国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
一九八七年第三期　总第五十九期　No.3 1987 Sum. 59

寻找二进制本原多项式的一种新方法

饶 世 麟

（电子技术系）

摘 要 本文提出了一种从已知的m次本原多项式寻找出所有的其他m次本原多项式的新方法，与传统的方法相比较，这种方法的计算量大为减少。

一、前　　言

二进制本原多项式（以下简称本原多项式）在编码领域有着广泛的应用，它是设计m序列与M序列的技术基础。本文提出一种从已知的m次本原多项式寻找所有的其他m次本原多项式的新方法，与传统的方法相比较，计算量大为减少。

二、传统的方法

传统的方法是以下述命题为基础的。

命题 1 设$F(x)$为已知的m次本原多项式，α为$F(x)$的一根，正整数l与(2^m-1)互素，且

$$\beta_i=\alpha^{2^{i-1}l} \qquad (i=1,2,\cdots,m) \tag{1}$$

则

$$G(x)=\prod_{i=1}^{m}(x+\beta_i) \tag{2}$$

亦为m次本原多项式。

因为β_i均为$GF(2^m)$域中的本原元，命题1显然成立。但是，要从$F(x)$寻找出$G(x)$，必须展开式(2)，计算出$G(x)$的各项系数。即令

$$G(x)=x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m \tag{3}$$

而

$$\left.\begin{aligned} b_1&=\beta_1+\beta_2+\cdots+\beta_m\\ b_2&=\beta_1\beta_2+\beta_1\beta_3+\cdots+\beta_{m-1}\beta_m\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ b_m&=\beta_1\beta_2\cdots\beta_m \end{aligned}\right\} \tag{4}$$

本文1986年6月9日收到

不难看出，这种计算方法必须先计算出$GF(2^m)$域中的所有元，其中包括$\beta_i(i=1,2,\cdots,m)$，再运用$GF(2^m)$中的乘法与加法计算出系数$b_1\cdot b_2\cdot\cdots\cdot b_m$，计算量是很大的。

例如，已知$F(x)=x^5+x^2+1$为本原多项式，α为$F(x)$的一根，$l=5$与$p=2^5-1=31$互素，则

$$G(x)=(x+\alpha^5)(x+\alpha^{10})(x+\alpha^{20})(x+\alpha^9)(x+\alpha^{18})$$

亦为5次本原多项式。令

$$G(x)=x^5+b_1x^4+b_2x^3+b_3x^2+b_4x+b_5$$

要计算出$b_1\cdot b_2\cdot b_3\cdot b_4\cdot b_5$，必须先从$F(x)$计算出$GF(2^5)$域中所有元如下表[3]：

$0=00000$	$1=00001$
$\alpha=00010$	$\alpha^2=00100$
……	……
$\alpha^{29}=01001$	$\alpha^{30}=10010$

于是

$$\begin{aligned}b_1&=\alpha^5+\alpha^{10}+\alpha^{20}+\alpha^9+\alpha^{18}\\&=(00101)+(10001)+(01100)+(11010)+(00011)\\&=(00001)=1\end{aligned}$$

同样，计算出$b_2=0$，$b_3=b_4=b_5=1$

$$\therefore\quad G(x)=x^5+x^4+x^2+x+1$$

可见计算量是很大的，特别当m很大时计算量就十分巨大。

三、新方法的原理

设$F(x)$的根为

$$\alpha_i=\alpha^{2^{i-1}}\quad(i=1,2,\cdots,m)\tag{5}$$

取$F(x)$之互反多项式，即本原多项式

$$f(x)=(1+\alpha_1x)(1+\alpha_2x)\cdots(1+\alpha_mx)\tag{6}$$

再取$f(x)$的导数

$$f'(x)=\sum_{i=1}^{m}\alpha_i\prod_{w\neq i}(1+\alpha_wx)\tag{7}$$

引理 1 $f'(x)$与$f(x)$互不可约。

证 用反证法。假设$f'(x)$包含因式$(1+\alpha_ix)$，则 $f'(\alpha_i^{-1})=0$

由式(7)得 $$\alpha_i\prod_{w\neq i}(1+\alpha_w\alpha_i^{-1})=0$$

必有某个 $$\alpha_w=\alpha_i$$

但由式(5)知，$F(x)$的诸根α_i均不相等，故假设不成立。所以$f'(x)$与$f(x)$互不可约。

证毕

定理 1 作除法的升幂展开式

$$f'(x)/f(x)=s_1+s_2x+s_3x^2+\cdots+s_kx^{k-1}+\cdots\tag{8}$$

则 $$s_k=\sum_{i=1}^{m}\alpha_i^k\tag{9}$$

为$F(x)$诸根之幂和对称函数。

证 由式(7)与(6)得

$$f'(x)/f(x)=\sum_{i=1}^{m}\alpha_i/(1+\alpha_i x)$$

$$=\sum_{i=1}^{m}\alpha_i(1+\alpha_i x+\alpha_i^2x^2+\cdots+\alpha_i^{k-1}x^{k-1}+\cdots)$$

