判定有限域上不可约多项式及本原多项式的一种高效算法*

王 鑫[1]，王新梅[1]，韦宝典[2]
（1. 西安电子科技大学综合业务网国家重点实验室，陕西 西安 710071；
2. 中山大学电子与通信工程系，广东 广州 510275）

摘 要：提出了一个判定有限域上任一多项式是否为不可约多项式、本原多项式的高效的确定性算法。分析了多项式次数与其不可约因式之间的内在联系，给出了有限域上任意 n 次多项式是否为不可约多项式、本原多项式的一个充要条件。通过利用欧几里得算法，该判定仅需做 $O((\log_2 n)n^3)$ 次域上乘法，属于多项式时间，易于硬件实现。为扩频通信与序列密码寻找和利用不可约多项式构造线性反馈移位寄存器提供了一种有效算法。

关键词：有限域；不可约；本原；多项式时间算法；扩频通信；序列密码
中图分类号：TP309 **文献标识码**：A **文章编号**：0529-6579（2009）01-0006-04

An Efficient and Deterministic Algorithm to Determine Irreducible and Primitive Polynomials over Finite Fields

WANG Xin[1], *WANG Xinmei*[1], *WEI Baodian*[2]
(1. State Key Laboratory of Integrated Service Networks State, Xidian University, Xi'an 710071, China;
2. Department of Electronics and Communication Engineering, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: An efficient and deterministic method is proposed to determine whether a polynomial over finite fields is irreducible (primitive) or not. The correlation between the degree of the polynomial and its irreducible factors is analyzed, and then a sufficient and necessary condition on judging whether a polynomial of arbitrary degree n over finite fields is irreducible (primitive) or not is presented. By applying the Euclidean Algorithm, this judgment can be verified with $O((\log_2 n)n^3)$ multiplicative operations over finite fields. The proposed algorithm is accomplished in polynomial time and easy to be implemented on hardware. And it is an efficient method for construction of the Linear Feedback Shift Register for spread communication and the stream cipher to find and use irreducible polynomials.

Key words: finite fields; irreducible; primitive; polynomial time algorithm; spread spectrum communication; sequence cipher

有限域上的不可约多项式与本原多项式在密码，编码理论及随机数的产生等方面有着广泛的应用。这是由于在扩频通信与序列密码中被广泛应用的伪随机序列，可在连续波雷达中用作测距信号，在遥控系统中用作遥控信号，在多址通信中用作地址信号，在数字通信中用作群同步信号，还可用作噪声源在保密通信中起加密作用。这些伪随机序列大部分是利用有限域上的不可约多项式和本原多项式通过反馈移位寄存器和其它非线性逻辑产生的。另一方面，多项式理论尤其是不可约多项式和本原

* 收稿日期：2008-05-13
基金项目：国家自然科学基金资助项目（90604009；60503010）
作者简介：王鑫（1979年生），女，博士生；E-mail：wangxin@mail.xidian.edu.cn

多项式又是分析伪随机性能和密码体制的一种有效工具，因此研究有限域上的不可约多项式与本原多项式具有重要意义[1-4]。

设 $GF(q)$ 为一个含 q 个元素的有限域，其中 $q=p^k$，p 为一素数，k 为正整数，那么对于任一正整数 n，一定存在 $GF(q)$ 上的 n 次不可约多项式[5]。目前，判定有限域上一个 n 次多项式是否不可约的方法一般有确定性（构造性）和概率性两种算法[6]。确定性算法由于检验的步骤多，计算量大，技术实现上比较复杂[7-9]，而概率性算法则是对随机给出的一个多项式，判别其是否为不可约多项式，重复某一过程直到给出肯定性判断为止，这便涉及算法成功的可能性有多大[10]。文[11]给出了一种新方案，但遗憾的是仅适用于少数特殊类型的多项式，即多项式的次数为素数或两个素数之积。本文通过对多项式的次数与其不可约因式之间的内在联系进行分析，给出了有限域上任意 n 次多项式为不可约多项式和本原多项式的充要条件。采用多项式快速模运算及欧几里德算法，该算法复杂度为 $O((\log_2 n)n^3)$，属于多项式时间，易于硬件实现。

