第10卷 第4期
1990年11月

数学研究与评论
JOURNAL OF MATHEMATICAL
RESEARCH AND EXPOSITION

Vol.10 No.4
NoV., 1990

关于有限域中原根分布的注记*

王 军

（大连理工大学应用数学研究所）

设 $f_1(x),\cdots,f_r(x)$ 是 $GF(q)$ 上的具有某种性质的多项式，其中 q 是一个素数的方幂．我们希望 $GF(q)$ 中存在元素 ξ，使得 $f_1(\xi),\cdots,f_r(\xi)$ 同是 $GF(q)$ 中的原根．关于这个问题的讨论至少从30年代就开始了（参见Davenport[1]），其中最具一般性的结果当属Carlitz在1956年得到的如下定理．

定理A[2] 设 $f_1(x),\cdots,f_r(x)$ 为 $GF(q)$ 上两两互素且无重因式的非零次多项式，N_r 表示 $GF(q)$ 中使 $f_1(\xi),\cdots,f_r(\xi)$ 同为原根的元素 ξ 的个数，则

$$N_r=\left[\frac{\phi(q-1)}{q-1}\right]^r q+O(kq^{\frac{1}{2}+\varepsilon}),\quad (q\to\infty) \tag{1}$$

其中 $k=\deg f_1+\cdots+\deg f_r$，$\varepsilon$ 为任意正数．

近年来，人们又重新提起这个问题，其着眼点主要是在讨论使 $N_r>0$ 的条件．其中最完整的结果是S. D. Cohen 在[3,4,5]中证明：除 $q=2,3,7$ 外 $GF(q)$ 中存在一对连续的原根，即存在 $\xi\in GF(q)$，使得 $\xi,\xi+1$ 同是原根．另外，王巨平[6]和孙琦[7]分别证明了当 $q\geqslant 2^{60}$ 时，$GF(q)$ 上的方程 $x+y=c$ 和 $ax+by=c$ 有原根解，其中 a,b,c 是 $GF(q)$ 中任意的非零元素．韩文报在[8]中证明，对 $GF(q)$ 上满足某种条件的多项式 $f(x)$ 和 $g(x)$，当 $\sqrt{q}\geqslant(m+n-1)4^{\omega(q-1)}$ 时，$GF(q)$ 中存在元素 ξ，使得 $f(\xi)$ 和 $g(\xi)$ 同为 $GF(q)$ 中的原根根，其中 m 和 n 分别为 $f(x)$ 和 $g(x)$ 的次数，$\omega(q-1)$ 表示 $q-1$ 的不同素因子的个数．

实际上，从式（1）中可以看出，当 q 充分大时有 $N_r>0$．利用[2]中的方法，容易得到如下结果．

定理 设 $f_1(x),\cdots,f_r(x)$，k 和 N_r 同定理 A，则当 $q\geqslant[(k-1)(2^{r\omega(q-1)}-1)]^2$ 时，$N_r>0$．

定理中 $r=2$ 时便是上面提到的[8]中的结果，而 $r=2$，$f_1(x)$，$f_2(x)$ 为两个一次多项式时，便可得到上面提到的[6,7]中的结果．

这里需要指出的是，定理A中对 $f_1(x),\cdots,f_r(x)$ 要求的条件不是必要的，但为简单起见，我们宁肯采用这一较强的条件、对一般性条件的讨论可参考[9]．本文中用小写希腊字母 χ 表示 $GF(q)$ 的乘法群的特征，简称特征，并规定 $\chi(0)=0$．

为证明定理，需要[2]中的一个引理，其证明用到了A. Weil 定理．

引理1[2] 设 $f_1(x),\cdots,f_r(x)$ 和 k 同定理 A，$\chi=\{\chi_1,\cdots,\chi_r\}$ 是 $GF(q)$ 的特征的集

合，设

$$S(f,\chi)=\sum_{a\in GF(q)}\chi_1(f_1(a))\cdots\chi_r(f_r(a)) \tag{2}$$

则当χ中的特征均为非主特征时 $|s(f,\chi)|\leqslant(k-1)q^{1/2}$

设σ是$I=\{1,2,\cdots,r\}$的一个子集，$\bar{\sigma}$是σ在I中的补集，$S_\sigma(f,\chi)$表示式（2）中定义的那样的特征和：χ中脚标在σ中的特征是非主特征，而其余的是主特征．则有

引理 2 $S_\phi(f,\chi)\geqslant q-k$ $|S_\sigma(f,\chi)|\leqslant(k-1)q^{1/2}-k_{\bar{\sigma}}(q^{1/2}-1)$．其中$\sigma\neq\phi$，$k_{\bar{\sigma}}=\sum_{i\in\bar{\sigma}}\deg f_i(x)$．

证明：设$Z_{\bar{\sigma}}$表示$\prod_{i\in\sigma}f_i(x)$在$GF(q)$中的零点的集合．显然$|Z_{\bar{\sigma}}|\leqslant k_{\bar{\sigma}}$．所以

$$\begin{aligned}|S_\sigma(f,\chi)|&=\Big|\sum_{a\in GF(q)}\chi_1(f(x))\cdots\chi_r(f_r(a))\Big|=\Big|\sum_{a\in GF(q)\setminus Z_{\bar{\sigma}}}\prod_{i\in\sigma}\chi_i(f_i(a))\Big|\\&=\Big|\sum_{a\in GF(q)}\prod_{i\in\sigma}\chi_i(f_i(a))-\sum_{a\in Z_{\bar{\sigma}}}\prod_{i\in\sigma}\chi_i(f_i(a))\Big|\leqslant(k_\sigma-1)q^{1/2}+k_{\bar{\sigma}}\\&=(k-1)q^{1/2}-k_{\bar{\sigma}}(q^{1/2}-1)．\end{aligned}$$

