

VỀ MỘT LỚP MÃ CYCLIC

Nguyễn Thị Lan Hương^{1*}, Hoàng Phương Khánh², Nguyễn Thị Nhung²

¹Trường Đại học Kinh tế và Quản trị kinh doanh – ĐH Thái Nguyên,

²Trường Đại học Công nghệ thông tin và Truyền thông – ĐH Thái Nguyên

TÓM TẮT

Với số nguyên tố p lẻ sao cho $p^m \equiv 1 \pmod{8}$, $p^m \equiv 5 \pmod{8}$ cấu trúc và đối ngẫu của các mã cyclic có độ dài $8p^s$ trên $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{u^2}$ hoàn toàn được xác định bằng các đa thức sinh của chúng. Mã đối ngẫu của tất cả các cyclic có độ dài $8p^s$ trên $\mathcal{R}$ cũng được đưa ra. Hơn nữa, chúng tôi đưa ra số các từ mã trong mỗi trường hợp của các mã cyclic này. Chúng tôi cũng thu được số các mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$.

Từ khóa: Mã cyclic; mã đối ngẫu; mã nghiệm lặp; vành chuỗi; vành địa phương

Ngày nhận bài: 25/9/2020; Ngày hoàn thiện: 03/11/2020; Ngày đăng: 30/11/2020

ON A CLASS OF CYCLIC CODES

Nguyen Thi Lan Huong^{1*}, Hoang Phuong Khanh², Nguyen Thi Nhung²

¹TNU – University of Economics and Business Administration,

²TNU - University of Information and Communication Technology

ABSTRACT

For any odd prime p such that $p^m \equiv 1 \pmod{8}$, $p^m \equiv 5 \pmod{8}$ the structures and duals of cyclic codes of length $8p^s$ over $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{u^2}$ are completely determined in term of their generator polynomials. Dual codes of all cyclic of length $8p^s$ over $\mathcal{R}$ are also investigated. Furthermore, we give the number of codewords in each of those cyclic codes. We also obtain the number of cyclic codes of length $8p^s$ over $\mathcal{R}$.

Keywords: cyclic codes; dual codes; repeated-root codes; chain rings; local rings.

Received: 25/9/2020; Revised: 03/11/2020; Published: 30/11/2020

* Corresponding author. Email: lanhuong@tueba.edu.vn

1. Giới thiệu

Lý thuyết mã hóa là một trong những lĩnh vực quan trọng của toán học, có ảnh hưởng đến rất nhiều lĩnh vực khoa học - công nghệ và kinh tế - xã hội. Thời nay, với sự phát triển rất nhanh của công nghệ thông tin và mạng internet thì mã hóa thông tin càng đóng vai trò quan trọng. Mã hóa là một phương pháp bảo vệ thông tin, bằng cách chuyển đổi thông tin từ dạng rõ (thông tin có thể dễ dàng đọc hiểu được) sang dạng mờ (thông tin đã bị che đi, nên không thể đọc hiểu được, để đọc được ta cần phải giải mã nó). Nó giúp ta có thể bảo vệ thông tin, để những kẻ đánh cắp thông tin, dù có được thông tin của chúng ta, cũng không thể hiểu được nội dung của nó. Mã hóa sẽ mang lại tính an toàn cao hơn cho thông tin, đặc biệt là trong thời đại internet ngày nay, khi mà thông tin phải đi qua nhiều trạm trung chuyển trước khi đến được đích.

Trong các loại mã thì lớp mã quan trọng nhất là mã cyclic. Nhiều mã nổi tiếng như BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen và mã nhị phân Hamming là mã cyclic hoặc được xây dựng từ mã cyclic.

Nếu độ dài n của mã chia hết cho đặc số p của trường thì mã được gọi là mã nghiệm lặp. Nếu độ dài n của mã không chia hết cho p thì mã đó được gọi là mã nghiệm đơn. Mã nghiệm lặp được nghiên cứu lần đầu tiên vào năm 1967 bởi S. D. Berman [1]. Sau đó nhiều nhà Toán học khác như J. L. Massey [2], G. Falkner [3], R. M. Roth và G. Seroussi [4],... cũng quan tâm nghiên cứu về loại mã này.

