^{\delta\theta}-\hbar_1^{\theta^2} f_1 & \hbar_1^{\theta\delta}+\hbar_1^{\delta\theta}+\hbar_0^{\theta^2}-\hbar_1^{\theta^2} f_2 \end{pmatrix}.$$

In order to find dual containing codes we have to impose that $\boldsymbol{M}^{\top}\cdot\boldsymbol{M}$ to be zero.

θ and δ as polynomial maps

- If A is a finite field $\mathbb{F}_q$ then θ is of the form $a \mapsto a^{p^m}$ and δ is of the form $a \mapsto \beta a - \theta(a)\beta$. $\Rightarrow$ All entries of $\boldsymbol{M}$ become polynomials in the coefficients of $\hbar$ and g and allow sophisticated computations.
- In general θ and δ are not polynomial maps

Example

For $A = \mathbb{F}_2[v]/(v^2+v) = \mathbb{F}_2[1,v]$ there is an automorphisms $\theta : v \mapsto v+1$ which is not a polynomial map over A.
Suppose that the automorphism θ is a polynomial map on A of the form

$$f : x \mapsto \sum_{i \in \mathbb{N}_0} (\alpha_{i,1} v + \alpha_{i,0}) x^i = \sum_{i \in \mathbb{N}_0} \alpha_{i,1} v x^i + \sum_{i \in \mathbb{N}_0} \alpha_{i,0} x^i \qquad (\alpha_{i,j} \in \mathbb{F}_2).$$

Then $\theta(0) = 0 \Rightarrow \alpha_{0,0} = 0$. Since $\alpha_{i,j} \in \{0,1\}$, $f(v)$ is a sum of positive powers of v. Since $v^2 = v$ we get that $f(v)$ is a sum of v, which is either v or 0 in this ring. Since $\theta(v) = v+1$, we obtain that θ is not a polynomial map on A.

Computing all Dual-Containing (θ, δ)-Codes

Idea

We choose the smallest unitary subring B of A such that $A = B[a_1, \ldots, a_s]$ ($s \in \mathbb{N}$) is a free algebra then

- θ and δ are polynomial maps over B
- all solutions of an equation system $\mathcal{E}$ in A^m correspond to the solutions of the corresponding equation system $\mathcal{E}'$ in B^{ms}

If a Gröbner basis algorithm exists for B, then we can compute all dual-containing cyclic left module (θ, δ)-codes $\mathcal{C} = Rg/Rf \subset R/Rf$ for the fixed parameters $[n, k]$ by solving the system $\mathcal{E}'$.

- Express the unknown coefficients $g_0, \ldots, g_{n-k-1}, \hbar_0, \ldots, \hbar_{k-1} \in A$ as linear combinations in a given B-basis $B[g_{0,1}, \ldots, g_{0,s}, \ldots, g_{n-k-1,1}, \ldots, g_{n-k-1,s}, \hbar_{0,1}, \ldots, \hbar_{0,s}, \ldots, \hbar_{k-1,1}, \ldots, \hbar_{k-1,s}]$
- Expressions in images under compositions of θ and δ of g and $\hbar$ become polynomials
- We impose that g divides $g\hbar$ on the right by imposing that all the coefficients of the remainder to be zero.
- We also impose $C^\perp \subset C$ by imposing all the entries $\boldsymbol{M}^\top \cdot \boldsymbol{M}$ to be zero.
- Multivariate polynomial system with coefficients in $B \Rightarrow$ Solve using Gröbner basis

Computational Results for $A = \mathbb{F}_2[v]/(v^2+v)$

Frobenius ring $A = \mathbb{F}_2[v]/(v^2+v)$ of order 4. There are two automorphisms $\theta_1 = \mathrm{Id}$ and θ_2 of order two, and two non-trivial endomorphisms θ_3 and θ_4. Any θ-derivations δ is determined by $\delta(u)$ (note that $\delta(1) = \delta(0) = 0$)

	Automorphism		*Endomorphism*	
	$\theta_1 = \mathrm{Id}$	$\theta_2(v) = v+1$	$\theta_3(v) = 0$	$\theta_4(v) = 1$
$\delta_1 = 0$	$v \mapsto 0$	$v \mapsto 0$	$v \mapsto 0$	$v \mapsto 0$
δ_2		$v \mapsto 1$		
δ_3		$v \mapsto v$	$v \mapsto v$	
δ_4		$v \mapsto v+1$		$v \mapsto v+1$

Computational Results for $A = \mathbb{F}_2[v]/(v^2+v)$

Table: Best Hamming, Lee and Bahoc d_H, d_L, d_B distance of dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$n \setminus k$	2	3	4	5	6	7	8	9	10	11	12
3	$1,1,2$										
4	$2,2,4$	$2,2,2$									
5		$\emptyset$	$\emptyset$								
6		$2,2,2$	$2,2,2$	$2,2,2$							
7			$3,3,5$	$\emptyset$	$\emptyset$						
8			$4,4,7$	$2,2,4$	$2,2,2$	$2,2,2$					
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,1,2$				
10				$2,2,2$	$2,2,2$	$\emptyset$	$\emptyset$	$2,2,2$			
11					$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$		

We follow define the Lee weight of $0, 1, v, v+1$ respectively as $0, 2, 1, 1$ and the Bachoc weight respectively as $0, 1, 2, 2$.

