MỘT SỐ BỘ MÃ CYCLIC TỐT XÂY DỰNG TRÊN VÀNH ĐA THỨC

Nguyễn Trung Hiếu*, Nguyễn Bình
Khoa Kỹ thuật điện tử 1, Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: Mã cyclic là một lớp mã tuyến tính và có khả năng ứng dụng trong điện tử dân dụng, các hệ thống lưu trữ dữ liệu và các hệ thống truyền thông. Phương pháp xây dựng mã cyclic dựa trên các phân hoạch của vành đa thức (gồm nhóm nhân cyclic, cấp số nhân cyclic) có nhiều ưu điểm nổi bật, được quan tâm nghiên cứu và có những kết quả bước đầu. Bài báo này trình bày phương pháp tìm mã cyclic cục bộ tốt xây dựng từ nhóm nhân cyclic, cấp số nhân cyclic trên vành đa thức và đề xuất một số mã cyclic cụ thể. Đồng thời, bài báo cũng trình bày mô phỏng, đánh giá chất lượng của một số bộ mã tìm được và khả năng ứng dụng vào việc truyền thông tin.

Từ khóa: Mã cyclic, Nhóm nhân cyclic (CMG- Cyclic Multiplicative Group), Cấp số nhân cyclic (CGP- Cyclic Geometric Progressions), tổng kiểm tra (CS- Check-sum), vành đa thức.

I. MỞ ĐẦU

Nghiên cứu về lý thuyết mã hóa được chia thành ba hướng chính: mã nguồn, mã kênh (có khả năng phát hiện và sửa lỗi) và mật mã [1], [2]. Hầu hết các mã sửa lỗi được cấu trúc theo lý thuyết mã hóa thứ hai của Shannon [2], với các phương pháp xây dựng cấu trúc mã điển hình như phương pháp tổ hợp, hình học và cấu trúc đại số.

Mã cyclic là mã khối tuyến tính là một loại mã kênh được nghiên cứu trong một thời gian dài và ứng dụng trong nhiều lĩnh vực cuộc sống, đặc biệt trong lĩnh vực thông tin và truyền thông [3], [4]. Mã cyclic cục bộ (LCC- Local Cyclic Code) bắt đầu được nghiên cứu vào những năm 1980 [3]. Mã LCC có đầy đủ các ưu điểm của mã cyclic thông thường (xây dựng từ Ideal), ngoài ra nó còn có thêm các ưu điểm khác như: số lượng mã tạo được nhiều hơn trên cùng một vành đa thức, mức độ tính toán cũng dễ hơn so với bộ mã cyclic thông thường tương đương [5], [6].[1]

Theo phương pháp cấu trúc đại số, mã cyclic và mã cyclic cục bộ được xây dựng từ các nhóm nhân cyclic, cấp số nhân cyclic trên vành đa thức [3], [5]. Trong đó mã cyclic được xây dựng dựa trên nhóm nhân cyclic, mã LCC được xây dựng từ các lớp kề của phân hoạch vành đa thức (hay các cấp số nhân cyclic) [5].

Bài báo này đề xuất phương pháp xây dựng mã cyclic tốt từ nhóm nhân, cấp số nhân cyclic trên vành đa thức, từ đó liệt kê một số mã cyclic tốt và mô phỏng đánh giá hiệu quả của một số bộ mã thông qua một mô hình truyền thông cơ bản.

Nội dung bài báo được chia làm bốn phần. Phần 2, trình bày cơ sở lý thuyết về nhóm nhân và cấp số nhân cyclic, mã cyclic trên vành đa thức, một số tiêu chí đánh giá mã tốt. Trong phần 3, đề xuất phương pháp tìm kiếm mã cyclic và cyclic cục bộ tốt. Trong khi đó, phần 4 sẽ mô phỏng, đánh giá một số mã tốt tìm kiếm được. Cuối cùng, phần 5 là kết luận của bài báo.

II. CƠ SỞ LÝ THUYẾT

Phần này trình bày về nhóm nhân, cấp số nhân, mã cyclic, mã cyclic cục bộ, tiêu chí đánh giá mã tốt.

A. Nhóm nhân và cấp số nhân cyclic

Nhóm nhân cyclic A với phần tử sinh $a(x)$ trên vành đa thức $\mathbb{Z}_2[x]/(x^n+1)$ được thiết lập như sau [5]:

$$A=\left\{a^i(x)\bmod(x^n+1), i=\overline{1,k}\right\} \quad (1)$$

Trong đó, k là cấp của $a(x)$.

Cấp số nhân cyclic (CGP - Cyclic Geometic Progressions) trên vành đa thức là một tập hợp con có dạng sau [5]:

$$A_{(a,q)}=\left\{a(x),a(x)q(x),...,a(x)q^{m-1}(x)\right\} \quad (2)$$

Trong đó: m là số các số hạng khác nhau của CGP.

$a(x)$ là số hạng đầu của CGP.

$q(x)$ là công bội.

$$a(x)q^m(x)\equiv a(x)\bmod x^n+1$$

B. Mã cyclic và cyclic cục bộ trên vành đa thức

Mã cyclic (n,k) là Ideal $I=\langle g(x)\rangle$ của vành đa thức $\mathbb{Z}_2[x]/(x^n+1)$.

Mã cyclic cục bộ là một mã tuyến tính có các dấu mã là một tập con không trống tuỳ ý các lớp kề trong phân hoạch của vành đa thức theo một nhóm nhân cyclic A.

Nhận xét:

+ Nếu chỉ chọn 1 lớp kề, khi đó mã LCC trở thành mã cyclic.

Tác giả liên hệ: Nguyễn Trung Hiếu,
email: hieunt@ptit.edu.vn
Đến tòa soạn: 6/2017, chỉnh sửa: 8/2017, chấp nhận đăng: 9/2017

+ Nếu các lớp kề được chọn có chứa nhóm nhân cyclic đơn vị $I=\{x^i, i=1,2,3...\}$ thì ta có mã LCC hệ thống.

Tập các trưởng lớp kề tạo mã sẽ mô tả đầy đủ mã LCC.

