GERAÇÃO DE POLINÔMIOS IRREDUTÍVEIS EM UM CAMPO FINITO

Valdemar Cardoso da Rocha Júnior

Departamento de Eletrônica e Sistemas - UFPE
Cidade Universitária 50.741, Recife-PE

R E S U M O

Um método é descrito para a geração de polinômios irredutíveis em um campo finito, a partir de um polinômio irredutível dado. Mostra-se que em campos finitos de característica 2, i.e., $GF(2^m)$, o número máximo de polinômios irredutíveis que podem ser gerados desta forma é 6. Em geral, em campos de característica $p \neq 2$, um número de polinômios irredutíveis maior que 6 é obtido. A característica principal deste método é não necessitar conhecer os elementos do campo explicitamente, ou seja, não requerer uma tabela contendo os elementos do campo. Esta teoria encontra aplicações no projeto de sistemas codificados e em sistemas criptográficos.

INTRODUÇÃO

Um método é descrito para a geração de polinômios irredutíveis em um campo finito, a partir de um polinômio irredutível dado. Mostra-se que em campos finitos de característica 2, i.e., $GF(2^m)$, o número máximo de polinômios irredutíveis que podem ser gerados desta forma é 6. Em geral, em campos de característica $p \neq 2$, um número de polinômios irredutíveis maior que 6 é obtido. A característica principal deste método é não necessitar conhecer os elementos do campo explicitamente, ou seja, não requerer uma tabela contendo os elementos do campo. Esta teoria encontra aplicações no projeto de sistemas codificados e em sistemas criptográficos.

Conforme é explicado abaixo, existem pelo menos três procedimentos conhecidos para fatorar $x^n - 1$ sobre um campo finito. O procedimento padrão para fatorar $x^n - 1$ encontra-se descrito nos textos de códigos corretores de erros, nos capítulos de revisão de álgebra [1],[2]. Encontra-se também na literatura [3],[4] um algorítmo para fatorar polinômios em campos finitos de autoria de E. Berlekamp. O terceiro procedimento é devido a John Gordon [5] e, apesar de extremamente simples, necessita de uma tabela com os elementos do campo.

O método de Gordon, na sua forma original, é aplicável apenas a campos finitos de característica 2. A extensão para um campo de Galois $GF(p^m)$, $p \neq 2$, é imediata e é apresentada neste trabalho. Como os dois primeiros procedimentos de fatoração são bastante divulgados, no que segue será descrito apenas o método de Gordon [5] em versão generalizada, antes da apresentação do novo método.

MÉTODO DE GORDON

Uma descrição alternativa para o método de Gordon foi obtida pelo autor, a qual permite visualizar com simplicidade o funcionamento do referido método, assim como também generalizá-lo para campos de Galois de característica $p \neq 2$.

Seja α uma raiz do polinômio $p(x)$, primitivo em $GF(p^m)$, portanto do grau m. Deseja-se determinar o polinômio mínimo $m_\beta(x)$, sobre $GF(p)$, de um elemento arbitrário β, não nulo, de $GF(p^m)$. Este polinômio é de grau igual ou inferior ao de $p(x)$ [1], tendo como raízes :

$\beta, \beta^p, \beta^{p^2}, \ldots\ldots, \beta^{p^{s-1}}$

onde s é o menor inteiro tal que $\beta^{p^s} = \beta$ e pode ser representado como :

$$m_\beta(x) = (x - \beta)(x - \beta^p)(x - \beta^{p^2})\ldots(x - \beta^{p^{s-1}}) \quad \ldots\ldots(1)$$

Sabe-se da álgebra [1] que o algorítmo da divisão de polinômios permite escrever :

$$m_\beta(x) = q(x)p(x) + r(x) \quad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

onde $q(x)$ na verdade é igual a zero ou 1, respectivamente, quando o grau de $m_\beta(x)$ é menor ou igual ao grau de $p(x)$ e $r(x)$ é de grau menor que m.