Computational Results for $A = \mathbb{F}_2[v]/(v^2+v)$

Table: Hamming weight enumerator of dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$[n,k]$	Hamming Weight	Constructed with (θ, δ)
[4,2]	$1+6w^2+9w^4$	all combinations (θ, δ) provide such an example
	$1+4w^2+4w^3+7w^4$	$(\theta_2,\delta_2),(\theta_3,\delta_3),(\theta_4,\delta_4)$
[6,3]	$1+9w^2+27w^4+\dots$	all combinations (θ, δ) provide such an example
[6,4]	$1+9w^2+24w^3+\dots$	all combinations (θ, δ) provide such an example
	$1+17w^2+24w^3+\dots$	$(\theta_2,\delta_3),(\theta_2,\delta_3)$
	$1+2w+11w^2+\dots$	$(\theta_3,\delta_3),(\theta_4,\delta_4)$
	$1+13w^2+24w^3+\dots$	$(\theta_3,\delta_3),(\theta_4,\delta_4)$
[8,4]	$1+12w^2+54w^4+\dots$	all combinations (θ, δ) provide such an example
	$1+28w^4+56w^5+\dots$	$(\theta_2,0)$
	$1+4w^2+38w^4+\dots$	$(\theta_2,\delta_2),(\theta_3,\delta_3),(\theta_4,\delta_4)$

Computational Results for $A = \mathbb{F}_2[v]/(v^2+v)$

Table: For the dual-containing codes C, is $C^\perp$ a cyclic module code?

$n \setminus k$	2	3	4	5	6	7	8	9
3	None							
4	All	Some						
5		/	/					
6		All	Some	Some				
7			All	/	/			
8			All	Some	Some	Some		
9				/	/	/	None	
10				All	Some	/	/	All

The frobenius chain ring $A = \mathbb{F}_2[u]/(u^2)$ is a free $\mathbb{F}_2$-algebra $\mathbb{F}_2[u]$ with $\mathbb{F}_2$ basis $[1, u]$. The only automorphism of A is the identity $\theta_1 : x \mapsto x$. There is a unique endomorphism defined by $\theta_2(u) = 0$ (note that $\theta_2(1) = 1$) which is a polynomial map on $\mathbb{F}_2$ and on A itself $\theta_2 : x \mapsto x^2$. .

	Automorphism	*Endomorphism*
	$\theta_1 = \mathrm{Id}$	$\theta_2 : u \mapsto 0$
$\delta_1 = 0$	$u \mapsto 0$	$u \mapsto 0$
δ_2	$u \mapsto 1$	
δ_3	$u \mapsto u$	$u \mapsto u$
δ_4	$u \mapsto u + 1$	

Computational Results for $A = \mathbb{F}_2[u]/(u^2)$

Table: Best Hamming, Lee, and Euclidean distances of dual-containing cyclic module (θ, δ)-codes over $\mathbb{F}_2[u]/(u^2)$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2, 4, 4$	$2, 2, 2$						
5		$\emptyset$	$1, 2, 2$					
6		$2, 4, 4$	$2, 2, 2$	$2, 2, 2$				
7			$3, 3, 3$	$\emptyset$	$1, 2, 2$			
8			$4, 4, 4$	$2, 4, 4$	$2, 2, 2$	$2, 2, 2$		
9				$\emptyset$	$\emptyset$	$\emptyset$	$1, 2, 2$	
10				$2, 4, 6$	$2, 4, 5$	$\emptyset$	$\emptyset$	$2, 2, 2$

We define the Lee weight of $0, 1, u, u + 1$ respectively as $0, 1, 2, 1$ and the Euclidean weight respectively as $0, 1, 4, 1$.

Computational Results for $A = \mathbb{F}_2[u]/(u^2)$

Table: Hamming weight enumerator of dual-containing (θ, δ)-codes over $\mathbb{F}_2[u]/[u^2]$.

$[n,k]$	Hamming Weight	Constructed with (θ, δ)
[4,2]	$1 + 2w^2 + 8w^3 + 5w^4$	$(\mathrm{Id}, 0), (\mathrm{Id}, \delta_2), (\mathrm{Id}, \delta_3), (\theta_2, \delta_2)$
	$1 + 6w^2 + 9w^4$	all maps
[8,4]	$1 + 4w^2 + 30w^4 + \dots$	$(\mathrm{Id}, 0), (\theta_2, \delta_2)$
	$1 + 4w^2 + 46w^4 + \dots$	$(\mathrm{Id}, 0)$
	$1 + 4w^2 + 16w^3 + \dots$	$(\mathrm{Id}, 0)$
	$1 + 12w^2 + 54w^4 + \dots$	all maps
	$1 + 26w^4 + 64w^5 + \dots$	(Id, δ_2)
[8,5]	$1 + 4w^2 + 16w^3 + 94w^4 + \dots$	$(\mathrm{Id}, 0), (\mathrm{Id}, \delta_2)$
	$1 + 4w^2 + 16w^3 + 110w^4 + \dots$	$(\mathrm{Id}, 0)$
	$1 + 12w^2 + 102w^4 + \dots$	all maps
	$1 + 16w^2 + 8w^3 + 114w^4 + \dots$	(Id, δ_2)

