PHƯƠNG PHÁP BIẾN ĐỔI ĐẠI SỐ GIẢI PHƯƠNG TRÌNH BẬC CAO TRONG TRƯỜNG GALOA MỞ RỘNG

Phạm Khắc Hoan[1*], Trần Thái Hà[1], Vũ Sơn Hà[2]

[1]*Khoa Vô tuyến điện tử, Đại học Kỹ thuật Lê Quý Đôn*

[2]*Viện Khoa học và Công nghệ quân sự*

Tóm tắt

Bài báo đề xuất phương pháp trực tiếp giải phương trình bậc 3, bậc 4 trong trường hữu hạn dựa trên biến đổi đại số phương trình đã cho về phương trình chính tắc bậc 2. Kết quả nhận được có thể tổng quát hóa để giải phương trình trong trường hữu hạn kích thước bất kỳ đồng thời cho phép giảm độ phức tạp và độ trễ xử lý đáng kể so với các phương pháp truyền thống, nhờ đó có thể ứng dụng trong các hệ thống thông tin tốc độ cao.

Từ khóa: *Trường Galoa; phép nhân trường hữu hạn; mã hóa sửa lỗi; cơ sở đa thức; cơ sở chuẩn hóa.*

1. Đặt vấn đề

Trường hữu hạn được ứng dụng rộng rãi trong kỹ thuật và khoa học máy tính như mã hóa chống nhiễu, mật mã học [1]. Một số trường hợp yêu cầu giải phương trình trong trường hữu hạn, ví dụ cần giải phương trình khóa khi giải mã mã BCH, Reed-Solomon, Goppa hoặc khi giải mã hệ mật dựa trên mã hóa như hệ mật Mc-Eliece. Berlekamp là một trong những tác giả có đóng góp đáng kể trong việc nghiên cứu vấn đề phân tích thừa số trong trường hữu hạn, trên cơ sở đó có thể tìm nghiệm của đa thức bậc cao thông qua các nhân tử của nó [2].

Giải phương trình bậc cao trong trường hữu hạn là một bài toán cổ điển luôn nhận được sự quan tâm của cộng đồng nghiên cứu và cho đến nay vẫn còn khá nhiều thách thức. Một số phương pháp gián tiếp để giải phương trình trong trường hữu hạn bao gồm: thực hiện các thuật toán lặp như thủ tục Chien, thực hiện thông qua biến đổi Fourier trên trường Galoa… [2, 3]. Tuy nhiên, các phương pháp này thường có độ trễ tính toán khá lớn do tính chất lặp của chúng. Thủ tục Chien thực chất cần phải lần lượt kiểm tra tất cả các phần tử của trường vì vậy có độ trễ xử lý lớn khi đa thức có bậc cao và trường có kích thước lớn.

Các phương pháp trực tiếp giải phương trình bậc cao trong trường hữu hạn đã được nghiên cứu từ khá sớm nhưng đều có độ phức tạp cao khi trường có kích thước lớn. Trong [4] Berlekamp trình bày một phương pháp tìm nghiệm cho phương trình bậc 2 dựa trên không gian con tuyến tính của GF(2^n) và tính chất của hàm vết, chỉ ra điều

[*] Email: hoanpk@lqdtu.edu.vn

https://doi.org/10.56651/lqdtu.jst.v17.n04.405

kiện để phương trình bậc 3 có 3 nghiệm phân biệt trong GF(2^n), tuy nhiên chưa xây dựng được công thức tìm nghiệm. Chen là tác giả đầu tiên xây dựng các công thức tính nghiệm cho phương trình bậc 2, tuy nhiên các công thức nhận được khá phức tạp, đặc biệt khi *n* lớn [5]. Các tác giả trong [6] đi sâu nghiên cứu cấu trúc của trường hữu hạn dựa trên việc phân chia thành các lớp kề cyclotomic và sử dụng thuật toán lặp để tìm ước chung lớn nhất của các đa thức. Tuy nhiên, thuật toán trên có cấu trúc lặp có độ phức tạp cao và có độ trễ lớn. Yiu trình bày một phương pháp lai cải tiến dựa vào việc tính toán trước nghiệm của phương trình bậc 2, bậc 3 chính tắc với các tham số cho trước và lưu trữ trong bảng tra [7], tuy nhiên kích thước bảng tra còn khá lớn khi *n* lớn. Gần đây Trifonov và cộng sự đề xuất phương pháp tìm nghiệm của đa thức trên trường hữu hạn dựa vào việc biến đổi về đa thức affine và tìm nghiệm của đa thức affine [8]. Tuy nhiên, phương pháp này phù hợp với tính toán trên phần mềm và bậc của đa thức affine khá lớn nên có nhiều khó khăn khi thực hiện trên phần cứng.