Substituindo x por α em (2), obtém-se :

$$m_\beta(\alpha) = \begin{cases} p(\alpha) + r(\alpha) = r(\alpha), \text{ para } m_\beta(x) \text{ de grau m .} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots\ldots\ldots(3) \\ r(\alpha) \quad , \quad \text{para } m_\beta(x) \text{ de grau menor que m.} \end{cases}$$

Utilizando a representação para $m_\beta(x)$ dada em (1), o valor de $r(\alpha)$ da expressão (3) pode ser obtido da seguinte forma:

$(\alpha - \beta)(\alpha - \beta^p)(\alpha - \beta^{p^2})\ldots(\alpha - \beta^{p^{s-1}}) = r(\alpha)$ .....(4)

Como r(x) é necessariamente de grau menor que o de p(x), a sua representação polinomial é obtida de (4) bastando para isso apenas mudar α por x. Assim sendo, $m_\beta(x)$ é finalmente obtido do seguinte modo :

$$m_\beta(x) = \begin{cases} p(x) + r(x), \text{ para } m_\beta(x) \text{ de grau m.} \\ \\ r(x), \text{ para } m_\beta(x) \text{ de grau menor que m.} \end{cases} \quad \ldots\ldots\ldots(5)$$

EXEMPLO 1

Considerar o polinômio binário $p(x) = x^4 + x + 1$, primitivo em GF(16). Seja α uma raiz de p(x), i.e., $p(\alpha) = 0$.

a) Determinar o polinômio mínimo de $\beta = \alpha^3$ sobre GF(2).

Solução :

$m_\beta(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$

$m_\beta(\alpha) = (\alpha - \alpha^3)(\alpha - \alpha^6)(\alpha - \alpha^{12})(\alpha - \alpha^9) = r(\alpha)$

Com a ajuda da tabela I do APÊNDICE, obtém-se :

$m_\beta(\alpha) = r(\alpha) = \alpha^9.\alpha^{11}.\alpha^{13}.\alpha^3 = \alpha^6 = \alpha^3 + \alpha^2$

Portanto,

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

Finalmente,

$m_\beta(x) = p(x) + r(x) = x^4 + x^3 + x^2 + x + 1$

b) Determinar o polinômio mínimo de $\beta = \alpha^5$ sobre GF(2)

Solução :

Procedendo de maneira análoga à descrita acima, resulta :

$m_\beta(x) = (x - \alpha^5)(x - \alpha^{10})$

$m_\beta(\alpha) = r(\alpha) = (\alpha - \alpha^5)(\alpha - \alpha^{10}) = \alpha^2.\alpha^8 = \alpha^{10}$

$r(\alpha) = \alpha^{10} = \alpha^2 + \alpha + 1$

Portanto,

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

Finalmente,

$m_\beta(x) = r(x) = x^2 + x + 1$

EXEMPLO 2

Considerar o polinômio $p(x) = x^2 + 4x + 2$, primitivo em GF(25). Seja α uma raiz de p(x), i.e., $p(\alpha) = 0$. Calcular o polinômio mínimo de $\beta = \alpha^3$ sobre GF(5).

Solução :

Seguindo passos análogos aos do EXEMPLO 1, resulta:

$m_\beta(x) = (x - \alpha^3)(x - \alpha^{15})$

$m_\beta(\alpha) = r(\alpha) = (\alpha - \alpha^3)(\alpha - \alpha^{15})$

Com a ajuda da Tabela II do APÊNDICE, obtém-se:

$r(\alpha) = \alpha^4.\alpha^{18} = \alpha^{22} = \alpha + 1$

Portanto,

$r(x) = x + 1$

Finalmente,

$m_\beta(x) = p(x) + r(x) = x^2 + 4x + 2 + x + 1 = x^2 + 3$

NOVO MÉTODO

Este método permite obter polinômios irredutíveis a partir de um polinômio irredutível f(x) dado, por meio de transformações de variáveis que preservam o grau de f(x). Essencialmente, apenas duas transformações básicas são empregadas :

$f(x) \longrightarrow f(1 + x)$ .....(6)

$f(x) \longrightarrow x^m f(1/x)$, onde m é o grau de f(x) .....(7)

A transformação indicada em (7) gera a transformada de raízes recíprocas [1] do polinômio f(x), a qual obviamente dá origem a um polinômio do mesmo grau que f(x). Não é obvio porém que a transformação indicada em (6) preserva o grau do polinômio usado.
O lema a seguir demonstra este fato.

