PHƯƠNG PHÁP GIẢI PHƯƠNG TRÌNH TRONG TRƯỜNG HỮU HẠN NHỜ NGHIỆM CỦA ĐA THỨC AFFINE

A METHOD OF SOLVING EQUATIONS OVER THE FINITE FIELDS USING THE SOLUSIONS OF AFFINE POLYNOMIALS

Phạm Khắc Hoan[1,*], Nguyễn Tiến Thái[1], Nguyễn Trung Thành[1]

TÓM TẮT

Một số bài toán như giải mã mã BCH, Reed-Solomon, mã Goppa, giải mã hệ mật dựa trên mã hóa gắn liền với việc giải phương trình trong trường hữu hạn. Vấn đề tìm nghiệm của đa thức trong trường hữu hạn có độ phức tạp cao và không sử dụng được các phương pháp số tìm nghiệm của đa thức trong trường vô hạn. Đa thức affine có tính chất tuyến tính do đó có thể tìm nghiệm của nó một cách hiệu quả hơn. Bài báo đề xuất một phương pháp tìm nghiệm của đa thức trong trường Galois mở rộng thông qua các nghiệm của đa thức affine. Phương pháp đề xuất cho phép giảm được độ trễ xử lý đáng kể so với các phương pháp truyền thống, vì vậy có thể ứng dụng trong các hệ thống thông tin tốc độ cao.

Từ khóa: *Trường hữu hạn, trường Galois, mã hóa kiểm soát lỗi, cơ sở đa thức.*

ABSTRACT

Several problems such as decoding BCH, Reed-Solomon, Goppa codes and decrypt code-based cryptosystems relate to solving equations over finite fields. Finding of polynomials over finite fields is highly complicated because numerical methods to find roots of polynomials over infinite fields can not be used. On the other hand, affine polynomials are linear and finding their roots, therefore, is much easier than of the other polynomials. The paper proposes a novel method to find roots of polynomials over extended Galois fields using roots of affine polynomials. This method can reduce processing time significantly compared to traditional methods, and therefore, can be more suitable for high speed communication systems.

Keywords**:** *Finite field, Galois field, Error control coding, Polynomal basis.*

[1]Học viện Kỹ thuật quân sự
[*]Email: hoanpk2012@gmail.com
Ngày nhận bài: 15/4/2022
Ngày nhận bài sửa sau phản biện: 15/6/2022
Ngày chấp nhận đăng: 27/6/2022

1. GIỚI THIỆU

Trường hữu hạn được ứng dụng rộng rãi trong kỹ thuật điện tử và khoa học máy tính ví dụ như mã hóa chống nhiễu, mật mã học. Một số bài toán gắn liền với việc giải phương trình trong trường hữu hạn, ví dụ với mã hóa chống nhiễu cần phương trình khóa khi giải mã BCH, Reed-Solomon, mã Goppa, giải mã hệ mật dựa trên mã hóa. Berlekamp là một trong những tác giả có đóng góp đáng kể trong việc giải quyết vấn đề phân tích thừa số trong trường hữu hạn, từ đó có thể chuyển bài toán tìm nghiệm của đa thức bậc cao về tìm nghiệm của các đa thức có bậc thấp hơn [1, 2].

Một số phương pháp gián tiếp để giải phương trình bậc cao trên trường hữu hạn bao gồm: thực hiện các thuật toán lặp như thủ tục Chien, thuật toán Berlekamp, sử dụng biến đổi Fourier trên trường Galois…[3-7]. Tuy nhiên các phương pháp này thường gắn liền độ trễ tính toán khá lớn và có độ phức tạp cao, đặc biệt khi trường có kích thước lớn.

Đa thức tuyến tính hóa và đa thức affine có một số tính chất đặc biệt cho phép đơn giản hóa việc tìm nghiệm của chúng. Tuy nhiên chỉ có số ít đa thức có thể là đa thức tuyến tính hóa và đa thức affine. Trên cơ sở các phép biến đổi đại số và tìm đa thức affine là bội của một đa thức đã cho có thể tìm nghiệm của đa thức này trong số các nghiệm của đa thức affine.