Trong một số trường hợp như cần giải mã sửa lỗi cho các bộ nhớ dung lượng lớn, sửa lỗi trong thông tin quang, hệ thống thông tin độ trễ cực thấp với đặc điểm số lỗi không quá lớn (không quá 4), việc giải mã cần giải phương trình bậc không lớn trên trường hữu hạn có kích thước lớn đặt ra yêu cầu cao về thông lượng và độ trễ xử lý [9-11]. Trên cơ sở kế thừa các kết quả nghiên cứu có liên quan, bài báo này đi sâu nghiên cứu phương pháp trực tiếp giải phương trình bậc cao trong trường hữu hạn dựa trên biến đổi đại số phương trình bậc cao về phương trình chính tắc bậc 2 và nhờ các phép thế ngược cho phép tìm nghiệm của phương trình bậc 3, bậc 4 ban đầu. Đồng thời trên cơ sở phân chia trường hữu hạn thành các lớp cyclotomic, bài báo đề xuất cải tiến để tìm nghiệm của phương trình bậc 2 chính tắc cho phép rút gọn không gian lưu trữ đáng kể. Phương pháp được đề xuất có tính hệ thống và tạo tiền đề cho việc thực thi thiết bị giải quyết nhiệm vụ này một cách hiệu quả. Các kết quả nhận được có thể mở rộng cho các trường với kích thước bất kỳ và cả trường phi nhị phân.

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 phân tích các trường hợp giải phương trình có bậc khác nhau. 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 là GF(*p*) (hoặc F_p) là tập Z_p của các số nguyên $\{0,1,...,p-1\}$ cùng với phép toán mod *p*.

Các tính chất cơ bản của trường hữu hạn:

- Trường hữu hạn F_q gồm $q = p^n$ phần tử (ký hiệu là GF(p^n)) bao gồm và chỉ gồm các nghiệm của phương trình:

$$x^q - x = 0 \quad (1)$$

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

- Với phần tử $c \in \text{GF}(p^n)$ vết của phần tử c được định nghĩa:

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

Tính chất:

+ $Tr(c) \in F_p$;

+ $Tr(c_1 + c_2) = Tr(c_1) + Tr(c_2)$;

+ $Tr(c^p) = Tr^p(c) = Tr(c)$;

+ Nếu $c \in F_p$ thì $Tr(c) = nc$;

+ $Tr(1) = n \bmod p$ với $p = 2$, $Tr(1) = 1$ khi n lẻ và $Tr(1) = 0$ khi n chẵn [12, 13].

2.2. Biểu diễn các phần tử của trường hữu hạn

Trường hữu hạn GF(p^n) được sinh bởi một đa thức bất khả quy $\pi(x)$ bậc n. Chú ý rằng mọi trường hữu hạn cùng bậc là đẳng cấu và trong thực tế sử dụng hai dạng biểu diễn thông dụng là cơ sở đa thức và cơ sở chuẩn hóa.

* *Cơ sở đa thức*

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

Mọi phần tử khác 0 của trường GF(p^n) tạo thành một nhóm nhân cyclic. Nhóm nhân đó có thể biểu diễn bởi số thứ tự thập phân N được gọi là logarit biến dạng [12]:

$$N = \log_\alpha(\alpha^i) + 1 = i + 1 = \log(\alpha^i) \quad (3)$$

* *Cơ sở chuẩn hóa*

Định nghĩa: Cho số nguyên dương n bất kỳ, 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 trên GF(p), cơ sở chuẩn hóa có dạng $\left\{\gamma, \gamma^{p^1}, \gamma^{p^2}, ..., \gamma^{p^{n-1}}\right\}$. Ví dụ với trường GF($2^4$) với

