# Construction of $\theta$-Cyclic Codes over an Algebra of Order 4

Irwansyah[1*], Intan Muchtadi-Alamsyah[1], Aleams Barra[1], Ahmad Muchlis[1], Djoko Supriyanto[2]

[1]*Algebra Research Group, Bandung Institute of Technology, Indonesia.*
[2]*Combinatorial mathematic research group, Institut Teknologi Bandung, Indonesia.*

Received: 20 September 2014 / Accepted: 30 November 2014

**Abstract:**
In this paper, we show that $\theta$-cyclic codes over algebra $A_1 = \mathrm{F}_2 + v\mathrm{F}_2$ can be constructed from binary cyclic codes using a bijection map from $A_1$ to $\mathrm{F}_2 \times \mathrm{F}_2$. We also give a decoding algorithm for $\theta$-cyclic codes which are constructed using well-known BCH codes over binary field.

**Key words:** *BCH codes, Berlekamp-Massey decoding algorithm, binary cyclic codes, $\theta$-cyclic codes, gray map*

## Introduction

Cyclic codes has many applications in data storage systems *e.g.* QR code, DVD, satellite communications *etc*. Therefore, many researchers put an attempt to study this code and its generalizations in order to find this type of codes with better parameter. $\theta$-cyclic codes or skew cyclic codes as a generalization of cyclic codes, has been extensively studied by researcher because it produces some codes with better parameter and has a nice structure.

Boucher and Ulmer [3] studied the structure of skew cyclic codes over Galois field $\mathrm{F}_q$ and using Gröbner bases, they compute all Euclidean and Hermitian self-dual $\theta$-cyclic codes over $\mathrm{F}_4$ of length less than 40, including a [36,18,11] Euclidean self-dual $\theta$-cyclic code which improve the previously best known bound. In [1], Abualrub *et al.* studied $\theta$-cyclic codes over algebra $A_1 = \mathrm{F}_2 + v\mathrm{F}_2$, where $v^2 = v$. They gave the generators for every $\theta$-cyclic codes over $A_1$ and characterized the generator of Euclidean and Hermitian $\theta$-cyclic codes over $A_1$. Furthermore, Gao [5] studied the structure of $\theta$-cyclic codes over $\mathrm{F}_p + v\mathrm{F}_p$, where $v^2 = v$ and $p$ is a prime number for special type of $\theta$. He found that $\theta$-cyclic codes over $\mathrm{F}_p + v\mathrm{F}_p$ are equivalent to either cyclic codes or quasi-cyclic codes and gave the enumeration of distinct $\theta$-cyclic codes over $\mathrm{F}_p + v\mathrm{F}_p$.

In this paper, we study $\theta$-cyclic codes over $A_1$ with different point of view with Abualrub *et al.* [1]. Our method gives a way to construct this codes from binary cyclic codes, so we can easily determine the size and minimum distance of $\theta$-cyclic codes over $A_1$.

## Construction of $\theta$-cyclic codes over $A_1$

Let $A_1 = \mathrm{F}_2 + v\mathrm{F}_2 = \{0,1,v,v+1\}$, where $v^2 = v$. Indeed, it is an algebra over binary field $\mathrm{F}_2$ of order 4. $A_1$ has a unique non-trivial automorphism $\theta$, where $\theta(\alpha+\beta v) = \alpha+\beta+\beta v$ for $\alpha,\beta \in \mathrm{F}_2$. $C$ is a $\theta$-cyclic codes of length $n$ over $A_1$ if it is a submodule of $A_1^n$ over $A_1$ and if $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, then $T_\theta(c) = (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C$ also. Let $\varphi$ is a Gray map from $A_1$ to $\mathrm{F}_2 \times \mathrm{F}_2$, where $\varphi(\alpha+\beta v) = (\alpha, \alpha+\beta)$ for $\alpha,\beta \in \mathrm{F}_2$. Using the inverse of Gray map $\varphi$, we have the following results.

*Proposition 1.* If $C_1$ is a binary cyclic code of length $n$, then $\varphi^{-1}(C_1, C_1)$ is a $\theta$-cyclic code over $A_1$ of length $n$.

*Proof.* For any $c_1, c_2 \in C_1$, consider $\varphi^{-1}(c_1, c_2)$. We will show that there exist $c_3, c_4 \in C_1$ such that

***Corresponding author:** Irwansyah,
E-mail: irwansyah@students.itb.ac.id

 

$T_\theta(\varphi^{-1}(c_1,c_2)) = \varphi^{-1}(c_3,c_4)$ . Let $c_1 = (c_{10}\ c_{11} \ldots c_{1\,n-1})$ and $c_1 = (c_{20}\ c_{21} \ldots c_{2\,n-1})$.

