中国科学: 数学 2010 年 第 40 卷 第 5 期: 447～456
www.springerlink.com math.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

有限域上与仿射多项式有关的一些多项式的可约性

曹喜望*, 赵正俊

南京航空航天大学数学系, 南京 211100
E-mail: xwcao@nuaa.edu.cn

收稿日期: 2008-07-21; 接受日期: 2009-11-10; * 通信作者
国家自然科学基金 (批准号: 10971250, 10771100) 资助项目

摘要 在这篇文章中, 研究了有限域上一些与仿射多项式有关的多项式的可约性. 对于有限域 $\mathbf{F}_p$ 上不是 $x^{p^{p^t}}-x-1$ 的仿射三项式, 得到了这些三项式的一个明确的因式. 完全确定了多项式 $g(x^{p^s}-ax-b)$ 在 $\mathbf{F}_p[x]$ 中的分解, 这里 $g(x)$ 是 $\mathbf{F}_p[x]$ 中一个不可约多项式. 证明了 $\mathbf{F}_p$ 上次数相同的不可约多项式的全体可以构成一个正则图. 同时给出了多项式 $g(x^{q^s}-x-b)$ 在 $\mathbf{F}_p[x]$ 不可约因式的个数公式, 这里 $g(x)$ 是 $\mathbf{F}_p$ 上一个不可约多项式.

关键词 有限域 仿射多项式 三项式

MSC (2000) 主题分类 11T06

1 引言

设 $\mathbf{F}_q$ 是 q 个元素的有限域, q 是素数幂. 在多项式环 $\mathbf{F}_q[x]$ 中, 形如 $A(x)=\sum_{i=0}^{m-1}a_ix^{q^i}+a$ 的多项式称为一个仿射多项式. 在这篇文章中, 我们讨论有限域上与仿射多项式有关的多项式的可约性. 首先, 我们考虑三项式. 一个三项式是指只含三个单项式的多项式. 有限域上的三项式有很多应用. 在编码学中, 三项式在表示有限域上的离散对数和幂的计算上具有高效性 [1]. 三项式也用来构造和刻画一些完全非线性函数 [2]. 三项式同时也与三重码和一些循环码的最小距离等有关 [3]. 三项式也可以产生一些具有特殊性质的序列 [4].

在这里我们考虑仿射三项式. 对于有限域 $\mathbf{F}_p$ (p 是素数) 上的一个仿射三项式, 只要不是 $x^{p^{p^t}}-x-b$, 我们得到了它的一个明确的因式. 同时我们证明了 $x^{p^{p^t}}-x-b$ 一定分解为一些次数为 p^{t+1} 的不可约多项式的乘积. 利用 Lidl[5] 的一个结果, 我们可以完全确定 $g(x^{p^s}-ax-b)$ 在 $\mathbf{F}_p[x]$ 中的分解, 这里 $g(x)$ 是 $\mathbf{F}_p$ 上一个不可约多项式, a 是 $\mathbf{F}_p$ 的一个本原元 (即 $\mathbf{F}_p$ 的乘法群的生成元), $b\in\mathbf{F}_p^*=\mathbf{F}_p-\{0\}$. 我们同时给出了有限域上具有相同次数的不可约多项式的一些有趣的组合性质. 利用这些性质, 我们给出了有限域上迹给定的不可约多项式的计数公式的一个不同的证明.

本文所考虑的多项式都是首 1 多项式.

2 $\mathbf{F}_p$ 上仿射三项式的可约性

现在我们考虑有限域 $\mathbf{F}_p$ 上的三项式, 这里 p 是一个素数.

引用格式: Cao X W, Zhao Z J. On the reducibility of some polynomials over finite fields with affine polynomials involved (in Chinese). Sci Sin Math, 2010, 40(5): 447–456

首先, 对于一个三项式 $x^{p^s}+ax+b\in\mathbf{F}_p[x]$. 如果 $a\neq -1$, 则 $x=-\frac{b}{1+a}\in\mathbf{F}_p$ 是 $x^{p^s}+ax+b$ 的一个根. 所以 $x^{p^s}+ax+b$ 在 $\mathbf{F}_p$ 上是可约的. 所以在后文中, 我们考虑形如 $x^{p^s}-x+b\in\mathbf{F}_p[x]$ 的三项式. 我们有下面的性质:

性质 2.1 如果 s 是一个正整数满足 $s\not\equiv 0 \bmod p$, 则 x^p-x-s^{-1} 在 $\mathbf{F}_p[x]$ 上整除 $x^{p^s}-x-1$, 这里我们将 $\mathbf{F}_p$ 等同于 $\{0,1,2,\ldots,p-1\}$.

证明 由文献 [5, 推论 3.79] 知, x^p-x-s^{-1} 在 $\mathbf{F}_p$ 上不可约, 令 ξ 是 x^p-x-s^{-1} 在 $\mathbf{F}_p$ 的扩域中的一个根. 则用归纳法可以证明 $\xi^{p^k}=\xi+ks^{-1}$ 对任意正整数成立. 于是 $\xi^{p^s}=\xi+1$, 从而 x^p-x-s^{-1} 整除 $x^{p^s}-x-1$.

下面的引理是 Daykin[6] 的一个结果的推论, 它刻画了 $x^{p^s}-x-b$ 的不可约因式的次数.

引理 2.2[6] 如果 p 是一个素数, 则 $x^{p^s}-x-b\,(b\in\mathbf{F}_p^*)$ 在 $\mathbf{F}_p[x]$ 上的每一个不可约因式的次数整除 ps.

这样, 我们有下面的推论:

推论 2.3 如果 p 是一个奇素数, 则仿射多项式 $x^{p^s}-x-b\,(b\in\mathbf{F}_p^*)$ 在 $\mathbf{F}_p$ 上是不可约的当且仅当 $s=1$.

证明 充分性显然.

反之, 如果 $x^{p^s}-x-b\,(b\in\mathbf{F}_p^*)$ 是不可约的, 则由引理 2.2 有 $p^s|ps$ 从而 $s=1$.