Mã nghiệm lặp được nghiên cứu trong trường hợp tổng quát vào năm 1991 bởi G. Castagnoli [5] và J. H. van Lint [6]. Trong các công trình [5] và [6] đã chỉ ra rằng mã cyclic nghiệm lặp có cấu trúc ràng buộc nhau. Việc tìm thêm các tính chất thú vị khác về mã cyclic nghiệm lặp là một điều khả thi và cũng chính là động lực thúc đẩy các nhà toán học khác nghiên cứu nhiều hơn nữa về vấn đề này [7], [8].

Trong bài báo này, chúng tôi xác định tất cả các mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$ với số nguyên tố p lẻ thỏa mãn $p^m \equiv 1 \pmod{8}, p^m \equiv 5 \pmod{8}$. Phần 2 của bài báo đưa ra một số kiến thức cơ sở. Phần 3 đưa ra cấu trúc của các mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$. Trong phần này, chúng tôi cũng xem các mã cyclic tự đối ngẫu. Số các mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$ cũng hoàn toàn được xác định.

2. Kiến thức chuẩn bị

Một ideal I của vành R được gọi là ideal chính nếu tồn tại một phần tử a của R sao cho $I = aR = \{ar: r \in R\}$. Một vành R gọi là ideal chính nếu tất cả các ideal của nó là ideal chính. Một vành giao hoán với đơn vị được gọi là vành chuỗi nếu tập hợp tất cả các ideal của nó là một chuỗi sắp thứ tự theo quan hệ bao hàm.

Với λ khả nghịch trong R , phép nâng τ_λ trên R^n được định nghĩa như sau:

$$\tau_\lambda(x_0, x_1, \dots, x_{n-1}) = (\lambda x_{n-1}, x_1, \dots, x_{n-2}).$$

Một mã C được gọi là λ -constacyclic nếu $\tau_\lambda(C) = (C)$, nghĩa là C đóng với phép nâng λ -constacyclic τ_λ . Nếu $\lambda=1$, thì C được gọi là mã cyclic.

Từ mã $c = (c_0, c_1, \dots, c_{n-1})$ được tương ứng 1-1 với đa thức biểu diễn dạng

$$c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}.$$

Tích trong của vectơ $x = (\dots), y = (\dots) \in R^n$ $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$ được định nghĩa như sau

$$x \cdot y = x_0y_0 + x_1y_1 + \dots + x_{n-1}y_{n-1}.$$

Mã đối ngẫu của C là tập

$$C^\perp = \{x | x \cdot y = 0, \forall y \in C\}.$$

Mã C được gọi là tự trực giao nếu $C \subseteq C^\perp$, và C được gọi là tự đối ngẫu nếu $C = C^\perp$.

3. Mã cyclic độ dài $8p^s$ trên R

Đầu tiên, chúng ta chỉ ra các đặc trưng của vành chuỗi như sau.

Mệnh đề 3.1. Cho R là vành giao hoán hữu hạn. Khi đó các phát biểu sau là tương đương:

i) R là vành địa phương và ideal tối đại M của R là vành chính, nghĩa là $M = \langle \gamma \rangle$ với $\gamma \in R$.

ii) R là vành ideal chính địa phương.

iii) R là vành chuỗi có các ideal dạng $\langle \gamma^i \rangle, 0 \leq i \leq \varpi$ với ϖ là chỉ số lũy linh của γ .

Chứng minh:

(i) $\Rightarrow$ (ii): Gọi I là một idêan của vành R .

- Nếu $I = R$ thì I được sinh bởi phần tử 1.

- Nếu $I \subsetneq R$ thì $I \subset M$. Theo (i) M được sinh bởi một phần tử, ta đặt $M = \langle \gamma \rangle$. Khi đó $I = \langle \gamma^k \rangle$ với k là số nguyên dương nào đó. Suy ra R là vành idêan chính địa phương.