đa thức sinh $\pi(x) = x^4 + x + 1$ 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 nhị phân

Các phép toán số học trên GF(2^n) thường 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, trong khi đó phép toán nhân trên trường GF(2^n) có độ phức tạp cao và tốn nhiều thời gian. Độ phức tạp thực thi còn phụ thuộc vào việc lựa chọn đa thức bất khả quy và cơ sở để biểu diễn các phần tử trong trường hữu hạn. Với cơ sở chuẩn hóa phép bình phương một phần tử là phép dịch vòng, nhưng phép nhân khá phức tạp. Phép nhân hai phần tử của trường với biểu diễn đa thức có thể thực hiện như phép nhân hai đa thức và kết quả nhận được lấy theo modulo của đa thức sinh $\pi(x)$. Trong thực tế, thường sử dụng các thiết bị nhân nhờ bảng logarit - antilogarit và hàm Zech. Phép nhân các phần tử biểu diễn lũy thừa thực hiện như phép nhân, phép chia lũy thừa với số mũ được lấy theo modulo $(2^n - 1)$. Trong quá trình tính toán nếu xen kẽ thực hiện phép cộng và phép nhân cần chuyển từ biểu diễn vectơ về biểu diễn lũy thừa và ngược lại nhờ bảng logarit và antilogarit. Để đánh giá chi tiết độ phức tạp thực thi các bài toán trên trường hữu hạn cần tính đến các vấn đề biểu diễn và thực thi các phép toán trường hữu hạn [14, 15].

3. Giải phương trình bậc cao trong trường GF(2^n)

3.1. Phương trình bậc 2

Mục này trình bày các kết quả đã biết về tìm nghiệm của phương trình bậc 2 trong trường hữu hạn là tiền đề để giải các phương trình bậc cao hơn trong các mục sau. Ngoài ra, mục này còn xem xét vấn đề phân lớp trường hữu hạn thành các lớp kề cyclotomic để đơn giản hóa việc tính nghiệm của phương trình bậc 2.

Cho phương trình bậc 2 trên trường hữu hạn:

$$a_2 x^2 + a_1 x + a_0 = 0, \quad a_2 \neq 0 \tag{4}$$

Không mất tính tổng quát, phương trình (4) có thể đưa về dạng:

$$x^2 + Ax + B = 0 \tag{5}$$

trong đó, $A = a_1 / a_2$, $B = a_0 / a_2$.

Nếu $AB = 0$ dễ dàng tìm được nghiệm của phương trình (5). Khi $AB \neq 0$, nhờ thay thế $x = Ay$ có thể đưa về dạng phương trình chính tắc:

$$y^2 + y + D = 0 \tag{6}$$

trong đó: $D = B / A^2 = (a_0 / a_2) / a_1^2$.

Phương trình (6) có thể xem xét trên trường tùy ý, ở đây xét trong trường GF(2^n).

Mệnh đề 1 [4, 12, 13]. Phương trình (6) trên trường GF(2^n) có hai nghiệm $y', y'' \in \mathrm{GF}(2^n)$ khi và chỉ khi $Tr(D) = 0.$

Trong [5] Chen xây dựng công thức tính nghiệm áp dụng với cơ sở đa thức, tuy nhiên khi n lớn việc tính nghiệm có độ phức tạp cao. Dưới đây khảo sát với trường hợp biểu diễn trường với cơ sở chuẩn hóa. Trong các ứng dụng thực tế có thể xây dựng các mạch điện để thực thi chuyển đổi cơ sở cho phù hợp với ứng dụng cụ thể.

Trong trường GF(2^n) tồn tại cơ sở chuẩn hóa $\{\gamma, \gamma^2, \gamma^4, ..., \gamma^{\vartheta}\}$, trong đó $\vartheta = 2^{n-1}$ với phần tử sinh γ. Phần tử trong trường GF(2^n) có thể biểu diễn ở dạng cơ sở chuẩn hóa:

$$D = d_0\gamma + d_1\gamma^2 + ... + d_{\vartheta}\gamma^{\vartheta} \tag{7}$$

Vết của nó có dạng:

$$Tr(D) = d_0 + d_1 + ... + d_{\vartheta} \tag{8}$$

Nhận xét rằng với phương trình (6) tổng hai nghiệm của phương trình bằng 1, vì vậy chỉ cần tìm một nghiệm y', nghiệm thứ hai được tính theo công thức $y'' = y' + 1 = L(y').$