注意当 $p=2$ 时, 由 Swan 的一个著名的结果 [7], 在 $\mathbf{F}_2$ 上的不可约的仿射三项式只有 x^2+x+1, x^4+x+1.

推论 2.4 如果 p 是一个素数, s 是一个正整数满足 $s\equiv p^t \bmod p^{t+1}$, 则 $x^{p^{p^t}}-x-b\,(b\in\mathbf{F}_p^*)$ 在 $\mathbf{F}_p[x]$ 上整除 $x^{p^s}-x-b$.

证明 设 $s=p^{t+1}s_1+p^t$. 如果 $s_1=0$, 结论显然. 注意到

$$x^{p^{p^{t+1}s_1+p^t}}-x-b-(x^{p^{p^t}}-x-b)=(x^{p^{p^{t+1}s_1}}-x)^{p^{p^t}}. \tag{1}$$

令 $w(x)$ 是 $x^{p^{p^t}}-x-b$ 在 $\mathbf{F}_p[x]$ 次数为 m 的一个不可约因式. 由引理 2.2 知, m 整除 p^{t+1}, 从而整除 $p^{t+1}s_1$. 这样 $w(x)$ 整除 $x^{p^{p^{t+1}s_1}}-x$.

性质 2.5 $x^{p^{p^t}}-x-b\,(b\in\mathbf{F}_p^*)$ 分解为 p^{p^t-t-1} 个次数为 p^{t+1} 的不可约因式的乘积.

证明 因为 $x^{p^{p^t}}-x-b$ 的每一个不可约因式的次数整除 p^{t+1}, $x^{p^{p^t}}-x-b$ 在 $\mathbf{F}_{p^{p^{t+1}}}$ 中分裂. 如果 $v(x)$ 是 $x^{p^{p^t}}-x-b$ 的一个不可约因式, 次数为 p^v, $v\leqslant t$. 令 ξ_0 为 $v(x)$ 在 $\mathbf{F}_p$ 的某扩域中的一个根. 则 $\xi_0^{p^{p^v}}=\xi_0$. 于是 $\xi_0^{p^{p^{v+1}}}=(\xi_0^{p^{p^v}})^{(p^{p^v})^{p-1}}=\xi_0$. 由归纳法可以证明 $\xi_0^{p^{p^t}}=\xi_0$, 这与 $\xi_0^{p^{p^t}}=\xi_0+b$ 矛盾. 于是 $x^{p^{p^t}}-x-b$ 的每一个不可约因式的次数等于 p^{t+1}.

下面的性质刻画了多项式 $x^{p^s}-x-b\in\mathbf{F}_p[x]$ 的分裂域.

性质 2.6 对于每个正整数 s 和素数 p, $b\in\mathbf{F}_p^*$, $x^{p^s}-x-b$ 的分裂域为 $\mathbf{F}_{p^{ps}}$.

为了证明这个性质, 我们引用下面的引理.

引理 2.7[5,第121页,定理3.80] 设 $b\neq 0$ 是 $\mathbf{F}_q$ 的一个子域 $\mathbf{F}_r$ 的一个元素, 则在 $\mathbf{F}_q[x]$ 中有下面的分解

$$x^q-x-b=\prod_{j=1}^{q/r}(x^r-x-\beta_j). \tag{2}$$

这里 $\beta_j\,(j=1,2,\ldots,q/r)$ 是 $\mathbf{F}_q$ 中满足 $\mathrm{Tr}_{F/K}(\beta_j)=b$ 的不同的元素.

现在我们给出性质 2.6 的证明.

证明 由假设有 $r=p, q=p^s$, 且

$$x^{p^s}-x-b=\prod_{j=1}^{p^{s-1}}(x^p-x-\beta_j), \tag{3}$$

这里 $\beta_j\in\mathbf{F}_{p^s}$ 满足 $\mathrm{Tr}_{F/K}(\beta_j)=b\neq 0$. 令 α 是 $x^{p^s}-x-b$ 在 $\mathbf{F}_p$ 的某扩域中的一个根. 则存在 β_j 满足 $\alpha^p-\alpha-\beta_j=0$. 易知 $x^p-x-\beta_j$ 在 $\mathbf{F}_{p^s}$ 是不可约的 (参见文献 [5, 推论 3.79]). 于是 $x^p-x-\beta_j=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\cdots(x-\alpha^{q^{p-1}})$ 并且 $x^p-x-\beta_j$ 的每个根是 α 的一个共轭元. 而 α 是 $x^p-x-\beta_j$ 的根当且仅当 α^p 是 $x^p-x-\beta_j^p$ 的一个根. 因为 $x^p-x-\beta_j^{p^k}$ 和 $x^p-x-\beta_j^{p^l}$ 互素, 对每一对非负整数 $k,l,k\neq l \bmod u_j$, 这里 u_j 是 β_j 的阶, α 在 $\mathbf{F}_p$ 上的最小多项式在 Frobenius 同构 $\alpha\mapsto\alpha^p$ 下是不变的. 于是 $x^{p^s}-x-b$ 在 $\mathbf{F}_p$ 的每一个不可约因式有下列形式

$$M_{\beta_j}(x)=(x^p-x-\beta_j)(x^p-x-\beta_j^p)\cdots(x^p-x-\beta_j^{p^{u_j-1}}),$$

这里 $\beta_j,\beta_j^p,\ldots,\beta_j^{p^{u_j-1}}$ 是 β_j 的共轭元. 由引理 2.2 知 $u_j|s$. 我们必须指出: 存在一个 u_j 等于 s. 由文献 [8], 存在一个元素 $\beta_j\in\mathbf{F}_{p^s}$ 使得 β_j 是 $\mathbf{F}_{p^s}$ 的一个本原元, 并且这个本原元的迹可以任意给定. 于是 β_j 的共轭元共有 s 个. 这样, 存在 $x^{p^s}-x-b$ 的一个不可约因式次数为 ps, 并且每一个不可约因式的次数整除 ps. 结论得证.

注 1 一般来讲, 性质 2.6 对于 $q=p^m(m>1)$ 的情况是不对的. 我们只能得到 $x^{q^s}-x-b\in\mathbf{F}_q[x]$ 在 $\mathbf{F}_{q^{qs}}$ 分裂.