(ii) $\Rightarrow$ (iii) Giả sử R là vành idêan chính địa phương với idêan tối đại $M = \langle \gamma \rangle$ và A, B là hai idêan thực sự của R . Ta có $A, B \subseteq M$. Khi đó tồn tại các số nguyên k, l sao cho $A = \langle \gamma^k \rangle, B = \langle \gamma^l \rangle$ (l, k nhỏ hơn chỉ số lũy linh của a). Suy ra $A \subseteq B$ hoặc $B \subseteq A$. Vậy R là vành chuỗi.

(iii) $\Rightarrow$ (i) Giả sử R là vành chuỗi giao hoán hữu hạn, rõ ràng R là vành địa phương (vì tồn tại duy nhất một idêan tối đại theo quan hệ bao hàm). Để chỉ ra rằng idêan tối đại của R là chính, chúng ta giả sử ngược lại, M được sinh bởi nhiều hơn một phần tử và b, c là hai phần tử sinh của M , với b không thuộc cR đồng thời c cũng không thuộc bR . Khi đó $\langle b \rangle \not\subseteq \langle c \rangle$ và $\langle c \rangle \not\subseteq \langle b \rangle$ mâu thuẫn với giả thiết R là vành chuỗi. Vậy M là idêan chính.

Tiếp theo, chúng tôi chỉ ra một tính chất quan trọng của mã cyclic.

Mệnh đề 3.2. Một mã tuyến tính C có độ dài n là cyclic trên R khi và chỉ khi C là một ideal của $\frac{R[x]}{\langle x^n - 1 \rangle}$.

Chứng minh:

Điều kiện cần:

Giả sử C là một mã cyclic trên R . Chúng ta cần chứng minh $C \subseteq \frac{R[x]}{\langle x^n - 1 \rangle}$ là một idêan.

Xét $f(x) + \langle x^n - 1 \rangle \in \frac{R[x]}{\langle x^n - 1 \rangle}$ và $c(x) \in C$ với

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}, c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

Ta có

$$a_0(c_0 + c_1x + \dots + c_{n-1}x^{n-1}) = a_0c_0 + a_0c_1x + \dots + a_0c_{n-1}x^{n-1} = a_0\tau c(x) \in C,$$

$$a_0x(c_0 + c_1x + \dots + c_{n-1}x^{n-1}) = c_{n-1} + a_1c_0x + \dots + a_1c_{n-2}x^{n-1} = a_1\tau c(x) \in C,$$

...

$$a_{n-1}x^{n-1}(c_0 + c_1x + \dots + c_{n-1}x^{n-1}) = a_{n-1}\tau^{n-1}(c(x)) \in C.$$

Suy ra $f(x)c(x) + \langle x^n - 1 \rangle \in C$.

Điều kiện đủ: Giả sử $C \subseteq \frac{R[x]}{\langle x^n - 1 \rangle}$ là một idêan. Chúng ta cần chứng minh $\tau(C) = C$.

Xét $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in C$. Suy ra

$$\begin{aligned} \tau(c(x)) &= c_{n-1} + c_0x + \dots + c_{n-2}x^{n-1} \\ &= x(c_0 + c_1x + \dots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}) \in C \end{aligned}$$

(do C là một idêan của $\frac{R[x]}{\langle x^n - 1 \rangle}$). Ngược lại, giả sử $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in C$. Khi đó $c(x) = \tau(1^{-1}c(x))$.

Do $c(x) \in C \subseteq \frac{R[x]}{\langle x^n - 1 \rangle}$ nên $1^{-1}c(x) \in C$, suy ra $c(x) \in \tau(C)$.

Vậy C là mã cyclic trên R .

Tiếp theo, chúng ta đưa ra một số đặc trưng về mã cyclic có độ dài $8p^s$ trên R .