Bài báo này nghiên cứu vấn đề tìm nghiệm của đa thức trong trường hữu hạn thông qua tìm nghiệm của đa thức affine là bội của đa thức đã cho đồng thời tạo cơ sở để xây dựng các thiết bị thực hiện nhiệm vụ này một cách hiệu quả. Các kết quả nhận được cho phép ứng dụng trong các trường hợp khác nhau, có thể mở rộng cho các trường kích thước tùy ý.

Phần còn lại của bài báo được tổ chức như sau. Mục 2 khái quát những vấn đề cơ bản về trường hữu hạn. Mục 3 nghiên cứu vấn đề tìm nghiệm của đa thức tuyến tính hóa, đa thức affine trong trường hữu hạn và giải phương trình trong trường hữu hạn thông qua tìm nghiệm của đa thức affine. Cuối cùng là một số kết luận.

2. MỘT SỐ VẤN ĐỀ CƠ BẢN VỀ TRƯỜNG HỮU HẠN

2.1. Khái niệm, tính chất của trường hữu hạn

Với số nguyên tố p đã cho, định nghĩa trường hữu hạn bậc p, ký hiệu GF(p) (còn được ký hiệu là F_p) là tập số nguyên Z_p của các số nguyên {0, 1,…, p-1} cùng với phép toán mod p. Với mọi n chia hết cho p, với mọi $\le a \in GF(p)$ ta có $na = 0$. Do đó, với mọi $a,b \in GF(p)$ ta có:

$$(a+b)^p = a^p + b^p \quad (1)$$

Các tính chất cơ bản của trường hữu hạn

- Trường hữu hạn F_q gồm $q = p^n$ phần tử bao gồm các nghiệm của phương trình

$$x^q - x = 0 \quad (2)$$

- Nhóm nhân của trường hữu hạn là nhóm cyclic, phần tử sinh của nhóm nhân gọi là phần tử nguyên thủy của trường. Tất cả các phần tử của trường bao gồm $\left\{0, \alpha, \alpha^2, ..., \alpha^{p^n-1}, \alpha^{p^n} = 1\right\}$.

- Phần tử nguyên thủy của trường hữu hạn F_q là nghiệm của đa thức bất khả quy bậc n trên vành $F_p[x]$.

- Ký hiệu F_q gồm $q = p^n$ phần tử. Với phần tử $c \in F_q$ vết của phần tử c được định nghĩa:

$$Tr(c) = c + c^p + c^{p^2} + ... + c^{p^{n-1}}. \quad (3)$$

Phương trình $x^2 + x + D = 0$ với $D \in GF(2^n)$ có nghiệm khi và chỉ khi $TR(D) = 0$.

2.2. Biểu diễn các phần tử của trường hữu hạn

Trường hữu hạn $GF(p^n)$ được sinh bởi một đa thức đa thức bất khả quy $\pi(x)$ bậc n. Đặc biệt khi sử dụng đa thức nguyên thủy $\pi(x)$ trường mở rộng $GF(p^n)$ từ trường GF(p) nhờ liên kết các nghiệm α của đa thức $\pi(x)$. Chú ý rằng mọi trường hữu hạn cùng bậc là đẳng cấu. Trong thực tế có hai dạng biểu diễn sử dụng cơ sở chính tắc (cơ sở đa thức) và cơ sở chuẩn hóa.

** Cơ sở đa thức*

Định nghĩa: Xét trường hữu hạn $GF(p^n)$ và cho $\alpha \in GF(p^n)$ là phần tử nguyên thủy của trường. Cơ sở đa thức của $GF(p^n)$ trên GF(p) là $\{1, \alpha, \alpha^2 ... \alpha^{n-1}\}$. Một phần tử bất kỳ của $GF(p^n)$ là tổ hợp tuyến tính của chúng với hệ số thuộc GF(p).

