CYCLIC CODE OF LENGTH $7P^S$ AND THEIR DISTANCES

MÃ CYCLIC CÓ ĐỘ DÀI $7P^S$ VÀ KHOẢNG CÁCH CỦA CHÚNG

Trần Thiên Ân[1]
[1]Trường Đại học Sư phạm, Đại học Đà Nẵng
Nguyễn Thị Thu Hà[2]
[2]Trường Đại học Công nghiệp thành phố Hồ Chí Minh

ABSTRACT: *Let $p>7$ be an odd prime and s, m be positive integers, such that $p^m \equiv 3 \pmod 7$ or $p^m \equiv 5 \pmod 7$. In this paper, using the relationship about distances between simple-root cyclic codes and repeated-root cyclic codes, the authors study the structure of cyclic codes and Hamming distance of all cyclic codes of length $7p^s$ over finite field F_{p^m}.*

Keywords: *Simple-root code, repeated-root code, Hamming distance, cyclic code.*

TÓM TẮT: *Với một số nguyên tố lẻ $p>7$ bất kì và s, m là một số nguyên dương thỏa mãn điều kiện $p^m \equiv 3 \pmod 7$ hoặc $p^m \equiv 5 \pmod 7$. Trong bài báo này, bằng việc sử dụng mối quan hệ giữa các mã cyclic nghiệm đơn và các mã cyclic nghiệm kép, nhóm tác giả sẽ nghiên cứu cấu trúc mã cyclic có độ dài $7p^s$ trên trường hữu hạn F_{p^m} và khoảng cách Hamming của chúng.*

Từ khóa: *Mã nghiệm đơn, mã nghiệm kép, khoảng cách Hamming, mã cyclic.*

1. GIỚI THIỆU

Lý thuyết mã hóa là một trong số những vấn đề được quan tâm hiện nay. Đặc biệt, trong việc giải quyết tình trạng xuất hiện lỗi trong quá trình truyền thông số liệu trên các kênh truyền.

Năm 1957, mã cyclic trên trường hữu hạn được nghiên cứu lần đầu tiên bởi Prange [4]. Lớp mã này sau đó được các nhà nghiên cứu để ý tới vì cấu trúc đại số tốt của chúng và ứng dụng được vào việc xây dựng các mã tốt trong thực tiễn. Nhiều mã tốt được biết tới như mã BCH, mã Kerdock, mã Golay, mã Reed-Muller, mã Preparata,… và mã Hamming nhị phân; chúng là các mã cyclic hoặc là các mã được xây dựng từ cấu trúc mã cyclic.

Cho F_{p^m} là trường hữu hạn, trong đó p là một số nguyên tố và m là một số nguyên dương. Mã cyclic có độ dài n trên F_{p^m} được phân loại như lớp iđêan $\langle g(x) \rangle$ của vành thương $\mathrm{F}_{p^m}[x]/\langle x^n - 1 \rangle$, trong đó đa thức sinh $g(x)$ là đa thức monic có bậc nhỏ nhất và duy nhất trong mã, với phần dư của phép chia cho $x^n - 1$. Vào năm 1967, Berman [5] nghiên cứu trường hợp $(n, p) = 1$ và các mã thỏa mãn điều kiện này được gọi là các mã nghiệm đơn (simple-root codes). Chung lại, các mã cyclic được phân loại thành hai nhóm: mã nghiệm đơn (simple-root codes) trong đó đa thức sinh $g(x)$ không có nhân tử bất khả quy lặp lại; mã nghiệm lặp (repeated-root cyclic

codes), trong đó đa thức sinh $g(x)$ có nghiệm lặp.

Trong bài báo này, các kết quả mới ở phần 3 được chia thành hai mục chính gồm: Mục 3.1. Cấu trúc mã cyclic có độ dài $7p^s$ đưa ra cấu trúc của mã cyclic có độ dài $7p^s$ trên trường hữu hạn có p^m phần tử, trong trường hợp $p^m \equiv 3 \pmod 7$ hoặc $p^m \equiv 5 \pmod 7$. Như một hệ quả, bài viết chỉ ra rằng không tồn tại mã tự đối ngẫu có độ dài $7p^s$ và có 4 mã cyclic LCD có độ dài $7p^s$ trên trường hữu hạn F_{p^m}; Mục 3.2. Khoảng cách Hamming của mã cyclic có độ dài $7p^s$, trong mục này dựa vào các kết quả của mục 3.1. đưa ra các kết quả về tính toán khoảng cách Hamming trong trường hợp nói trên.