由性质 2.6 的证明, 我们定义记号

$$N(u,b;s)=\sharp\{\beta\in\mathbf{F}_{p^s}|\mathrm{Tr}_p^{p^s}(\beta)=b,\ \beta\text{ 的共轭类中恰有 }u\text{ 个元素}\},$$

这里 $\mathrm{Tr}_p^{p^s}$ 表示 $\mathbf{F}_{p^s}$ 到 $\mathbf{F}_p$ 的迹映射. 即: $\mathrm{Tr}_p^{p^s}(x)=x+x^p+x^{p^2}+\cdots+x^{p^{s-1}}$.

事实上, $N(u,b;s)/u$ 是形如 $x^u+bx^{u-1}+a_{u-2}x^{u-2}+\cdots+a_1x+a_0\in\mathbf{F}_p[x]$ 的不可约多项式的个数.

由这个记号和性质 2.5 的结果有:

推论 2.8 (1) 对每一个正整数 s 和素数 p, 设 $b\in\mathbf{F}_p^*$. 则 $x^{p^s}-x-b$ 在 $\mathbf{F}_p[x]$ 分解为次数为 pu 的不可约多项式的乘积, 这里 u 是 $\beta\in\mathbf{F}_{p^s}$ 的共轭类中 $\mathrm{Tr}_p^{p^s}(\beta)=b$ 满足的元素个数. 并且次数为 pu 的不可约因式的个数为 $N(u,b;s)/u$.

(2) $N(p^t,b;p^t)=p^{p^t-1}$.

注 2 (1) 文献 [8] 中的一个主要结果是 $N(s,b;s)>0$.

(2) 用文献 [8] 中同样的方法, 可以证明当 $u|s$ 时, $N(u,b;s)>0$.

下面给出一个例子说明可以用上面的结果来分解三项式.

例 2.9 令 β 是 $\mathbf{F}_{3^3}$ 中满足 $\beta^3-\beta+1=0$ 的一个本原元. 为方便读者, 我们列出 $\mathbf{F}_{27}$ 中元素的迹如下表 (表 1).

定义集合 $T_1=\{i|\mathrm{Tr}(\beta^i)=1,\beta\in\mathbf{F}_{27},0\leqslant i\leqslant 25\}$. 易知 $T_1=\{5,8,15,17,19,20,23,24,25\}=\{5,15,19\}\cup\{8,24,20\}\cup\{17,23,25\}$. 于是, $N(3,1;3)=9$, 并且 $x^{27}-x-1$ 分解为 3 个次数为 9 的不可约多项式的乘积. $x^{27}-x-1$ 的分裂域为 $\mathbf{F}_{3^9}$. 事实上, 令

$$M_{\beta^5}(x)=(x^3-x-\beta^5)(x^3-x-\beta^{15})(x^3-x-\beta^{19})=1+2x+2x^2+2x^4+2x^6+x^9,$$
$$M_{\beta^8}(x)=(x^3-x-\beta^8)(x^3-x-\beta^{24})(x^3-x-\beta^{20})=2+x+2x^2+x^3+2x^4+2x^6+x^9,$$

表 1 F_{27}^* 中元素的迹

i	β^i	Tr	i	β^i	Tr	i	β^i	Tr	i	β^i	Tr	i	β^i	Tr
0	100	0	1	010	0	2	001	2	3	210	0	4	021	2
5	212	1	6	111	2	7	221	2	8	202	1	9	110	0
10	011	2	11	211	2	12	201	2	13	200	0	14	020	0
15	002	1	16	120	0	17	012	1	18	121	2	19	222	1
20	112	1	21	101	2	22	220	0	23	022	1	24	122	1
25	102	1												

$$M_{\beta^{17}}(x) = (x^3 - x - \beta^{17})(x^3 - x - \beta^{23})(x^3 - x - \beta^{25}) = 1 + 2x^2 + 2x^3 + 2x^4 + 2x^6 + x^9.$$

则有

$$\begin{aligned} x^{27} - x - 1 &= M_{\beta^5}((x)M_{\beta^8}(x)M_{\beta^{17}}(x) \\ &= (1 + 2x + 2x^2 + 2x^4 + 2x^6 + x^9)(2 + x + 2x^2 + x^3 + 2x^4 + 2x^6 + x^9) \\ &\quad \times (1 + 2x^2 + 2x^3 + 2x^4 + 2x^6 + x^9). \end{aligned}$$

当然, 人们可以用 Berlekamp 算法 (见文献 [5], 第 136 页) 来分解 $x^{27} - x - 1$. 这个算法需要解一个有 27 个未知量的线性方程组, 并且求一个 27 阶矩阵的 3- 秩. 显然, Berlekamp 算法没有本文给出的方法简单.

注 3 由推论 2.4, 只要 s 不是素数 p 的幂, 则容易求出 $x^{p^s} - x - 1$ 的一个因式. 例如, 如果 $p = 2$, $s = 68 = 2^6 + 4$, 则 $x^{2^{68}} - x - 1$ 有因式 $x^{2^4} - x - 1$. 如果 $p = 5, s = 628 = 5^4 + 3$, 则 $x^{5^{628}} - x - 1$ 有因式 $x^{5^3} - x - 1$.