C. Một số tiêu chí đánh giá mã tuyến tính tốt

Khả năng lựa chọn các mã tuyến tính (n,k,d_0) làm mã sửa lỗi là khá phong phú, để có thể thực hiện việc lựa chọn các bộ mã tốt thỏa mãn được định lý mã hóa thứ hai của Shanon, các nhà nghiên cứu về mã sửa lỗi đã xây dựng một bộ các tiêu chuẩn giới hạn để xác định và lựa chọn các bộ mã tốt, có thể đưa ra một số giới hạn cơ bản làm tiêu chí lựa chọn các bộ mã tốt sau [2], [3]:

Giới hạn Griesmer

Đối với mã tuyến tính nhị phân, giới hạn Griesmer được xây dựng theo công thức:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil \quad (3)$$

Trong đó n là độ dài của từ mã, k là số dấu thông tin trong từ mã và d là khoảng cực tiểu của từ mã.

Giới hạn Griesmer được sử dụng trong trường hợp cố định khoảng cách cực tiểu d, số dấu thông tin k, với yêu cầu tìm độ dài từ mã n là nhỏ nhất.

Giới hạn Plotkin

Giới hạn Plotkin được xây dựng theo công thức:

$$d \leq \frac{n.2^{k-1}}{2^k - 1} \quad (4)$$

Giới hạn Plotkin được xây dựng trong trường hợp cố định độ dài từ mã n và k dấu thông tin, yêu cầu xác định khoảng cách cực tiểu d.

Giới hạn Hamming

Giới hạn Hamming được xây dựng theo công thức:

$$2^{n-k} \geq \sum_{i=0}^{t} C_n^i \quad (5)$$

Giới hạn Hamming được xây dựng trong trường hợp cố định độ dài từ mã n và giá trị t sai có thể sửa được cho trước, xác định độ thừa của từ mã $r = n - k$ là nhỏ nhất.

III. PHƯƠNG PHÁP TÌM MÃ CYCLIC TỐT

A. Mã cyclic tối ưu xây dựng từ nhóm nhân, cấp số nhân cyclic

Định lý 3.1:

Mã cyclic $(2^k - 2, k)$ trên vành đa thức $Z_2[x]/(x^k + 1)$ sử dụng tất cả đa thức khác không (trừ đa thức $e_0(x) = \sum_{i=0}^{k-1} x^i$) làm dấu mã là mã tối ưu đạt giới hạn Griesmer và thỏa mãn giới hạn Plotkin, có khoảng cách mã $d_0 = 2^{k-1} - 1$.

Chứng minh:

Dựa vào tính chất của phân hoạch vành đa thức theo nhóm nhân cyclic đơn vị, ta có 2^{k-1} đa thức có trọng số lẻ và 2^{k-1} đa thức có trọng số chẵn. Khi thiết lập tổng kiểm tra trực giao ứng với một dấu mã bất kỳ, ta cần ít nhất 3 dấu mã [10]:

$$a_i(x) + a_j(x) = a_m(x) \quad (6)$$

Nếu cố định dấu $a_i(x)$ và cho $a_j(x)$ biến đổi thì phương trình (6) luôn tồn tại nghiệm với $\forall j \neq i$, có nghĩa là ứng với mỗi $a_j(x)$, ta xác định được $a_m(x)$. Vậy ta có tổng kiểm tra trực giao với dấu $a_i(x)$ như phương trình (7):

$$a_i(x) = a_j(x) + a_m(x) \quad (7)$$

Theo định lý, số dấu của từ mã là $n = 2^k - 2$ (loại bỏ đa thức $e_0(x) = \sum_{i=0}^{k-1} x^i$ lớp kề có một đa thức), để thiết lập số tổng kiểm tra trực giao giải mã cho một dấu mã nào đó sẽ đạt tối đa là:

$$J_{\max} = \left\lfloor \frac{n-1}{2} \right\rfloor = \left\lfloor \frac{2^k - 2 - 1}{2} \right\rfloor = 2^{k-1} - 2 \quad (8)$$

Theo phương pháp giải mã ngưỡng, khoảng cách mã d_0 được xác định:

$$d_0 = J_{\max} + 1 = 2^{k-1} - 1 \quad (9)$$

Kiểm tra theo giới hạn Griesmer: $n \geq \sum_{j=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil$ thay $d_0 = 2^{k-1} - 1$, ta được:

$$n \geq (2^{k-1} - 1) + 2^{k-2} + \cdots + 1$$

Áp dụng công thức tính tổng của cấp số nhân, có:

$$n \geq 2^k - 2$$

Theo định lý, số dấu của bộ mã là: $n = 2^k - 2$. Vậy bộ mã $(2^k - 2, k)$ đạt được giới hạn Griesmer.

Kiểm tra giới hạn Plotkin: $d_0 \leq n.\frac{2^{k-1}}{2^{k-1}}$

Thay $n = 2^k - 2$ vào vế phải, kết quả của vế phải:

$$(2^k - 2).\frac{2^{k-1}}{2^k - 1} = \frac{(2^k - 1).2^{k-1} - 2^{k-1}}{2^k - 1} = 2^{k-1} - \frac{1}{2 - \left(\frac{1}{2^{k-1}}\right)}$$

Với $d_0 = 2^{k-1} - 1$ nên bộ mã thỏa mãn giới hạn Plotkin.

Định lý 3.2:

Mã cyclic $(2^{k-1} - 1, k)$ trên vành đa thức $Z_2[x]/(x^k + 1)$ với k lẻ và sử dụng tất cả đa thức trọng số lẻ (trừ đa thức $e_0(x) = \sum_{i=0}^{k-1} x^i$) làm dấu mã là mã tối ưu đạt giới hạn Griesmer và thỏa mãn giới hạn Plotkin, có khoảng cách $d_0 = 2^{k-2} - 1$.

Chứng minh:

Phân hoạch của vành $Z_2[x]/(x^k + 1)$ theo nhóm nhân đơn vị $\{x^i\}$ cấp k luôn tồn tại 2^{k-1} đa thức có trọng số chẵn và 2^{k-1} đa thức có trọng số lẻ (theo tính chất của vành đa thức).

Trọng số của đa thức $e_0(x) = W\left(\sum_{i=0}^{k-1} x^i\right) = k$. Khi k lẻ, đa thức $e_0(x)$ có trọng số lẻ, thuộc lớp kề trọng số lẻ một phần tử và là một lũy đẳng. Khi k chẵn, đa thức $e_0(x)$ có trọng số chẵn không được chọn làm dấu mã và cũng không tồn tại lớp kề trọng số lẻ có một phần tử.

