NGHIÊN CỨU CẤU TRÚC ĐẠI SỐ CỦA CÁC MÃ REPEATED-ROOT CYCLIC VÀ NEGACYCLIC VỚI ĐỘ DÀI $9P^S$

NGUYỄN THỊ THU HÀ[1*], LÊ HOÀNG NHUẬN[2]
[1] *Khoa Khoa học Cơ bản, Trường Đại học Công nghiệp Thành phố Hồ Chí Minh*
[2] *Khoa Toán, Trường Đại học Sư phạm, Đại học Đà Nẵng*
** Tác giả liên hệ: nguyenthithuha@iuh.edu.vn*
DOIs: https://doi.org/10.46242/jstiuh.v69i03.5114

Tóm tắt. Trong bài báo này chúng tôi nghiên cứu cấu trúc đại số của các mã repeated-root cyclic và negacyclic với độ dài $9p^s$ trên $\mathbb{F}_{p^m}$ ở đây $p \geq 5$ là số nguyên tố. Cụ thể chúng tôi đưa ra phân tích của $x^{9p^s}-1$ và $x^{9p^s}+1$ thành tích của các nhân tử bất khả quy chuẩn tắc trên trường $\mathbb{F}_{p^m}$, trên cơ sở đó xây dựng cấu trúc của các mã cyclic, negacyclic, các mã đối ngẫu của chúng và các mã đối ngẫu bổ sung.

Từ khóa: mã cyclic, mã repeated-root cyclic, mã negacyclic.

1. GIỚI THIỆU

Mã constacyclic với độ dài n trên một trường hữu hạn F là một ideal của vành $\frac{F[x]}{x^n-\lambda}$. Mã cyclic là trường hợp riêng của mã constacyclic khi $\lambda=1$, mã negacyclic là trường hợp riêng của mã constacyclic khi $\lambda=-1$.

Trong lý thuyết mã hóa, các mã constacyclic nói chung và các mã cyclic, negacyclic nói riêng đóng một vai trò vô cùng quan trọng. Chúng có nhiều ứng dụng trong kỹ thuật vì chúng được mã hóa nhờ các thanh ghi dịch chuyển. Trong đó các mã cyclic được nghiên cứu nhiều nhất trong tất cả các mã, vì chúng dễ mã hóa. Mã cyclic được bắt đầu nghiên cứu với hai báo cáo AFCRL năm 1957 và 1959 của E. Prange. Kể từ đó, đại số lý thuyết mã hóa đã đạt được tiến bộ lớn trong việc nghiên cứu các mã cyclic cho cả sửa lỗi ngẫu nhiên và sửa lỗi chùm. Năm 1961 cuốn sách của W. W. Peterson đã tổng hợp các kết quả mở rộng về mã cyclic và đặt khuôn khổ cho phần lớn lý thuyết ngày nay. Năm 1972, cuốn sách này được mở rộng và xuất bản chung bởi Peterson.và EJ Weldon. Nhiều lớp mã bao gồm mã Golay, mã nhị phân Hamming và mã tương đương với mã Reed–Muller là mã cyclic hoặc được mở rộng từ mã cyclic.

Về mặt cổ điển, hầu hết các nhà toán học tập trung nghiên cứu trường hợp độ dài n của mã nguyên tố cùng nhau với đặc số p của trường F.

Trường hợp độ dài n của mã chia hết cho đặc số p của trường F ta có cái gọi là các mã repeated-root. Mã repeated-root lần đầu tiên được khảo sát một cách tổng quát nhất vào những năm 1990 bởi Castagnoli và cộng sự, và van Lint . Họ đã chứng minh rằng các mã repeated-root cyclic có một cấu trúc và tiệm cận xấu. Tuy nhiên, các nghiên cứu đã chỉ ra rằng các mã repeated-root cyclic tối ưu vẫn tồn tại. Kể từ đó, vấn đề về nghiên cứu các cấu trúc đại số và khoảng cách Hamming của các mã repeated-root cyclic và các mã constacyclic nói chung, đã nhận được sự quan tâm ngày càng tăng.