3 仿射三项式与不可约多项式的复合多项式的可约性

在这一节, 我们考虑仿射三项式与不可约多项式的复合多项式的可约性. 设 $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbf{F}_q[x]$ 是一个不可约多项式, 这里 q 是素数 p 的幂. 设 $b \in \mathbf{F}_q$. 在文献 [5] 中证明了 $g(x^p - x - b)$ 在 $\mathbf{F}_q[x]$ 中不可约当且仅当 $\mathrm{Tr}_p^q(mb - a_{m-1}) \neq 0$(参见文献 [5], 第 121 页, 定理 3.82). 于是, 人们自然要问当 $\mathrm{Tr}_p^q(mb - a_{m-1}) = 0$ 时情况如何? 下面的定理回答了这个问题:

定理 3.1 设 $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbf{F}_q[x]$ 是次数大于 1 的一个不可约多项式, q 是素数 p 的幂. 设 $b \in \mathbf{F}_q$ 满足 $\mathrm{Tr}_p^q(mb - a_{m-1}) = 0$. 则有下列结果:

(1) $g(x^p - x - b)$ 在 $\mathbf{F}_q[x]$ 中分解为次数为 m 的 p 个不可约多项式的乘积;

(2) 如果 $\gcd(m, p) = 1$, 则 $g(x^p - x - b)$ 在 $\mathbf{F}_q[x]$ 中的 p 个不可约因式的次项系数 (即 x^{m-1} 的系数) 是不同的;

(3) 如果 $p|m$, 则 $g(x^p - x - b)$ 在 $\mathbf{F}_q[x]$ 中的 p 个不可约因式的次项系数 (即 x^{m-1} 的系数) 是相同的;

(4) 如果 $g(x^p - x - b)$ 分解为 $\theta_0(x)\theta_1(x)\cdots\theta_{p-1}(x), \deg(\theta_i(x)) = m$, 则

$$\theta_0(x^p - x - b) = \theta_1(x^p - x - b) = \cdots = \theta_{p-1}(x^p - x - b).$$

证明 设 $\alpha \in \mathbf{F}_{q^m}$ 是 $g(x)=0$ 的一个根. 则 $g(x)=\prod_{i=0}^{m-1}(x-\alpha^{q^i})$, 并且

$$g(x^p-x-b)=\prod_{i=0}^{m-1}(x^p-x-b-\alpha^{q^i}), \tag{4}$$

记 $x^p-x-b-\alpha$ 为 $a(x)$. 因为 $\mathrm{Tr}_q^{q^m}(b+\alpha)=mb-a_{m-1}=0$, 由迹映射的传递性有 $\mathrm{Tr}_p^{q^m}(b+\alpha)=\mathrm{Tr}_p^q\left(\mathrm{Tr}_q^{q^m}(b+\alpha)\right)=0$. 设 γ 是 $a(x)=0$ 在 $\mathbf{F}_q$ 的某扩域中的一个根, 则 $a(x)=0$ 的 p 个根为 $\gamma+k, k=0,1,\ldots,p-1$. 进一步, 因为 $\alpha=\gamma^p-\gamma-b\notin\mathbf{F}_q$, 得知 $\gamma\notin\mathbf{F}_q$. 因有 $[\mathbf{F}_q(\alpha):\mathbf{F}_q]=m$, 及 $\mathbf{F}_q(\alpha)\subseteq\mathbf{F}_q(\gamma)$. 于是 $[\mathbf{F}_q(\gamma):\mathbf{F}_q]$ 是 m 的倍数.

设 $q=p^s$, 则

$$\begin{aligned}\gamma^{q^m}-\gamma&=(\gamma^p-\gamma)+(\gamma^p-\gamma)^p+\cdots+(\gamma^p-\gamma)^{p^{ms-1}}\\&=(b+\alpha)+(b+\alpha)^p+\cdots+(b+\alpha)^{p^{ms-1}}\\&=\mathrm{Tr}_p^{q^m}(b+\alpha)=0.\end{aligned}$$

于是 $\gamma\in\mathbf{F}_{q^m}$ 并且 $\mathbf{F}_q(\alpha)=\mathbf{F}_q(\gamma)$. 所以 $a(x)$ 在 $\mathbf{F}_{q^m}$ 中分裂.

因为 $\gamma^{q^i}+k\,(k=0,1,\ldots,p-1)$ 是 $x^p-x-b-\alpha^{q^i}=0$ 的根, 由 (4) 式可知

$$g(x^p-x-b)=\prod_{i=0}^{m-1}\prod_{k=0}^{p-1}(x-\gamma^{q^i}-k)=\prod_{k=0}^{p-1}\left(\prod_{i=0}^{m-1}(x-\gamma^{q^i}-k)\right), \tag{5}$$

记 $v_k(x)=\prod_{i=0}^{m-1}(x-\gamma^{q^i}-k)$. 易知 $v_k(x)$ 是 $\gamma+k$ 在 $\mathbf{F}_q[x]$ 中的最小多项式, 所以它在 $\mathbf{F}_q[x]$ 不可约. 所以 $g(x^p-x-b)$ 在 $\mathbf{F}_q[x]$ 中分解为 p 个次数为 m 的不可约多项式的乘积. 这就证明了 (1) 式成立.

进一步, 设 $\gcd(m,p)=1$. 因为 $v_k(x)$ 中 x^{m-1} 的系数为 $\mathrm{Tr}(\gamma+k)=mk+\mathrm{Tr}(\gamma)$, 而 $mk+\mathrm{Tr}(\gamma)=ml+\mathrm{Tr}(\gamma)$ 当且仅当 $k=l$, 这就得到 (2) 式.

如果 $p|m$, 则 $v_k(x)$ 中 x^{m-1} 的系数为 $\mathrm{Tr}(\gamma+k)=mk+\mathrm{Tr}(\gamma)=\mathrm{Tr}(\gamma)$.

最后, 由 (1) 的证明, 可以设 $\theta_k(x)=v_k(x), k=0,1,\ldots,p-1$. 记 $\gamma+k$ 为 η_k, 于是 $v_k(x)=\prod_{i=0}^{m-1}(x-\eta_k^{p^i})$. 从而

$$\theta_k(x^p-x-b)=\prod_{i=0}^{m-1}(x^p-x-b-\eta_k^{p^i})=\prod_{i=0}^{m-1}(x^p-x-b-\gamma^{p^i}-k),$$

重复 (1) 的证明可得 (4). 证毕.

在文献 [9] 中, Agou 得到了 $f(x^{p^s}-ax)$ 的不可约因式的个数. 在文献 [10] 中, Long 也得到了 $f(x^{q^s}-x)$ 在 $\mathbf{F}_q$ 中不可约因式的个数. 但是注意对于任意两个多项式 $f_1(x), f_2(x)$, 由 $f_1(f_2(x))$ 的分解一般不能给出 $f_1(f_2(x)-a)$ 的分解. 尽管我们知道 $f(x)$ 的分解式可以确定 $f(x-a)$ 的分解式. 所以 [9,10] 的结果并没有覆盖本文的结果.