Nếu số dấu mã bớt đi một dấu là đa thức $e_0(x)$, thì số dấu mã của bộ mã là $n = 2^{k-1} - 1$.

Theo phương pháp giải mã ngưỡng để thiết lập được một tổng kiểm tra có khả năng trực giao cho hai dấu mã nào đó, ta cần ít nhất 4 dấu mã như trong phương trình (10) [11]:

$$a_i(x) + a_j(x) + a_s(x) = a_m(x) \qquad (10)$$

Theo phương trình (10), vế phải là một tổng 3 dấu mã của từ mã và mỗi dấu mã là một đa thức có trọng số lẻ, do đó kết quả vế phải là một đa thức có trọng số lẻ. Vậy phương trình (10) luôn còn nghiệm với $\forall i \neq j \neq s \neq m$. Nếu ta cố định một cặp hai dấu $a_i(x)$, $a_j(x)$, thì ứng với mỗi $a_s(x)$ ta luôn xác định được $a_m(x)$. Phương trình (10) có dạng:

$$[a_i(x) + a_j(x)] = a_s(x) + a_m(x) \qquad (11)$$

Số dấu còn lại của từ mã bằng $(n-2)$. Như vậy số tổng kiểm tra thiết lập được để giải mã là:

$$J_{\max} = \left\lfloor \frac{n-2}{2} \right\rfloor = \left\lfloor \frac{(2^{k-1}-1)-2}{2} \right\rfloor = 2^{k-2} - 2 \qquad (12)$$

Khoảng cách mã Hamming d_0 xác định là:

$$d_0 = J_{\max} + 1 = 2^{k-2} - 1 \qquad (13)$$

Kiểm tra theo giới hạn Griesmer: $n \geq \sum_{j=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil$ thay $d_0 = 2^{k-2} - 1$, ta được:

$$n \geq (2^{k-2} - 1) + 2^{k-3} + \cdots + 1 + 1$$

Áp dụng công thức tính tổng của cấp số nhân, có:

$$n \geq 2^{k-1} - 1$$

Theo định lý 3.2, số dấu của bộ mã: $n = 2^{k-1} - 1$. Vậy bộ mã $(2^{k-1} - 1, k)$ đạt được giới hạn Griesmer.

Kiểm tra giới hạn Plotkin: $d_0 \leq n.\frac{2^{k-1}}{2^k - 1}$

Thay $n = 2^{k-1} - 1$ vào vế phải, kết quả vế phải:

$$(2^{k-1} - 1).\frac{2^{k-1}}{2^k - 1} = \frac{(2^k - 1).2^{k-2} + 2^{k-2} - 2^{k-1}}{2^k - 1} = 2^{k-2} - \frac{1}{4 - \left(\frac{1}{2^{k-2}}\right)}$$

Với $d_0 = 2^{k-2} - 1$ nên bộ mã thỏa mãn giới hạn Plotkin.

Như vậy, theo định lý 3.1 và 3.2 thì các bộ mã cyclic được xây dựng từ nhóm nhân cyclic, cấp số nhân cyclic có dạng $(2^k - 2, k)$ và $(2^{k-1} - 1, k)$ là các bộ mã tối ưu đặt giới hạn Griesmer và Plotkin.

Đối với mã cyclic xây dựng từ các cấp số nhân cyclic, về cơ bản có thể xây dựng mã $(2^k - 2, k)$ bằng việc lấy tất cả các lớp kề của vành đa thức trừ phần tử 0 và phần tử $e_0(x) = \sum_{i=0}^{k-1} x^i$; có thể xây dựng mã $(2^{k-1} - 1, k)$ bằng việc lấy tất cả các lớp kề có trọng số lẻ của vành đa thức trừ phần tử $e_0(x) = \sum_{i=0}^{k-1} x^i$.

Đối với mã cyclic xây dựng từ các nhóm nhân cyclic thì có thể xây dựng các bộ mã này như sau:

+ Nếu cấp cực đại của các đa thức thuộc vành $Z_2/(x^k + 1)$ bằng $2^{k-1} - 1$ thì chọn đa thức có cấp cực đại làm phần tử sinh của bộ mã [7].

+ Nếu cấp cực đại của các đa thức thuộc vành $Z_2/(x^k + 1)$ không nhỏ hơn $2^{k-1} - 1$ thì chọn đa thức thuộc vành lớn hơn (vành $Z_2/(x^p + 1)$, với $p > k$) và có cấp bằng với $2^{k-1} - 1$ sau đó hạ bậc đa thức theo $h(x)$ [8] thì được đa thức mới có thể chọn làm phần tử sinh của bộ mã.

Việc thực hiện hạ bậc đa thức theo $h(x)$ còn được gọi là thực hiện phân hoạch hỗn hợp trên hai vành đa thức bất kỳ [8]. Xét 2 vành $x^p + 1$ và $x^k + 1$ với $p > k$ nếu trên vành $x^p + 1$ ta tìm được đa thức $h(x)$ thỏa mãn điều kiện: $h(x)$ là tích của một vài đa thức bất khả quy và $\deg h(x) = k$ thì ta có thể thực hiện được phân hoạch hỗn hợp trên hai vành này.

Để có thể dễ dàng tìm được đa thức $h(x)$ ta nên chọn ít nhất một vành là vành lẻ. Xét phân tích của một số vành đa thức sau:

$$x^3 + 1 = (1+x)(1+x+x^2)$$

$$x^5 + 1 = (1+x)(1+x+x^2+x^3+x^4)$$

$$x^7 + 1 = (1+x)(1+x^2+x^3)(1+x+x^3)$$

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

$$x^{11} + 1 = (1+x)\sum_{i=0}^{10} x^i$$

$$x^{13} + 1 = (1+x)\sum_{i=0}^{12} x^i$$

$$x^{15} + 1 = (1+x)(1+x+x^2)(1+x^3+x^4)(1+x+x^4)(1+x+x^2+x^3+x^4)$$

$$x^{17} + 1 = (1+x)(1+x^3+x^4+x^5+x^8)(1+x+x^2+x^4+x^6+x^7+x^8)$$

$$x^{19} + 1 = (1+x)\sum_{i=0}^{18} x^i$$

$$x^{21} + 1 = (1+x)(1+x+x^2)(1+x+x^3)(1+x^2+x^3)(1+x+x^2+x^4+x^6)(1+x^2+x^4+x^5+x^6)$$

$$x^{23} + 1 = (1+x)(1+x^2+x^4+x^5+x^6+x^{10}+x^{11})(1+x+x^5+x^6+x^7+x^9+x^{11})$$

$$x^{25} + 1 = (1+x)(1+x+x^2+x^3+x^4)(1+x^5+x^{10}+x^{15}+x^{20})$$

Theo các phân tích này ta có thể tìm được các giá trị k, p và đa thức $h(x)$ thỏa mãn điều kiện phân hoạch hỗn hợp như trong bảng I.