Khi $Tr(D) = 0,$ các nghiệm y', y'' của phương trình (6) được tính theo công thức [12]:

$$y' = \sum_{i=0}^{n-1} y_i \gamma^{2^i}, \; y'' = \sum_{i=0}^{n-1} \overline{y}_i \gamma^{2^i} \tag{9}$$

trong đó: $\overline{y}_i = 1 + y_i, \;\; y_i \in \{0,1\}.$

Các hệ số y_i được xác định theo biểu thức:

$$y_0 = 0; \;\; y_1 = d_1; \;\; y_2 = d_1 + d_2; ...; \;\; y_{n-1} = \sum_{i=1}^{n-1} d_i \tag{10}$$

Ví dụ 1. Tìm nghiệm của phương trình trên trường GF(2^4) với đa thức sinh $x^4 + x + 1,$ trong đó các hệ số được biểu diễn theo logarit biến dạng như biểu thức (3):

$$x^2 + 4x + 12 = 0 \tag{11}$$

Thay thế $x = 4y$ phương trình (11) biến đổi về dạng chính tắc (6) với $D = 12/4^2 = 6.$ Biểu diễn $D = 6$ với cơ sở chuẩn hóa $\{\gamma, \gamma^2, \gamma^4, \gamma^8\}$, trong đó $\gamma = \alpha^7$ nhận được $D = (0101)_{\gamma}.$ Vì $Tr(D) = d_3 + d_2 + d_1 + d_0 = 0,$ phương trình (11) có 2 nghiệm được xác định theo công thức (9) và (10):

$$y' = (y_4, y_3, y_2, y_1) = (1100)_{\gamma} = 5;$$

$$y'' = (\overline{y}_4, \overline{y}_3, \overline{y}_2, \overline{y}_1) = (0011)_{\gamma} = 2.$$

Trong [7] Yiu đề xuất xây dựng bảng tra tính toán một nghiệm của phương trình chính tắc (6) cho mỗi trường hữu hạn với tham số D thay đổi (tính toán trước nghiệm này theo công thức được Chen đề xuất trong [5] với các tham số D có vết bằng 0). Dung lượng bộ nhớ như vậy với mỗi trường đã cho là $2^n.n$.

Trên cơ sở phân chia trường hữu hạn thành các lớp kề cyclotomic dưới đây đề xuất một giải pháp hiệu quả hơn là xây dựng bảng tra kết hợp với biểu diễn orbit các phần tử của trường.

Ký hiệu y' là một nghiệm của (6), nâng lên bình phương đẳng thức $y'^2 + y' + D = 0$ ta có:

$$y'^4 + y'^2 + D^2 = 0 \tag{12}$$

Như vậy, y'^2 là nghiệm của phương trình chính tắc (6) với tham số là D^2.

Xét trường GF(2^4) trong ví dụ 1, trong trường này 3 lớp kề cyclomic với các đại diện lớp kề 1, 2, 6 có vết bằng 0. Tham số $D = 1,2,6$ có các cặp nghiệm tương ứng (6,11); (8, 10); (2,5). Do đó, 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*

D		y'	y''
$\{1\}$	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 $D = 2$ phương trình có nghiệm $y' = 8,\ y'' = 10$, khi $D = 2^2$ các nghiệm $y' = 8^2 = 15,\ y'' = 10^2 = 4,...$ Như vậy, ta chỉ cần tính toán cặp nghiệm với 3 giá trị đại diện của các lớp kề $D = 1,2,6$. Các nghiệm với các tham số D khác trong một lớp kề cyclotomic được xác định thông qua các lũy thừa 2, 4, 8… của nghiệm tương ứng với đại diện của lớp kề tương ứng.

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, so sánh với phương pháp lưu trữ trong [7] dung lượng bộ nhớ giảm từ $2^n.n$ xuống còn khoảng n^2, nghĩa là dung

lượng bộ nhớ cần lưu trữ giảm $2^n / n$ lần. Bảng 2 trình bày biểu diễn orbit với tham số D 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.