故式(9)成立。 证毕

定理 2 展开式(8)具有周期$p=2^m-1$。

证 因α_i为$GF(2^m)$域中的本原元，故

$$\alpha_i^p=1$$

于是 $$s_{k+p}=\sum_{i=1}^{m}\alpha_i^{k+p}=\sum_{i=1}^{m}\alpha_i^k=s_k$$ 证毕

根据上述定理作展开式时，仅需作出s_1至$s_p x^{p-1}$前p项即可。

例如，$F(x)=x^5+x^2+1$，$f(x)=1+x^3+x^5$，$f'(x)=x^2+x^4$，$p=2^5-1=31$。

$f'(x)/f(x)=x^2+x^4+x^5+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{16}+x^{17}+x^{19}+x^{20}+x^{21}+x^{23}+x^{25}+x^{30}+\cdots$

即 $$[s_1s_2s_3s_4\cdots s_{29}s_{30}s_{31}]$$

$$=[00101100111110001101110101000 01]$$

与此类似，因为l与p互素，为$\beta=\alpha^l$为根的二进制既约多项式$G(x)$亦为m次本原多项式。取$G(x)$的互反多项式$g(x)$及其导数$g'(x)$，则

$$g(x)=\prod_{i=1}^{m}(1+\beta_i x) \tag{10}$$

$$g'(x)=\sum_{i=1}^{m}\beta_i\prod_{w\neq i}(1+\beta_w x) \tag{11}$$

也作除法的升幂展开式

$$g'(x)/g(x)=s_1'+s_2'x+s_3'x^2+\cdots+s_k'x^{k-1}+\cdots \tag{12}$$

定理 3 $$s_k'=s_{kl} \tag{13}$$

证 根据定理1有

$$s_k'=\sum_{i=1}^{m}\beta_i^k$$

为$G(x)$诸根之幂和对称函数。由式(1)知

$$\beta_i=\alpha_i^l \quad (i=1,2,\cdots,m)$$

$$\therefore\quad s_k'=s_{kl}$$ 证毕

有了定理3，就可从式(8)直接得出式(12)。因为展开式(12)亦具有周期$p=2^m-1$，也仅需作出s_1'至$s_p'x^{p-1}$前p项，此外s_{kl}的下标kl以p为模。已知式(12)的右端就不难计算出$g'(x)$、$g(x)$与$G(x)$。不过，文献[4]告诉我们，还有一个更简单的方法，其原理如下。

命题 2 设R为一域，$\varphi(x)$、$Q(x)$为$R[x]$中给定的两互素多项式，$Q(x)$的次数为m，$\varphi(x)$的次数小于m。设$\varphi(x)\equiv Q(x)s(x)\ \mathrm{mod}x^{2m}$，而$s(x)=s_1'+s_2'x+s_3'x^2+\cdots+s_{2m}'x^{2m-1}\neq 0$。若$R$为满足基于Euclidian算法的序列

$$r_{-1}(x)=x^{2m},\ r_0(x)=s(x),\ r_1(x),\ \cdots,\ r_i(x),\ \cdots$$

中次数小于m的最高次余式$r_i(x)$的下标号i，则

$$\varphi(x)=\delta r_k(x)$$

而常数$\delta\in R$，在二进制场合，$\delta=1$。

运用命题2到我们的方法中有

$$g'(x)\equiv g(x)s(x)\bmod x^{2m} \tag{14}$$

$$\begin{aligned}s(x)&=s'_1+s'_2x+s'_3x^2+\cdots+s'_{2m}x^{2m-1}\\&=s_1+s_{21}x+s_{31}x^2+\cdots+s_{2m1}x^{2m-1}\end{aligned} \tag{15}$$

这就是说，仅需作出展开式(12)的前$2m$项，即可计算出$g'(x)$、$g(x)$与$G(x)$。

在上例中，$m=5$

$$s'_1=s_5=1,\quad s'_2=s_{10}=1,\quad s'_3=s_{15}=0,\quad s'_4=s_{20}=1,$$
$$s'_5=s_{25}=0,\quad s'_6=s_{30}=0,\quad s'_7=s_{35}=s_4=0,\ s'_8=s_{40}=s_9=1,$$
$$s'_9=s_{45}=s_{14}=0,\ s'_{10}=s_{50}=s_{19}=0$$