Bảng I. Một số cặp vành có thể phân hoạch hỗn hợp

k	p phù hợp	Các đa thức $h(x)$ thỏa mãn
3	6, 9, 15, 21	$h_1(x)=1+x^3$;
	7, 21	$h_2(x)=1+x^2+x^3$; $h_3(x)=1+x+x^3$
4	5, 15, 25	$h_1(x)=1+x+x^2+x^3+x^4$
	7	$h_2(x)=(1+x)(1+x^2+x^3)$; $h_3(x)=(1+x)(1+x+x^3)$
	15	$h_1(x)=1+x+x^2+x^3+x^4$ $h_4(x)=1+x^3+x^4$; $h_5(x)=1+x+x^4$
	21	$h_6(x)=1+x^2+x^4$; $h_7(x)=1+x+x^2+x^4$
5	15, 25	$h_1(x)=1+x^5$;
	15	$h_2(x)=(1+x)(1+x^3+x^4)$; $h_3(x)=(1+x)(1+x+x^4)$
6	7	$h_1(x)=(1+x^2+x^3)(1+x+x^3)$;
	9	$h_2(x)=(1+x^3+x^6)$
	15	$h_3(x)=(1+x+x^2)(1+x^3+x^4)$; $h_4(x)=(1+x+x^2)(1+x+x^4)$; $h_5(x)=(1+x+x^2)(1+x+x^2+x^3+x^4)$
	21	$h_6(x)=(1+x+x^3)(1+x^2+x^3)$; $h_7(x)=1+x+x^2+x^4+x^6$; $h_8(x)=1+x^2+x^4+x^5+x^6$
7	9	$h_1(x)=(1+x)(1+x^3+x^6)$
	15	$h_2(x)=(1+x)(1+x+x^2)(1+x^3+x^4)$ $h_3(x)=(1+x)(1+x+x^2)(1+x+x^4)$ $h_4(x)=(1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)$
	21	$h_5(x)=1+x^7$ $h_6(x)=(1+x)(1+x+x^2+x^4+x^6)$ $h_7(x)=(1+x)(1+x^2+x^4+x^5+x^6)$
8	9	$h_1(x)=(1+x+x^2)(1+x^3+x^6)$
	15	$h_2(x)=(1+x^3+x^4)(1+x+x^4)$ $h_3(x)=(1+x^3+x^4)(1+x+x^2+x^3+x^4)$ $h_4(x)=(1+x+x^4)(1+x+x^2+x^3+x^4)$
	17	$h_5(x)=(1+x^3+x^4+x^5+x^8)$ $h_6(x)=(1+x+x^2+x^4+x^6+x^7+x^8)$
	21	$h_7(x)=(1+x+x^2)(1+x+x^2+x^4+x^6)$ $h_8(x)=(1+x+x^2)(1+x^2+x^4+x^5+x^6)$
9	17	$h_1(x)=(1+x)(1+x^3+x^4+x^5+x^8)$ $h_2(x)=(1+x)(1+x+x^2+x^4+x^6+x^7+x^8)$
	21	$h_3(x)=(1+x)(1+x+x^2)(1+x+x^2+x^4+x^6)$ $h_4(x)=(1+x)(1+x+x^2)(1+x^2+x^4+x^5+x^6)$ $h_5(x)=(1+x+x^3)(1+x+x^2+x^4+x^6)$ $h_6(x)=(1+x+x^3)(1+x^2+x^4+x^5+x^6)$ $h_7(x)=(1+x^2+x^3)(1+x+x^2+x^4+x^6)$ $h_8(x)=(1+x^2+x^3)(1+x^2+x^4+x^5+x^6)$

Dựa trên kết quả hai định lý 3.1, 3.2 cùng với phân tích trong bảng I có thể nhận thấy rằng luôn có thể xây dựng được các bộ cyclic mã tối ưu trên các vành đa thức từ các cấp số nhân (hay lớp kề) cyclic.

Khi xây dựng mã cyclic từ các nhóm nhân với phần tử sinh là đa thức có cấp cực đại trên vành $Z_2/(x^k+1)$ và thỏa mãn cấp của đa thức là $2^{k-1}-1$ thì bộ mã cũng đạt giới hạn tối ưu.

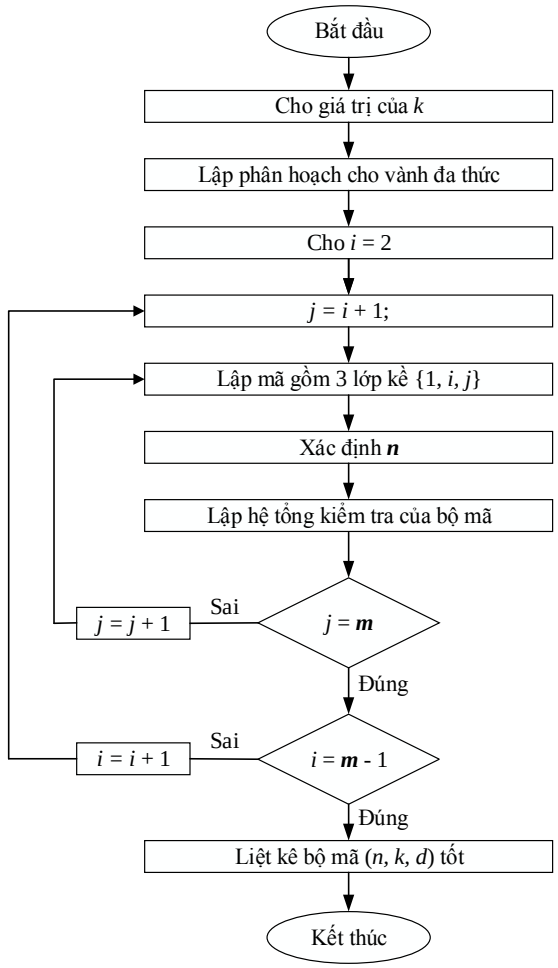
Trường hợp cấp cực đại của đa thức trên vành không đạt $2^{k-1}-1$ thì có thể hạ bậc của đa thức có cấp bằng $2^{k-1}-1$ và thuộc vành lớn hơn theo $h(x)$ như bảng I thì có thể tìm được bộ mã tối ưu.