Gần đây, các nhà toán học đã thiết lập cấu trúc đại số về đa thức sinh của tất cả các mã repeated-root constacyclic có độ dài $2p^s, 3p^s, 4p^s$ và $6p^s$ trên $\mathbb{F}_{p^m}$.

Trong bài báo này chúng tôi tập trung nghiên cứu, khảo sát cấu trúc của các mã repeated-root cyclic và negacyclic với độ dài $9p^s$ trên $\mathbb{F}_{p^m}$ ở đây $p \geq 5$ là số nguyên tố. Cụ thể chúng tôi đưa ra phân tích của $x^{9p^s}-1$ và $x^{9p^s}+1$ thành tích của các nhân tử bất khả quy chuẩn tắc trên trường $\mathbb{F}_{p^m}$, trên cơ sở đó xây dựng cấu trúc của các mã cyclic, negacyclic , các mã đối ngẫu của chúng và các mã đối ngẫu bổ sung. Các khái niệm không được đề cập trong bài báo xin mời độc giả tìm hiểu thêm trong các tài liệu (Williams &

Sloane, 1998), (Hai, 2012), (H.Q. Dinh, 2014), (San Ling & Chaoping Xing, 2004), (Huffman & Vera, 2003) mà chúng tôi liệt kê trong danh mục tài liệu tham khảo.

2. CƠ SỞ LÝ THUYẾT

Định nghĩa 2.1. C được gọi là một mã có độ dài n trên bảng chữ cái A, khi đó C là một tập (khác rỗng) các từ mã $(a_1, a_2, ..., a_n)$ trong đó $a_i \in A$. Có thể kí hiệu $C \subseteq A^n$.

Định nghĩa 2.2. C là mã tuyến tính có độ dài n nếu như C là một $R-module$ con của R^n. Mỗi phần tử của C được gọi là một từ mã.

Định nghĩa 2.3. Mã đối ngẫu của của một mã C được kí hiệu là $C^\perp$ là tập hợp các từ mã mà chúng trực giao với tất cả các từ mã trong C.

$$C^\perp = \{x \in A^n \mid x.y = 0, \forall y \in C\}$$

C được gọi là tự đối ngẫu nếu $C = C^\perp$.

C được gọi là tự trực giao nếu $C \subseteq C^\perp$.

C được gọi là tự độc lập nếu $C^\perp \subseteq C$.

C được gọi là tuyến tính với đối ngẫu bổ sung (LCD code - linear with complementary dual code) nếu $C \cap C^\perp = \{0\}$.

Trong bài báo này, chúng tôi ký kiệu $q = p^m$ là lũy thừa nguyên tố với số nguyên tố $p \geq 5$ và m là số nguyên dương. Cho F là một trường hữu hạn, một phần tử $(x_0, x_1, ..., x_{n-1}) \in F^n$, thanh trượt cyclic τ và thanh trượt negacyclic υ được định nghĩa như sau:

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

và

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

Một mã C được gọi là cyclic nếu $\tau(C) = C,$ và C được gọi là negacyclic nếu $\upsilon(C) = C.$ Tổng quát hơn, nếu λ là một phần tử khác không của F, thì thanh trượt λ-constacyclic (λ-xoắn) τ_λ trên F^n là thanh trượt $\tau_\lambda(x_0, x_1, ..., x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, ..., x_{n-2}),$

Mã C được gọi là λ-constacyclic nếu $\tau_\lambda(C) = C,$ nghĩa là nếu C đóng dưới thanh trượt λ-constacyclic τ_λ. Từ định nghĩa, khi $\lambda = 1$, các mã λ-constacyclic là cyclic, và khi $\lambda = -1$ thì các mã λ-constacyclic là negacyclic.

Mệnh đề 2.4. *Một mã tuyến tính C với độ dài n là λ-constacyclic trên F nếu và chỉ nếu C là ideal của $\frac{F[x]}{\langle x^n - \lambda \rangle}$. Hơn nữa, $\frac{F[x]}{\langle x^n - \lambda \rangle}$ là một vành chính, trong đó các ideal của nó được sinh bởi các nhân tử của $x^n - \lambda$.*

Mệnh đề 2.5. *Đối ngẫu của một mã λ-constacyclic là một mã λ^{-1}-constacyclic.*

Mệnh đề 2.6. *Cho λ là một phần tử khác không của F và*

$$a(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1}, b(x) = b_0 + b_1 x + ... + b_{n-1} x^{n-1} \in F[x]$$

thì $a(x)b(x) = 0$ trong $\frac{F[x]}{\langle x^n - \lambda \rangle}$ khi và chỉ khi $(a_0, a_1, ..., a_{n-1})$ trực giao với $(b_{n-1}, b_{n-2}, ..., b_0)$ và tất cả các thanh trượt λ^{-1}-constacyclic của nó.