得

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

运用Euclidian算法得序列

$$r_{-1}(x)=x^{10},\qquad r_0(x)=x^7+x^3+x+1,$$
$$r_1(x)=x^6+x^4+x^3,\quad r_2(x)=x^5+x^4+x^3+x+1,$$
$$r_3(x)=x^4+x^2+1,\qquad \cdots\cdots$$

因此$k=3$为最高次余式$r_i(x)$的下标号i，使$r_i(x)$的次数为$4<m$，故

$$g'(x)=r_3(x)=x^4+x^2+1$$

$$\therefore\quad g(x)\equiv g'(x)/s(x)\bmod x^{10}$$

然后$g'(x)$及$s(x)$按升幂排列相除，展开后以x^{10}为模得

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

相应地得出以$\beta=\alpha^5$为根的本原多项式为

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

从上面可以看出，新方法不需要计算$GF(2^5)$域中所有元，而代之以展开式(8)；不需要运用$GF(2^5)$中的乘法与加法计算出系数$b_1\cdot b_2\cdot b_3\cdot b_4\cdot b_5$，而代之以Euclidian算法。可见计算量大为减少。

四、计算步骤

根据以上的分析，可以归纳出计算所有其他的m次本原多项式的步骤如下：

(1) 已知$F(x)$为一m次本原多项式。

(2) 周期为$p=2^m-1$。

(3) 将p分解为素数的乘积，设

$$p=p_1^{e_1}\ p_2^{e_2}\cdots p_u^{e_u}$$

则欧拉函数$\phi(p)=p(1-1/p_1)(1-1/p_2)\cdots(1-1/p_u)$表示$GF(2^m)$域中本原元的数目，而$1/m\phi(p)$表示$m$次本原多项式的数目。

(4) 根据$f(x)=x^m F(1/x)$找出$F(x)$之互反本原多项式，将$f(x)$取导数得出$f'(x)$。

(5) 按升幂排列展开一个周期，即

$$f'(x)/f(x)=s_1+s_2x+s_3x^2+\cdots+s_px^{p-1}+\cdots$$

写出$[s_1s_2s_3\cdots s_p]=[\cdots\cdots]$。

(6) 将小于p且与p互素的数l，按下列方法排成$1/m\phi(p)$行：

$$\left.\begin{array}{l}1,\ 2,\ 4,\ \cdots\cdots,\ 2^{m-1}\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ l,\ 2l,\ 4l,\ \cdots\cdots,\ 2^{m-1}l\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\end{array}\right\}\qquad(16)$$

上述各数均以$p=2^m-1$为模。

例如，$m=6$，$p=63=3^2\cdot7$　$1/m\phi(p)=1/6\cdot63(1-1/3)(1-1/7)=6$；得下表

$$\left.\begin{array}{l}1,\ 2,\ 4,\ 8,\ 16,\ 32\\ 5,\ 10,\ 20,\ 40,\ 17,\ 34\\ 11,\ 22,\ 44,\ 25,\ 50,\ 37\\ 13,\ 26,\ 52,\ 41,\ 19,\ 38\\ 23,\ 46,\ 29,\ 58,\ 53,\ 43\\ 31,\ 62,\ 61,\ 59,\ 55,\ 47\end{array}\right.$$

(7) 每次从式(16)第2至末行中选取最小的数l，令$\beta=\alpha^l$，得

$$s(x)=s_l+s_{2l}x+s_{3l}x^2+\cdots+s_{2ml}x^{2m-1}$$

s的下标以p为模，其值由$[s_1s_2s_3\cdots s_p]$中取出。

(8) 令　　$g'(x)\equiv g(x)s(x)\bmod x^{2m}$

运用Euclidian算法计算出

$$g'(x)=r_k(x)。$$

(9) 由$g'(x)$及$s(x)$按升幂排列相除，计算出

$$g(x)\equiv g'(x)/s(x)\bmod x^{2m}。$$

(10) 计算出

$$G(x)=x^m g\left(\frac{1}{x}\right)$$

则$G(x)$及$g(x)$为所求的m次本原多项式。

(11) 重复(7)至(10)，将所有的m次本原多项式计算出来为止。

参 考 文 献

[1] W.Wesley Peterson, E.J.Weldon, Jr.著, Error—Correcting Codes, 1971年第2版.

[2] 万哲先编著，代数和编码，科学出版社 1976年。

[3] 锐世麟编，编码原理，国防科技大学1981年版。

[4] Paul F.Camion, Improving an Algorithm for Factoring Polynomials Over a Finite Field. and Constructing Large Irreducible Polynomials, IEEE Transaction on Information Theory, Vol IT—29, NO.3, May 1983.

A New Method of Finding out the Binary Primitive Polynomials

Yao Shilin

Abstract

In this paper a new method of finding out all other primitive polynomials of degree m from a known one is proposed. Comparing with the conventional method, this new one can reduce greatly the amount.