2. CƠ SỞ LÝ THUYẾT

Định nghĩa 2.1. C được gọi là một mã có độ dài n trên bảng chữ cái A, nếu C là một tập (khác rỗng) của A^n, các phần tử của C được gọi là 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 trên R là một $R-$ *môđun* con của R^n. Mỗi phần tử của C được gọi là một từ mã.

Định nghĩa 2.3. Với mỗi từ mã $x = (x_0, x_1, ..., x_{n-1}) \in R^n$, trọng Hamming của x, kí hiệu $wt(x)$ là số các thành phần khác không của x.

Khoảng cách Hamming giữa vectơ $x, y \in C^n$ là số cặp tọa độ mà trong đó $x_i \neq y_i$, kí hiệu

$$d_H(x, y) := \left|\{i : x_i \neq y_i\}\right|.$$

Hơn nữa, $d_H(x, y) = wt(x - y)$.

Tỉ lệ khoảng cách Hamming giữa $x, y \in C^n$ là

$$\delta_{(x,y)} = \frac{d_H(x, y)}{n}.$$

Định nghĩa 2.4. Khoảng cách tối thiểu của một mã $C \subseteq A^n$ là $\min d_H(c, c')$, $c \neq c' \in C$, cũng có thể gọi là khoảng cách của mã C.

Định nghĩa 2.5. Mã đối ngẫu 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

$$C \cap C^\perp = \{0\}.$$

Định nghĩa 2.6. Với mỗi phần tử đơn vị λ của R, toán tử λ-constacyclic τ_λ của R^n được xác định như sau:

$$\tau_\lambda(c_0, c_1, ..., c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, ..., c_{n-2})$$

và C được gọi là một mã λ-constacyclic nếu như $\tau_\lambda(C) = C$, nghĩa là C đóng dưới toán tử τ_λ.

Trong trường hợp $\lambda = 1$, khi đó mã λ-constacyclic được gọi là mã cyclic.

Trong trường hợp $\lambda = -1$, khi đó mã λ-constacyclic được gọi là mã negacyclic.

Với mỗi từ mã $c = (c_0, c_1, ..., c_{n-1})$ thường được định nghĩa thông qua cách biểu diễn

$$c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

và mã C lần lượt được xác định bằng tập tất cả các đa thức biểu diễn của nó. Khi đó trong vành $\frac{R[x]}{\langle x^n-\lambda\rangle}$, $xc(x)$ tương ứng với toán tử λ-constacyclic của $c(x)$.

Hơn nữa một mã cyclic có độ dài n trên R có thể được xác định như là một iđêan của vành thương $R[x]/\langle x^n-1\rangle$ thông qua đẳng cấu $R-môđun$ sau:

$$\varphi:\ R^n \rightarrow R[x]/\langle x^n-1\rangle$$
$$(c_0,c_1,...,c_{n-1}) \mapsto c_0+c_1x+c_2x^2+...+c_{n-1}x^{n-1}+\langle x^n-1\rangle.$$

3. KẾT QUẢ CHÍNH

3.1. Cấu trúc mã cyclic có độ dài $7p^s$

Mã cyclic có độ dài $7p^s$ là iđêan của vành $R=\frac{\mathrm{F}_{p^m}[x]}{\langle x^{7p^s}-1\rangle}$. Trong đó F_{p^m} là kí hiệu của trường hữu hạn có p^m phần tử.

Đầu tiên ta sẽ phân tích nhân tử hóa của $x^{7p^s}-1$ thành tích của các đa thức monic bất khả quy. Trên trường F_{p^m}, ta có

$$x^{7p^s}-1=(x^7-1)^{p^s}$$
$$=[(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)]^{p^s}.$$

Bổ đề 3.1.1 [1].

Cho $f(x)=\sum_{i=0}^{n}c_ix^i \in K[x]$ là một đa thức có bậc dương. Khi đó tồn tại một trường phân rã F của $f(x)$ trên K. Hơn nữa, nếu $\rho: K \rightarrow K'$ 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 $\varphi: F \rightarrow F'$ sao cho $\varphi(a)=\rho(a)$ với mọi $a \in K$.

Bổ đề 3.1.2 [1]. 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 $[K(\alpha):K]=deg(p(x))$. Hơn nữa, nếu $deg(p(x))=n$ thì $S=\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$ là một cơ sở của K-không gian vector $K(\alpha)$.