为完整起见, 我们给出两个定理, 这两个定理的证明与定理 3.1 的证明是类似的, 所以省略了证明.

记

$$N(n,q)=\sum_{d|n}\mu(d)q^{n/d}, \tag{6}$$

这里 μ 是 Möbius 函数, 则有

定理 3.2 设 $f(x)=x^r+a_{r-1}x^{r-1}+\cdots+a_1x+a_0\in\mathbf{F}_q[x]$ 是一个次数大于 1 的不可约多项式, q 是素数 p 的幂. 设 s 是一个正整数. 记 $\gcd(r,s)=d$, $\frac{s}{d}=s_1$, $\frac{r}{d}=r_1$, 设 $b\in\mathbf{F}_q{}^*$. 如果 $\mathrm{Tr}_{q^d}^{q^s}(b+\alpha)=0$,

表 2　$g(x^5-x-1)$ 的分解

1304	1323	1311	1343	1302	1322	1312	1341
1043	1032	1011	1024	1042	1033	1014	1021
1114	1101	1131	1141	1113	1102	1134	1143
1223	1213	1244	1201	1222	1214	1242	1203
1323	1311	1343	1302	1322	1312	1341	1304
1412	1403	1431	1442	1411	1404	1434	1444

注: 符号串 "$1\lambda\mu\nu$" 表示多项式 $x^3+\lambda x^2+\mu x+\nu$

这里 α 是 $f(x)$ 在 $\mathbf{F}_q$ 的某扩域中的一个根, 则 $f(x^{q^s}-x-b)$ 是一些次数为 st 的不可约多项式的乘积, 这里 $t\mid r_1$. 对每个 $t\mid r_1$, 次数为 st 的不可约因式的个数是 $\sum_{v|d,(t,\frac{d}{v})=1}N(vt,q)/t$.

定理 3.3　设 $f(x)=x^r+a_{r-1}x^{r-1}+\cdots+a_1x+a_0\in\mathbf{F}_q[x]$ 是一个次数大于 1 的不可约多项式, q 是素数 p 的幂. 设 s 是一个正整数. 记 $\gcd(r,s)=d$, $\frac{s}{d}=s_1$, $\frac{r}{d}=r_1$, 设 $b\in\mathbf{F}_q{}^*$. 如果 $\mathrm{Tr}_{q^d}^{q^s}(b+\alpha)\neq 0$, 这里 α 是 $f(x)$ 在 $\mathbf{F}_q$ 的某扩域中的一个根, 设 $r_1=p^kl$, $(p,l)=1$, $k\geqslant 0$. 则 $f(x^{q^s}-x-b)$ 是一些次数为 $p^{k+1}st$ 的不可约因式的乘积, 这里 $t\mid l$. 并且对每个 $t\mid l$, 次数为 $p^{k+1}st$ 的不可约因式的个数为 $\sum_{v|p^kd,(t,\frac{p^kd}{v})=1}N(vt,q)/p^{k+1}t$.

下面的例子说明不可约多项式具有一些有趣的组合性质.

例 3.4　设 $m=3$, $p=5$. 令 $b=1$. 多项式 $g(x^5-x-1)$ 的分解列在表 2 中. 第一行是 $\mathbf{F}_5$ 上次数为 3 的一些不可约多项式, 并且它们的次高次项的系数为 3. 每一列从第二行到第四行的 4 个多项式恰为 $g(x^5-x-1)$ 的因式, 这里 $g(x)$ 为该列的第一个多项式.

易知所有次数为 3 的 (首 1) 不可约多项式都含在表 2 中. 即对每一个次数为 3 的不可约多项式, 设为 $m(x)$, 有一个 3 次不可约多项式 $g(x)$ 使得 $g(x^5-x-1)$ 是 $m(x)$ 的倍式. 这样可以构造一个有向图 $\mathscr{G}=(\mathscr{V},\mathscr{E})$,

$$\mathscr{V}=\{g(x)\in\mathbf{F}_5[x]|\deg(g)=3,\text{和 } g(x)\text{ 在 }\mathbf{F}_5[x]\text{ 中不可约}\},$$
$$\mathscr{E}=\{(g(x),m(x))\in\mathscr{V}^2|\text{如果存在 } b\in\mathbf{F}_5 \text{ 使得 } m(x)|g(x^5-x-b)\}.$$

因为 $\mathscr{G}$ 的每一个点的出次和入次都是 5, $\mathscr{G}$ 是一个正则有向图. 如果有一条边从 $g(x)$ 连向 $m(x)$, 称 $g(x)$ 为 $m(x)$ 的父辈, $m(x)$ 为 $G(x)$ 的儿子. 此时 $m(x)$ 的儿子称为 $g(x)$ 的孙子. 显然, 每一个多项式都有 5 个父辈, 5 个儿子. 有趣的是, 由定理 3.1, 如果 $m_1(x),m_2(x),\ldots,m_5(x)$ 是 $g(x)$ 的 5 个儿子, 则 $m_i(x), i=1,2,\ldots,5$ 有共同的 5 个儿子. 这种关系由图 1 所示. 易知图 $\mathscr{G}$ 是一个强连通有向图. 这种图可以用来构造电力网络, 见 [11, 第 36 页].

上面的例子表明, 当 $q=p$ 是一个素数并且 $\gcd(m,p)=1$ 时, $\mathbf{F}_p[x]$ 中次数为 m 的不可约多项式的个数是 p 的倍数, 并且给定次数 (为 m) 的不可约多项式全体对迹而言是等分布的. 下面我们利用定理 3.1 来证明这个结论具有一般性.

用 $N_q(m)$ 记 $\mathbf{F}_q[x]$ 中次数为 m 的不可约多项式的个数. 孰知 (参见文献 [5, 第 86 页])

$$N_q(m)=\frac{1}{m}\sum_{d|m}\mu(d)q^{m/d},$$

这里 $\mu(d)$ 是 Möbius 函数.

