第35卷第5期
1995年10月
大连理工大学学报
Journal of Dalian University of Technology
Vol. 35, No. 5
Oct. 1995

有限域上的广义 Euler 函数*

冯 红
（大连理工大学应用数学系 116024）

摘要 利用反演的方法给出了有限域上 Euler 函数的推广形式；在此基础上给出了广义 Euler 函数的一些结果在有限域上一元多项式环中的模拟. 并且证明了一种新型的广义 Euler Φ-函数在一定条件下，计算了满足 $\deg B<\deg A$ 且 $(B,A)_r=1$ 的多项式 B 的个数.

关键词：Euler Φ-函数；Mobius 函数；卷积
分类号：O157.1

设 F_q 是 q 个元素的有限域，$F_q[x]$ 是 F_q 上的一元多项式环；其元素用 A、B、C、…表示. 设 Ω 表示 $F_q(x)$ 中所有首项系数为 1 的多项式集合；Δ 表示 Ω 中所有不可约多项式的集合，其元素一般用 P 表示. 对任意的 $A\in F_q[x]$，$A\neq 0$，记 $|A|=q^{\deg A}$（$\deg A$ 表示多项式 A 的次数)，即剩余类环 $F_q[x]/(A)$ 中的元素个数. 定义 $\Phi(A)$ 为 $F_q[x]/(A)$ 中单位的个数，即 $\Phi(A)$ 等于 $F_q[x]$ 中次数小于 A 的次数且与 A 互素的多项式的个数. 因为 Φ 是 Euler 函数 $\varphi(n)$ 在 $F_q[x]$ 中的模拟，所以称 Φ 为 $F_q[x]$ 中的 Euler 函数，简称 Φ-函数. Φ-函数有如下熟知的结果：

$$\Phi(A)=|A|\prod_{\substack{P\in\Delta\\ P|A}}(1-|P|^{-1}) \tag{1}$$

$\prod$ 表示对 A 的所有素因子取积. 对于一般的 Euler 函数 $\varphi(n)$ 的推广形式，文[1]给出了一些结果，本文讨论了这些结果在一元多项式环 $F_q[x]$ 中的模拟.

1 $F_q[x]$ 上的算术函数的某些性质

与普通的算术函数类似，定义 $F_q[x]$ 上的算术函数为 Ω 到复数域内的映射. 用 $\mathscr{A}$ 表示所有这样的映射的集合. 对任意 f、$g\in\mathscr{A}$，定义其 Dirichlet 卷积为

$$(f*g)A=\sum_{D|A}f(D)g(A/D),\ A\in\Omega$$

其中的和式是对 A 的所有在 Ω 中的因子求和，$f\cdot g$ 表示通常的乘积，A/D 表示 D 除以 A 所得的商式. 不难验证，这个运算满足结合律和交换律，并且有单位元 e_0；$(\mathscr{A},*,e_0)$ 构成一个交换半群.

算术函数 f 称为是可乘的，如果 $f(1)=1$，并且当 $(A,B)=1$（互素）时，有

$$f(AB)=f(A)f(B) \tag{2}$$

---

* 国家自然科学基金资助项目
收稿日期：1994-10-20；修订日期：1995-05-25

如果式(2)对所有的 A、$B\in\Omega$ 都成立，则称 f 是完全可乘的.

易见，对任意的 $\tau\in\mathscr{A}$，如果 $\tau(1)\neq0$，则存在唯一的 $\nu\in\mathscr{A}$，使得 $\tau*\nu=e_0$. 这时称 τ 是一个 Dirichlet 可逆函数，简称可逆函数. ν 称为 τ 的逆，记作 τ^{-1}. 显然可乘函数是可逆的，并且所有可乘函数的集合 M 在 Dirichlet 卷积运算下构成一个 Abel 群. 令 ζ 是 $\mathscr{A}$ 中恒等于 1 的函数，则 ζ 是可逆的，它的逆函数便是熟知的 Möbius 函数，即

$$\mu(A)=\begin{cases}1, & \text{如果 } A=1,\\ (-1)^k, & \text{如果 } A \text{ 是 } k \text{ 个互不相同的不可约多项式之积},\\ 0, & \text{其他}.\end{cases}$$