Cho R là một vành giao hoán, S là một tập con khác rỗng của R, ta kí hiệu linh tử của S là ann(S) được xác đinh như sau: $ann(S) = \{f \mid fg = 0, \forall g \in S\}$.

Dễ dàng thấy rằng ann(S) là một ideal của R.

Cho f là một đa thức bậc k thì đa thức nghịch đảo $x^k f\left(x^{-1}\right)$ của nó được kí hiệu là f^*.

Mệnh đề 2.7. *Cho λ là một phần tử của F sao cho $\lambda^2 = 1$. Giả sử C là một mã λ - constacyclic có độ dài n trên F thì đối ngẫu của C, kí hiệu là $C^\perp$, chính là $ann^*(C)$.*

3. CÁC KẾT QUẢ CHÍNH

Trong bài báo này chúng tôi thực hiên khảo sát các mã cyclic và negacyclic với độ dài $9p^s$, với $p \geq 5$. Ta cố định ξ là căn nguyên thủy bậc $p^m - 1$ của đơn vị sao cho

$\mathbb{F}_{p^m} = \{0, \xi, \xi^2, ..., \xi^{p^m-2}, \xi^{p^m-1} = 1\}$.

Các mã cyclic với độ dài $9p^s$ là các ideal của vành $R_1 = \dfrac{\mathbb{F}_{p^m}[x]}{\left\langle x^{9p^s} - 1 \right\rangle}$.

Các mã như vậy được sinh bởi các nhân tử của $x^{9p^s} - 1$. Do đó chúng ta cần phân tích $x^{9p^s} - 1$ thành tích các nhân tử bất khả quy chuẩn tắc. Trong trường $\mathbb{F}_{p^m}$ ta có

$$x^{9p^s} - 1 = \left(x^9 - 1\right)^{p^s} = \left[(x-1)\left(x^2 + x + 1\right)\left(x^6 + x^3 + 1\right)\right]^{p^s}.$$

Trong trường hợp $p \geq 5$ là số nguyên tố và $p^m \equiv 2 \pmod 9$ hay $p^m \equiv 5 \pmod 9$ thì ta có sự phân tích

$$x^9 - 1 = (x-1)\left(x^2 + x + 1\right)\left(x^6 + x^3 + 1\right)$$

Chúng tôi xét tính bất khả quy của đa thức $x^2 + x + 1$ bằng bổ đề sau:

Bổ đề 3.1. *Cho $p \geq 5$ là số nguyên tố và đa thức $f(x) = x^2 + x + 1 \in \mathbb{F}_{p^m}[x]$. Khi đó f(x) khả quy khi và chỉ khi $p^m \equiv 1 \pmod 3$. Trong trường hợp đó:*

$$f(x) = \left(x - \xi^{\frac{p^m-1}{3}}\right)\left(x - \xi^{\frac{2\left(p^m-1\right)}{3}}\right)$$

Chứng minh. $f(x) = x^2 + x + 1$ khả quy khi và chỉ khi $x^2 + x + 1$ có nghiệm trong $\mathbb{F}_{p^m}$, khi và chỉ khi $x^3 - 1$ có nghiệm khác 1 (vì 1 không phải là nghiệm của $f(x)$), khi và chỉ khi tồn tại $\gamma \neq 1$ sao cho $\gamma^3 = 1$.

Giả sử tồn tại $\gamma \neq 1$ sao cho $\gamma^3 = 1$ thì cấp của γ là 1 hay 3. Nếu cấp γ là 1 thì $\gamma = 1$ mâu thuẫn, vậy cấp của γ là 3 nên theo Định lý Lagrange suy ra $3 \mid p^m - 1$ (do 0 không là nghiệm của $f(x)$ nên γ thuộc nhóm nhân $\mathbb{F}_{p^m}^*$ và $\mathbb{F}_{p^m}^*$ có $p^m - 1$ phần tử) , do đó $p^m \equiv 1 \pmod 3$.