Mệnh đề 3.1.3. Với một số nguyên tố $p>7$, và $\phi_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$ là đa thức chia đường tròn trên F_{p^m}. Nếu $p^m \equiv 3 \pmod 7$ hoặc $p^m \equiv 5 \pmod 7$, thì $\phi_7(x)$ là bất khả quy.

Chứng minh

Theo **Bổ đề 3.1.1**, tồn tại một trường F chứa F_{p^m} sao cho $\phi_7(x)$ phân rã trên F. Trước hết, ta khẳng định nếu $\alpha \in K$ là một nghiệm của $\phi_7(x)$ thì $\alpha^n \neq 1$ với mọi $n \in \{1,2,3,4,5,6\}$ và $\alpha^7=1$. Thật vậy, rõ ràng $x^7-1=(x-1)\phi_7(x)$. Do đó, α là nghiệm của x^7-1. Suy ra $\alpha^7=1$. Nếu $\alpha=1$ thay vào $\phi_7(x)$ thì $7=0 \in \mathrm{F}_{p^m}$ và do đó 7 là bội của p^m điều này mâu thuẫn với giả thiết về p là số nguyên tố lớn hơn 7. Nếu $\alpha^2=1$ thì $1=\alpha^7=(\alpha^2)^3\alpha=\alpha$, điều này là vô lí. Nếu $\alpha^3=1$ thì $1=\alpha^7=(\alpha^3)^2\alpha=\alpha$, vô lí. Nếu $\alpha^4=1$ thì $1=\alpha^7=\alpha^4\alpha^3=\alpha^3$, vô lí. Nếu $\alpha^5=1$ thì $1=\alpha^7=\alpha^5\alpha^2=\alpha^2$, vô lí. Nếu $\alpha^6=1$ thì $1=\alpha^7=\alpha^6\alpha=\alpha$, vô lí.

Như vậy, $\alpha^n \neq 1$ với mọi $n \in \{1,2,3,4,5,6\}$ và $\alpha^7 = 1$. Khẳng định được chứng minh.

Giả sử $\phi_7(x)$ khả quy trên F_{p^m}. Vì $deg(\phi_7(x)) = 6$ nên $\phi_7(x)$ có nhân tử bất khả quy bậc d với $d \in \{1,2,3\}$.

Nếu $\phi_7(x)$ có nhân tử bậc nhất thì $\phi_7(x)$ có nghiệm $\alpha \in \mathrm{F}_{p^m}$. Vì $\phi_7(0) = 1 \neq 0$ nên $\alpha \neq 0$. Do đó, $\alpha \in \mathrm{F}_{p^m}^*$. Theo khẳng định trên, phần tử α có cấp 7 trong nhóm nhân $\mathrm{F}_{p^m}^*$. Vì $\mathrm{F}_{p^m}^*$ có cấp $p^m - 1$ nên theo Định lý Lagrange, 7 là ước của $p^m - 1$. Điều này mâu thuẫn với giả thiết về p.

Giả sử $\phi_7(x)$ có nhân tử bất khả quy $q(x) \in \mathrm{F}_{p^m}[x]$ với $deg(q(x)) = 2$. Lấy $\alpha \in F$ là một nghiệm của $q(x)$. Đặt $T = \mathrm{F}_{p^m}[\alpha] = \{g(\alpha) \mid g(x) \in \mathrm{F}_{p^m}[x]\}$. Theo

Bổ đề 3.1.2. T là một trường chứa F_{p^m} và $\{1, \alpha\}$ là một cơ sở của F_{p^m}-không gian vector T. Vì thế, T có p^{2m} phần tử. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Từ khẳng định ở phần đầu chứng minh ta suy ra cấp của α trong nhóm nhân T^* là 7. Theo Định lí Lagrange, 7 là ước của cấp của nhóm nhân T^*. Chú ý rằng T^* có cấp $p^{2m} - 1$. Tuy nhiên, $p^{2m} - 1$ không chia hết cho 7 vì theo giả thiết ta suy ra được $p^{2m} - 1 \equiv 3 (\mathrm{mod}\, 7)$ hoặc $p^{2m} - 1 \equiv 1 (\mathrm{mod}\, 7)$. Điều này là vô lí, do đó $\phi_7(x)$ không có nhân tử bậc 2.