本文所研究的多项式均为首一，非首一多项式可通过乘以非零常数化为首一，不影响其不可约性。我们用 $\deg(f)$ 表示多项式 $f(x)$ 的次数；$\gcd(f(x),g(x))$ 表示 $f(x)$ 和 $g(x)$ 的最大公因式；以 S_n 表示自然数 n 的所有正因子的集合；符号 $|$ 表示整除，$\nmid$ 表示不能整除。

1　不可约与本原多项式的判定

定义 1[6]　设有限域 $F_q=GF(q)$，$F_q[x]$ 为 $GF(q)$ 上的多项式环，$f(x)$ 称为不可约多项式是指 $f(x)$ 在 $F_q[x]$ 中除了常数 $c\in F_q$ 和 $cf(x)$ 外没有其它因式。

引理 1[5]　F_q 为一有限域，其中 $|F_q|=q=p^m$，则：

$$x^{q^n}-x=\prod_{d|n}V_d[x]$$

其中 $V_d[x]$ 是 $F_q[x]$ 上所有 d 次首一不可约多项式的乘积。

该引理表明：$x^{q^n}-x$ 实际上是由 $F_q[x]$ 上次数整除 n 的所有（相异，没有重复的）首一不可约多项式的乘积所构成。例如：当 $n=6$，$x^{q^6}-x$ 就等于 F_q 上的所有的 1、2、3 和 6 次首一不可约多项式的乘积。

下述定理更进一步的揭示出 $f(x)$ 与其不可约因式之间的联系。

定理 1　$n(\geq 1)$ 次多项式 $f(x)\in F_q[x]$，设 $f(x)$ 的所有不可约因式为 $f_i(x)(i=1,\cdots,s)$，则 $f(x)\,|\,x^{q^n}-x$ 当且仅当 $(f(x),f'(x))=1$，且对所有 $i(=1,\cdots,s)$ 均有 $\deg(f_i)\,|\,n$。

证明　由 $(x^{q^n}-x,(x^{q^n}-x)')=1$ 知 $x^{q^n}-x$ 没有重因式，再由引理 1，该结论成立。

由于一次多项式总是不可约多项式，因此，下面只讨论二次以上的多项式的不可约性。

设自然数 n 的因式分解为 $n=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$，$p_i$ 为素数，e_i 是正整数 $(i=1,\cdots,t)$，用 n_i 表示对应的 n/p_i。令 $M=\{n/p_1,\cdots,n/p_t\}$，则有：

定理 2　F_q 上的 $n(\geq 2)$ 次多项式 $f(x)$ 为不可约多项式的充要条件是：

(1) $f(x)\,|\,x^{q^n-1}-1$；

(2) 对任意 $c\in F_q$，$f(c)\neq 0$；

(3) 对任意的 $n_i\in M$，均有 $\gcd(x^{q^{n_i}-1}-1,f(x))=1$。

首先简要解释上述三个条件。条件 (1) 旨在说明 $f(x)$ 是由以 n 的因子为次数的不可约多项式之积；(2) 表明 $f(x)$ 无一次因式；(3) 是为了说明 $f(x)$ 事实上并不含有次数小于 n 的不可约因式。因此 $f(x)$ 只能为一 n 次不可约因式。

证明　为了证明定理 2，首先证明这样一个结论：对任意的自然数 n，有 $\bigcup_{n_i\in M}\{m:m\,|\,n_i\}=S_n\setminus\{n\}$ 成立。事实上，设 $a\in\bigcup_{n_i\in M}\{m:m\,|\,n_i\}$，那么 $a\,|\,n_i\,|\,n$。因 p_i 为素数，故 $n_i\neq n$，从而 $a\in S_n\setminus\{n\}$。反之，设 $aS_n\setminus\{n\}$，则对 $a=p_1^{k_1}\cdots p_t^{k_t}$，有 $k_i\leqslant e_i$ $(1\leqslant i\leqslant t)$，且至少存在一个 k_j $(1\leqslant j\leqslant t)$ 满足 $k_j<e_j$（否则，$a=n$，矛盾）。故 $a\,|\,n_j$，$a\in\bigcup_{n_i\in M}\{m:m\,|\,n_i\}$。