Computational Results for $A = \mathbb{F}_4$

Consider $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ where $\alpha^2 = \alpha + 1$. The automorphism group is of order 2, generated by the frobenius automorphism $x \mapsto x^2$ which is a polynomial map on $\mathbb{F}_4$ and $\mathbb{F}_2$.

	Automorphism	
	$\theta_1 = \mathrm{Id}$	$\theta_2(\alpha) = \alpha + 1$
$\delta_1 = 0$	$\alpha \mapsto 0$	$\alpha \mapsto 0$
δ_2		$\alpha \mapsto 1$
δ_3		$\alpha \mapsto \alpha$
δ_4		$\alpha \mapsto \alpha + 1$

Computational Results for $A = \mathbb{F}_4$

Table: The best Hamming, Lee and Euclidean d_H, d_L, d_E distance of θ_2-Hermitian dual-containing codes $Rg/Rf \subset R/Rf$ over $\mathbb{F}_4$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,2,2$	$2,2,2$						
5		$3,3,3$	$1,1,1$					
6		$4,4,4$	$2,2,2$	$2,2,2$				
7			$3,3,3$	$\emptyset$	$1,1,1$			
8			$2,2,2$	$2,2,2$	$2,2,2$	$2,2,2$		
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,1,1$	
10				$(4,4,4)$	$(3,3,3)$	$(2,2,2)$	$(2,2,2)$	$(2,2,2)$

We define the Lee weight of $0, 1, \alpha, \alpha+1$ respectively as $0, 2, 1, 1$ and we define the Euclidean weight respectively as $0, 1, 2, 1$.

Table: Weight enumerator of θ_2-Hermitian dual-containing cyclic module (θ, δ) codes over $\mathbb{F}_4$.

$[n,k]$	Hamming Weight Enumerator	Constructed with (θ, δ)
[4,3]	$1+18w^2+24w^3+211w^4$	all maps
	$1+6w+12w^2+18w^3+27w^4$	(θ_2, δ_2)
[5,4]	$1+9w+30w^2+54w^3+81w^4+81w^5$	(θ_2, δ_2)
[6,5]	$1+45w^2+120w^3+315w^4+360w^5+183w^6$	all maps
	$1+12w+57w^2+144w^3+243w^4+324w^5+243w^6$	(θ_2, δ_2)
[7,6]	$1+15w+93w^2+315w^3+675w^4+1053w^5+\ldots$	(θ_2, δ_2)
[8,7]	$1+84w^2+336w^3+1470w^4+\ldots$	all maps
	$1+18w+138w^2+594w^3+1620w^4+\ldots$	(θ_2, δ_2)
[9,8]	$1+21w+192^2+1008w^3+3402w^4+\ldots$	(θ_2, δ_2)
[10,9]	$1+135w^2+720w^3+4410w^4+15120w^5+\ldots$	all maps
	$1+24w+255w^2+1584w^3+6426w^4+\ldots$	(θ_2, δ_2)

Computation Results for the Galois Ring $A = GR(4,2)$

$A = GR(4,2) = \mathbb{Z}_4[u] = (\mathbb{Z}/4\mathbb{Z})[u]/(u^2+u+1)$ is a frobenius ring of order 16 and has two automorphisms:

- $\theta_1 = \mathrm{Id}$
  - The zero derivation is the only id-derivation
- $\theta_2(u) = 3u + 3$
  - θ_2 is isomorphic to the cyclic group C_2 of order 2
  - The θ_2-derivations are all inner and all 16 possibilities exist (i.e. $\delta : a \mapsto \beta a - \theta_2(a)\beta, \forall \beta \in A$)

Computation Results for the Galois Ring $A = GR(4, 2)$

Table: The best Hamming distance d_H of dual-containing codes $Rg/Rf \subset R/Rf$ over $GR(4, 2)$.

$[n, k]$	existing code for map (θ_i, δ_j)	best d_H	Weight Distribution
[3,2]	$(1, 1), (2, 2), (2, 4), (2, 6), (2, 8),$ $(2, 10), (2, 12), (2, 14), (2, 16)$	2	$1 + 45w^2 + 210w^3$
$[4, 2]$	$(2, 1), (2, 3), (2, 9), (2, 11)$	3	$1 + 60w^3 + 195w^4$
$[4, 3]$	All maps	2	$1 + 90w^2 + 840w^3 + 3165w^4$
$[5, 3]$	$\emptyset$	/	/