Nếu $p^m \equiv 1 \pmod 3$ thì $f(x)$ có 2 nghiệm $\xi^{\frac{p^m-1}{3}}$ và $\xi^{\frac{2\left(p^m-1\right)}{3}}$. □

Mệnh đề 3.2. *Nếu $p^m \equiv 2 \pmod 9$ hay $p^m \equiv 5 \pmod 9$ thì $f(x) = x^2 + x + 1$ là bất khả quy.*

Chứng minh. Nếu $p^m \equiv 2\,(mod\,9)$ hay $p^m \equiv 5\,(mod\,9)$ thì $p^m \equiv 2\,(mod\,3)$. Theo Bổ đề 3.1. ta có $f(x) = x^2 + x + 1$ là bất khả quy. □

Chúng ta tiếp tục xét tính bất khả quy của $x^6 + x^3 + 1$.

Bổ đề 3.3. *Cho $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ là một đa thức có bậc dương. Khi đó tồn tại một trường phân rã F của $f(x)$ trên K. Hơn nữa, nếu $\rho : K \to K'$ là một đẳng cấu trường và F' là một trường phân rã của đa thức $g(x) = \sum_{i=0}^{n} \rho(c_i) x^i$ trên K' thì tồn tại một đẳng cấu $\phi : F \to F'$ sao cho $\phi(a) = \rho(a)$ với mọi $a \in K$.*

Bổ đề 3.4. *Cho E/K là một mở rộng trường và $\alpha \in E$ là phần tử đại số trên K. Giả sử $p(x) \in K[x]$ là đa thức bất khả quy nhận α làm nghiệm. Khi đó $K(\alpha) = K[\alpha]$ và $[K(\alpha) : K] = deg(p(x))$. Ngoài ra, nếu $deg(p(x)) = n$ thì $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ là một cơ sở của K - không gian vector $K(\alpha)$.*

Mệnh đề 3.5. *Cho $p \geq 5$ là số nguyên tố, $g(x) = x^6 + x^3 + 1$ là 1 đa thức trên $\mathbb{F}_{p^m}[x]$. Nếu $p^m \equiv 2(mod 9)$ hay $p^m \equiv 5(mod 9)$ thì $g(x) = x^6 + x^3 + 1$ là bất khả quy.*

Chứng minh. Ta có tồn tại một trường F chứa $\mathbb{F}_{p^m}$ sao cho $g(x)$ phân rã trên F. Rõ ràng nếu $\alpha \in K$ là một nghiệm của $g(x)$ thì $\alpha^n \neq 1$ với mọi $n \in \{1,2,3,4,5,6,7,8\}$ và $\alpha^9 = 1$.

Thật vậy, ta có $x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$, do đó α là nghiệm của $x^9 - 1$ suy ra $\alpha^9 = 1$.

Nếu $\alpha = 1$ thì $3.1 = 0$ mâu thuẫn vì $p \geq 5$.

Nếu $\alpha^2 = 1$ thì $1 = \alpha^9 = (\alpha^2)^4 \alpha = \alpha$ suy ra $1 = \alpha$ mâu thuẫn.

Nếu $\alpha^3 = 1$ thì $1 = \alpha^9 = \alpha^6 \alpha^3$ suy ra $1 = \alpha^6$ mà $\alpha^6 + \alpha^3 + 1 = 0$ suy ra $3.1 = 0$ mâu thuẫn.

Nếu $\alpha^4 = 1$ thì $1 = \alpha^9 = (\alpha^4)^2 \alpha$ suy ra $\alpha = 1$ mâu thuẫn.

Nếu $\alpha^5 = 1$ thì $1 = \alpha^9 = \alpha^4 \alpha^5$ suy ra $\alpha^4 = 1$ mâu thuẫn.

Nếu $\alpha^6 = 1$ thì $1 = \alpha^9 = \alpha^3 \alpha^6$ suy ra $\alpha^3 = 1$ mâu thuẫn.