定理的证明：如所知，对$GF(q)$中的任一元素a，a是原根的充分必要条件是

$$\sum_{d\mid q-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi^{(d)}}\chi^{(d)}(a)\neq0,$$

其中ϕ和μ分别表示Euler函数和Mobius函数，其内和表示对$GF(q)$中所有$\phi(d)$个d阶特征求和．因此要证明$N_r>0$，只须证明

$$T=\sum_{a\in GF(q)}\prod_{i=1}^{r}\sum_{d_i\mid q-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_i^{(d_i)}}\chi_i^{(d_i)}(f_i(a))\neq0.$$

我们有

$$T=\sum_{\substack{d_i\mid q-1\\1\leqslant i\leqslant r}}\frac{\mu(d_1)\cdots\mu(d_r)}{\phi(d_1)\cdots\phi(d_r)}\sum_{a=(a_1,\cdots,a_r)}\sum_{\chi^{(d)}}S(f,\chi^{(d)})$$

其中内和表示对特征$\{\chi_1^{(d_1)},\cdots,\chi_r^{(d_r)}\}$求和．设$M_i$表示$I$的所有$i$-子集的集合，显然$|M_i|=\binom{r}{i}$　由引理2我们有

$$\begin{aligned}&+\sum_{i=1}^{r}\sum_{\sigma\in M_i}\sum_{\substack{d_j\mid q-1\\j\in\sigma}}\prod_{j\in\sigma}\frac{\mu(d_j)}{\phi(d_j)}\sum_{d=(d_1,\cdots,d_r)}\sum_{\chi^{(d)}}S_\sigma(f,\chi^{(d)})\\&\geqslant q-k-\sum_{i=1}^{r}\sum_{\sigma\in M_i}\sum_{\substack{d_j\mid q-1\\j\in\sigma}}\prod_{j\in\sigma}\frac{|\mu(d_j)|}{\phi(d_j)}\sum_{d=(d_1,\cdots,d_r)}\sum_{\chi^{(d)}}|S_\sigma(f,\chi^{(d)})\\&\geqslant q-k-\sum_{i=1}^{r}\sum_{\sigma\in M_i}\sum_{\substack{d_j\mid q-1\\d_j>1\\j\in\sigma}}\prod_{j\in\sigma}|\mu(d_j)|\left[(k-1)q^{1/2}-k_\sigma(q^{1/2}-1)\right]\\&=q-(k-1)q^{1/2}\sum_{i=1}^{r}\sum_{\sigma\in M_i}\sum_{\substack{d_j\mid q-1\\d_j>1\\j\in\sigma}}\prod_{j\in\sigma}|\mu(d_j)|+\Big(\sum_{i=1}^{r}\sum_{\sigma\in M_i}\sum_{\substack{d_j\mid q-1\\d_j>1\\j\in\sigma}}\prod_{j\in\sigma}|\mu(d_j)|k_\sigma(q^{1/2}-1)-k\Big)\end{aligned}$$

易见上式后一括号中的量是大于0的，所以

$$T>q-(k-1)q^{1/2}\sum_{i=1}^{r}\sum_{\sigma\in M_i}(2^{\omega(q-1)}-1)^i$$

$$=q-(k-1)q^{1/2}\sum_{i=1}^{r}\binom{r}{i}(2^{\omega(q-1)}-1)^i$$

$$=q-(k-1)q^{1/2}(2^{\omega(q-1)r}-1)$$

再由定理的条件得$T>0$. 这就完成了定理的证明.

参 考 文 献

[1] Davenport, H., On primitive roots in finite fields, Quart. J. Math., 8(1937), 308-312.

[2] Carlitz, L., Sets of primitive roots, Compsitio Math. 13(1956), 65—70.

[3] Cohen, S. D., Consecutive primitive roots in a finite field, Proc. Amer. Math. Soc., 93(1985) 189-197.

[4] Cohen, S. D., primitive roots in a finite field Ⅱ, Proc. Amer. Math. Soc., 94(1985), 605-611.

[5] Cohen, S. D., Pairs of primitive roots, Mathematika, 32(1985), 276-285.

[6] 王巨平，关于Golomb猜想，中国科学，9(1987)，927-935.

[7] Sun Qi (孙琦), On primitive roots in a finite field, 数学进展，2(1987)，214-215.

[8] 韩文报，有限域上的多项式和原根，数学学报，1(1989)，110-117.

[9] Schmidt, *M*., Equations over Finite Fields: An Elementary Approach, Lecture Notes in Math. 536, Springer-Verlag, Berlin-Heidelbeng-New York, 1976.

A Note on Distribution of Primitive Roots in a Finite Field

Wang Jun

(Institute of Appl. Math. Dalian Univ. of Tech.)

Let $f_1(x),\cdots,f_r(x)$ denote quadratfree polynomials over $GF(q)$ that are relatively prime in pairs and of degree$\geqslant$1. We have proved that if $q\geqslant(k-1)^2(2^{r\omega(q-1)}-1)^2$, then all the $f_i(\xi)$ are primitive roots of $GF(q)$ for some $\xi\in GF(q)$, where $k=\deg f_1+\cdots+\deg f_r$. With extending the results obtained by Wang Juping, Sun Qi and Han Wenbao respectively, we have also given a quantitative analysis of Carlitz's result.