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

n	*D*	*y′*	*y″*	*n*	*D*	*y′*	*y″*	*n*	*D*	*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

Như vậy, phương pháp tìm nghiệm của phương trình bậc 2 gồm các bước sau:

Bước 1: Biến đổi phương trình về dạng chính tắc (6).

Bước 2: Biểu diễn tham số D theo cơ sở chuẩn hóa và tìm nghiệm của phương trình chính tắc theo công thức (9), (10).

Bước 3: Với tham số D có vết bằng 0, xây dựng lớp kề cyclotomic của nó: $D, D^2, D^4, ..., D^{2^{n-1}}$.

Bước 4: Xây dựng bảng tra nghiệm của phương trình chính tắc với đại diện của các lớp kề.

3.2. Phương trình bậc 3

Trong mục này đề xuất phương pháp biến đổi đại số để biến đổi phương trình bậc 3 về phương trình chính tắc bậc 2 và sử dụng các kết quả nói trên để tìm nghiệm của

phương trình bậc 2 và biến đổi ngược để tìm nghiệm của phương trình bậc 3.

Xét phương trình trong trường GF(2^n)

$$x^3 + Ax^2 + Bx + C = 0 \tag{13}$$

Nếu $B + A^2 = 0$ dễ dàng biến đổi để tìm được 3 nghiệm giống nhau $x = A + \sqrt[3]{C + A^3}$. Nếu $B + A^2 \neq 0$ nhờ thay biến

$$x = y\sqrt{B + A^2} + A \tag{14}$$

có thể biến đổi phương trình (13) về dạng chính tắc

$$y^3 + y + E = 0 \tag{15}$$

trong đó,

$$E = (C + AB) / \sqrt{(B + A^2)^3} = (C + AB) / \left[(B + A^2)\sqrt{(B + A^2)} \right] \tag{16}$$

Nếu $E = 0$ phương trình (15) chỉ có nghiệm bằng 0 và 2 nghiệm $\sqrt{1}$. Vì hệ số của y^2 bằng 0 nên tổng các nghiệm (nếu có) bằng 0, vì vậy phương trình (15) hoặc có 3 nghiệm, hoặc có 1 nghiệm hoặc vô nghiệm.

Mệnh đề 2 [4, 12]. Phương trình (15) có nghiệm duy nhất trên GF(2^n) khi và chỉ khi

$$Tr(1/E) \neq Tr(1) \tag{17}$$

Từ đó suy ra quan hệ dưới đây là điều kiện cần (không phải là điều kiện đủ) để phương trình (15) có 3 nghiệm

$$Tr(1/E) = Tr(1) \tag{18}$$

Tiếp theo, ta biến đổi phương trình bậc 3 chính tắc (15) về phương trình bậc 2 và chỉ xét trường hợp có 3 nghiệm phân biệt. Ta đưa vào biến mới $y = z + 1/z$, phương trình (15) chuyển về dạng:

$$z^6 + Ez^3 + 1 = 0 \tag{19}$$

Ký hiệu $z^3 = u$, $u = \sqrt[3]{z}$ ta nhận được phương trình:

$$u^2 + Eu + 1 = 0 \tag{20}$$

Thay thế $u = Ev$, ta nhận được phương trình bậc 2 chính tắc:

$$v^2 + v + D = 0, \; D = 1/E^2 \tag{21}$$

Chú ý rằng trên GF(2^n) ta có: $Tr(1/E^2) = \left[Tr(1/E^2) \right]^2 = Tr(1/E)$.

Xét 2 trường hợp như sau: Nếu *n* lẻ, $Tr(1) = 1$, do đó điều kiện (18) mâu thuẫn với điều kiện có nghiệm của phương trình (21) nên phương trình (21) không có nghiệm trên

GF(2^n) (có nghiệm trên trường mở rộng). Trường hợp n chẵn có thể tìm nghiệm của phương trình (15) thông qua nghiệm của phương trình (21). Phương pháp giải phương trình bậc 3 gồm các bước sau:

Bước 1: Biến đổi phương trình (13) về dạng chính tắc (15) sử dụng phép thế (14).

Bước 2: Sử dụng phép thế $y = z + 1/z,$ biến đổi phương trình (15) về phương trình (19).