Then, we have

$\varphi^{-1}(c_1,c_2) = (c_{10} + (c_{10} + c_{20})v \ldots c_{10} + (c_{1\,n-1} + c_{2\,n-1})v)$

So,

$$\varphi(c = T_\theta(\varphi^{-1}(c_1,c_2))) = \begin{pmatrix} c_{2\,n-1} & c_{20} & \cdots & c_{2\,n-2} \\ c_{1\,n-1} & c_{10} & \cdots & c_{1\,n-2} \end{pmatrix}$$

Then, let $c_i^1 = (c_{i\,n-1}\ c_{i0} \ldots c_{i\,n-2})$, for $i = 1,2$. Choose $c_3 = c_2^1$ and $c_4 = c_1^1$, we have $\varphi^{-1}(c_3,c_4) = c = T_\theta(\varphi^{-1}(c_1,c_2))$. Hence, $\varphi^{-1}(C_1,C_1)$ is a $\theta$-cyclic code. *QED*

Let $T(C)$ is the set of first shift of all code words in $C$, *i.e.* if $c = (c_0,\ldots,c_{n-1}) \in C$, then $T(c) = (c_{n-1},c_0,\ldots,c_{n-2})$. We have the following weak characterization.

*Proposition 2.* $C$ is a $\theta$-cyclic code over $A_1$, if and only if $C = \varphi^{-1}(C_0,C_1)$, where $C_0$ and $C_1$ are binary quasi-cyclic codes of index 2 such that $T(C_i) = C_{i+1 \mod 2}$ for $i = 0,1$.

*Proof.* ($\Leftarrow$) For any $c \in C$, there exist codewords $c_1 \in C_0$ and $c_2 \in C_1$ such that $c = \varphi^{-1}(c_1,c_2)$. Let $c_i = (c_{i0},\ldots,c_{i\,n-1})$ for $i = 0,1$. Then, we have

$$c = (c_{00} + (c_{00} + c_{10})v,\ldots,c_{0\,n-1} + (c_{0\,n-1} + c_{1\,n-1})v)$$

we will show that $T_\theta(c) \in C$. We can see that,

$$T_\theta(c) = (c_{0\,n-1} + (c_{0\,n-1} + c_{1\,n-1})v,\ldots,c_{0\,n-2} + (c_{0\,n-2} + c_{1\,n-2})v)$$

So, if we choose $c_3 = T(c_2) \in C_0$ and $c_4 = T(c_1) \in C_1$, we have $\varphi^{-1}(c_3,c_4) = T_\theta(c)$. Therefore, $C$ is a cyclic code. The other direction also follows similarly. *QED*

*Theorem 1.* For $n$ is an odd integer, $C$ is a $\theta$-cyclic code over $A_1$ of length $n$ if and only if $C = \varphi^{-1}(C_1,C_1)$, where $C_1$ is a binary cyclic code.

*Proof.* Let $C = \varphi^{-1}(C_1,C_2)$. For any $c_1 \in C_1$, let $c_1 = (c_{10} \ldots c_{1\,n-1})$, consider

$$\varphi^{-1}(c_1,0) = (c_{10} + c_{10}v \ldots c_{1\,n-1} + c_{1\,n-1}v)$$

we can see that,

$$T_\theta^i(\varphi^{-1}(c_1,0)) = \begin{cases} (c_{1,0+i} + c_{1,0+i}v,\ldots,c_{1,n-1+i} + c_{1,n-1+i}v), & i\ even \\ (c_{1,0+i}v,\ldots,c_{1,n-1+i}v), & i\ odd \end{cases}$$

so

$$T_\theta^{n+1}(\varphi^{-1}(c_1,0)) = (c_{1\,n-1} + c_{1\,n-1}v, c_{10} + c_{10}v \ldots c_{1\,n-2} + c_{1\,n-2}v)$$

Then, if we choose $c_3 = c_1^1$, then we have $\varphi^{-1}(c_3,0) = T_\theta^{n+1}(\varphi^{-1}(c_1,0)) \in C$, and $c_3 = c_1^1 \in C_1$, which means $C_1$ is a binary cyclic code. Conclusion for $C_2$ we obtain in similar ways.

For any $c_1 \in C_1$, let $c_1 = (c_{10} \ldots c_{1\,n-1})$. By equation for $T_\theta^i(\varphi^{-1}(c_1,0))$, we have

$$\varphi(T_\theta^n(c_1,0)) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ c_{10} & c_{11} & \cdots & c_{1\,n-1} \end{pmatrix} = \varphi^{-1}(0,c_1)$$

Consequently, $c_1 \in C_2$, which implies $C_1 \subseteq C_2$. By similar arguments, we also have $C_2 \subseteq C_1$. Therefore, $C_1 = C_2$. *QED*

*Proposition 3.* If $C = \varphi^{-1}(C_1,C_2)$ is a $\theta$-cyclic codes over $A_1$, where $C_2 \subseteq C_1$ and $n$ is an even integer, then $C_1$ is a binary cyclic code.