Xét vành $Z_2/(x^9+1)$, cấp cực đại của các đa thức bằng 63 (theo phụ lục 1) nên không xây dựng được mã cyclic tối ưu từ các nhóm nhân cyclic với phần tử sinh là đa thức thuộc vành, tuy nhiên theo bảng I ta thấy rằng có thể hạ bậc đa thức có cấp bằng 255 trong vành $Z_2/(x^{17}+1)$ theo $h_1(x)$ hoặc $h_2(x)$ để xây dựng mã. Ví dụ chọn đa thức $a(x)=1+x+x^2+x^3+$

$x^8 + x^9 + x^{10} + x^{11} + x^{12}$ có cấp là 255 (theo phụ lục 1) là phần tử sinh của nhóm nhân cyclic xây dựng trên vành $Z_2/(x^{17}+1)$, chọn $h_1(x)$ để hạ bậc các phần tử trong nhóm nhân cyclic trên ta được một nhóm nhân có cấp là 255 trên vành vành $Z_2/(x^9+1)$, từ đây xây dựng được bộ mã cyclic $(255,9,127)$ là mã tối ưu đạt giới hạn Griesmer và Plotkin.

B. Mã cyclic tốt xây dựng từ cấp số nhân cyclic trên vành đa thức

Các mã cyclic tối ưu (n,k,d) được nghiên cứu và đề xuất ở trên có ưu điểm là sửa sai tốt (d lớn), xây dựng bộ mã dễ dàng, tuy nhiên tồn tại một nhược điểm lớn là hiệu suất mã (k/n) thường khá nhỏ, do đó tác giả cũng tiến hành nghiên cứu và đề xuất phương pháp tìm mã cyclic tốt xây dựng từ các cấp số nhân/ lớp kề cyclic với các giá trị (n,k,d) phù hợp, đặc biệt là đề xuất các mã tốt xây dựng từ 3 lớp kề cyclic trên vành (hướng tới mục tiêu đạt hiệu suất mã $\frac{k}{n} > \frac{1}{3}$ với khả năng sửa lỗi hợp lý).



Hình 1. Lưu đồ thuật toán tìm bộ mã cyclic tốt từ cấp số nhân cyclic

Để tìm mã cyclic tốt xây dựng trên 3 lớp kề cyclic sử dụng phương pháp giải mã ngưỡng [3], [9], [10], [11], ta thực hiện theo các bước sau đây:

Bước 1:

+ Cho giá trị k của vành đa thức $Z_2/(x^k+1)$.

+ Lập phân hoạch cho vành đa thức, xác định số lớp kề $\boldsymbol{m}$ **(số lượng lớp kề trong vành)**

+ Cho $i = 2$

Bước 2: + Gán $j = i + 1$

Bước 3:

+ Lập mã gồm 3 lớp kề $\{1, i, j\}$

+ Xác định giá trị n trong bộ mã (n,k,d), trong đó n là tổng số phần tử của 3 lớp kề được chọn (cũng là độ dài từ mã).

+ Tính tổng kiểm tra của bộ mã theo cả 3 trường hợp CS trực giao, CS có khả năng trực giao, CS λ liên hệ, sau đó lưu lại số CS của bộ mã ứng với mỗi trường hợp. Từ số CS sẽ tính được khoảng cách Hamming d.

+ Nếu $j = \boldsymbol{m}$ thì chuyển sang bước 4, nếu $j < \boldsymbol{m}$ thì tăng j và lặp lại bước 3.

Bước 4:

+ Nếu $i = \boldsymbol{m} - 1$ thì chuyển sang bước 5, nếu $i < \boldsymbol{m} - 1$ thì tăng i và lặp lại bước 2.

Bước 5: Tính toán bộ tham số (n,k,d) ứng với các bộ mã, so sánh với các giới hạn tối ưu. Liệt kê bộ mã (n,k,d) tốt nhất thu được.

Từ các bước trên có thể xây dựng được lưu đồ thuật tìm các bộ mã cyclic tốt theo lưu đồ thuật toán như trên hình 1 và danh sách một số bộ mã cyclic tốt tìm được như trong bảng II.

Thực hiện tìm mã cyclic tốt với nhiều lớp kề hơn cũng cho những bộ mã tốt, tuy nhiên lại phải trả giá về hiệu suất mã (tỉ số k/n thấp). Hướng nghiên cứu tiếp theo, tác giả sẽ tiếp tục tìm các bộ mã cyclic tốt với nhiều lớp kề hơn và các bộ mã cyclic ứng với các phương pháp giải mã khác.