2　广义 Euler 函数

定义 1　设 τ 为 Ω 上的一个 Dirichlet 可逆函数，称 Ω 上函数

$$\Phi_\tau^{(k)}(A)=\sum_{D|A}|D|^k\tau(A/D)$$

为关于 τ 的 Φ-函数. τ 称为 $\Phi_\tau^{(k)}$ 的核，而 $\Phi_{\tau^{-1}}^{(k)}$ 称为 $\Phi_\tau^{(k)}$ 的对偶函数. 为方便起见，记 $\Phi_\tau=\Phi_\tau^{(1)}$.

定义 2　设 $\Phi_\tau^{(k)}$ 为关于 Dirichlet 可逆函数 τ 的 Φ-函数. 称 $\Phi_\tau^{(k)}$ 是一个一阶 Φ-函数，如果 $\tau=\mu f$，其中 f 是一个完全可乘函数.

引理 1　设 f 是 Ω 上一个可乘函数，$A\in\Omega$ 的标准分解式是 $A=P_1^{\alpha_1}\cdots P_s^{\alpha_s}$，$P_i\in\Delta$，$P_i\neq P_j$ $(i\neq j)$，则

$$\sum_{D|A}f(D)=\prod_{\substack{P|A\\P\in\Delta}}\sum_{i=0}^{\mathrm{ord}_p(A)}f(P^i),$$

其中 $\mathrm{ord}_p(A)$ 表示非负整数 k，使得 P^k 整除 A，但 P^{k+1} 不整除 A，$P\in\Delta$.

定理 1　一阶 Φ-函数具有乘积公式

$$\Phi_\tau^{(k)}(A)=|A|^k\prod_{\substack{P|A\\P\in\Delta}}\left(1-\frac{f(P)}{|P|^k}\right)$$

定理 2　对任意 $P\in\Delta$，设 $\mathscr{F}_P$ 为 $F_q[x]/(P)$ 上 k 维线性空间的一个子集. 于是唯一存在一个完全可乘函数 f，使得 $f(P)$ 等于 $\mathscr{F}_P$ 中元素个数. 令 $\tau=\mu\cdot f$，则 $\Phi_\tau^{(k)}(A)$ 等于满足下述条件的有序多项式组 $(A_1,\cdots,A_k)$ 的个数，$\deg A_i<\deg A$，并且对 A 的任一不可约因子 $P\in\Delta$，恒有 $(A_1+(P),\cdots,A_k+(P))$ 不在 $\mathscr{F}_P$ 中.

设 $A\neq1$，$A\in\Omega$，称 $B\in\Omega$ 与 A 是 r 阶互素的，记作 $(B,A)_r=1$. 如果对于 A 的每一不可约因子 $P\in\Delta$，存在 B_0，B_1，$\cdots$，B_{r-1}，$B_r\in\Omega$，使

$$B=B_0+B_1P+\cdots+B_{r-1}P^{r-1}+B_rP^r$$

其中对 $1\leqslant i\leqslant r-1$，$B_i\neq0$，$\deg B_i<\deg P$.

设 $N_r(A)$ 为满足下列条件 B 的个数：$\deg B<\deg A$，且 $(B,A)_r=1$，$B\in\Omega$. 为了计算 $N_r(A)$，先讨论一个 Φ-函数[2]. 记

$$\mu_r(D)=\prod_{\substack{P|D\\P\in\Delta}}\binom{r}{\mathrm{ord}_p(D)}(-1)^{\mathrm{ord}_p(D)}$$

称 μ_r 为 r 阶 Möbius 函数. 显然 $\mu_1=\mu$，且 μ_r 是可乘函数.

$$\Phi_{\mu_r}(A)=\sum_{D|A}|A/D|\mu_r(D)=|A|\prod_{\substack{P|A\\P\in\Delta}}\sum_{i=0}^{\mathrm{ord}_p(A)}\binom{r}{i}\left(-\frac{1}{|P|}\right)^i$$

最后一等式由引理1得出.