Giả sử $\phi_7(x)$ có nhân tử bất khả quy $q(x) \in \mathrm{F}_{p^m}[x]$ với $deg(q(x)) = 3$. Lấy $\alpha \in F$ là một nghiệm của $q(x)$. Đặt $T = \mathrm{F}_{p^m}[\alpha] = \{g(\alpha) \mid g(x) \in \mathrm{F}_{p^m}[x]\}$. Theo

Bổ đề 3.1.2, T là một trường chứa F_{p^m} và $\{1, \alpha, \alpha^2\}$ là một cơ sở của F_{p^m}-không gian vector T. Vì thế T có p^{3m} phần tử. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Từ khẳng định ở phần đầu chứng minh ta suy ra cấp của α trong nhóm nhân T^* là 7. Theo Định lí Lagrange, 7 là ước của cấp của nhóm nhân T^*. Chú ý rằng T^* có cấp $p^{3m} - 1$. Nghĩa là 7 là ước của $p^{3m} - 1$ hay $p^m \equiv 6 (\mathrm{mod}\, 7)$. Tuy nhiên, $p^{3m} - 1$ không chia hết cho 7 vì theo giả thiết ta suy ra được $p^{3m} - 1 \equiv 5 (\mathrm{mod}\, 7)$. Điều này là vô lí, do đó $\phi_7(x)$ không có nhân tử bậc 3.

Vậy, trong trường hợp $p^m \equiv 3 (\mathrm{mod}\, 7)$ hoặc $p^m \equiv 5 (\mathrm{mod}\, 7)$, $\phi_7(x)$ là bất khả quy.

Bổ đề 3.1.3 [3]. Cho λ là một phần tử khả nghịch của F sao cho $\lambda^2 = 1$, nghĩa là $\lambda = 1$ hoặc $\lambda = -1$. Giả sử C là một mã λ-constacylic có độ dài n trên trường F. Khi đó, mã đối ngẫu $C^\perp$ của C là $ann^*(C)$.

Định lý 3.1.4. Nếu $p^m \equiv 3 (\mathrm{mod}\, 7)$ hoặc $p^m \equiv 5 (\mathrm{mod}\, 7)$ thì mã cyclic có độ dài $7p^s$ trên F_{p^m} là iđêan

$$C = \langle (x-1)^i (\phi_7(x))^j \rangle \in R,$$

trong đó $0 \leq i, j \leq p^s$. Mỗi mã $C = \langle (x-1)^i (\phi_7(x))^j \rangle$ thu được

$p^{m(7p^s-i-6j)}$ từ mã và mã đối ngẫu của nó là $C^{\perp}=\langle(x-1)^{p^s-i}(\phi_7(x))^{p^s-j}\rangle$.

Chứng minh

Cấu trúc mã cyclic theo sự phân tích $x^{7p^s}-1$ thành các nhân tử bất khả quy theo mệnh đề trên.

Đối với đối ngẫu của mã, ta thấy rằng $(x-1)^*=-(x-1), \phi_7(x)^*=\phi_7(x)$. Do đó, ta có:

$$\begin{aligned} C^{\perp} &= ann^*(C) \\ &= \left\langle \left(x-1\right)^{p^s-i}\left(\phi_7(x)\right)^{p^s-j}\right\rangle^* \\ &= \left\langle \left[\left(x-1\right)^*\right]^{p^s-i}\left[\left(\phi_7(x)\right)^*\right]^{p^s-j}\right\rangle \\ &= \left\langle \left(x-1\right)^{p^s-i}\left(\phi_7(x)\right)^{p^s-j}\right\rangle. \end{aligned}$$

Hệ quả 3.1.5. Không tồn tại mã tự đối ngẫu có chiều dài $7p^s$ trên trường F_{p^m} trong trường hợp $p^m \equiv 3 (\mathrm{mod}\, 7)$ hoặc $p^m \equiv 5 (\mathrm{mod}\, 7)$.

Chứng minh

Theo định lý trên ta thấy, $C=C^{\perp}$ khi và chỉ khi $p^s-i=i, p^s-j=j$ nghĩa là $p^s=2i=2j$. Điều này là không thể vì p là số nguyên tố.

Định lý 3.1.6. Nếu $p^m \equiv 3 (\mathrm{mod}\, 7)$ hoặc $p^m \equiv 5 (\mathrm{mod}\, 7)$ thì có 4 mã cyclic LCD có độ dài $7p^s$ trên F_{p^m}.