Khi $p^m \equiv 1 \pmod{8}, p^m \equiv 5 \pmod{8}$ đa thức $x^{8p^s} - 1$ được phân tích thành các đa thức đơn bất khả quy như sau:

$$\begin{aligned} x^{8p^s} - 1 &= (x^8 - 1)^{p^s} \\ &= (x^{p^s} - 1)(x^{p^s} + 1)(x^{2p^s} + 1)(x^{4p^s} + 1) \end{aligned}$$

Theo Định lý Thặng dư Trung Hoa, ta có:

$$\begin{aligned} \frac{R[x]}{\langle x^{8p^s} - 1 \rangle} &\cong \frac{R[x]}{\langle x^{p^s} - 1 \rangle} \oplus \frac{R[x]}{\langle x^{p^s} + 1 \rangle} \\ &\oplus \frac{R[x]}{\langle x^{2p^s} + 1 \rangle} \oplus \frac{R[x]}{\langle x^{4p^s} + 1 \rangle} \end{aligned}$$

Từ đẳng cấu trên, ta có thể xác định cấu trúc đại số của tất cả các mã cyclic có độ dài $8p^s$ trên R . Hơn nữa, số các từ mã của các mã này cũng được đưa ra.

Định lý 3.3. Cho C là mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$. Khi đó ta có:

i) $C = C_1 \oplus C_2 \oplus C_3 \oplus C_4$, với C_1, C_2, C_3, C_4 lần lượt các ideal của các vành $\frac{\mathcal{R}[x]}{\langle x^{8p^s}-1 \rangle}, \frac{\mathcal{R}[x]}{\langle x^{p^s}+1 \rangle}, \frac{\mathcal{R}[x]}{\langle x^{2p^s}+1 \rangle}, \frac{\mathcal{R}[x]}{\langle x^{4p^s}+1 \rangle}$.

ii) $|C| = |C_1||C_2||C_3||C_4|$.

iii) Đối ngẫu của C là

$$C^\perp = C_1^\perp \oplus C_2^\perp \oplus C_3^\perp \oplus C_4^\perp,$$

với $C_1^\perp$ là mã đối ngẫu của C_1 , $C_2^\perp$ là mã đối ngẫu của C_2 , $C_3^\perp$ là mã đối ngẫu của C_3 , $C_4^\perp$ là mã đối ngẫu của C_4 .

$$\begin{aligned} \frac{\mathcal{R}[x]}{\langle x^{8p^s}-1 \rangle} &\cong \frac{\mathcal{R}[x]}{\langle (x+1)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x+1)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-\gamma^2)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-\gamma^6)^{p^s} \rangle} \\ &\oplus \frac{\mathcal{R}[x]}{\langle (x-\gamma)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-\gamma^3)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-\gamma^5)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-\gamma^7)^{p^s} \rangle}. \end{aligned}$$

Điều này cho thấy rằng mọi mã cyclic độ dài $8p^s$ trên $\mathcal{R}$ có thể được biểu diễn dưới dạng tổng trực tiếp của mã cyclic, mã negacyclic, mã α -constacyclic, mã $-\alpha$ -constacyclic, mã γ -constacyclic, mã γ^3 -constacyclic, γ^5 -constacyclic mã, mã γ^7 -constacyclic độ dài p^s trên $\mathcal{R}$. Chúng ta có kết quả sau.

Định lý 3.4. Nếu C là mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$ thì C có thể được biểu diễn dưới dạng

$C = C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_6 \oplus C_7 \oplus C_8$, trong đó C_1 là mã cyclic, C_2 là mã cyclic, C_3 là mã α -constacyclic, C_4 là mã $-\alpha$ -constacyclic, C_5 là mã γ -constacyclic, C_6 là mã γ^3 -constacyclic, C_7 là mã γ^5 -constacyclic và C_8 là mã γ^7 -constacyclic mã có độ dài p^s trên $\mathcal{R}$. Hơn nữa,

$$|C| = |C_1||C_2||C_3||C_4||C_5||C_6||C_7||C_8|.$$

Áp dụng Mệnh đề 3.2, chúng ta có thể tìm được cấu trúc của mã cyclic độ dài $8p^s$ trên $\mathcal{R}$ như sau.