Bảng II. Đề xuất một số bộ mã cyclic tốt

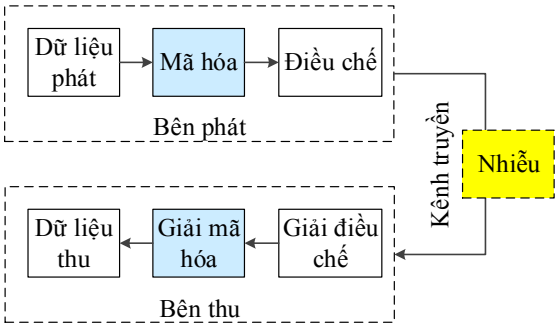
Vành	CGPs/CMG	TTG	CKNTG	TTGλLH
x^5+1	{(1), (7), (11)}		(15,5,7)	
x^6+1	{(1), (11), (21)}			(14,6,5) λ = 2, CS = 8
	{(1), (13), (21)}			(14,6,5) λ = 2, CS = 8
x^7+1	{(1), (23), (29)}	(21,7,7)		
x^8+1	{(1), (11), (87)}	(24,8,7)		
	{(1), (13), (87)}	(24,8,7)		
	{(1), (31), (91)}	(24,8,7)		
	{(1), (47), (61)}	(24,8,7)		
	{(1), (13), (19)}			(24,8,7) λ = 2, CS =

Vành	CGPs/CMG	TTG	CKNTG	TTGλLH
				12
	{(1), (13), (25)}			(24,8,7) λ = 2, CS = 12
	{(1), (37), (47)}			(24,8,7) λ = 2, CS = 12
	{(1), (37), (61)}			(24,8,7) λ = 2, CS = 12
$x^9 + 1$	{(1), (11), (61)}	(27,9,9)		
	{(1), (13), (47)}	(27,9,9)		
	{(1), (19), (59)}	(27,9,9)		
	{(1), (25), (55)}	(27,9,9)		
	{(1), (41), (87)}	(27,9,9)		
	{(1), (41), (117)}	(27,9,9)		

IV. MÔ PHỎNG ĐÁNH GIÁ MỘT SỐ BỘ MÃ

A. *Đề xuất kịch bản mô phỏng, đánh giá*

Sơ đồ tổng quát của một hệ thống truyền đề xuất để thực hiện mô phỏng, đánh giá mã cyclic như hình 2, trong đó sử dụng các phương pháp điều chế/giải điều chế khác nhau và kênh truyền sử dụng nhiễu Gause trắng cộng, các bộ mã cyclic cần mô phỏng, đánh giá được đưa vào các khối mã hóa và giải mã hóa.



Hình 2. Sơ đồ hệ thống thông tin sử dụng mô phỏng đánh giá mã cyclic

Phân tích sơ đồ hệ thống

Bên phát gồm:

- Dữ liệu phát: là phần thông tin gốc được truyền đi.

- Mã hóa: là bước sử dụng bộ mã cyclic để mã hóa tín hiệu gốc. Các bộ mã thay đổi sẽ ảnh hưởng đến dãy bit đưa tới khối điều chế.

- Điều chế: là các phương pháp điều chế, chương trình mô phỏng sẽ sử dụng các kiểu điều chế khác nhau để hỗ trợ đánh giá bộ mã.

Kênh truyền gồm:

- Nhiễu: được tạo ra trên kênh truyền, trong các mô phỏng ở phần này đều sử dụng bộ tạo nhiễu Gause.

Bên thu:

Là các bước ngược của bên phát, bao gồm: giải điều chế, giải mã hóa và khôi phục thông tin từ phía phát. Phần giải điều chế, giải mã hóa được thực hiện tương ứng với phương pháp điều chế và bộ mã hóa được xây dựng ở phía phát.

Hoạt động của hệ thống

Trong một chu kỳ mô phỏng cần thực hiện:

- Tạo nhiễu Gause trắng cộng.

- Cố định bộ mã cyclic, phương pháp điều chế.

- Tạo ngẫu nhiên dãy dữ liệu phát.

- Lần lượt tăng tỉ số E_b/N_0 ở phía phát theo bước nhảy phù hợp.

- Đo tỉ số lỗi bit BER của chuỗi bit nhận được.

Phương pháp đánh giá:

- Vẽ đồ thị biểu thị mối quan hệ E_b/N_0 và BER của bộ mã từ nguồn dữ liệu mô phỏng thu được.

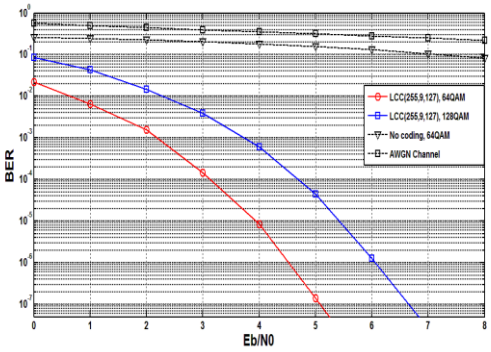
- Thực hiện đánh giá hiệu của của bộ mã, so sánh bộ mã với các bộ mã khác (nếu có).

B. *Kết quả mô phỏng, đánh giá một số bộ mã cyclic*

Trong phần này, tác giả thực hiện mô phỏng, đánh giá một số bộ mã cyclic tốt được liệt kê trong bảng II.

1) Bộ mã cyclic $(255, 9, 127)$

Chọn đa thức $a(x) = 1 + x + x^2 + x^3 + x^8 + x^9 + x^{10} + x^{11} + x^{12}$ có cấp là 255 [7] là phần tử sinh của CMG xây dựng trên vành $Z_2/(x^{17} + 1)$, chọn $h_1(x) = (1 + x)(1 + x^3 + x^4 + x^5 + x^8)$ để hạ bậc $a(x)$ ta xây dựng được CMG tương ứng có cấp 255 trên vành $Z_2/(x^9 + 1)$, tiến hành xây dựng bộ mã hóa và giải mã ứng với CMG này ta thu được bộ mã cyclic (255,9,127) đạt giới hạn Griesmer và Plotkin. Kết quả mô phỏng bộ mã cyclic (255,9,127) thể hiện như hình 3.



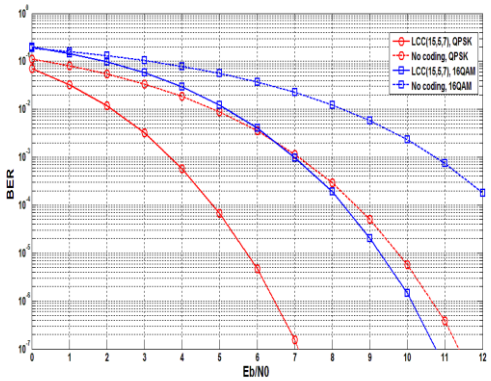
Hình 3. Kết quả mô phỏng bộ mã cyclic (255,9,127)

Trong mô phỏng ứng với bộ mã này, tác giả sử dụng nhiễu Gause trắng cộng trên kênh truyền. Thử nghiệm với các phương pháp điều chế khác nhau (QPSK, 16QAM,…), cho

chất lượng rất tốt. Trên hình 3 biểu thị kết quả mô phỏng của bộ mã ứng với điều chế 64QAM, 128QAM và so sánh với trường hợp truyền dẫn chỉ điều chế 64QAM không mã hóa và trường hợp truyền dẫn không điều chế, không mã hóa. Kết quả cho thấy bộ mã đạt $BER \approx 10^{-7}$ với $\frac{E_b}{N_0} = 5$ (trường hợp điều chế 64QAM), và $BER \approx 10^{-7}$ với $\frac{E_b}{N_0} = 6{,}5$ (trường hợp điều chế 128QAM).