Bước 3: Sử dụng phép thế $z^3 = u$ biến đổi phương trình (19) về dạng (20).

Bước 4: Sử dụng phép thế $u = Ev,$ biến đổi phương trình (20) về dạng phương trình chính tắc (21).

Bước 5: Tìm nghiệm của phương trình chính tắc (21) theo biểu diễn orbit, sử dụng các phép thế ngược để tìm nghiệm của phương trình ban đầu.

Ví dụ 2. Giải phương trình sau trên trường GF(2^4) với đa thức sinh $\pi(x) = x^4 + x + 1$:

$$x^3 + 7x^2 + 10x + 10 = 0 \tag{22}$$

Thế $x = y\sqrt{B + A^2} + A = 5y + 7,$ ta nhận được phương trình chính tắc (15) với $E = 11.$ Bởi vì $Tr(1) = 0 = Tr(1/E) = Tr(6),$ điều kiện (18) được đảm bảo, phương trình (15) có 3 nghiệm. Tiếp tục thay thế $y = \sqrt[3]{u} + 1/\sqrt[3]{u} = \sqrt[3]{Ev} + 1/\sqrt[3]{Ev},$ ta nhận được phương trình (21) với $D = (1/E)^2 = 6^2 = 11.$ Theo bảng 1 xét lớp cyclotomic tương ứng phương trình này có một nghiệm $v = 3.$ Từ đó ta có:

$u = Ev = 13;\ \ z = \sqrt[3]{u} \in \{5, 10, 15\};$

$y = z + 1/z \in \{14, 6, 8\};\ \sqrt{B + A^2} = 5;$

$x' = y\sqrt{B + A^2} \in \{3, 10, 12\};\ \ x = x + A \in \{4, 6, 2\}.$

Sau đây ta đánh giá về độ phức tạp khi giải phương trình bậc 3 theo phương pháp đề xuất. Để tính giá trị của E theo (16) cần sử dụng 1 phép bình phương, 2 phép nhân, 2 phép cộng, một phép căn bậc 2, một phép nghịch đảo. Sau khi xác định được nghiệm của (21) cần tính $z = \sqrt[3]{u} = \sqrt[3]{Ev}$ cần 1 phép nhân và một phép tính căn bậc 3. Ví dụ với n chẵn, $n = 2m$ mọi phần tử khác 0 của trường đều là thặng dư bậc 3 và có thể tính gián tiếp căn bậc 3 thông qua phần tử nguyên thủy của trường, căn bậc 3 có dạng: $z = \sqrt[3]{u} = \alpha^i,$ với giá trị i nào đó $1 \le i \le k,\ \ k = \dfrac{2^{2m} - 1}{3},$ hai giá trị khác là α^{i+k} và $\alpha^{i+2k}.$ Để tính $y = z + 1/z$ cần 1 phép cộng, 1 phép nghịch đảo và để tìm được nghiệm theo (14) cần 1 phép nhân, 1 phép cộng. Như vậy, tổng cộng các phép biến đổi trung

gian cần 4 phép cộng, 1 phép bình phương, 3 phép nhân, 2 phép nghịch đảo, 1 phép tính căn bậc 2 và một phép tính căn bậc 3 trong trường hữu hạn. Độ phức tạp của từng phép toán này phụ thuộc vào phương pháp thực thi và cơ sở được biểu diễn, nhưng có thể ước lượng phép cộng và phép bình phương, phép tính căn bậc 2 có độ phức tạp $O(n)$, độ phức tạp của phép nhân và phép tính căn bậc 3 có dạng $O(n^2)$, phép nghịch đảo có độ phức tạp $O(n^3)$. Với phương pháp truyền thống độ phức tạp thực thi của thủ tục Chien tìm nghiệm đa thức bậc t trong $GF(2^n)$ có dạng $O(2^n t^2)$. Độ phức tạp về thời gian của thủ tục Chien là [8]:

$$T_{ch} = (\tau_{add} + \tau_{mul})t(2^n - 1) \tag{23}$$

Độ phức tạp thời gian thực hiện phương pháp đề xuất:

$$T = (4\tau_{add} + 3\tau_{mul} + \tau_{sq} + 2\tau_{inv} + \tau_{sqr} + \tau_{cubr}) \tag{24}$$