（必要性）　由定理 1 和 $f(x)$ 不可约分别可知 (1)，(2) 成立。又对任意的 $n_i\in M$，$\gcd(x^{q^{n_i}-1}-1,f(x))=1$ 成立。否则，设 $p(x)=\gcd(x^{q^{n_i}-1}-1,f(x))$，$\deg(p)\geqslant 1$。因为 $f(x)$ 是不可约多项式，且 $p(x)\,|\,f(x)$，故有 $p(x)=f(x)$，从而 $f(x)\,|\,x^{q^{n_i}-1}-1$，再由定理 1，$\deg(f)\,|\,n_i$，这与 $\deg(f)=n$ 矛盾。故 (3) 成立。

（充分性）　由于 $x^{q^n-1}-1$ 无重因式，所以 $f(x)$ 无重因式，故可设 $f(x)$ 在 $F_q[x]$ 的因式分解为：$f(x)=f_1(x)f_2(x)\cdots f_s(x)$，其中 $f_j(x)$ 为 $f(x)$ 的互不相同的不可约因式。由 (2)，因 $f(x)$ 无一次因式，即 $f_i(x)$ 均非一次因式，故有

$f_j(x)\mid x^{q^n-1}-1$，从而 $\deg(f_j)\mid n$。又因为 $\gcd(x^{q^{n_i}-1}-1,f(x))=1$，所以 $\deg(f_j)\nmid n_i$（对任意的 $n_i\in M$）（否则，若存在因式 $f_{j_0}(x)$，$\deg(f_{j_0})\mid n_i$ 则有 $f_{j_0}(x)\mid x^{q^n}-x$，进而 $f_{j_0}(x)\mid x^{q^{n_i-1}}-1$，这与 $(f(x),x^{q^n-1}-1)=1$ 矛盾）。因此，$\deg(f_j)\notin\{m:m\mid n_i,n_i\in M\}$，再由一开始所证结论，可得 $\deg(f_j)\notin S_n\setminus\{n\}$，因此 $f_j(x)$ 的次数只能为 n，而 $f_j(x)$ 为不可约多项式，所以首一时，$f_j(x)=f(x)$，即 $f(x)$ 为一不可约多项式。

判断 $\gcd(x^{q^{n_i-1}}-1,f(x))$ 是否为1，并不直接运用欧几里得算法，而是分两步：①先按下述快速模指数算法（即对多项式平方以使指数翻倍）求出 $(x^{q^{n_i-1}}-1)\bmod f(x)$ 的余式 $r(x)$；②再运用欧几里德算法求最大公因式 $\gcd(f(x),r(x))$。

设 t 的二进制表示为 $t=\sum_{i=0}^{s-1}(l_i2^i)$，$x^t\bmod f(x)$ 的算法如下：

$$r(x)=1$$
$$\text{for } i=s-1 \text{ to } 0 \text{ step}(-1)$$
$$r(x)=r(x)*r(x)\bmod f(x)$$
$$\text{if } l_i=1$$
$$\text{then } r(x)=x*r(x)\bmod f(x)$$
$$\text{return } r(x)$$

该算法需 $O(ln^2)$ 次 F_q 上乘法运算，其中 $l=[\log_2 t]$。这里 $t=q^{n_i}-1$，故指数模多项式运算为 $O(n^3)$ 次域上乘法。由于事先把 $q^{n_i}-1$ 次和 n 次多项式的最大公因式转换成求两个不超过 n 次的多项式 $f(x)$ 和 $r(x)$ 的最大公因式，因此运用欧几里德算法只需 $O(n^2)$ 次域上乘法，所以，完成对一个 n_i 的判断需 $O(n^3)$ 次域上乘法。而 n 所含素因子数不超过 $\log_2 n$，故判断一个 n 次多项式是否为不可约多项式共需 $O((\log_2 n)n^3)$ 次 F_q 上乘法，该算法属于多项式时间，易于硬件实现。