Nếu $\alpha^7 = 1$ thì $1 = \alpha^9 = \alpha^2 \alpha^7$ suy ra $\alpha^2 = 1$ mâu thuẫn.

Nếu $\alpha^8 = 1$ thì $1 = \alpha^9 = \alpha \alpha^8$ suy ra $\alpha = 1$ mâu thuẫn. Vậy khẳng định được chứng minh.

Giả sử $g(x)$ khả quy trên $\mathbb{F}_{p^m}[x]$. Vì $deg(g(x)) = 6$ nên $g(x)$ có nhân tử bất khả quy bậc d với $d \in \{1,2,3\}$. Ta xét các khả năng xảy ra như sau.

Giả sử $g(x)$ có nhân tử bất khả quy bậc 1 thì $g(x)$ có nghiệm $\alpha \in \mathbb{F}_{p^m}$. Vì $g(0) = 1 \neq 0$ nên $\alpha \in \mathbb{F}_{p^m}^*$. Theo khẳng định trên, α có cấp 9 trong nhóm nhân $\mathbb{F}_{p^m}^*$. Vì $\mathbb{F}_{p^m}^*$ có cấp $p^m - 1$ nên theo Định lý Lagrange $9 | p^m - 1$ suy ra $p^m \equiv 1(mod\,9)$. Mâu thuẫn với giả thiết của mệnh đề.

Giả sử $g(x)$ có nhân tử bất khả quy bậc 2 $q(x) \in \mathbb{F}_{p^m}[x]$. Ta lấy $\alpha \in F$ là một nghiệm của $q(x)$. Đặt $T = \mathbb{F}_{p^m}[\alpha] = \{h(\alpha) | \ h(x) \in \mathbb{F}_{p^m}[x]\}$. Theo Bổ đề 3.4 ta có T là 1 trường chứa $\mathbb{F}_{p^m}$ và $\{1, \alpha\}$ là một cơ sở của $\mathbb{F}_{p^m}$ - không gian vectơ T. Vì thế T có p^{2m} phần tử. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Từ khẳng định đầu của chứng minh, ta suy ra cấp của α trong nhóm nhân T^* là 9. Theo Định lý Lagrange ta có $9 | p^{2m} - 1$, tuy nhiên

Nếu $p^m \equiv 2(mod 9)$ thì $p^{2m}-1 \equiv 3(mod 9)$

Nếu $p^m \equiv 5(mod 9)$ thì $p^{2m}-1 \equiv 6(mod 9)$

Mâu thuẫn.

Giả sử $g(x)$ có nhân tử bất khả quy bậc 3 $q(x) \in \mathbb{F}_{p^m}[x]$. Ta lấy $\alpha \in F$ là một nghiệm của $q(x)$. Đặt $T = \mathbb{F}_{p^m}[\alpha] = \{h(\alpha) | h(x) \in \mathbb{F}_{p^m}[x]\}$. Theo Bổ đề 3.4 ta có T là 1 trường chứa $\mathbb{F}_{p^m}$ và $\{1, \alpha, \alpha^2\}$ là 1 cơ sở của $\mathbb{F}_{p^m}$ - không gian vectơ T. Vì thế T có p^{3m} phần tử. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Từ khẳng định đầu của chứng minh, ta suy ra cấp của α trong nhóm nhân T^* là 9. Theo Định lý Lagrange ta có $9 | p^{3m}-1$, tuy nhiên theo giả thiết của mệnh đề:

Nếu $p^m \equiv 2(mod 9)$ thì $p^{3m}-1 \equiv 7(mod 9)$

Nếu $p^m \equiv 5(mod 9)$ thì $p^{3m}-1 \equiv 7(mod 9)$

Mâu thuẫn.