** Cơ sở chuẩn hóa*

Định nghĩa: Cho số nguyên dương n bất kỳ, trên $GF(p^n)$, luôn tồn tại một cơ sở chuẩn hóa (normal basic) cho trường hữu hạn $GF(p^n)$ trên GF(p). Nếu $\gamma \in GF(p^n)$ là phần tử sinh (phần tử chuẩn hóa) trên GF(p), thì cơ sở chuẩn hóa được biểu diễn là $\left\{\gamma, \gamma^{p^1}, \gamma^{p^2} \ldots \gamma^{p^{n-1}}\right\}$. Ví dụ $\{\alpha, \alpha^2\}$ là cơ sở chuẩn hóa của $GF(2^2)$ trên GF(2), $\left\{\alpha, \alpha^2, \alpha^4, \alpha^8\right\}$ là cơ sở chuẩn hóa của $GF(2^4)$ trên GF(2). Với trường $GF(2^4)$ được sinh bởi $\pi(x) = x^4 + x + 1$ có 2 cơ sở chuẩn hóa sinh bởi phần tử nguyên thủy $\gamma = \alpha^7$ và phần tử phi nguyên thủy $\gamma = \alpha^3$.

2.3. Các phép toán trong trường hữu hạn

Lựa chọn cơ sở cho việc cài đặt phần cứng:

Các phép toán số học thông thường trên $GF(2^n)$ được thực hiện theo modulo của đa thức bất khả quy $\pi(x)$ trên GF(2). Các phép cộng và trừ số học được thực hiện theo modulo 2. Phép cộng 2 đa thức khá đơn giản nhờ phép toán XOR của biểu diễn nhị phân, nhưng phép toán nhân trên trường $GF(2^n)$ có độ phức tạp cao và tốn nhiều thời gian. Độ phức tạp còn phụ thuộc vào việc lựa chọn đa thức bất khả quy và cơ sở được sử dụng để biểu diễn các phần tử hữu hạn.

Trong thực thi phần cứng khi lựa chọn cơ sở chuẩn hóa phép bình phương một phần tử đơn giản chỉ là phép dịch vòng. Do vậy, phép bình phương trong cơ sở chuẩn hóa rất dễ thực hiện nhưng phép nhân trong cơ sở chuẩn hóa lại khá phức tạp. Phép nhân hai phần tử của trường với cơ sở đa thức có thể thực hiện như phép nhân hai đa thức thông thường và kết quả nhận được lấy theo modul của đa thức sinh $\pi(x)$. Trong thực tế thường sử dụng các thiết bị nhân nhờ bảng logarit - antiloarit và hàm Zech. Trong quá trình tính toán nếu xen kẽ thực hiện phép cộng và phép nhân cần chuyển từ biểu diễn vector về biểu diễn số mũ và ngược lại nhờ logarit và antilogarit [4, 8].

3. ĐA THỨC TUYẾN TÍNH HÓA VÀ NGHIỆM CỦA ĐA THỨC TUYẾN TÍNH HÓA

Thủ tục Chien để tìm nghiệm đa thức, phương pháp giải tích tìm nghiệm của đa thức trong trường hữu hạn có độ phức tạp khá lớn khi kích thước của trường lớn, đặc biệt khi bậc phương trình cao. Tồn tại một lớp đa thức đặc biệt gọi là đa thức tuyến tính hóa, việc tìm nghiệm của nó trở nên đơn giản hơn. Trong mục này xem xét đa thức tuyến tính hóa, tìm đa thức tuyến tính hóa là bội nhỏ nhất của đa thức đã cho, việc tìm nghiệm của đa thức được thực hiện nhờ khảo sát các nghiệm của đa thức tuyến tính hóa.

3.1. Đa thức tuyến tính hóa

Đa thức L(z) trên trường $GF(p^n)$ được gọi là đa thức tuyến tính hóa nếu có dạng

$$L(z) = \sum_i L_i z^{p^i}. \quad (4)$$

Ví dụ đa thức $L(z) = z + z^2 + z^4$ là đa thức tuyến tính hóa với mọi n

Chú ý rằng tác giả trong [1] đã chứng minh rằng giả sử các nghiệm của L(z) thuộc trường mở rộng $GF(p^m)$, $m > n$ các nghiệm này tạo thành một không gian vector con trong $GF(p^m)$. Ngược lại, cho U là không gian vector con n chiều trên $GF(p^m)$ khi đó đa thức $L(z) = \prod_{\beta \in U} (z - \beta)$ là đa thức tuyến tính hóa trên $GF(p^m)$, nghĩa là

$$L(z) = \sum_i L_i z^{p^i} = L_0 z + L_1 z^p + ... + L_{n-1} z^{p^{n-1}} + z^{p^n}. \quad (5)$$

Các nghiệm của đa thức tuyến tính hóa L(z) tạo thành một không gian con M trên $GF(p^n)$. Nếu $\gamma \in M$ thì $\gamma^p \in M$ bởi vì $L^p(\gamma) = L(\gamma^p)$. Nếu $L_0 \neq 0$ thì L(z) không có nghiệm bội và sau đây ta chỉ xét trường hợp này.

