

Chapter 5 Exponential Sums

5.1 Characters

Definition 5.0 Character, Character Multiplication, Character Group

设 G 是有限交换群, 阶为 $|G|$, 单位元为 1_G .

群 G 的**特征** χ 被定义为 G 到非零复数乘法群 U 的群同态, 即 $\chi: G \rightarrow U$.

即对于 $g_1, g_2 \in G$, 有 $\chi(g_1 g_2) = \chi(g_1) \chi(g_2)$. 显然有 $\chi(1_G) = 1$. 此外, 对于任意 $g \in G$:

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$$

因此 χ 的值域就是 $|G|$ 次单位根, 可以记为

$$\zeta_n = e^{\frac{2\pi i}{n}}$$

n 阶交换群 G 的特征 χ 都取值于 n 阶循环群

$$\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$$

可以发现 $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$. 因此有 $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$, 这里的 $\overline{\chi(g)}$ 表示复共轭.

在 G 的所有特征中, 定义**平凡特征** χ_0 为 $\chi_0(g) = 1$. 其他的特征都称为非平凡特征.

对于特征 χ , 定义 $\bar{\chi}$ 为共轭特征. $\bar{\chi}(g) = \overline{\chi(g)}$.

下面定义特征乘法, 设有限个特征 χ_1, \dots, χ_n , 那么 $(\chi_1 \dots \chi_n)(g) = \chi_1(g) \dots \chi_n(g)$.

如果 $\chi_1 = \dots = \chi_n = \chi$, 则记 $\chi_1 \dots \chi_n = \chi^n$.

用 \hat{G} 表示 G 的所有特征所组成的集合, \hat{G} 对于上面的乘法运算形成群, 这个群定义为**特征群**.

由于 G 中的值只能是 $|G|$ 次单位根, 所以这个群是有限群.

Example 5.1

设 G 是一个阶为 n 的有限循环群, 设生成元为 g . 那么对于确定的整数 $j, 0 \leq j \leq n-1$, 函数

$$\chi_j(g^k) = e^{\frac{2\pi i}{n} jk}, k = 0, 1, \dots, n-1$$

定义了 G 的一个特征.

另一方面来看, 若 χ 是 G 的任一特征, 那么 $\chi(g)$ 一定是 n 次单位根, 即存在 $0 \leq j \leq n-1$ 使得 $\chi(g) = e^{2\pi i j/n}$.

那么就有 $\chi = \chi_j$. 因此 \hat{G} 正好包括了这些特征 $\chi_0, \chi_1, \dots, \chi_{n-1}$.

Theorem 5.2

设 H 是有限交换群 G 的子群, ψ 是 H 的特征. 那么 ψ 可以拓展成 G 的特征, 即存在一个 G 的特征 χ 使得对于任意 $h \in H$ 都有 $\chi(h) = \psi(h)$.

证明: 设 H 是 G 的真子群. 取元素 $a \in G$ 且 $a \notin H$. 令 H_1 是由 H 和 a 生成的 G 的子群.

设 m 是满足 $a^m \in H$ 的最小正整数, 那所有元素 $g \in H_1$ 都可以唯一写成 $g = a^j h$ 的形式, 其中 $0 \leq j < m, h \in H$.

定义 H_1 上的函数 ψ_1 为 $\psi_1(g) = \omega^j \psi(h)$, 其中 ω 是一个确定的满足 $\omega^m = \psi(a^m)$ 的复数.

为了检验 ψ_1 具体是不是 H_1 的特征, 设 $g_1 = a^k h_1, 0 \leq k < m, h_1 \in H, g_1$ 是 H_1 中的另一个元素, 若 $j + k < m$, 则

$$\psi_1(gg_1) = \omega^{j+k} \psi(hh_1) = \psi_1(g)\psi_1(g_1)$$

如果 $j + k \leq m$, 则 $gg_1 = a^{j+k-m}(a^m h h_1)$, 则

$$\begin{aligned}\psi_1(gg_1) &= \omega^{j+k-m} \psi(a^m h h_1) \\ &= \omega^{j+k-m} \psi(a^m) \psi(h h_1) = \omega^{j+k} \psi(h h_1) = \psi_1(g)\psi_1(g_1)\end{aligned}$$

那么显然就有 $\psi_1(h) = \psi(h)$ 对于所有 $h \in H$ 都成立.

如果 $H_1 = G$ 那么命题成立, 否则重复上述步骤, 一定可以把 ψ 扩展到 G .

Corollary 5.3

对于两个任意的不同元素 $g_1, g_2 \in G$, 存在一个 G 的特征 χ 使得 $\chi(g_1) \neq \chi(g_2)$.

证明: 只需要证明对于 $h = g_1 g_2^{-1} \neq 1_G$, 存在一个 G 的特征 χ 使得 $\chi(h) \neq 1$.

通过 Example 5.1 和 Theorem 5.2 可以知道, 令 H 是由 h 生成的循环群 G 的子群就可以满足这个条件.

Theorem 5.4

设 χ 是有限交换群 G 的非平凡特征, 那么

$$\sum_{g \in G} \chi(g) = 0 \quad (1)$$

若 $g \in G, g \neq 1_G$, 则

$$\sum_{\chi \in \hat{G}} \chi(g) = 0 \quad (2)$$

证明: 因为 χ 非平凡, 那么存在 $h \in G$ 使得 $\chi(h) \neq 1$, 那么

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g)$$

因此就有

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0$$

所以 $\sum_{g \in G} \chi(g) = 0$.