推论1 设 $f(x)$ 是 $F_q[x]$ 的一个 n 次多项式，n 为素数，则 $f(x)$ 为不可约多项式的充要条件为：

（1）对任意的 $c\in F_q$，$f(c)\neq 0$；

（2）$f(x)\mid x^{q^n-1}-1$。

证明 注意到 n 为素数，由定理2，易见结论成立。

推论2 $f(x)$ 是 $F_q[x]$ 上的一个 n 次多项式，$n=n_1\cdot n_2$（n_1，n_2 均为素数），则 $f(x)$ 为不可约多项式的充要条件为：

（1）对任意 $c\in F_q$，$f(c)\neq 0$；

（2）$f(x)\mid x^{q^n-1}-1$；

（3）$f(x)\nmid x^{q^{n_1}-1}-1$，且 $f(x)\nmid x^{q^{n_2}-1}-1$。

证明 当 $n_1=n_2$，易见结论成立。当 $n_1\neq n_2$，由定理2得出的 $f(x)$ 为不可约多项式的充要条件为：(1′) 对任意 $c\in F_q$，$f(c)\neq 0$；(2′) $f(x)\mid x^{q^n-1}-1$；(3′) $\gcd(f(x),x^{q^{n_1}-1}-1)=1$，$\gcd(f(x),x^{q^{n_2}-1}-1)=1$。即需证明：条件（1′），（2′），（3′）与条件（1），(2)，(3) 等价。（必要性） 注意到 $n_i(i=1,2)$ 为素数即得。（充分性） 由（1），（2），（3）知 $f(x)$ 没有一次因式，只能有 n_1、n_2 或 n 次不可约因式。而事实上 $f(x)$ 并不含有 n_1（或 n_2）次的不可约多项式。否则，设 $f(x)$ 是由 k 个 n_1 次和 l 个 n_2 次不可约多项式构成，则有二元一次不定方程：$n=kn_1+ln_2$，解出其所有正整数解为：$k=n_2,l=0$ 和 $k=0,l=n_1$，均与条件（3）矛盾，因此 $f(x)$ 不含 n_1（或 n_2）次的不可约多项式，从而 $\gcd(f(x),x^{q^{n_i-1}}-1)=1$ $(i=1,2)$。

文［11］所给出的算法即为上述推论。判断素数次或素数乘积次的多项式 $f(x)$ 是否可约至多需要3次形如 $x^{q^n-1}\bmod f(x)$ 的值是否为1来确定。故只需进行 $O(n^3)$ 次 F_q 上的乘法运算。

定义2 设 $f(x)$ 是 $F_q[x]$ 上 n 次不可约多项式，如果满足 $f(x)\mid x^l-1$ 的最小正整数为 q^n-1，则称 $f(x)$ 为 $F_q[x]$ 上的本原多项式。

定理3 F_q 上的 $n(\geq 2)$ 次多项式 $f(x)$ 为本原多项式的充要条件是：

（1）$f(x)\mid x^{q^n-1}-1$；

（2）对任意 $c\in F_q$，$f(c)\neq 0$；

（3）对任意 $n_i\in M$，均有 $\gcd(x^{q^{n_i-1}}-1,f(x))=1$；

（4）对 q^n-1 的任意因子 t（t 大于1），均有 $f(x)\nmid x^{\frac{q^n-1}{t}}-1$。

证明 必要性显然，下证充分性。

由定理2，知 $f(x)$ 为不可约多项式。（反证）设存在 t_0，$0<t_0<q^n-1$，使得 $f(x)\mid(x^{t_0}-1)$。因 $f(x)\mid x^{q^n-1}-1$，从而 $f(x)\mid\gcd(x^{q^n-1}-1,x^{t_0}-1)=x^{\gcd(q^n-1,t_0)}-1$，设 $d=\gcd(q^n-1,t_0)$ 及 $\frac{q^n-1}{d}$ 的素因子为 r，则 r 也为 q^n-1 的素因子，因此存在正整数 h，使得 $\frac{q^n-1}{d}=rh$，也即 $\frac{q^n-1}{r}=dh$。那么由上述 $f(x)\mid x^d-1$，可得 $f(x)\mid x^{dh}-1$，也即 $f(x)\mid x^{\frac{q^n-1}{r}}-1$，与条件（4）矛盾。故对任意的 t，$0<t<q^n-1$，均有 $f(x)\nmid x^t-1$，即 $f(x)$ 为本原