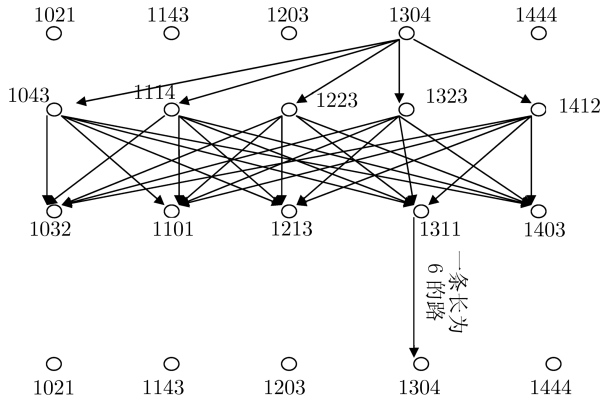

图 1 图的关系

推论 3.5 对于给定的元素 $a \in \mathbf{F}_q$ 和给定的正整数 $m > 1$, 记

$$I_q(m,a) = \{g(x) \in \mathbf{F}_q[x] | g(x) = x^m + ax^{m-1} + \cdots + a_m \text{ 在 } \mathbf{F}_q[x] \text{ 中不可约}\},$$

即 $\mathbf{F}_q[x]$ 中给定迹给定次数的不可约多项式的个数. 则

(1) 当 $a, b \in \mathbf{F}_q^*$ 时, $\sharp I_q(m,a) = \sharp I_q(m,b)$.

(2) 如果 $\gcd(m,p) = 1$ 并且 $q = p$, 则 $\sharp I_q(m,a) = \frac{1}{q} N_q(m)$.

证明 (1) 首先, 由 Cohen[8] 的结果可知, $I_q(m,a)$ 是非空的, 即存在任意给定迹和给定次数的不可约多项式. 其次, 因为 $f(x)$ 不可约当且仅当 $f(ax)$ 不可约, 这里 $a \neq 0$. 这样 (1) 得证.

(2) 如果 $\gcd(m,p) = 1$ 并且 $q = p$, 则由定理 3.1 可知, 对任意 $g(x) \in I_q(m,0)$, 可以找到 $h(x) \in I_q(m,1)$, 不同的 $g(x)$ 给出不同的 $h(x)$. 所以 $\sharp I_q(m,0) \leqslant \sharp I_q(m,1)$. 反之亦然. 所以 $\sharp I_q(m,0) = \sharp I_q(m,1)$. 再由 (1) 以及 $\sum_{a \in \mathbf{F}_q} \sharp I_q(m,a) = N_q(m)$ 得 (2). □

下面的定理刻画了另一类仿射多项式与不可约多项式的复合多项式的分裂域.

定理 3.6 设 $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbf{F}_p[x]$ 是 $\mathbf{F}_p$ 上次数为 m 的一个不可约多项式, 设 $a, b \in \mathbf{F}_{p^m}$, $\mathbf{F}_{p^m}$ 是 $g(x)$ 的 m 次扩域, 它含有 $g(x)$ 的所有根. 设二项式 $x^{p^s-1} - a$ 在 $\mathbf{F}_{p^m}$ 上不可约. 则 $g(x^{p^s} - ax - b)$ 的分裂域是 $\mathbf{F}_{p^{m(p^s-1)}}$.

下面的引理可以用来判定二项式是否可约.

引理 3.7[12] 二项式 $x^t - a \in \mathbf{F}_q[x]$ 在 $\mathbf{F}_q$ 上可约当且仅当正整数 t 满足

(1) t 的每一个素因子整除 e 但不整除 $(q-1)/e$, 这里 e 是 a 在 $\mathbf{F}_q^*$ 中的阶; 并且

(2) 如果 $4|t$, 则 $4|(q-1)$.

下面给出定理 3.6 的证明.

证明 设 $q = p^m$, $\alpha \in \mathbf{F}_q$ 是 $g(x)$ 的一个根. 则 $g(x) = (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{m-1}})$.

于是

$$g(x^{p^s} - ax - b) = (x^{p^s} - ax - b - \alpha)(x^{p^s} - ax - b - \alpha^p)\cdots(x^{p^s} - ax - b - \alpha^{p^{m-1}}).$$

记 $x^{p^s} - ax - b - \alpha$ 为 $h(x)$. 利用文献 [5, 第 122 页, 定理 3.83], 知 $h(x)$ 是一个一次多项式和一个 $(p^s - 1)$ 次不可约多项式的乘积. 我们将要用到这个结果的证明, 所以我们将它引用在此. 因为 $h'(x) = -a \neq 0$, $h(x)$ 无重根. 注意到 $h(x)$ 是一个仿射多项式, $h(x)$ 的任意不同两根之差是 $x^{p^s} - ax$ 的根, 从而是 $x^{p^s-1} - a$ 的根. 由假设 $x^{p^s-1} - a$ 在 $\mathbf{F}_q$ 上不可约, 知道存在 $h(x)$ 的一个根 γ 不属于

$\mathbf{F}_q$. 这样 $\gamma^q\,(\neq\gamma)$ 也是 $h(x)$ 的一个根, 从而 $\gamma^q-\gamma$ 是 $x^{p^s-1}-a$ 的根, 这样 $[\mathbf{F}_q(\gamma^q-\gamma):\mathbf{F}_q]=p^s-1$. 因为 $\mathbf{F}_q(\gamma^q-\gamma)\subseteq\mathbf{F}_q(\gamma)$, 得到 $[\mathbf{F}_q(\gamma):\mathbf{F}_q]$ 是 (p^s-1) 的倍数. 另一方面, γ 是 $h(x)$ 的一个根, 并且 $[\mathbf{F}_q(\gamma):\mathbf{F}_q]\leqslant p^s$. 从而只有一种情形, 即 $[\mathbf{F}_q(\gamma):\mathbf{F}_q]=p^s-1$. 得到 $h(x)$ 分解为一个一次多项式和一个 (p^s-1) 次不可约多项式的乘积. 这样的推理同样适合于多项式 $x^{p^s}-ax-b-\alpha^{p^i}$. 于是 $[\mathbf{F}_q(\gamma'):\mathbf{F}_q]=p^s-1$, 这里 γ' 是 $x^{p^s}-ax-b-\alpha^{p^i}$ 的某个根. 于是 $g(x^{p^s}-ax-b)$ 的分裂域是 $\mathbf{F}_{p^{m(p^s-1)}}$. 证毕. □

我们有下列的推论.