2) Bộ mã cyclic $(15, 5, 7)$

Chọn mã cyclic cục bộ xây dựng từ ba lớp kề cyclic {(1), (7), (11)} trên vành $Z_2/(x^5 + 1)$ sẽ tạo ra bộ mã (15,5) (các phần tử của ma trận sinh của bộ mã này cũng tương đương CMG được tạo bởi phần tử sinh là đa thức trọng số lẻ đạt cấp cực đại trên vành $Z_2/(x^5 + 1)$), tiến hành xây dựng bộ mã hóa và giải mã ta thu được bộ mã cyclic (15,5,7) đạt giới hạn Griesmer và Plotkin. Kết quả mô phỏng bộ mã cyclic (15,5,7) thể hiện như hình 3 và hình 4.



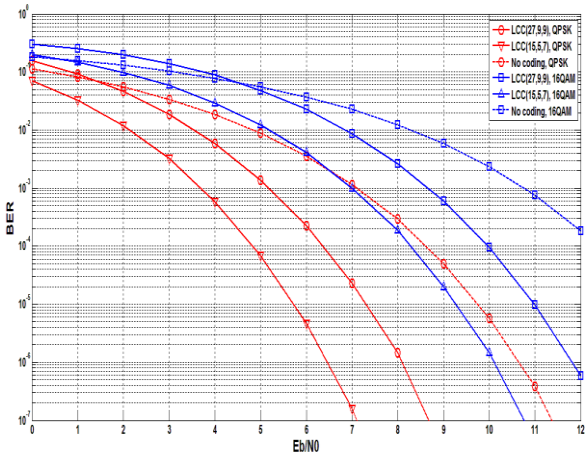
Hình 4. Kết quả mô phỏng bộ mã cyclic (15,5,7)

Tương tự như mô phỏng bộ mã *(255,9,127)*, ta sử dụng nhiễu Gause trắng cộng trên kênh truyền. Thử nghiệm với các phương pháp điều chế QPSK, 4QAM, 16QAM cho chất lượng khá tốt. Trên hình 4 biểu thị kết quả mô phỏng của bộ mã ứng với điều chế QPSK, 16QAM và so sánh với trường hợp truyền dẫn tín hiệu chỉ điều chế (QPSK, 16QAM) không mã hóa. Kết quả cho thấy với điều chế QPSK tại $\frac{E_b}{N_0} = 7$, nếu không mã hóa thì kênh truyền đạt $BER \approx 1{,}2.10^{-3}$, nếu sử dụng bộ mã cyclic (15,5,7) thì kênh truyền đạt $BER \approx 1{,}5.10^{-7}$ (tốt hơn trường hợp không mã hóa khoảng 8000 lần); với điều chế 16QAM tại $\frac{E_b}{N_0} = 10$, nếu không mã hóa thì kênh truyền đạt $BER \approx 2{,}5.10^{-3}$, sử dụng bộ mã cyclic (15,5,7) thì kênh truyền đạt $BER \approx 1{,}5.10^{-6}$ (tốt hơn trường hợp không mã hóa hơn 1600 lần). Kết quả mô phỏng cũng cho thấy đường truyền sử dụng cùng một bộ mã, thì điều chế QPSK cho BER tốt hơn 16QAM (ví dụ, tại $\frac{E_b}{N_0} = 7$, điều chế QPSK cho $BER \approx 1{,}5.10^{-7}$, trong khi điều chế 16QAM cho $BER \approx 10^{-3}$) là phù hợp với lý thuyết.

3) Bộ mã cyclic $(27, 9, 9)$

Chọn mã cyclic cục bộ xây dựng từ ba lớp kề cyclic {(1), (11), (61)} trên vành $Z_2/(x^9 + 1)$, tiến hành xây dựng bộ mã hóa và giải mã ta thu được bộ mã cyclic (27,9,9). Kết quả mô phỏng bộ mã cyclic (27,9,9) thể hiện như hình 5.

Tương tự, tác giả sử dụng nhiễu Gause trắng cộng trên kênh truyền. Thử nghiệm với các phương pháp điều chế QPSK, 4QAM, 16QAM cho chất lượng khá tốt. Trên hình 5 biểu thị kết quả mô phỏng của bộ mã ứng với điều chế QPSK, 16QAM, so sánh với trường hợp truyền dẫn sử dụng bộ mã cyclic (15,5,7) và trườn hợp truyền dẫn tín hiệu chỉ điều chế (QPSK, 16QAM) không mã hóa. Kết quả cho thấy với phương pháp điều chế QPSK tại $\frac{E_b}{N_0} = 7$, nếu không mã hóa thì kênh truyền đạt $BER \approx 1{,}2.10^{-3}$, nếu sử dụng bộ mã cyclic (27,9,9) thì kênh truyền đạt $BER \approx 2{,}4.10^{-5}$, sử dụng bộ mã cyclic (15,5,7) thì đạt $BER \approx 1{,}5.10^{-7}$; với phương pháp điều chế 16QAM tại $\frac{E_b}{N_0} = 10$, nếu không mã hóa thì kênh truyền đạt $BER \approx 2{,}5.10^{-3}$, sử dụng bộ mã cyclic (27,9,9) thì kênh truyền đạt $BER \approx 9.10^{-5}$, sử dụng bộ mã cyclic (15,5,7) thì đạt $BER \approx 1{,}5.10^{-6}$.