3.2. Nghiệm của đa thức tuyến tính hóa

Cho L(z) là đa thức tuyến tính hóa trên GF(p^n), mô tả bởi biểu thức (4), giả sử γ là một nghiệm nguyên thủy của nó, L(z) là đa thức bậc p^n, các nghiệm của đa thức này có dạng:

$$\delta_0\gamma + \delta_1\gamma^p + ... + \delta_{n-1}\gamma^{p^{n-1}} \quad (6)$$

trong đó $\delta_i \in GF(p)$.

Dưới đây ta sẽ xem vấn đề tìm nghiệm của đa thức tuyến tính hóa.

Ký hiệu $\alpha^0, \alpha^1, ..., \alpha^{n-1}$ là cơ sở đa thức của trường GF(p^n), ta có các mệnh đề sau.

Mệnh đề 1 [2].

Cho L(z) là đa thức tuyến tính hóa trên GF(p^n), phần tử z được biểu diễn $z = \sum_k Z_k\alpha^k$, $Z_k \in GF(p)$ khi đó

$$L(z) = \sum_k Z_k L(\alpha^k). \quad (7)$$

Khi sử dụng biểu diễn đa thức của các phần tử $L(\alpha^i) = \sum_{j=0}^{m-1} C_{i,j}\alpha^j$. Do đó hệ số khai triển đa thức L(z) theo cơ sở đa thức được tính như sau:

$$[L_0, L_1, ..., L_{n-1}] = [Z_0, Z_1, ..., Z_{n-1}].C, \quad (8)$$

trong đó:

$$C = \begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,1} & . & . & . & C_{0,n-1} \\ C_{1,0} & C_{1,1} & C_{1,2} & . & . & . & C_{1,n-1} \\ . & . & . & . & . & . & . \\ C_{n-1,0} & C_{n-1,1} & C_{n-1,2} & . & . & . & C_{n-1,n-1} \end{bmatrix}. \quad (9)$$

Ví dụ 1. Xét đa thức $L(z) = z^4 + \alpha^7 z^2 + \alpha^{18} z$ trên trường GF(2^5) có đa thức sinh $x^5 + x^2 + 1$, ta có:

$L(1) = 1 + \alpha^7 + \alpha^{18} = \alpha + \alpha^2 + \alpha^4$;

$L(\alpha) = \alpha^4 + \alpha^9 + \alpha^{19} = \alpha^2 + \alpha^3$;

$L(\alpha^2) = \alpha^8 + \alpha^{11} + \alpha^{20} = \alpha + \alpha^2$; .

$L(\alpha^3) = \alpha^{12} + \alpha^{13} + \alpha^{21} = \alpha + \alpha^3$;

$L(\alpha^4) = \alpha^{16} + \alpha^{15} + \alpha^{22} = 1 + \alpha^4$;

vì vậy ma trận C có dạng:

$$C = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Giả sử cần tìm nghiệm của phương trình $z^4 + \alpha^7 z^2 + \alpha^{18} z + \alpha^{10}$, nghĩa là tìm nghiệm của $L(z) = \alpha^{10} = 1 + \alpha^4$. Sử dụng biểu thức (8) ta có:

$$[Z_0 \quad Z_1 \quad Z_2 \quad Z_3 \quad Z_4].\begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [1 \quad 0 \quad 0 \quad 0 \quad 1]$$

Giải hệ phương trình này tìm được hai nghiệm [0 0 0 0 1] và [0 1 1 1 1], nghĩa là phương trình đã cho có 2 nghiệm α^4 và α^{24} trên GF(2^5).

Đa thức trong ví dụ trên được gọi là đa thức affine. Đa thức A(z) trên GF(p^n) được gọi là đa thức affine nếu A(z) = L(z) - u trong đó L(z) là đa thức tuyến tính và $u \in GF(p^n)$. Nghiệm của đa thức affine có thể tìm được nhờ giải hệ phương trình tuyến tính như ví dụ 1.