LEMA 1

Dado o polinômio f(x), de grau m, irredutível em GF(p), tal que $f(\beta) = 0$, $\beta \in GF(p^m)$, então f(1 + x) é também irredutível em GF(p).

PROVA.

Como β é raiz de f(x), então decorre que :

$\beta, \beta^p, \beta^{p^2}, \ldots\ldots\ldots, \beta^{p^{m-1}}$

são as raízes de f(x) [1]. Aplicando a transformação (6) em f(x) resulta f(x + 1) que tem como raízes :

$\beta-1, \beta^p-1, \beta^{p^2}-1, \ldots\ldots, \beta^{p^{m-1}}-1$

Se $\beta^{p^i} - 1 = \beta^{p^j} - 1$, $0 \leq i,j \leq m - 1$, $i < j$

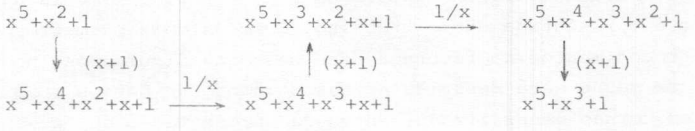
então $\beta^{p^i} = \beta^{p^j}$, ou seja, $\beta^{p^j - p^i} = 1 = \beta^{p^m}$,

portanto $p^j - p^i = p^m$

o que é uma contradição. Portanto, f(x + 1) tem o mesmo número de raízes que f(x), todas distintas, sendo assim irredutível em GF(p). CQD.
O polinômio f(x + 1) é na verdade o polinômio mínimo [1] de $\beta - 1$. No caso binário, i.e., p = 2 as transformações indicadas em (6) e (7) são aplicadas sucessivamente e repetidamente, parando quando o resultado obtido for f(x), conforme é mostrado no EXEMPLO 3. Em geral, para $p \neq 2$, aplica-se (6) p - 1 vezes seguido de uma aplicação de (7), depois (6) por mais p - 1 vezes, depois (7), etc., e assim sucessivamente até repetir f(x), conforme é mostrado no EXEMPLO 4.

EXEMPLO 3

Considerar o polinômio $f(x) = x^5 + x^2 + 1$, irredutível em GF(2). A aplicação das transformações (6) e (7) fornece a seguinte sequência de polinômios irredutíveis :



EXEMPLO 4

Considerar o polinômio $f(x) = x^2 + x + 2$, irredutível em GF(5). A aplicação das transformações (6) e (7) fornece a seguinte sequência de polinômios irredutíveis :

$$x^2+x+2 \xrightarrow{x+1} x^2+3x+4 \xrightarrow{x+1} x^2+3 \xrightarrow{x+1} x^2+2x+4 \xrightarrow{x+1} x^2+4x+2$$

$$\downarrow 1/x$$

$$x^2+2 \xleftarrow{x+1} x^2+3x+3 \xleftarrow{x+1} x^2+x+1 \xleftarrow{x+1} x^2+4x+1 \xleftarrow{x+1} x^2+2x+3$$

A determinação do comprimento de um ciclo de transformações, ou seja, do número de polinômios irredutíveis gerados, pode ser feita conforme é indicado a seguir .

a) Caso binário

A sequência de polinômios irredutíveis é obtida assim :

$$\begin{array}{lllll}
(1)\ f(x) & (4)\ (1+x)^m f(1+1/(1+x)) & \xrightarrow[(5)]{1/x} & x^m(1+1/x)^m f\left(1+\frac{1}{1+1/x}\right) \\
\downarrow x+1 & \uparrow x+1 & & \downarrow x+1 \\
(2)\ f(1+x) & & & \\
\searrow 1/x & (3)\ x^m f(1+1/x) & (6)\ (1+x)^m\left(1+\frac{1}{1+x}\right)^m & f\left(1+\frac{1}{1+\frac{1}{1+x}}\right)
\end{array}$$