推论 3.8 设 $g(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_0\in\mathbf{F}_p[x]$ 是一个 m 次不可约多项式, 并且 $\gcd(p-1,m)=1$. 设 $b\in\mathbf{F}_p^*$. 令 $a\in\mathbf{F}_p$ 是 $\mathbf{F}_p$ 的一个本原元. 则 $g(x^p-ax-b)\mathbf{F}_p[x]$ 中一个 m 次不可约多项式和一个 $m(p-1)$ 次不可约多项式的乘积.

证明 首先, 我们断言当 a 是 $\mathbf{F}_p$ 的一个本原元时, 二项式 $x^{p-1}-a$ 在 $\mathbf{F}_{p^m}$ 上不可约.

这是因为 a 在 $\mathbf{F}_{p^m}$ 中的阶是 $e=p-1$, 由引理 3.6, 只要证明 $t=p-1$ 与 $\frac{p^m-1}{p-1}$ 互素.

注意到

$$\begin{aligned}\gcd\left(p-1,\frac{p^m-1}{p-1}\right)&=\gcd(p-1,1+p+p^2+\cdots+p^{m-1})\\&=\gcd(p-1,1+(p-1+1)+(p-1+1)^2+\cdots+(p-1+1)^{m-1})\\&=\gcd(p-1,m)=1.\end{aligned}$$

由引理 3.7, $x^{p-1}-a$ 在 $\mathbf{F}_{p^m}$ 上不可约.

其次, 如果 $\alpha\in\mathbf{F}_{p^m}$ 是 $g(x)$ 的一个根, 则

$$g(x)=(x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{m-1}})$$

于是有

$$g(x^p-ax-b)=(x^p-ax-b-\alpha)(x^p-ax-b-\alpha^p)\cdots(x^p-ax-b-\alpha^{p^{m-1}}).\tag{7}$$

由定理 3.6 的证明, 知 $h(x)=x^p-ax-b-\alpha$ 在 $\mathbf{F}_{p^m}$ 上分解为一个一次因式和一次 $(p-1)$ 次不可约因式的乘积. 于是可以假设 $h(x)=(x-\zeta)u(x)$, 这里 $\zeta\in\mathbf{F}_{p^m}$, $u(x)$ 是 $\mathbf{F}_{p^m}[x]$ 上一个次数为 $(p-1)$ 的因式. 因为 ζ 是 $x^p-ax-b-\alpha$ 的根, 当且仅当 ζ^p 是 $x^p-ax-b-\alpha^p$ 的一个根, 所以

$$\begin{aligned}g(x^p-ax-b)&=(x^p-ax-b-\alpha)(x^p-ax-b-\alpha^p)\cdots(x^p-ax-b-\alpha^{p^{m-1}})\\&=(x-\zeta)(x-\zeta^p)\cdots(x-\zeta^{p^{m-1}})u_1(x)u_2(x)\cdots u_m(x),\end{aligned}$$

这里 $u_i(x)\in\mathbf{F}_{p^m}[x]$ $(i=1,2,\ldots,m)$ 是一个次数为 $(p-1)$ 的不可约多项式.

注意到对每对 $i,j,i\neq j$, $\gcd(x^p-ax-b-\alpha^{p^i},x^p-ax-b-\alpha^{p^j})=1$ 互素. 所以 $\zeta^{p^i}\neq\zeta^{p^j}$ 并且 $g_1(x)=(x-\zeta)(x-\zeta^p)\cdots(x-\zeta^{p^{m-1}})$ 在 $\mathbf{F}_p$ 上不可约.

最后, 我们证明 $g_2(x)=u_1(x)u_2(x)\cdots u_m(x)$ 是 $\mathbf{F}_p$ 上一个不可约多项式.

用 Frobenius 映射 ρ 到

$$g(x^p-ax-b)=g_1(x)g_2(x)\tag{8}$$

的两边, 有

$$g_1(x)g_2(x)=g(x^p-ax-b)=(g(x^p-ax-b))^\rho=(g_1(x))^\rho(g_2(x))^\rho=g_1(x)(g_2(x))^\rho,\tag{9}$$

于是 $(g_2(x))^\rho=g_2(x)$, 故 $g_2(x)\in\mathbf{F}_p[x]$.

表 3 $\mathbf{F}_5$ 上次数为 3 的不可约多项式

1404	1412	1442	1434	1403	1411	1444	1431
1134	1213	1113	1203	1131	1214	1114	1201
1242	1101	1222	1143	1244	1102	1223	1141
1304	1011	1312	1043	1302	1014	1311	1042
1343	1033	1323	1024	1341	1032	1322	1021

注: 符号串 "$1\lambda\mu\nu$" 表示多项式 $x^3+\lambda x^2+\mu x+\nu$

设 γ 是 $g_2(x)$ 在 $\mathbf{F}_p$ 的某个扩域中的根. 则存在 $u_j(x)$, 使得 $u_j(\gamma)=0$. 不失一般性, 设 $j=1$. 因为 $u_i(\gamma^{p^i})=0$, 多项式 $u_1(x)$ 和 $u_i(x)$ 有相同的分裂域. 由定理 3.6 得到 $g_2(x)$ 的分裂域是 $\mathbf{F}_{p^{m(p-1)}}$. 注意到 $\deg(g_2(x))=m(p-1)$. 从而 $g_2(x)$ 是 $\mathbf{F}_p$ 上一个不可约多项式. 证毕.

定义

$$I(m,p)=\{g(x)\in\mathbf{F}_p[x]|\deg(g(x))=m,\ \text{且 } g(x) \text{ 在 } \mathbf{F}_p[x] \text{ 中不可约}\}.$$

由推论 3.8, 对于每个 $g(x)\in I(m,p)$, $g(x^p-ax-b)$ 的分解将给出一个次数为 m 的不可与多项式, 记为 $g_1(x)$, 见 (9) 式. 这样可以定义一个映射

$$\tau(m;a,b):I(m,p)\to I(m,p);\quad g(x)\mapsto g_1(x).$$

易知 $\tau(m;a,b)$ 是单射从而是满射. 这样 $\tau(m;a,b)$ 诱导出 $I(m,p)$ 上的一个置换. 见下面的例子.