Các tính chất cơ bản của đa thức tuyến tính, đa thức affine [2].

1. Đa thức L(z) là đa thức tuyến tính hóa khi và chỉ khi các nghiệm của nó tạo thành không gian tuyến tính trên GF(p), các nghiệm của chúng có cùng bội và là lũy thừa của p.

2. Đa thức A(z) là đa thức affine khi và chỉ khi các nghiệm của nó tạo thành không gian affine trên GF(p), các nghiệm của chúng có cùng bội và là lũy thừa của p.

3. Ước chung lớn nhất của 2 đa thức affine là một đa thức affine.

4. Ước chung lớn nhất của 2 đa thức tuyến tính hóa là một đa thức tuyến tính hóa.

Trường hợp đặc biệt với đa thức affine bậc 2 trên GF(2^n) có thể tính toán nghiệm của nó mà không cần giải hệ phương trình tuyến tính. Phương trình bậc 2 có thể đưa về dạng

$$y^2 + y = u \quad (10)$$

Phương trình (8) có nghiệm trên GF(2^n) khi và chỉ khi Tr(u) = 0 Giả sử y_i là một nghiệm của (10), khi đó y_i^2 là nghiệm của phương trình $y^2 + y = u^2$. Trên cơ sở đó có thể phân chia các giá trị u (với Tr(u) = 0) thành các lớp cyclotomic $\left\{u, u^2, u^4, ..., u^{2^{n-1}}\right\}$.

Ví dụ 2. Tìm nghiệm của phương trình trên trường GF(2^4) với đa thức sinh $x^4 + x + 1$

$$x^2 + 4x + 12 = 0 \quad (11)$$

Thay thế x = 4y phương trình (11) biến đổi về dạng chính tắc

$$y^2 + y + u = 0 \text{ với } u = 12/4^2 = 6 \quad (12)$$

trong trường này 3 lớp kề cyclomic với các trưởng lớp kề 1, 2, 6 có vết bằng 0. Tham số u = 1, 2, 6 có các cặp nghiệm tương ứng (6,11); (8, 10); (2,5), biểu diễn orbit cho trường GF(2^4) được mô tả ở bảng 1.

Bảng 1. Biểu diễn orbit các phần tử của trường GF(2^4) và các nghiệm

u		y_1	y_2
{1}	1	6	11
{2, 3, 5, 9}	2	8	10
	3	15	4
	5	14	7
	9	12	13
{6, 11}	6	2	5
	11	3	9

Chú ý rằng, khi u = 2 phương trình có nghiệm $y_1 = 8$, $y_2 = 10$ khi $u = 2^2$ các nghiệm $y_1 = 8^2 = 15$, $y_2 = 10^2 = 4$,….

Trong trường GF(2^n) có một nửa các phần tử có vết bằng 0 và một nửa còn lại có vết bằng 1. Nhờ phân chia trường thành các lớp kề cyclotomic có thể lưu trữ các nghiệm hiệu quả hơn. Khi sử dụng biểu diễn orbit theo các lớp kề cyclotomic số lượng phần tử cần xét giảm từ 2^n xuống còn khoảng n đại diện lớp kề, do vậy giảm dung lượng bộ nhớ cần lưu trữ khoảng $2^n/n$ lần. Bảng 2 trình bày biểu diễn orbit với tham số u theo đại diện lớp kề và các nghiệm tương ứng trên các trường GF(2^n) với các đa thức sinh $x^3 + x + 1$; $x^4 + x + 1$; $x^5 + x^2 + 1$; $x^6 + x + 1$; $x^7 + x + 1$. Bằng cách tương tự có thể xây dựng các orbit cho các trường kích thước lớn hơn và lưu trữ trong các bộ nhớ dùng để tính toán nghiệm của phương trình chính tắc bậc 2. Chú ý rằng trong bảng này các phần tử của trường được biểu diễn bởi số thứ tự thập phân N được gọi là logarit biến dạng:

$$N = \log_{\alpha}(\alpha^i) + 1 = i + 1 = \log(\alpha^i). \quad (13)$$

Bảng 2. Biểu diễn orbit theo tham số u trên trường GF(2^n) và các nghiệm

n	u	y′	y″	n	u	y′	y″	n	u	y′	y″
3	2	3	7		1	22	43		2	17	113
	1	6	11		2	18	48		4	26	106
4	2	8	10		4	15	53		6	7	127
	6	2	5	6	8	2	7		10	27	111
	2	4	30		10	23	57	7	12	45	95
5	8	3	6		14	31	47		16	37	107
	16	22	26		28	37	55		24	72	80
									30	43	115
									56	81	103