Chứng minh

Xét

$C \cap C^{\perp} = \langle (x-1)^{\max\{i, p^s-i\}} (\phi_7(x))^{\max\{j, p^s-j\}} \rangle$

$C \cap C^{\perp} = 0$ nếu và chỉ nếu $p^s = \max\{i, p^s-i\} = \max\{j, p^s-j\}$, tương đương với $i, j \in \{0, p^s\}$.

3.2. Khoảng cách Hamming của mã cyclic có độ dài $7p^s$

Cho C là mã cyclic có độ dài $7p^s$ với đa thức sinh

$$\begin{aligned} g(x) &= (x-1)^i(x^6+x^5+x^4+x^3+x^2+x+1)^j \\ &= (x-1)^i(\phi_7(x))^j \end{aligned}$$

trong đó $0 \le i, j \le p^s$.

Đa thức sinh của mã $\overline{C}_z$ là

$$\overline{g}_z = \begin{cases} 1 & \text{nếu } i, j \le z \\ x-1 & \text{nếu } j \le z < i \\ \phi_7(x) & \text{nếu } i \le z < j \\ x^7-1 & \text{nếu } z < i, j. \end{cases}$$

Mệnh đề 3.2.1. Cho $i \le j$ và $C_t = \langle \overline{g}_z \rangle$ là mã cyclic có độ dài 7 trên F_{p^m}, trong đó $\overline{g}_z$ được định nghĩa như ở trên. Khi đó,

$$d_H(\overline{C}_z) = \begin{cases} 1 & \text{nếu } i, j \le z \\ 6 & \text{nếu } i \le z < j \\ \infty & \text{nếu } z < i, j \end{cases}.$$

Chứng minh

Ta sẽ chia ra thành 3 trường hợp.

Trường hợp 1: $i \le j \le z$. Trong trường hợp này $\overline{C}_z = \langle 1 \rangle$. Do đó, $d_H(\overline{C}_z) = 1$.

Trường hợp 2: $i \le z < j$. Trong trường hợp này $\overline{C}_z = \langle \phi_7(x) \rangle$. Mỗi phần tử của $\overline{C}_z$ có dạng $r.\phi_7(x)$, trong đó $r \in \mathrm{F}_{p^m}$. Và $wt_H(\phi_7(x)) = 6$, nên $d_H(\overline{C}_z) = 6$.

Trường hợp 3: $z < i, j$. Trong trường hợp này $\overline{C}_z = \langle x^7-1 \rangle$ nên $d_H(\overline{C}_z) = \infty$.

Bổ đề 3.2.2. [6] Cho C là một mã cyclic khác không và $C \ne \mathrm{F}_{p^m}[x]/\langle x^n-1 \rangle$. Khi đó $d_H(C) \ge 2$.

Mệnh đề 3.2.3. Cho $j \le i$ và $C_t = \langle \overline{g}_z \rangle$ là mã cyclic có độ dài 7 trên F_{p^m}, trong đó $\overline{g}_z$ được định nghĩa như ở trên. Khi đó,

$$d_H(\overline{C}_z) = \begin{cases} 1 \ \textit{nếu} \ j,i \le z \\ 2 \ \textit{nếu} \ j \le z < i \\ \infty \ \textit{nếu} \ z < j,i \end{cases}.$$

Chứng minh

Ta sẽ chia ra thành 3 trường hợp.

Trong đó có 2 trường hợp tương tự mệnh đề ở trên.

Trường hợp 3: $j \le z < i$. Trong trường hợp này $\overline{C}_z = \langle x-1 \rangle$. Vì $wt_H(x-1) = 2$ và theo bổ đề trên, suy ra $d_H(\overline{C}_z) = 2$.

Định lý 3.2.4. Gọi z là một số nguyên sao cho $0 \le z \le p^s - 1$. Chúng ta kí hiệu mã cyclic nghiệm đơn $\overline{C}_z = \langle \overline{g}_z(x) \rangle \in \mathrm{F}_q[x]/\langle (x^7-1) \rangle$ phụ thuộc vào C và z. Khi đó

$$d_H(\overline{C}_z) = \begin{cases} 1 \ \textit{nếu} \ g_z = 1 \\ 2 \ \textit{nếu} \ g_z = x-1 \\ 6 \ \textit{nếu} \ g_z = \phi_7(x) \\ \infty \ \textit{nếu} \ g_z = x^7 - 1 \end{cases}$$