当 A 是 r-powerful 多项式时，即对 A 的每一不可约因子 P，$\mathrm{ord}_p(A)\geqslant r$ 时，有

$$\Phi_{\mu_r}(A)=|A|\prod_{\substack{P|A\\P\in\Delta}}\left(1-\frac{1}{|P|}\right)^r$$

定理3 设 A 是 r-powerful 多项式时，$N_r(A)=\Phi_{\mu_r}(A)$.

以上概念和结果可推广到 k-集情形.

设 $\alpha=(A_1,\cdots,A_k)$ 是一有序 k-多项式组，$A_i\in\Omega$，对任一 $P\in\Delta$，唯一存在 $F_q[x]/(P)$ 上 $r\times k$ 矩阵 $\mathscr{B}_P(\alpha)$，使得

$$\alpha=(1,P,P^2,\cdots,P^{r-1})\mathscr{B}_P(\alpha)+P^r(\overline{A}_1,\overline{A}_2,\cdots,\overline{A}_k)$$

定义3 设 $A\in\Omega$，$A\neq1$，$\alpha=(A_1,\cdots,A_k)$，$A_i\in\Omega$，称 α 与 A r 阶互素，记作 $(\alpha,A)_r=1$. 如果 A 的任一不可约因子 $P\in\Delta$，矩阵 $\mathscr{B}_p(\alpha)$ 的每一个行向量都是非零的.

定理4 设 A 是 r-powerful 多项式，$A\in\Omega$，则与 A r 阶互素的 $\alpha=(A_1,A_2,\cdots,A_k)$，$\deg A_i<\deg A$ 的个数为

$$\Phi_{\mu_r}^{(k)}(A)=\sum_{D|A}|D|^k\mu_r(A/D)=|A|^k\prod_{\substack{P|A\\P\in\Delta}}(1-|P|^{-k})^r$$

定义4 设 $\Phi_\tau^{(k)}$ 为关于 τ 的 Φ-函数，如果 $\tau=\mu_r\cdot f$，其中 f 是一个完全可乘函数，则称 $\Phi_\tau^{(k)}$ 是一个 r 阶 Φ-函数.

显然，当 A 是 r-powerful 多项式时，r 阶 Φ-函数具有下面的乘积公式

$$\Phi_\tau^{(k)}(A)=|A|^k\prod_{\substack{P|A\\P\in\Delta}}\left(1-\frac{f(P)}{|P|^k}\right)^r$$

其中 $\tau=\mu_r\cdot f$.

定理5 设 $\mathscr{F}_P$，f 的意义同定理2. 对任意有序多项式组 $\alpha=(A_1,A_2,\cdots,A_k)$，$A_i\in\Omega$，记 $(\alpha,A)_{\mathscr{F}}=1$，如果对于 A 的任一素因子 $P\in\Delta$，$\mathscr{B}_P(\alpha)$ 中每一个行向量均不在 $\mathscr{F}_P$ 中. 令 $\tau=\mu_r\cdot f$，则当 A 是 r-powerful 多项式时，$\Phi_r^{(k)}(A)$ 等于满足如下条件的有序多项式组 $\alpha=(A_1,\cdots,A_k)$ 的个数：$\deg A_i<\deg A$，$(\alpha,A)_{\mathscr{F}}=1$.

证明 设 $A=P_1^{e_1},\cdots,P_s^{e_s}$ 是 r-powerful 多项式；其中 $P_i\in\Delta$，$P_i\neq P_j(i\neq j)$，$e_i\geqslant r$. 设 $N_r(A,k)$ 为下列有序多项式组 α 的个数：$\alpha=(A_1,\cdots,A_k)$，$A_i\in\Omega$，$\deg A_i<\deg A$，$(\alpha,A)_{\mathscr{F}}=1$. 由中国剩余定理[3]，对于任意有序多项式组 $\alpha_1=(A_{11},A_{12},\cdots,A_{1k})$；$\alpha_2=(A_{21},\cdots,A_{2k})$，$\cdots$，$\alpha_s=(A_{s1},\cdots,A_{sk})$，存在唯一的 $\alpha=(A_1,\cdots,A_k)$，$\deg A_i<\deg A$，使得

$$\alpha\equiv\alpha_1(\mathrm{mod}P_1^{e_1}),\ \alpha\equiv\alpha_2(\mathrm{mod}P_2^{e_2}),\cdots,\alpha\equiv\alpha_s(\mathrm{mod}P_s^{e_s})$$