3.3. Đa thức affine là bội của một đa thức cho trước

Hầu hết các đa thức trên GF(p^n) không là đa thức affine. Ví dụ với p = 2, đa thức bậc 3 không là đa thức affine, tuy nhiên ta có thể tìm được một đa thức affine bậc 4 là bội của đa thức bậc 3. Nghiệm của đa thức bậc 3 có thể tìm được từ nghiệm của đa thức affine bậc 4. Tổng quát, cho đa thức monic bậc d $f(z) = f_0 + f_1 z + f_2 z^2 + \ldots + f_{d-1} z^{d-1} + z^d$ ta có thể sử dụng thuật toán sau để tìm bội affine L(z) - u của đa thức này.

Thuật toán 1.

1. Tính $z^k \bmod f(z)$ với $k = d, d+1, \ldots, (d-1)p$;

2. Dựa trên kết quả ở bước 1 tính các phần dư $r^{(0)}(z), r^{(1)}(z), \ldots, r^{(i)}(z)$, với $r^{(i)}(z) = z^{p^i} \bmod f(z)$;

3. Giải hệ phương trình tuyến tính

$$[u, L_0, L_1, \ldots, L_{d-1}] \begin{bmatrix} 0 & 0 & \ldots & 0 & -1 \\ r_{(d-1)}^{(0)} & \ldots & \ldots & r_1^{(0)} & r_0^{(0)} \\ r_{(d-1)}^{(1)} & \ldots & \ldots & r_1^{(1)} & r_0^{(1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ r_{(d-1)}^{(d-1)} & \ldots & \ldots & r_1^{(d-1)} & r_0^{(d-1)} \end{bmatrix} \quad (14)$$

Thuật toán giải phương trình bậc 3 (hệ số cao nhất bằng 1) trong trường nhị phân như sau.

Thuật toán 2.

1. Tính $z^k \bmod f(z)$ với k = 3, 4;

2. Tính các phần dư $r^{(0)}(z), r^{(1)}(z), \ldots, r^{(i)}(z)$, với $r^{(i)}(z) = z^{p^i} \bmod f(z)$;

3. Giải hệ phương trình

$$[u, L_0, L_1, L_2] \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ r_1^{(2)} & r_1^{(2)} & r_0^{(1)} \end{bmatrix} = 0.$$

4. Tìm nghiệm của đa thức affine $A(z) = u + L_0 z + L_1 z^2 + z^4 = 0$ sử dụng biểu thức (8).

5. Chọn nghiệm z_1, phân tích đa thức $f(z) = (x + z_1)\left[x^2 + (f_2 - z_1)x + f_0 / z_1\right]$.

6. Tìm nghiệm của phương trình $x^2 + (f_2 - z_1)x + f_0 / z_1 = 0$ nhờ phương pháp biểu diễn orbit theo các lớp kề.

Ví dụ 3.

Cho đa thức $f(z) = z^3 + \alpha^{13} z^2 + z + \alpha^3$, với $\alpha^4 + \alpha + 1 = 0$. Tìm đa thức affine là bội của f(z). Ta tính:

$z^3 \bmod f(z) = \alpha^{13} z^2 + z + \alpha^3$;

$z^4 \bmod f(z) = \alpha^{13} z^3 + z^2 + \alpha^3 z =$

$= \alpha^{26} z^2 + \alpha^{13} z + \alpha^{16} + z^2 + \alpha^3 z =$

$= (\alpha^{11} + 1) z^2 + (\alpha^{13} + \alpha^3) z + \alpha =$

$= \alpha^{12} z^2 + \alpha^8 z + \alpha.$

Tính $r^{(i)}(z) = z^{2^i} \bmod f(z)$;

$r^{(0)}(z) = z^1 \bmod f(z) = z$;

$r^{(1)}(z) = z^2 \bmod f(z) = z^2$;

$r^{(2)}(z) = z^4 \bmod f(z) = \alpha^{12} z^2 + \alpha^8 z + \alpha.$

Ta có hệ phương trình:

$$[u, L_0, L_1, L_2]\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ \alpha^{12} & \alpha^8 & \alpha \end{bmatrix} = 0.$$

Giả sử chọn nghiệm $u = \alpha^2, L_0 = \alpha^8, L_1 = \alpha^{12}, L_2 = 1$ và $L(z) = \alpha^8 z + \alpha^{12} z^2 + z^4$.