Tất cả các mã cyclic có độ dài $7p^s$ đều có dạng $C = \langle (x-1)^i \phi_7(x)^j \rangle$ với $0 \le i, j \le p^s$, trong đó $p^m \equiv 3 (\mathrm{mod}\, 7)$ hoặc $p^m \equiv 5 (\mathrm{mod}\, 7)$. Nếu $i = 0$ và $j = 0$, khi đó $C = \mathrm{F}_q[x]/\langle x^7 - 1 \rangle$. Nếu $i = p^s$ và $j = p^s$, khi đó $C = \langle 0 \rangle$. Đây là những mã tầm thường của mã cyclic có độ dài $7p^s$ trên F_q. Tiếp theo ta sẽ xác định khoảng cách Hamming tối thiểu của tất cả các mã cyclic không tầm thường có độ dài $7p^s$ trên F_q.

Bổ đề 3.2.5. [6] Cho $C = \langle g(x) \rangle$ là mã cyclic nghiệm lặp có độ dài $7p^s$ trên F_q, trong đó p, s là số nguyên dương. Khi đó

$$d_H(C) = \min\{P_t d_H(C_t) : t \in T\}$$

$$T = \{t : 0 \le t \le p^s - 1\},$$

trong đó $t = \sum_{m=0}^{s-1} t_m p^m, 0 \le t_m \le p-1,$.

$$P_t = \prod_{m=0}^{s-1} (t_m + 1) = wt_H((x-1)^t)$$

Bổ đề 3.2.6. [6] Cho β, τ là số nguyên dương thỏa mãn $0 \le \beta \le p-2$ và $0 \le \tau \le s-1$, khi đó

$$\min\{P_t \mid t \ge l, t \in T\} = (\beta+1)p^\tau$$

trong đó l là một số nguyên dương sao cho $p^s - p^{s-\tau} + \beta p^{s-\tau-1} + 1 \le l \le p^s$.

Bổ đề 3.2.7. [6] Giả sử $0 \le \varphi \le p-2$ và $0 \le \theta \le s-1$. Cho

$p^s - p^{s-\theta} + \varphi p^{s-\theta-1} + 1 \le i,$
$i \le p^s - p^{s-\theta} + (\varphi+1)p^{s-\theta-1},$ khi đó $wt_H((x^7-1)^i) \ge (\varphi+2)p^\theta$ và dấu bằng xảy ra khi $i = p^s - p^{s-\theta} + (\varphi+1)p^{s-\theta-1}$. Hơn nữa, nếu $i \le j \le p^s - 1$, ta có $wt_H((x^7-1)^j) \ge (\varphi+2)p^\theta$.

3.2.1. Trường hợp 1: $0 \le j \le i \le p^s$

Bổ đề 3.2.1.1. Cho i, j là số nguyên dương sao cho $0 \le i \le p^s$ và $j = 0$. Khi đó $d_H(C) = 2$.

Chứng minh

Ở trường hợp này ta có $C = \langle (x-1) \rangle$ và $wt_H(x-1) = 2$ nên $d_H(C) = 2$.

Bổ đề 3.2.1.2. Cho i, j là hai số nguyên dương thỏa mãn

$p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le i,$
$i \le p^s - p^{s-\tau_0} + (\beta_0+1)p^{s-\tau_0-1}$ và

$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j,$
$j \le p^s - p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}$, trong đó

$0 \le \beta_0, \beta_1 \le p-2$ và $0 \le \tau_1 \le \tau_2 \le s-1$.
Nếu $C = \langle (x-1)^i (\phi_7(x))^j \rangle$, thì
$d_H(C) = \min\{(\beta_0+2)p^{\tau_0}, 2(\beta_1+2)p^{\tau_1}\}$.

Chứng minh

Nếu $j \le i \le t$

$\min\{P_t : t \in T, t \ge i \ge j\} = (\beta_0+2)p^{\tau_0}$

và $d_H(C_t) = 1$. Suy ra

$\min\{P_t d_H(C_t) : t \in T, t \ge i \ge j\} = (\beta_0+2)p^{\tau_0}.$
Nếu $j \le t < i$ thì

$\min\{P_t : t \in T, j \le t < i\} = (\beta_1+2)p^{\tau_1}$

và $d_H(C_t) = 2$. Suy ra

$\min\{P_t d_H(C_t) : t \in T, t \ge i \ge j\} = 2(\beta_1+2)p^{\tau_1}$

Bổ đề 3.2.1.3. Cho i, j là hai số nguyên dương thỏa mãn

$i = p^s$,
$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j$. Khi đó
$j \le p^s - p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}$

$d_H(C) = 2(\beta_1+2)p^{\tau_1}$.