Định lý 3.5. Cho $C = C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_6 \oplus C_7 \oplus C_8$, là mã cyclic độ dài $8p^s$ trên $\mathcal{R}$, trong đó C_1 là mã cyclic, C_2 là mã negacyclic, C_3 là mã α -constacyclic, C_4 là mã $-\alpha$ -constacyclic, C_5 là mã γ -constacyclic, C_6 là mã γ^3 -constacyclic, C_7 là mã γ^5 -constacyclic và C_8 là mã γ^7 -constacyclic mã có độ dài p^s trên $\mathcal{R}$. Khi đó $C_1^\perp$ là mã cyclic, $C_2^\perp$ là mã negacyclic, $C_3^\perp$ là mã α -constacyclic, $C_4^\perp$ là mã $-\alpha$ -constacyclic, $C_5^\perp$ là mã γ^7 -constacyclic, $C_6^\perp$ là mã γ^5 -constacyclic, $C_7^\perp$ là mã γ^3 -constacyclic và $C_8^\perp$ là mã γ -constacyclic mã có độ dài p^s trên $\mathcal{R}$.

Số lượng mã cyclic độ dài $8p^s$ trên $\mathcal{R}$ được đưa ra trong kết quả sau.

Định lý 3.6. Số lượng mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$ là

$$\left[\frac{2(p^m+1)(p^m)^{\frac{p^s-1}{2}} - 2^{2m} - 2}{(p^m-1)^2} + \frac{(2p^m+3)(p^m)^{\frac{p^s-1}{2}} - 2p^s - 1}{p^m-1} + (p^m)^{\frac{p^s-1}{2}} + 2 \right]^8$$

Trường hợp 2: $p^m \equiv 5 \pmod{8}$ tức là $4|(p^m-1)$ và $8|(p^m-1)$.

Trong trường hợp này $x^2+1 = (x-\eta)(x+\eta)$, trong đó $\eta = \xi^{\frac{p^m-1}{4}}$. Vì $\eta, -\eta$ không phải là số chính phương nên $x^2+\eta$ và $x^2-\eta$ là bất khả quy trên $\mathcal{R}[x]$. Ta có:

$$x^4+1 = (x^2-\eta)(x^2+\eta)$$

Do đó, $x^8+1 = (x-1)(x+1)(x-\eta)$

$$(x+\eta)(x^2-\eta)(x^2+\eta).$$

Trường hợp 1: $p^m \equiv 1 \pmod{8}$. Ta có:

$$\left(\xi^{\frac{p^m-1}{4}} \right)^2 = \xi^{\frac{p^m-1}{2}} = -1$$

$$\text{Suy ra } \left(\xi^{\frac{p^m-1}{8}} \right)^4 = \xi^{\frac{p^m-1}{2}} = -1$$

Đặt $\gamma = \xi^{\frac{p^m-1}{8}}; \alpha = \xi^{\frac{p^m-1}{4}}$. Do đó $x^2+1 = (x-\alpha)(x+\alpha)$.

Từ $\gamma, \gamma^3, \gamma^5, \gamma^7$ là phân biệt, ta có thể chứng minh rằng:

$$x^4+1 = (x-\gamma)(x-\gamma^3)(x-\gamma^5)(x-\gamma^7).$$

Theo Định lý Thặng dư Trung Hoa, ta có :

Theo Định lý Thặng dư Trung Hoa, ta có

$$\frac{\mathcal{R}[x]}{\langle x^{8p^s}-1 \rangle} \cong \frac{\mathcal{R}[x]}{\langle (x+1)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-1)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x-\eta)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x+\eta)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^2-\eta)^{p^s} \rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^2+\eta)^{p^s} \rangle}$$

Vậy mọi mã C cyclic độ dài $8p^s$ trên $\mathcal{R}$ được biểu diễn dưới dạng

$$C = C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_6,$$

trong đó C_1 là mã cyclic, C_2 là mã negacyclic, C_3 là mã η -constacyclic, C_4 là mã $-\eta$ -constacyclic có độ dài p^s trên $\mathcal{R}$, C_5 và C_6 là mã η -constacyclic và mã $-\eta$ -constacyclic có độ dài $2p^s$ trên $\mathcal{R}$. Các cấu trúc đại số của tất cả mã constacyclic có độ dài p^s và $2p^s$ trên $\mathcal{R}$ được nghiên cứu trong [9] và [10]. Chúng ta có thể xác định cấu trúc đại số của tất cả các mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$ trong trường hợp này. Vì số lượng từ mã trong mỗi mã constacyclic độ dài p^s và $2p^s$ trên $\mathcal{R}$ được nghiên cứu trong [9] và [10], chúng tôi có thể thu được số lượng từ mã trong mỗi mã có độ dài $8p^s$ trên $\mathcal{R}$.