Để tìm nghiệm của đa thức tuyến tính này ta tính các giá trị:

$L(1) = \alpha^8 + \alpha^{12} + 1 = 1 + \alpha + \alpha^3$;

$L(\alpha) = \alpha^9 + \alpha^{14} + \alpha^4 = 0$;

$L(\alpha^2) = \alpha^{10} + \alpha^{16} + \alpha^8 = 0$;

$L(\alpha^3) = \alpha^{11} + \alpha^{18} + \alpha^{12} = 1 + \alpha^3$.

Từ đó ta có thể tìm nghiệm của phương trình L(z) = α nhờ giải hệ phương trình

$$[Z_0, Z_1, Z_2, Z_3]\begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = [0100].$$

Hệ phương trình trên có nghiệm $Z = [1011] = \alpha^{13}$; $Z = [1111] = \alpha^{12}$. Đây là 2 nghiệm trên GF(2^4) trong đó α^{12} là nghiệm của f(z). Ta có thể phân tích ra thừa số:

$$f(z) = z^3 + \alpha^{13} z^2 + z + \alpha^3 = (z + \alpha^{12})(z^2 + \alpha z + \alpha^6).$$

Tiến hành tìm nghiệm của đa thức $z^2 + \alpha z + \alpha^6$ theo phương pháp nói trên ta tìm được hai nghiệm α^7, α^{14}.

Tổng quát hơn đa thức bậc 3 dạng $f(z) = z^3 + az^2 + bz + c$ có thể tìm được đa thức bội affine dạng:

$$A(z) = (z^3 + az^2 + bz + c)(z + a)$$
$$= z^4 + (a^2 + b)z^2 + (ab + c)z + ac.$$

3.4. Giải phương trình bậc 4

Trong trường GF(2^n) thực hiện phương pháp kết hợp biến đổi đại số và đa thức affine để tìm nghiệm hiệu quả hơn như sau.

Xét phương trình bậc 4 trên trường GF(2^n)

$$x^4 + Ax^3 + Bx^2 + Cx + D = 0. \quad (15)$$

Nhờ phép thế $x = y^{-1} + \sqrt{C/A}$, $A \neq 0$, có thể đưa về phương trình

$$a_3 y^4 + a_2 y^2 + a_1 y + a_0 = 0, \quad (16)$$

trong đó

$$a_3 = D + BC/A + (C/A)^2; \; a_2 = B + \sqrt{AC}, a_1 = A, a_0 = 1. \quad (17)$$

Khi a_3, $a_2 \neq 0$ thay thế $y = z\sqrt{a_2/a_3}$ ta nhận được phương trình

$$z^4 + z^2 + E_1 z + E_2 = 0, \quad (18)$$

trong đó $E_1 = a_1\sqrt{a_3/a_2^3}$; $E_2 = a_3/a_2^2$.

Trong trường hợp này vế trái của (18) là một đa thức affine và có thể tìm nghiệm của nó dựa trên phương pháp giải hệ phương trình tuyến tính như đã trình bày trong mục 3.2. Sau khi tìm được nghiệm sử dụng các phép thế ngược để tìm nghiệm của phương trình ban đầu.

Trong [7] Chien đề xuất phương pháp kết hợp giải phương trình bậc 2, 3, 4 nhờ biến đổi đại số phương trình bậc 4 về dạng phương trình chính tắc bậc 3 và sử dụng phương pháp bảng tra để tìm nghiệm của phương trình bậc 2, bậc 3 chính tắc. Với phương pháp này để giải phương trình bậc 2, bậc 3 chính tắc Chien xây dựng bảng phân tích thừa số của các hàm vết Tr(x) với tham số n ≤ 6. Với n lớn việc phân tích thừa số khá phức tạp. So sánh với phương pháp đề xuất trong bài báo sử dụng đa thức affine, phương trình bậc 3 dễ dàng biến đổi về phương trình bậc 4 có dạng affine, phương trình bậc 2 chính tắc có dạng đa thức affine và việc tìm nghiệm theo bảng tra của các lớp kề cyclotomic đã giảm dung lượng lưu trữ $2^n/n$ lần.