Chứng minh

Tương tự trường hợp trên.

Định lý 3.2.1.4. Cho $0 \le \beta_0, \beta_1 \le p-2$ và $0 \le \tau_1 \le \tau_0 \le s-1$. Nếu $0 \le j \le i \le p^s$, thì $C = \left\langle (x-1)^i (\phi_7(x))^j \right\rangle$ là một $[7p^s, 7p^s - i - 6j]$-mã với khoảng cách Hamming cho ở Bảng 1.

3.2.2. Trường hợp 2: $0 \le i \le j \le p^s$

Mệnh đề 3.2.2.1. Cho i, j là hai số nguyên dương thỏa mãn $i = 0, 0 \le j \le p^s$, khi đó

$$d_H(\overline{C}_z) = \begin{cases} 2 \text{ nếu } i = 0, 0 < j \le p^s \\ 3 \text{ nếu } i = 0, p^{s-1} < j \le 2p^{s-1} \\ 4 \text{ nếu } i = 0, 2p^{s-1} < j \le 3p^{s-1} \\ 5 \text{ nếu } i = 0, 3p^{s-1} < j \le 4p^{s-1} \\ 6 \text{ nếu } i = 0, 4p^{s-1} < j \le 5p^{s-1} \\ 7 \text{ nếu } i = 0, 5p^{s-1} < j \le p^s. \end{cases}$$

Chứng minh

Ta có,

$d_H(C_t)$
$= \min\{wt_H((x^7-1)^t . d_H(C_t)) \mid (k-2)p^{s-1} < t < (k-1)p^{s-1}\}$
$= k$
với $k = 2, 3, 4, 5, 6$ và

$d_H(C_t) = \min\{wt_H((x^7-1)^t . d_H(C_t)) \mid 5p^{s-1} < t < p^s\} \ge 7.$

Mệnh đề 3.2.2.2. Cho i, j là hai số nguyên dương thỏa mãn
$p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le j$
$j \le p^s - p^{s-\tau_0} + (\beta_0+1)p^{s-\tau_0-1}$ và

$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le i$
$i \le p^s - p^{s-\tau_1} + (\beta_1+1)p^{s-\tau_1-1}$, trong đó

$0 \le \beta_0, \beta_1 \le p-2$ và $0 \le \tau_1 \le \tau_2 \le s-1$.
Nếu $C = \langle (x-1)^i (\phi_7(x))^j \rangle$, thì
$d_H(C) = \min\{(\beta_0+2)p^{\tau_0}, 6(\beta_1+2)p^{\tau_1}\}$.

Chứng minh

Nếu $i \le j \le t$ thì

$\min\{P_t : t \in T, t \ge j \ge i\} = (\beta_0+2)p^{\tau_0}$ và

$d_H(C_t) = 1$. Suy ra

$\min\{P_t d_H(C_t) : t \in T, t \ge i \ge j\} = (\beta_0+2)p^{\tau_0}$
Nếu $i \le t < j$ thì

$\min\{P_t : t \in T, i \le t < j\} = (\beta_1 + 2)p^{\tau_1}$ và

$d_H(C_t) = 6$. Suy ra

$\min\{P_t d_H(C_t) : t \in T, t \ge i \ge j\} = 6(\beta_1 + 2)p^{\tau_1}$.

Mệnh đề 3.2.2.3. Cho i, j là hai số nguyên dương thỏa mãn $j = p^s, p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le i$

$i \le p^s - p^{s-\tau_1} + (\beta_1 + 1)p^{s-\tau_1-1}$

Khi đó $d_H(C) = 6(\beta_1 + 2)p^{\tau_1}$.

Chứng minh

Tương tự trường hợp trên.

Định lý 3.2.2.4. Cho $0 \le \beta_0, \beta_1 \le p-2$ và $0 \le \tau_1 \le \tau_0 \le s-1$. Với $0 \le i \le j \le p^s$, thì $C = \left\langle (x-1)^i (\phi_7(x))^j \right\rangle$ là một $[7p^s, 7p^s - i - 6j]$-mã với khoảng cách Hamming cho ở Bảng 2.