O próximo termo seria

$$x^m(1+1/x)^m\left(1+\frac{1}{1+1/x}\right)^m f\left(1+\frac{1}{1+\frac{1}{1+1/x}}\right) = f(x)$$

Visto que

$$x^m(1+1/x)^m\left(1+\frac{1}{1+1/x}\right)^m = 1$$

$$f\left(1+\frac{1}{1+\frac{1}{1+1/x}}\right) = f(x)$$

Portanto, no caso binário, são gerados no máximo 6 polinômios irredutíveis.

b) Caso não binário

A sequência de polinômios irredutíveis é obtida assim :

$$\begin{array}{lllll}
f(x) & (x+q-1)^m f\left(q-1+\frac{1}{q-1+x}\right) & \xrightarrow{1/x} & x^m(1/x+q-1)^m f\left(q-1+\frac{1}{q-1+1/x}\right) \\
\downarrow 1+x & \uparrow & & \downarrow 1+x \\
f(1+x) & & & \\
\downarrow 1+x & \uparrow & & \\
f(2+x) & (x+2)^m f\left(q-1+\frac{1}{2+x}\right) & & \\
\downarrow & \uparrow 1+x & & \\
 & (x+1)^m f\left(q-1+\frac{1}{1+x}\right) & & \\
\downarrow 1+x & \uparrow 1+x & & \\
f(q-1+x) & \xrightarrow{1/x} x^m f(q-1+1/x) & &
\end{array}$$

onde q é um número primo.

E assim sucessivamente até a obtenção do termo cujo argumento de f( ) é o seguinte :

$$q-1+\cfrac{1}{q-1+\cfrac{1}{q-1+\ddots\ \cfrac{1}{q-1+1/x}}} = x \qquad \ldots\ldots\ldots\ldots\ldots\ (8)$$

O período da sequência de transformações pode ser obtido de (8), somando os valores do primeiro membro a partir do último termo, i.e.,

$(q - 1) + 1/x = [(q - 1)x + 1] / x.$

Uma expressão de recorrência pode ser deduzida para calcular a referida soma, tendo o seguinte termo genéri - co :

$$A_i(x) = \frac{(q-1)a_{i-1}(x) + a_{i-2}(x)}{a_{i-1}(x)} = \frac{a_i(x)}{a_{i-1}(x)} \qquad \ldots\ldots\ldots\ (9)$$

onde as condições iniciais são $a_1(x) = x$ e $a_0(x) = 1$, i.e.,

$A_1(x) = [(q-1)x + 1]/x$

$$A_2(x) = \frac{(q-1)^2x + x + (q-1)}{(q-1)x + 1} = \frac{x[(q-1)^2 + 1] + (q-1)}{(q-1)x + 1}$$

:

e assim sucessivamente, parando no termo $A_n(x) = x$.
A expressão (9) serve para implementar o seguinte algorítmo, para cálculo do número de termos :

i	$a_i(x)$	$a_{i-1}(x)$	$A_i(x)$
1	x	1	x
2	(q-1)x + 1	x	[(q-1)x + 1] / x
3	[(q-1) + 1]x + (q-1)	(q-1)x + 1	$a_3(x) / a_2(x)$
.	.	.	.
.	.	.	.
n	ax	a	x

onde a ε GF(p).

EXEMPLO 5

Determinação do comprimento máximo do ciclo de transformações quando p = 5.

i	$a_i(x)$	$a_{i-1}(x)$	$A_i(x)$
1	x	i	x
2	4x + 1	x	(4x+1)/x
3	2x + 4	4x + 1	(2x+4)/(4x+1)
4	2x + 2	2x + 4	(2x+2)/(2x+4)
5	2	2x + 2	2/(2x+2)
6	2x	2	x

Assim, no máximo 25 polinômios irredutíveis em GF(5) são gerados.