Chú ý rằng với phương pháp đề xuất, bước có độ phức tạp cao nhất là tính toán các giá trị $L(\alpha^i)$, để tính $(\alpha^i)^{2^d}$ cần 2^d phép nhân các phần tử giống nhau trong trường hữu hạn, có độ phức tạp $O(n2^d)$. Giả sử sử sụng cơ sở đa thức, so sánh với phương pháp truyền thống sử dụng thủ tục tìm kiếm Chien bằng cách thử tất cả các phần tử của trường cần sử dụng $2^n d^2$ phép nhân với độ phức tạp $O(2^n d^2)$. Vì vậy phương pháp đề xuất cho phép giảm độ phức tạp thực thi đáng kể khi d < n và đặc biệt khi trường có kích thước lớn do độ phức tạp thực thi và lưu trữ đều giảm từ hàm mũ 2^n trở thành hàm tuyến tính theo n Do đó phương pháp đã đề xuất có độ trễ xử lý thấp và rất phù hợp với trường hợp d < n. Tuy nhiên nếu d ≥ n đa thức affine nhận được có bậc khá cao và việc phân tích đa thức thành nhân tử trở nên phức tạp.

4. KẾT LUẬN

Bài báo đề xuất giải pháp tìm nghiệm của phương trình chính tắc bậc 2 sử dụng biểu diễn orbit theo các lớp kề cyclotomic cho phép giảm dung lượng lưu trữ khoảng $2^n/n$ lần. Đồng thời bài báo đề xuất phương pháp giải phương trình bậc 3, bậc 4 trong trường hữu hạn nhờ biến đổi về bài toán tìm nghiệm của đa thức affine bậc 4. Với cơ sở đa thức phương pháp giải phương trình nhờ tìm nghiệm của đa thức affine độ phức tạp thực khi từ $O(2^n d^2)$ xuống $O(n2^d)$ khi so sánh với sử dụng thủ tục tìm kiếm Chien. Vì vậy phương pháp đề xuất cho phép giảm độ phức tạp đáng kể khi giải phương trình bậc không quá lớn (d ≤ 4), từ đó cho phép nâng cao tốc độ xử lý trong các mạch giải mã mã BCH, mã Reed-Solomon.

TÀI LIỆU THAM KHẢO

[1]. Elwyn R. Berlekamp, 2015. *Algebraic Coding Theory* (Revised Edition). World Scientific Publishing Co. Pte. Ltd.

[2]. F. J. MacWilliams, N. J. A.Sloane, 1977. *The theory of error correction codes*. Elselvier.

[3]. R. P. Chen, 1982, *Formulas for solutions of quadratic equations over GF(2^m)*. IEEE Transactions on information theory, Vol. IT-28, N 5, pp 792-794.

[4]. Mutter, V.M., 1990. *Fundamentals of noise-immune television transmission of information*. L .: Energoatomizdat, Leningrad branch

[5]. K. Huber, et al, 1992. *Solving Equations in Finite Fields and Some Results Concerning the Structure of* GF(p^m). EEE Trans. on Information Theory 38(3):1154-1162.

[6]. Fedorenko S. V., Trifonov P. V., 2002. *Finding roots of polynomials over finite fields*. IEEE Transactions on Communications, 2002, Vol. 50, Issue 11, pp. 1709–1711.

[7]. R. T. Chien, B. D. Cunningham, I. B. Oldham, 1969. *Hybrid method for finding roots of a polynomial with application to BCH decoding.* IEEE Transactions on information theory, March, 1969, pp. 328-335.

[8]. C. C. Chen, C. Y. Lee, E. H. Lu, 2008. *Scalable and systolic montgomery multipliers over GF(2^m)*. IEICE Transaction Fundamentals, Vol. E91, No.7, pp. 1763-1771.

AUTHORS INFORMATION

Pham Khac Hoan, Nguyen Tien Thai, Nguyen Trung Thanh

Military Technical Academy