Định lý 3.7. Nếu C là mã cyclic độ dài $8p^s$ trên $\mathcal{R}$ thì C có thể được biểu diễn dưới dạng

$$C = C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_6,$$

trong đó C_1 là mã cyclic, C_2 là mã negacyclic, C_3 là mã η -constacyclic, C_4 là mã $-\eta$ -constacyclic độ dài p^s trên $\mathcal{R}$, C_5 và C_6 là mã η -constacyclic và mã $-\eta$ -constacyclic có độ dài $2p^s$ trên $\mathcal{R}$. Hơn nữa, $|C| = |C_1||C_2||C_3||C_4||C_5||C_6|$.

Áp dụng Mệnh đề 3.2, mã đối ngẫu của mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$ được xác định bằng định lý sau.

Định lý 3.8. Cho $C = C_1 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_6$,

là mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$, trong đó C_1 là mã cyclic, C_2 là mã negacyclic, C_3 là mã η -constacyclic, C_4 là mã $-\eta$ -constacyclic có độ dài p^s trên $\mathcal{R}$, C_5 và C_6 là mã η -constacyclic và mã $-\eta$ -constacyclic có độ dài $2p^s$ trên $\mathcal{R}$. Khi đó $C_1^\perp$ là mã tuần hoàn, $C_2^\perp$ là mã negacyclic, $C_3^\perp$, $C_4^\perp$ là những mã η -constacyclic và mã $-\eta$ -constacyclic có độ dài

p^s trên $\mathcal{R}$, và $C_5^\perp, C_6^\perp$ là những mã η -constacyclic và mã $-\eta$ -constacyclic có độ dài $2p^s$ trên $\mathcal{R}$.

4. Kết luận

Bài báo đưa ra cấu trúc của một lớp mã cyclic. Mã tự đối ngẫu cũng được xác định. Hơn nữa, chúng tôi cũng đưa ra công thức tính số các mã cyclic có độ dài $8p^s$ trên $\mathcal{R}$

Khi $p^m \equiv 1 \pmod{8}$, $p^m \equiv 5 \pmod{8}$.

Lời cảm ơn

Bài báo này là sản phẩm của đề tài B2019 – TNA-02.T, tác giả xin được cảm ơn sự hỗ trợ của Bộ Giáo dục và Đào tạo Việt Nam.

TÀI LIỆU THAM KHẢO/ REFERENCES

- [1]. S. D. Berman, "Semisimple cyclic and Abelian codes. II," *Kibernetika (Kiev)*, vol. 3, pp. 21-30, 1967.
- [2]. J. L. Massey, D. J. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inform. Theory*, vol. 19, pp. 101-110, 1973.
- [3]. G. Falkner, B. Kowol, W. Heise, and E. Zehendner, "On the existence of cyclic optimal codes," *Atti Sem. Mat. Fis. Univ. Modena*, vol. 28, pp. 326-341, 1979.
- [4]. R. M. Roth, and G. Seroussi, "On cyclic MDS codes of length q over $GF(q)$," *IEEE Trans. Inform. Theory*, vol. 32, pp. 284-285, 1986.
- [5]. G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, "On repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 337-342, 1991.
- [6]. J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 343-345, 1991.
- [7]. C. S. Nedeloaia, "Weight distributions of cyclic self-dual codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1582-1591, 2003.
- [8]. L.-Z. Tang, C. B. Soh, and E. Gunawan, "A note on the q -ary image of a $q \supset m$ -ary repeated-root cyclic code," *IEEE Trans. Inform. Theory*, vol. 43, pp. 732-737, 1997.
- [9]. B. Chen, H. Q. Dinh, H. Liu, and L. Wang, "Constacyclic codes of length $2p^s$ over $\mathcal{R}$," *Finite Fields & Appl.*, vol. 36, pp. 108-130, 2016.
- [10]. H. Q. Dinh, "Constacyclic codes of length p^s over $\mathcal{R}$," *J. Algebra*, vol. 324, pp. 940-950, 2010.