多项式。

2　结　语

不可约多项式及本原多项式在密码和编码中有重要的应用。本文对任意正整数 n，给出了判定 n 次多项式为不可约多项式及本原多项式的一种实用、高效的确定性算法，该算法仅需做 $O((\log_2 n)n^3)$ 次 F_q 上乘法，属于多项式时间算法，易于硬件实现。

参考文献：

[1] 肖国镇. 伪随机序列及其应用 [M]. 北京：国防工业出版社，1985.

[2] 万哲先. 代数和编码 [M]. 北京：科学出版社，1980.

[3] UDAR S, KAGARIS D. LFSR reseeding with irreducible polynomials [C]. 13th IEEE International Online Testing Symposium, IEEE Computer Society, 2007, 293 - 297.

[4] IMANA J L, HERMIDA R, TIRADO F. Low complexity bit-parallel multipliers based on a class of irreducible pentanomials [J]. IEEE Transactions on VLSI Systems, 2006, 14 (12): 1388 - 1393.

[5] MCELIECE R J. Finite field for computer scientists and engineers [M]. Boston: Kluwer Academic Publisher, 1987.

[6] 裴定一，祝跃飞. 算法数论 [M]. 北京：科学出版社，2002.

[7] SHPARLINSKI I. Finding irreducible and primitive polynomials [J]. Appl Alg Eng Comm Comp, 1993 (4): 263 - 268.

[8] RIFA J, BORRELL J. A fast algorithm to compute irreducible and primitive polynomials in finite fields [J]. Math Systems Theory, 1995 (28): 13 - 20.

[9] 郭宝安，蔡长年. 有限域上的不可约多项式 [J]. 北京邮电大学学报，1994, 17 (1): 23 - 26.
GUO B A, CAI C N. The irreducible polynomials over finite fields [J]. Journal of Beijing University of Posts and Telecommunications, 1994, 17 (1): 23 - 26.

[10] 曹涵，陈恭亮. 基于素性检验思想的不可约多项式判断[J]. 信息安全与通信保密，2006 (3): 73 - 74.
CAO H, CHEN G L. Test of irreducible polynomials based on primality test [J]. China Information Security, 2006 (3): 73 - 74.

[11] 王泽辉，方小洵. F_p 上不可约与本原多项式的高效确定算法[J]. 中山大学学报：自然科学版，2004, 43 (6): 89 - 92.
WANG Z H, FANG X X. Highly efficient deriving calculation method of irreducible polynomial and primitive polynomial over F_p [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43 (6): 89 - 92.

·简　讯·

本刊被评为首批中国精品科技期刊

最近，中国科技信息研究所在北京举办的年度信息发布会公布了中国精品科技期刊遴选结果，《中山大学学报自然科学版》被评定为首批中国精品科技期刊。

中国精品科技期刊是由国家科技部通过立项推进“中国精品科技期刊战略研究”等课题，为提升中国科技期刊的整体水平，增强国际竞争力，建设精品科技期刊数据库平台，加强我国科技期刊的资源建设，促进科技期刊的可持续发展而推出的重要举措。

该研究项目由两位院士牵头，成员来自国家科技部、新闻出版总署、中宣部、卫生部、中国科协、国家自然科学基金委、教育部等管理部门及其相关专家。遴选指标由定量指标和定性指标两部分组成，定量指标为主，定性指标为辅。定量指标主要包括学术质量水平指标和国际竞争力水平指标，定性指标主要是指期刊的可持续发展潜力指标。

首批精品科技期刊由 23 种中国国际化精品科技期刊（英文版）和 300 种中国精品科技期刊组成。

（本刊通讯员）