Hình 5. Kết quả mô phỏng bộ mã cyclic (27,9,9)

Kết quả mô phỏng trên hình 5 cho thấy dù sử dụng phương pháp điều chế nào thì bộ mã cyclic (15,5,7) đạt giới hạn tối ưu Griesmer và Plotkin (có khả năng sửa $t = 3$ bit lỗi, và $t/n = 3/15$) cho khả năng sửa lỗi tốt hơn (hay tỉ số BER thấp hơn) bộ mã cyclic (27,9,9) là mã cyclic tốt (có khả năng sửa $t = 4$ bit lỗi, và $t/n = 4/27$). Tác giả cũng đã mô phỏng đánh giá bộ mã với điều chế 64QAM, 128QAM thì cho tỉ lệ lỗi lớn và khả năng sửa lỗi không tốt như mã (255,9,127).

V. KẾT LUẬN

Mã cyclic có hạn chế lớn nhất là độ dự thừa từ mã khá lớn (hay hiệu suất mã hóa thông tin không cao), tuy nhiên ưu điểm nổi bật là dễ thực hiện về mặt kỹ thuật và số lượng mã nhiều. Các nghiên cứu trước đây thường tập trung vào việc kiến trúc mã chứ ít quan tâm đến việc tìm kiếm và đánh giá các bộ mã tốt về năng lực sửa lỗi. Bài báo này đã tập trung nghiên cứu để tìm kiếm các bộ mã cyclic tốt tiến tới các giới hạn tối ưu Griesmer và Plotkin. Nội dung bài báo đã trình bày phương pháp tìm mã cyclic tốt thông qua đề xuất và chứng minh hai định lý về mã cyclic tối ưu, xây dựng thuật toán tìm bộ mã cyclic tốt và bước đầu lập được bảng một số mã cyclic tốt,

thông qua kết quả mô phỏng, đánh giá hiệu năng của các bộ mã có thể nhận xét rằng kết quả nghiên cứu đã góp phần chỉ ra cách xác định các mã cyclic tốt có thể ứng dụng vào thực tế. Ngoài ra, các bộ mã cyclic xây dựng từ nhóm nhân cyclic, cấp số nhân cyclic như trình bày ở trên có khả năng thay đổi được độ dài từ mã tùy theo nhu cầu sử dụng là ưu điểm có thể ứng dụng trong mã mạng phục vụ các hệ thống truyền thông không dây hợp tác [12].

LỜI CẢM ƠN

Tác giả xin chân thành cám ơn Học viện Công nghệ Bưu chính Viễn thông đã tạo điều kiện giúp đỡ, hỗ trợ tôi thực hiện hướng nghiên cứu này.

TÀI LIỆU THAM KHẢO

[1] Menezes A. J, Van Oorchot P. C., Handbook of Applied Cryptography, CRC Press, (1998).

[2] Todd K. Moon, Error Correction Coding: Mathematical Methods and Algorithm. John Wiley & Sons, Inc, (2005).

[3] Nguyễn Bình, Giáo trình Lý thuyết thông tin, Nhà xuất bản Bưu điện, (2008).

[4] C. Ding, "Cyclic codes from the two-prime sequences", IEEE Transactions on Information Theory, ISSN 0018-9448, 58(6), 2012, pp. 357–363.

[5] Nguyễn Bình, Các mã xyclic và xyclic cục bộ trên vành đa thức, Tạp chí Khoa học và Công nghệ, ISSN 0866 708X, Tập 50, Số 6, 2012, trang 735-749.

[6] Nguyen Trung Hieu, Nguyen Van Trung, Nguyen Binh, A Classification of Linear Codes Based on Algebraic Structures and Local Cyclic Codes, Proceedings of The 2014 International Conference on Advanced Technologies for Communications, Hanoi, Vietnam, October 15 - 17, 2014, Pages 349-354.

[7] Nguyễn Trung Hiếu, Ngô Đức Thiện, Một phương pháp tìm kiếm các đa thức có cấp cực đại trên vành đa thức, Tạp chí Khoa học và Công nghệ các trường Đại học Kỹ thuật, ISSN 2354-1083, số 110, 2016, trang 75-80.

[8] Ngo Duc Thien, Nguyen Binh, Some Local Cyclic Codes Based on Compound Decomposition of Two Polynomial Rings, International Conference on Advanced Technologies for Communications (ATC 2008 - REV'11), Hanoi, Vietnam, October 2008.

[9] Nguyễn Bình, Nguyễn Xuân Quỳnh, Giải mã ngưỡng dựa trên hệ tổng kiểm tra λ liên kết chặt, Hội nghị tự động hóa toàn quốc lần 2 (VICA-2), 1996.

[10] Nguyễn Bình, Nguyễn Thế Truyện, Các mã xyclic cục bộ tự trực giao, Hội nghị Vô tuyến Điện tử toàn quốc lần thứ 6 (REV'96), 1996.

[11] Nguyễn Bình, Nguyễn Thế Truyện, Các mã xyclic cục bộ có khả năng trực giao, Hội nghị Vô tuyến Điện tử toàn quốc lần thứ 6 (REV'96), 1996.

[12] Suwen Wu; Jinkang Zhu; Ling Qiu; Ming Zhao, Network-coding-based coded cooperation, Journal of Communications and Networks, Vol 12 (4), 2010, pp. 366 - 374.

GOOD LOCAL CYCLIC CODERS ARE CONSTRUCTED ON POLYNOMIAL RING

Abstract: The cyclic code is a linear code layer and is applicable in civil electronics, data storage systems, and communication systems. Cyclic code generation based on polynomial ring decomposition (cyclic multiplicative groups, cyclic geometric progressions) has many outstanding advantages, is of interest for research and has initial results. This paper presents the method of code generation and proposes some good local cyclic code from cyclic multiplicative group, cyclic geometric progressions on polynomial ring. At the same time, the article also presents simulations, evaluates the quality of some of the code found and its applicability to the transmission of information.

Keywords: cyclic code, Cyclic Multiplicative Group (CMG), Cyclic Geometric Progressions (CGP), Check-sum (CS), polynomial ring.

Nguyễn Trung Hiếu, Nhận học vị Thạc sỹ năm 2010. Hiện nay đang công tác và làm nghiên cứu sinh tiến sĩ tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Lý thuyết thông tin, mã hóa, mật mã, hệ thống số, hệ thống nhúng.

Nguyễn Bình, Nhận học vị Tiến sỹ năm 1984. Hiện là Giáo sư tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Lý thuyết thông tin, mã hóa, mật mã.