Như vậy $f(x)$ là bất khả quy. □

Để tìm số từ mã của mã cyclic và đối ngẫu của nó ta sử dụng 2 bổ đề sau:

Bổ đề 3.6. *Cho $g(x)$ là đa thức sinh của một ideal của $F_q[x]/(x^n-1)$, khi đó mã cyclic tương ứng có số chiều là k nếu bậc của $g(x)$ là $n-k$.*

Bổ đề 3.7. *Cho C là một mã tuyến tính với độ dài n trên trường F_q. Khi đó:*

i. $|C| = q^{dim(C)}$, *nghĩa là* $dim(C) = log_q|C|$

ii. $C^\perp$ *là một mã tuyến tính và* $dim(C) + dim(C^\perp) = n$

iii. $(C^\perp)^\perp = C$

Định lý 3.8. *Cho $p \geq 5$ là số nguyên tố, nếu $p^m \equiv 2(mod 9)$ hay $p^m \equiv 5 (mod 9)$ thì $x^{9p^s}-1$ được nhân tử hóa thành các nhân tử bất khả quy có dạng*

$$x^{9p^s}-1 = (x-1)^{p^s}(x^2+x+1)^{p^s}(x^6+x^3+1)^{p^s}$$

Các mã cyclic có độ dài $9p^s$ trên $\mathbb{F}_{p^m}$ là các ideal

$$C = \langle (x-1)^i (x^2+x+1)^j (x^6+x^3+1)^k \rangle$$

với $0 \leq i, j, k \leq p^s$. Mỗi mã cyclic C như vậy chứa $p^{m(9p^s-i-2j-6k)}$ từ mã.

Đối ngẫu của nó là

$$C^\perp = \langle (x-1)^{p^s-i} (x^2+x+1)^{p^s-j} (x^6+x^3+1)^{p^s-k} \rangle$$

nó chứa $p^{m(i+2j+6k)}$ từ mã.

Chứng minh. Nếu $p^m \equiv 2(mod 9)$ hay $p^m \equiv 5 (mod 9)$ thì x^9-1 được nhân tử hóa thành các nhân tử bất khả quy có dạng

$$x^9-1 = (x-1)(x^2+x+1)(x^6+x^3+1)$$

Phân tích thành nhân tử của x^{9p^s-1} dựa trên cơ sở rằng trong $\mathbb{F}_{p^m}[x]$ thì $x^{9p^s-1}=\left(x^9-1\right)^{p^s}$, do đó ta có $x^{9p^s-1}=(x-1)^{p^s}\left(x^2+x+1\right)^{p^s}\left(x^6+x^3+1\right)^{p^s}$.

Vì các mã cyclic với độ dài $9p^s$ trên $\mathbb{F}_{p^m}[x]$ là các ideal được sinh bởi các nhân tử của $x^{9p^s}-1$ nên ta thu được các mã cyclic như trên.

Ta tìm số từ mã của các mã cyclic có độ dài $9p^s$ trên $\mathbb{F}_{p^m}$: Ta có số chiều của mã cyclic C là $dim(C)=9p^s-i-2j-6k.$ Từ công thức $|C| = q^{dim(C)}$ với $q=p^m$ ta có số từ mã của mã cyclic C là $p^{m\left(9p^s-i-2j-6k\right)}$.

Về đối ngẫu, ta nhận xét rằng $(x-1)^*=-(x-1),\left(x^2+x+1\right)^*=x^2+x+1,\left(x^6+x^3+1\right)^*=x^6+x^3+1.$ Nên ta có

$$\begin{aligned}C^\perp &= ann^*(C)\\ &=\left\langle (x-1)^{p^s-i}\left(x^2+x+1\right)^{p^s-j}\left(x^6+x^3+1\right)^{p^s-k}\right\rangle^*\\ &=\left\langle \left[(x-1)^*\right]^{p^s-i}\left[\left(x^2+x+1\right)^*\right]^{p^s-j}\left[\left(x^6+x^3+1\right)^*\right]^{p^s-k}\right\rangle\\ &=\left\langle (x-1)^{p^s-i}\left(x^2+x+1\right)^{p^s-j}\left(x^6+x^3+1\right)^{p^s-k}\right\rangle.\end{aligned}$$

Từ công thức $dim(C)+dim\left(C^\perp\right)=n$ với $n=9p^s$, ta có số chiều của mã cyclic $C^\perp$ là $dim\left(C^\perp\right)=i+2j+6k$, vậy số từ mã của mã cyclic $C^\perp$ là $\left|C^\perp\right|=q^{dim\left(C^\perp\right)}=p^{m(i+2j+6k)}$. □

So sánh C và $C^\perp$ ta có nếu $p^m\equiv 2(mod\,9)$ hay $p^m\equiv 5(mod 9)$ thì $C=C^\perp$ nếu và chỉ nếu $p^s=2i=2j=2k,$ điều này không thể xảy ra vì p lẻ. Từ nhận xét này ta có Hệ quả sau.