*Proof.* Any $c_1 \in C_1$, we can let $c_1 = (c_{10} \ldots c_{1\,n-1})$, then we have

$$T_\theta(\varphi^{-1}(c_1,0)) = \begin{pmatrix} 0 & \cdots & 0 \\ c_{1\,n-1} & \cdots & c_{1\,n-2} \end{pmatrix}$$

which implies $c_1^1 \in C_1$. *QED*

*Proposition 4.* If $C = \varphi^{-1}(C_1,C_2)$ is a $\theta$-cyclic codes over $A_1$, where $C_1$ and $C_2$ are binary cyclic codes, then $C_2 = C_1$.

*Proof.* Take any $c_1 \in C_1$, and let $c_1 = (c_{10} \ldots c_{1\,n-1})$, we can see that

$$\varphi(T_\theta(\varphi^{-1}(c_1^{n-1},0))) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ c_{10} & c_{11} & \cdots & c_{1\,n-1} \end{pmatrix}$$

so, $C_1 \subseteq C_2$. By similar arguments, we also have $C_2 \subseteq C_1$. Hence, $C_1 = C_2$. *QED*

We also have several direct consquences for Euclidean and Hermitian $\theta$-cyclic codes over $A_1$ which can be proved using our results combined with Lemma 3.1 and Lemma 3.2 in [2].

*Corollary 1.* If $C_1$ is a binary self-dual cyclic code, then $C = \varphi^{-1}(C_1, C_1)$ is an Euclidean and Hermitian $\theta$-cyclic code over $A_1$.

*Corollary 2.* If $C = \varphi^{-1}(C_1, C_2)$ is an Euclidean $\theta$-cyclic codes over $A_1$, where $C_2 \subseteq C_1$ and $n$ is an even integer, then $C_1$ is a binary self-dual cyclic code.

*Corollary 3.* If $C = \varphi^{-1}(C_1, C_2)$ is a Hermitian $\theta$-cyclic codes over $A_1$, where $C_2 \subseteq C_1$ and $n$ is an even integer, then $C_1$ is a binary self-dual cyclic code and $C_1 = C_2$.

The above results show that we can construct a $\theta$-cyclic code $C$ over $A_1$ using a binary cyclic code $C_1$ simply using relation $C = \varphi^{-1}(C_1, C_1)$, and we can easily know that minimum distance of $C$ is equals to minimum distance of $C_1$ and size of $C$ is equals to square of the size of $C_1$.

## Decoding algorithm

If $C_1$ is a binary BCH code of length $n = 2^m - 1$ for some $m$, then we can have decoding algorithm for $\theta$-cyclic code $C = \varphi^{-1}(C_1, C_1)$ simply using decoding algorithm of BCH codes with some additional steps. Note that, $n = 2^m - 1$ is an odd integer, thats why we only need one binary BCH code to construct $\theta$-cyclic over $A_1$ in this situation. The simplified algorithm is as follows.

1. Let *c'* be the original message, but vector $c \in A_1^n$ received. Then calculate $\varphi(c) = (c_1, c_2)$ to have $c_1, c_2 \in \mathrm{F}_2^n$.
2. Apply decoding algorithm for BCH codes to each $c_1$ and $c_2$ to get $c_1', c_2' \in C_1$.
3. Calculate $\varphi^{-1}(c_{1'}, c_{2'})$, and $c' = \varphi^{-1}(c_1', c_2')$ is the original message.

## Conclusions

We can construct several $\theta$-cyclic codes over $A_1$ using binary cyclic codes, so as a consequence, we can easily determine its minimum distance and size. We are able to apply decoding algorithm for binary BCH codes to decode $\theta$-cyclic codes which constructed using binary BCH code also.


## Acknowledgement

This research is supported by Beasiswa Unggulan BPKLN DIKTI through Program Doktor Unggulan Batch 3-B FMIPA ITB and Hibah Riset dan Inovasi KK ITB.


## References


[1] T. Abualrub, N. Aydin, and P. Seneviratne, On $\theta$-Cyclic Codes over $\mathrm{F}_2 + v\mathrm{F}_2$, *Australasian Journal of Combinatorics*, **54**, 2012, 115-126.

[2] K. Betsumiya and M. Harada, Optimal self-dual codes over $\mathrm{F}_2 \times \mathrm{F}_2$ with respect to the Hamming weight, *IEEE Transactions on Information Theory*, **50**(2), 2004, 356-358.

[3] D. Boucher and F. Ulmer, Coding with Skew Polynomial Rings, *Journal of Symbolic Computation*, **44**, 2009, 1644-1656.

[4] D. Boucher, W. Geiselmann, and F. Ulmer, Skew Cyclic Codes, *Appl. Algebra Eng. Commun. Comput.*, **18**, 2007, 379-389.

[5] J. Gao, Skew Cyclic Codes over $\mathrm{F}_p + v\mathrm{F}_p$, *J. Appl. Math. and Informatics*, **31**(3-4), 2013, 337-342.