4. KẾT LUẬN

Bài báo này đã đưa ra cấu trúc của mã cyclic có độ dài $7p^s$ trên trường hữu hạn F_{p^m} trong trường hợp $p^m \equiv 3 \pmod 7$ hoặc $p^m \equiv 5 \pmod 7$. Cấu trúc của mã đối ngẫu của mã cyclic trong trường hợp này, từ đó chỉ ra được không tồn tại mã tự đối ngẫu có độ dài $7p^s$ và có 4 mã cyclic LCD có độ dài $7p^s$ trên F_{p^m} ở mục 3.1.

Mục 3.2 của bài báo đưa ra các kết quả về khoảng cách Hamming của lớp mã cyclic trong trường hợp này.

i	j	$d_H(C)$
0	0	1
$0 \le i \le p^s$	$j = 0$	2
$p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le i \le p^s - p^{s-\tau_0} + (\beta_0 + 1)p^{s-\tau_0-1}$	$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j \le p^s - p^{s-\tau_1} + (\beta_1 + 1)p^{s-\tau_1-1}$	$\min\{(\beta_0 + 2)p^{\tau_0}, 2(\beta_1 + 2)p^{\tau_1}\}$
$i = p^s$	$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j \le p^s - p^{s-\tau_1} + (\beta_1 + 1)p^{s-\tau_1-1}$	$2(\beta_1 + 2)p^{\tau_1}$
$i = p^s$	$j = p^s$	0

Bảng 1. Khoảng cách Hamming trong trường hợp $0 \le j \le i \le p^s$

i	j	$d_H(C)$
0	0	1
1	$p^{s-1} < j \le 2p^{s-1}$	2
$i = 0$	$p^{s-1} < j \le 2p^{s-1}$	3
$i = 0$	$2p^{s-1} < j \le 3p^{s-1}$	4
$i = 0$	$3p^{s-1} < j \le 4p^{s-1}$	5
$i = 0$	$4p^{s-1} < j \le 5p^{s-1}$	6
$i = 0$	$5p^{s-1} < j \le p^s$	7
$p^s - p^{s-\tau_0} + \beta_0 p^{s-\tau_0-1} + 1 \le i$ $i \le p^s - p^{s-\tau_0} + (\beta_0 + 1)p^{s-\tau_0-1}$	$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le j$ $j \le p^s - p^{s-\tau_1} + (\beta_1 + 1)p^{s-\tau_1-1}$	$\min\{(\beta_0 + 2)p^{\tau_0}, 6(\beta_1 + 2)p^{\tau_1}\}$
$p^s - p^{s-\tau_1} + \beta_1 p^{s-\tau_1-1} + 1 \le i$ $i \le p^s - p^{s-\tau_1} + (\beta_1 + 1)p^{s-\tau_1-1}$	$j = p^s$	$6(\beta_1 + 2)p^{\tau_1}$
$i = p^s$	$i = p^s$	0

Bảng 2. Khoảng cách Hamming trong trường hợp $0 \le i \le j \le p^s$

TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1] Lê Thị Thanh Nhàn (2015), *Giáo trình lý thuyết đa thức*, NXB Đại học Quốc gia.

Tiếng Anh:

[2] Hai Q. Dinh, Xiaoqiang Wang, Paravee Maneejuk (2020), "On the Hamming Distance of Repeated-Root Cyclic Codes of Length $6p^s$," *IEEE Access*.

[3] Hai Q. Dinh (2000), "Repeated-root Cyclic and Negacyclic Codes of Length $6p^s$," *2000 Mathematics Subject Classification*. Primary 94B15; Secondary 12Y05.

[4] E. Prange (1957), "Cyclic error-correcting codes in two symbols," *Air Force Cambridge Research Center*.

[5] S. D. Berman (1967), "Semisimple cyclic and Abelian codes," *II Kibernetika,* vol. 3, no. 3, pp. 21–30.

[6] Hai Q.Dinh, X. Wang, J. Sirisrisakulchai (2020), "On the Hamming distance of constacyclic codes of length $5p^s$", *IEEE Access*.

Liên hệ:

Trần Thiên Ân

Sinh viên Khoa Toán, Trường Đại học Sư phạm, Đại học Đà Nẵng

Địa chỉ: 459 Tôn Đức Thắng, quận Liên Chiểu, TP. Đà Nẵng

Email: tranthienanmath@gmail.com

Ngày nhận bài: 3/4/2023

Ngày gửi phản biện: 6/4/2023

Ngày duyệt đăng: 01/8/2023