Trong các biểu thức trên τ_{add}, τ_{mul}, τ_{sq}, τ_{inv}, τ_{sqr}, τ_{cubr} tương ứng là độ trễ của các phép toán cộng, nhân, bình phương, nghịch đảo, căn bậc 2, căn bậc 3. Độ trễ của các phép toán cơ bản phụ thuộc vào phương pháp thực thi, tuy nhiên chỉ phụ thuộc tuyến tính theo *n*. Như vậy, độ phức tạp thực thi và độ trễ xử lý của phương pháp truyền thống tăng hàm mũ theo *n* còn với phương pháp đề xuất độ phức tạp thực thi có dạng hàm bậc 3 của *n*, độ trễ xử lý tuyến tính theo *n*.

3.3. Phương trình bậc 4

Mục này trình bày phương pháp biến đổi phương trình bậc 4 về dạng không có thành phần bậc 3 sau đó sử dụng bảng tra để tìm nghiệm hoặc phân tích đa thức bậc 4 thành tích của hai đa thức bậc 2.

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

$$x^4 + Ax^3 + Bx^2 + Cx + D = 0 \tag{25}$$

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

$$a_3 y^4 + a_2 y^2 + a_1 y + a_0 = 0 \tag{26}$$

trong đó:

$$a_3 = D + BC/A + (C/A)^2;\ a_2 = B + \sqrt{AC};\ a_1 = A;\ a_0 = 1 \tag{27}$$

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

$$z^4 + z^2 + E_1 z + E_2 = 0 \tag{28}$$

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

Phương trình (28) có 2 tham số và có thể xây dựng bảng các nghiệm theo các tham số này. Tương tự như phương trình bậc 2 cũng có thể sử dụng biểu diễn orbit dựa trên các lớp cyclotomic để giảm dung lượng của bảng này.

Ngoài ra, có thể giảm bớt yêu cầu lưu trữ nghiệm phương trình bậc 4 dạng (28) nhờ phân tích thành tích của hai đa thức bậc 2 như sau:

$$z^4 + z^2 + E_1 z + E_2 = (z^2 + A_1 z + B_1)(z^2 + A_1 z + C_1) \quad (29)$$

Dùng phương pháp đồng nhất thức nhận được:

$$A_1^2 + B_1 + C_1 = 1;\ A_1(B_1 + C_1) = E_1;\ B_1 C_1 = E_2 \quad (30)$$

Sau khi biến đổi nhận được biểu thức:

$$A_1^3 + A_1 + E_1 = 0 \quad (31)$$

$$B_1^2 + (1 + A_1^2) B_1 + E_2 = 0 \quad (32)$$

$$\beta^2 + \beta + D_1 = 0 \quad (33)$$

trong đó:

$$D_1 = E_2 / (1 + A_1^2)^2;\ \beta = B_1 / (1 + A_1^2) \quad (34)$$

Phương pháp giải phương trình bậc 4 gồm các bước sau:

Bước 1: Sử dụng phép thế $x = y^{-1} + \sqrt{C/A},\ A \neq 0,$ biến đổi phương trình (25) về dạng (26).

Bước 2: Sử dụng phép thế $y = z\sqrt{a_2 / a_3}$ biến đổi phương trình (26) về dạng (27).

Bước 3: Tìm nghiệm A_1 của phương trình bậc 3 dạng chính tắc (31) (sử dụng phương pháp trong mục 3.2).

Bước 4: Tìm nghiệm của phương trình (33) sử dụng quan hệ (34) để tính B_1 và tính $C_1 = 1 + A_1^2 + B_1$.

Bước 5: Giải phương trình $z^2 + A_1 z + B_1 = 0,\ z^2 + A_1 z + C_1 = 0$ và sử dụng các phép thế $y = z\sqrt{a_2 / a_3};\ x = y^{-1} + \sqrt{C/A}$ để tìm nghiệm của phương trình ban đầu.