Hệ quả 3.9. *Với mọi số nguyên tố $p\geq 5$ và $p^m\equiv 2(mod\,9)$ hay $p^m\equiv 5\,(mod\,9)$ thì không tồn tại mã tự đối ngẫu có chiều dài $9p^s$.*

Hệ quả 3.10. *Với mọi số nguyên tố $p\geq 5$ và $p^m\equiv 2(mod 9)$ hay $p^m\equiv 5(mod 9)$ thì có 8 mã cyclic LCD có độ dài $9p^s$ trên $\mathbb{F}_{p^m}$. Cụ thể là*

$$\left\langle (x-1)^i\left(x^2+x+1\right)^j\left(x^6+x^3+1\right)^k\right\rangle$$

với $i,j,k\in\{0,p^s\}$.

Chứng minh. Ta có

$$C\cap C^\perp=\left\langle (x-1)^{max\{i,p^s-i\}}\left(x^2+x+1\right)^{max\{j,p^s-j\}}\left(x^6+x^3+1\right)^{max\{k,p^s-k\}}\right\rangle$$

Vậy ta có $C\cap C^\perp=\{0\}$ khi và chỉ khi

$$p^s=\max\{i,p^s-i\}=\max\{j,p^s-j\}=\max\{k,p^s-k\}$$

Điều này tương đương với $i,j,k\in\{0,p^s\}$. Vậy có tất cả 8 mã cyclic LCD có độ dài $9p^s$ trên $\mathbb{F}_{p^m}$.

4. KẾT LUẬN

Mặc dù chúng tôi đã có những kết quả ban đầu về cấu trúc đại số của các mã repeated-root cyclic và negacyclic với độ dài $9P^S$ nhưng hướng nghiên cứu này vẫn còn rất mới mẻ và nhiều khía cạnh chưa được khai thác. Chúng tôi mong muốn sẽ có nhiều kết quả tốt hơn về lĩnh vực này trong tương lai.

TÀI LIỆU THAM KHẢO

F.J. MacWilliams and N.J.A. Sloane (1998). *The theory of error-correcting codes*, 10^{th} impression, North-Holland, Amsterdam.

Hai, Q. Dinh (2012). *Repeated-root constacyclic codes of length* $2p^s$. Finite Fields Appl, 18 (2012), no. 1, 133-143, DOI 10.1016/j. ffa.2011.07.003. MR2874911.

H.Q. Dinh (2014). *Repeated-root cyclic and negacyclic codes of length* $6p^s$. AMS Contemp. Math. 609, pp. 69–87.

San Ling and Chaoping Xing (2004). *Coding Theory A First Course*. Cambridge University press.

W. Cary Huffman and Vera Pless (2003). *Fundamentals of error-correcting codes*. Cambridge University Press. Cambridge. MR 1996953 (2004k:94077).

RESEARCH OF THE ALGEBRAIC STRUCTURE OF REPEATED-ROOT CYCLIC AND NEGACYCLIC CODE WITH LENGTH $9P^S$

NGUYEN THI THU HA[1*], LE HOANG NHUAN[2]

[1] *Faculty of Fundamental Science, Industrial University of Ho Chi Minh City*

[2] *Department of Mathematics, University of Science and Education, The University of Danang*

Abstract. In this paper, we study the algebraic structure of repeated-root cyclic and negacyclic codes with length $9p^s$ over $\mathbb{F}_{p^m}$ with $p \geq 5$ being prime. In particular, we give the analysis of and the product of the normal irreducible factors on the field $\mathbb{F}_{p^m}$, on the basis of which, we construct the structure of cyclic, negacyclic codes, their dual codes and dual codes additional.

Keywords: cyclic code, repeated-root cyclic code, negacyclic code.

Ngày gửi bài:09/05/2023
Ngày chấp nhận đăng:12/09/2023