COMENTÁRIOS

O grupo de transformações indicadas por (6) e (7) tem ordem 6 no caso binário e foi utilizado [6] para a fa-

toração de trinômios em GF(2).

Como conseqüência do lema 1, mostra-se facilmente que (6) aplicada a um polinômio composto de dois ou mais fatores irredutíveis, dá como resultado um polinômio composto de dois ou mais fatores irredutíveis.

O método introduzido é caracterizado pela simplicidade. Pode ser automatizado para uso com computador digital ou circuito digital.

Sobre os polinômios gerados pode-se dizer apenas que são irredutíveis, nada se sabendo quanto ao fato de serem primitivos. O comprimento máximo do ciclo de transformações não foi determinado exatamente e observa-se que depende da sequência em que são aplicadas as transformações (6) e (7). Quanto a possíveis aplicações em criptografia, chaves para "stream ciphers" que fazem uso de polinômios irredutíveis, podem vir a explorar as relações de dependência que existem entre os polinômios de um mesmo ciclo.

Para finalizar, o método aqui apresentado reduz bastante a tarefa de encontrar polinômios irredutíveis, quando comparado com outros métodos, e pode ser usado com vantagem em combinação com eles.

AGRADECIMENTO

Este trabalho recebeu apoio parcial do Conselho Nacional de Desenvolvimento Científico e Tecnológico-CNPq.

BIBLIOGRAFIA

[1] PETERSON, W.W. & WELDON, E.J., Error - Correcting Codes, MIT Press, 1972, Segunda edição.

[2] LIN, S. & COSTELLO, D.J., Error Control Coding, Prentice Hall, 1983.

[3] BERLEKAMP, E.R., Algebraic Coding Theory, McGraw Hill, 1968.

[4] McELIECE, R.J., Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987.

[5] GORDON, J.A., Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field. Electronics Letters, vol. 12, Nº 25, pp. 663-664.

[6] GOLOMB, S.W., Shift-Register Sequences, Holden Day 1967.

APÊNDICE

TABELA I. Elementos não-nulos de GF(16), módulo $p(x) = x^4 + x + 1$

0	α^3	$\alpha^7=\alpha^3+\alpha+1$	$\alpha^{11}=\alpha^3+\alpha^2+\alpha$
1	$\alpha^4=\alpha+1$	$\alpha^8=\alpha^2+1$	$\alpha^{12}=\alpha^3+\alpha^2+\alpha+1$
α	$\alpha^5=\alpha^2+\alpha$	$\alpha^9=\alpha^3+\alpha$	$\alpha^{13}=\alpha^3+\alpha^2+1$
α^2	$\alpha^6=\alpha^3+\alpha^2$	$\alpha^{10}=\alpha^2+\alpha+1$	$\alpha^{14}=\alpha^3+1$

TABELA II. Elementos não-nulos de GF(25), módulo $p(x) = x^2 + 4x + 2$

0	$\alpha^5=4\alpha+1$	$\alpha^{11}=3\alpha+2$	$\alpha^{17}=\alpha+4$	$\alpha^{23}=2\alpha+3$
1	$\alpha^6=2$	$\alpha^{12}=4$	$\alpha^{18}=3$	
α	$\alpha^7=2\alpha$	$\alpha^{13}=4\alpha$	$\alpha^{19}=3\alpha$	
$\alpha^2=\alpha+3$	$\alpha^8=2\alpha+1$	$\alpha^{14}=4\alpha+2$	$\alpha^{20}=3\alpha+4$	
$\alpha^3=4\alpha+3$	$\alpha^9=3\alpha+1$	$\alpha^{15}=\alpha+2$	$\alpha^{21}=2\alpha+4$	
$\alpha^4=2\alpha+2$	$\alpha^{10}=4\alpha+4$	$\alpha^{16}=3\alpha+3$	$\alpha^{22}=\alpha+1$	