例 3.9 设 $m=3$, $p=5$. 则 $a=2$ 是 $\mathbf{F}_5$ 的一个本原元. 令 $b=1$. $\mathbf{F}_5$ 上次数为 3 的不可约多项式见表 3.

有趣的是对每个本原元 $a\in\mathbf{F}_5$, $b\in\mathbf{F}_5^*$, $\tau(3;a,b)^8=\mathrm{id}$, 即恒等置换. 表 3 的行是 $\tau(3;2,1)$ 作用在 $I(3,5)$ 上的轨道. 用 Maple 9.0 计算发现有 5 个次数为 3 的不可约多项式, 记为 g_0,g_1,g_2,g_3, g_4, 使得

$$I(3,5)=\bigcup_{j=0}^{4}\bigcup_{i=0}^{7}\tau(m;a,b)^i(g_j). \tag{10}$$

并且事实上

$$\begin{aligned}I(3,5)=&\Big(\bigcup_{i=0}^{7}\tau_{2,1}^i(1404)\Big)\cup\Big(\bigcup_{i=0}^{7}\tau_{2,1}^i(1134)\Big)\cup\Big(\bigcup_{i=0}^{7}\tau_{2,1}^i(1242)\Big)\\&\cup\Big(\bigcup_{i=0}^{7}\tau_{2,1}^i(1304)\Big)\cup\Big(\bigcup_{i=0}^{7}\tau_{2,1}^i(1343)\Big).\end{aligned}$$

由 (10) 式, 我们可以构造一个参数为 $(40,3774873600)$ 的纠错码. 符号集是 $I(3,5)$, 每一个形如 (9) 式的分解称为一个码字. 我们称 $\mathfrak{C}$ 为一个τ- 拟循环码. 关于这种码的性质的进一步研究将在另文中介绍.

4 结束语

在这篇文章中, 研究了一些仿射多项式的可约性. 如果 s,t 是正整数满足 $s\equiv p^t \bmod p^{t+1}$, 证明了 $x^{p^{p^t}}-x-b$ 整除 $x^{p^s}-x-b$. 同时完全确定了 $x^{p^s}-x-b\in\mathbf{F}_p[x]$ 的分裂域. 进一步, 如果 a 是 $\mathbf{F}_p$

的一个本原元, $b \in \mathbf{F}_p^*$, $g(x) \in \mathbf{F}_p[x]$ 是 $\mathbf{F}_p$ 上一个 m 次不可约多项式, 则可以完全确定 $g(x^p - ax - b)$ 在 $\mathbf{F}_p$ 上的分解, 这里 p 是一个素数. 利用这个分解, 可以定义 $\mathbf{F}_p$ 上次数为 m 的全体不可约多项式的集合上的一些变换. 得到了这些变换的一些有趣的组合性质. 同时利用这些结果, 给出了给定迹的不可约多项式的计数公式的一个不同的证明. 在本文的最后, 我们提出两个公开问题:

(1) 推广例 3.4 和例 3.9;

(2) 确定 $N(u, b; s)$.

致谢 感谢审稿人提出的修改意见.

参考文献

1 Schroeppel R, Orman H. O′Malley S. Fast key exchange with elliptic curve systems. In: Advances in Cryptology. Proceedings of Crypto'95. LNCS 963. Berlin-Heidelberg: Springer, 1995, 43–56

2 Carlet C, Charpin P, Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs Codes Crypto, 1998, 15: 125–156

3 Charpin P, Tietäväinen A, Zinoviev V A. On binary cyclic codes with minimum distance $d = 3$. Problems Inform Trans, 1997, 33: 287–296

4 Golomb S W, Gong G. Periodic binary sequences with the "trinomial property". IEEE Trans Inform Theory, 1999, 45: 1276–1279

5 Lidl R, Niederreiter H. Introduction to Finite Fields and Their Applications. Cambridge: Cambridge University Press, 1994

6 Daykin D E. The irreducible factors of $(cx+d)x^{q^n} - (ax+b)$ over $GF(q)$. Quart J Math Oxford Ser, 1963, 14: 61–64

7 Swan Richard G. Factorization of polynomials over finite fields. Pacific J Math, 1962, 12: 1099–1106

8 Cohen S D. Primitive elements and polynomials with arbitary trace. Discrete Math, 1990, 83: 1–7

9 Agou S. Factorisation sur un corps fini $\mathbf{F}_{p^n}$ des polynômes compsês $f(x^{p^r} - ax)$ lorsque $f(x)$ est un polynômes irréductible de $\mathbf{F}_{p^n}$. J Number Theory, 1977, 9: 229–239

10 Long A F. Factorization of irreducible polynomials over a finte field with substitution $x^{q^r} - x$ for x. Duke Math J, 1973, 40: 63–76

11 Chen W K. Applied Graph Theory, Graphs and Electrical Networks. Amsterdam: North-Holland Publishing Company, 1976

12 Menezes A J. Applications of Finite Fields. Dordrecht: Kluwer Academic Publishers, 1993

On the reducibility of some polynomials over finite fields with affine polynomials involved

CAO XiWang & ZHAO ZhengJun

Abstract In this paper, the reducibility of some polynomials over finite fields with affine polynomials involved is investigated. For a given affine trinomial except for $x^{p^{p^t}} - x - 1$ over $\mathbf{F}_p$, an explicit factor of it is obtained. The decomposition of $g(x^{p^s} - ax - b)$ over $\mathbf{F}_p$ has been determined completely. It is also proved that the set of all irreducible polynomials over $\mathbf{F}_p$ with the same degree forms a regular graph. In addition, an explicit formula for the number of irreducible factors of $g(x^{q^s} - x - b)$ over $\mathbf{F}_p$ is presented, where $g(x)$ is an irreducible polynomial over $\mathbf{F}_p$.

Keywords: **finite fields, affine polynomials, trinomial**

MSC(2000): **11T06**