反之，对于任意 k-多项式组 α，存在唯一的一组 $\alpha_i(\mathrm{mod}P_i^{e_i})$ 满足上述同余式. 因此 $(\alpha,A)_{\mathscr{F}}=1$ 当且仅当 $(\alpha_i,P_i^{e_i})_{\mathscr{F}}=1$，$1\leqslant i\leqslant s$. 因此 $N_r(A,k)$ 关于 A 是可乘的.

为此只须对 $A=P^e$，$P\in\Delta$，$e\geqslant r$ 的情况讨论. 设 $\alpha=(A_1,A_2,\cdots,A_k)$，$\deg A_i<\deg A$，$(\alpha,A)_{\mathscr{F}}=1$，则 α 可唯一写成

$$\alpha=(1,P,P^2,\cdots,P^{r-1})\mathscr{B}_P(\alpha)+P^r(\overline{A}_1,\overline{A}_2,\cdots,\overline{A}_k)$$

其中 $\mathscr{B}_P(\alpha)$ 是 $F_q[x]/(P)$ 上的 $r\times k$ 矩阵，$\deg\overline{A}_i<(e-r)\deg P$ $(i=1,2,\cdots,k)$. 设

$$\overline{A}_i=\sum_{m=0}^{(e-r)\deg P-1}\lambda_m x^m,\qquad \lambda_m\in F_q,$$

故 $\overline{A}_i$ 有 $q^{(e-r)\deg P}=|P|^{e-r}$ 种选择. 显然 $(\alpha,A)_{\mathscr{F}}=1$ 当且仅当 $\mathscr{B}_P(\alpha)$ 的每一个行向量皆在 $(F_q[x]/(P))^k\setminus\mathscr{F}_P$ 中. 因此 α 的个数是

$$(|P|^k-f(P))^r(|P|^{e-r})^k=|P|^{ek}\left(1-\frac{f(P)}{|P|^k}\right)^r$$

因此
$$N_r(A,k)=|A|^k\prod_{\substack{P|A\\P\in\Delta}}\left(1-\frac{f(P)}{|P|^k}\right)^r$$
证毕

在定理 5 中，取 $r=1$，则得定理 2. 取 $\mathscr{F}_P=\{0\}$ 及 $\mathscr{F}_P=\{0,0,\cdots,0\}$($k$ 维零向量)，则分别得定理 3 及定理 4.

例 1　在定理 5 中，取 $r=1$，$k=1$，

$$\mathscr{F}_P=\{a_1+(P),a_2+(P),\cdots,a_q+(P)\}\subset F_q[x]/(P)$$

其中 a_1，a_2，…，a_q 为 F_q 中全部元素. 则

$$\Phi_r(A)=|A|\prod_{\substack{P|A\\P\in\Delta}}\left(1-\frac{f(P)}{|P|}\right)=|A|\prod_{\substack{P|A\\P\in\Delta}}(1-q^{1-\deg P})$$

是 $F_q[x]$ 中满足如下条件的 B 的个数：$\deg B<\deg A$，与 A 互素，且减去任一常数后仍与 A 互素.

感谢王军教授对本文工作的指导与帮助.

参　考　文　献

1　王　军，徐利治. 怎样推广 Euler Φ-函数. 全国第五届组合数学学术会议论文，上海，1994.

2　Hsu L C. A difference-operational appoach to the Möbius inversion formulae. **Fibonacci Quarterly**，1995，**30**(2)：169～173

3　Lidl R，Niederreiter H. **Finite Fields**. Addison-Wesley：Reading MA，1983.

Euler functions in finite fields

Feng　Hong

(Dept. of Applied Mathematics，DUT)

Abstract　The generalized Euler-type functions in finite fields are given by using the method of inversion. Based on this condition，some results on the generalized Euler-type functions are shown in a polynomial ring over finite fields analytically.

Key Words：Euler Φ-functions；Mobius functions；convolutions