4. Kết luận

Bài báo đề xuất cải tiến công thức tính nghiệm của phương trình chính tắc bậc 2 nhằm giảm dung lượng lưu trữ các bảng tra nhờ biểu diễn orbit theo các lớp kề cyclotomic khoảng $2^n / n$ lần. Đồng thời bài báo đề xuất phương pháp trực tiếp giải phương trình bậc 3, bậc 4 trong trường hữu hạn nhờ biến đổi về phương trình chính tắc

bậc 2. Phương pháp giải phương trình trong trường hữu hạn sử dụng thủ tục tìm kiếm Chien bằng cách thử tất cả các phần tử của trường có độ phức tạp hàm mũ theo *n*. Phương pháp trực tiếp giải phương trình đã đề xuất có thể tính được các nghiệm với một vài phép toán để biến đổi ngược có độ phức tạp thực thi thấp hơn, ví dụ với phương trình bậc 3 có dạng hàm bậc 3 theo *n*, độ trễ xử lý tuyến tính theo *n*. Vì vậy, phương pháp trực tiếp tìm nghiệm của phương trình trong trường hữu hạn cho phép xây dựng các thiết bị thực thi có tốc độ xử lý cao, độ trễ rất thấp, cho phép ứng dụng trong các hệ thống thông tin tốc độ cao, các mạch sửa lỗi trong thiết kế chip, bộ nhớ, xây dựng các hệ mật mã dựa trên mã hóa.

Tài liệu tham khảo

[1] Bijan Ansari, "Finite field arithmetic and its application in cryptography," Dissertation for the degree Doctor of Philosophy in Electrical Engineering, University of California, Los Angeles, 2012.

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

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

[4] E.R. Berlekamp, H. Rumsey, G. Solomon, "On the Solution of Algebraic Equations over Finite Fields," *Information and Control*, Vol. 10, 1967, pp. 553-564.

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

[6] K. Huber et al., "Solving Equations in Finite Fields and Some Results Concerning the Structure of GF(p^m), 5.1992 *IEEE Trans. on Information Theory*, 38(3):1154-1162.

[7] K.P. Yiu, "On the root computation of polynomial over a finite field using a stored table approach," *Proceedings of the IEEE*, Vol. 71, No. 4, April 1983.

[8] Fedorenko S.V., Trifonov P.V., "Finding roots of polynomials over finite fields," *IEEE Transactions on Communications*, Vol. 50, Issue 11, 2002.

[9] D. Strukov, "The area and latency tradeoffs of binary bit-parallel BCH decoders for prospective nano electronic memories," *ACSSC Papers*, 2007.

[10] Bo Jeng et al., "High-Throughput Low-Latency Encoder and Decoder for a Class of Generalized Reed-Solomon Codes for Short-Reach Optical Communications," *IEEE Transaction on circuit and systems*, Vol. 67, Issue 4, April 2020.

[11] X. Zhang, Z. Wang, "A low complexity three error correcting for optical transport network," *IEEE Transaction on Circuit and Systems*, Vol. 59, Issue 10, October 2012.

[12] Муттер, В.М., *Основы помехоустойчивой телепередачи информации,* Л.: Энергоатомиздат, Ленинградское отделение, 1990.

[13] Конопелько, В.К. и др. *Теория прикладного кодирования.* Мн.: БГУИР, 2004.

[14] Hosseinzadeh Namin, Parham, "Efficient Implementation of Finite Field Multipliers over Binary Extension Fields," Electronic Theses and Dissertations, 2016.

[15] Chin-Chin Chen, Chiou Yng Lee, Erl-Huei Lu, Scalable and systolic montgomery multipliers over GF(2^m), *IEICE Transaction Fundamentals*, Vol. E91, No. 7, July 2008.

AN ALGERAIC TRANSFORMATION METHOD TO SOLVING EQUATIONS IN THE EXTENDED GALOIS FIELD

Abstract: *This article proposes a method to solve cubic and quartic equations over finite fields using its algebraic transformations on quadratic equations. The obtained results can be generalized to solve equations over finite fields of any size and at the same time allow to reduce the complexity and processing delay significantly compared to traditional methods, so that it can be applied in high-speed communication systems.*

Keywords: Galois field; finite field multiplier; error control coding; polynomial basis; normal basis.

Nhận bài: 15/02/2022; *Hoàn thiện sau phản biện:* 26/08/2022; *Chấp nhận đăng:* 16/09/2022

❑