对于第二部分, 定义函数 $\hat{g}(\chi) = \chi(g)$, 这个函数 \hat{g} 是有限交换群 \hat{G} 的一个特征. 这个特征非平凡.

那么根据 Corollary 5.3 就存在 $\chi \in \hat{G}$ 使得 $\chi(g) \neq \chi(1_G) = 1$. 那么根据 (1) 式就有

$$\sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} \hat{g}(\chi) = 0$$

Theorem 5.5 Number of Character

有限交换群 G 的特征的个数为 $|G|$.

证明:

$$|\hat{G}| = \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} \sum_{g \in G} \chi(g) = |G|$$

Discussion A: The Combination of 5.4 and 5.5; Annihilate

上面 Theorem 5.4 和 Theorem 5.5 可以合并为特征的正交关系. 设 χ 和 ψ 是 G 的特征, 那么

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)} = \begin{cases} 0 & \chi \neq \psi \\ 1 & \chi = \psi \end{cases} \quad (3)$$

第一部分是通过对式 (1) 应用在特征 $\chi\bar{\psi}$ 上. 第二部分显然.

进一步看, 如果 g, h 是 G 中的元素, 那么

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(g) \overline{\chi(h)} = \begin{cases} 0 & g \neq h \\ 1 & g = h \end{cases} \quad (4)$$

第一部分是通过对式 (2) 应用在特征 $g\bar{h}$ 上. 第二部分由 Theorem 5.5 可知.

特征理论通常用于**获得一个有限交换群 G 中方程组解的数量的表达式.**

设 f 是笛卡尔积 G^n 到 G 的映射. 那么对于确定的 $h \in G$, 满足 $f(g_1, \dots, g_n) = h$ 的 n 元组 $(g_1, \dots, g_n) \in G^n$ 的组数 $N(h)$ 为

$$N(h) = \frac{1}{|G|} \sum_{g_1 \in G} \dots \sum_{g_n \in G} \sum_{\chi \in \hat{G}} \chi(f(g_1, \dots, g_n)) \overline{\chi(h)} \quad (5)$$

一个特征 χ 虽然可能是非平凡的, 但是仍然可以**零化(annihilate)** G 的子群 H , 即对于所有 $h \in H$ 都有 $\chi(h) = 1$.

G 的所有可以零化其子群 H 的特征集合被称为 H 在 \hat{G} 中的**零化子(annihilator)**.

Theorem 5.6

设 H 是有限交换群 G 的子群. 那么 H 在 \hat{G} 中的零化子是 \hat{G} 的一个阶为 $|G|/|H|$ 的子群.

证明: 设零化子是 A . 首先根据定义 A 是 \hat{G} 的子群. 设 $\chi \in A$, 那么 $\mu(gH) = \chi(g), g \in G$ 是商群 G/H 的良定义的特征.

反过来, 如果 μ 是 G/H 的特征, 那么 $\chi(g) = \mu(gH), g \in G$ 定义了一个可以零化 H 的 G 的特征. A 中的不同元素对应了 G/H 中不同的特征. 因此 A 和 $(\widehat{G/H})$ 中的元素一一对应, 因此二者阶相等, 为 $|G/H| = |G|/|H|$.

对于一个域 \mathbb{F}_q 需要讨论其加法交换群和乘法交换群.

考虑加法交换群, 设 p 是域 \mathbb{F}_q 的特征, 那么素域 \mathbb{F}_p 包含于 \mathbb{F}_q . 可以用 $\mathbb{Z}/(p)$ 表示. 设映射 $Tr: \mathbb{F}_q \rightarrow \mathbb{F}_p$ 是绝对迹函数, 那么

$$\chi_1(c) = e^{2\pi i Tr(c)/p}, c \in \mathbb{F}_q \quad (6)$$

是 \mathbb{F}_q 的加法群的一个特征. 因为对于 $c_1, c_2 \in \mathbb{F}_q$ 有 $Tr(c_1 + c_2) = Tr(c_1) + Tr(c_2)$, 所以 $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$.

这种特征被称为 \mathbb{F}_q 的**加法特征**. (6) 式里的特征 χ_1 被称为 \mathbb{F}_q 的**主加法特征**. 所有 \mathbb{F}_q 的加法特征都可以用含有 χ_1 的项来表示.

Theorem 5.7

对于 $b \in \mathbb{F}_q$, 函数 χ_b 定义为 $\chi_b(c) = \chi_1(bc)$ 是 \mathbb{F}_q 的加法特征, 其中 $c \in \mathbb{F}_q$. 且每个 \mathbb{F}_q 的加法特征都可以通过这个方法得到.

证明: 对于 $c_1, c_2 \in \mathbb{F}_q$ 有

$$\begin{aligned} \chi_b(c_1 + c_2) &= \chi_1(bc_1 + bc_2) \\ &= \chi_1(bc_1)\chi_1(bc_2) = \chi_b(c_1)\chi_b(c_2) \end{aligned}$$

所以 χ_b 是 \mathbb{F}_q 的加法特征.

因为迹函数 Tr 把 \mathbb{F}_q 映射到 \mathbb{F}_p 上, 所以 χ_1 是一个非平凡特征. 那么对于 $a, b \in \mathbb{F}_q, a \neq b$, 存在 $c \in \mathbb{F}_q$ 使得

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1$$

因此 χ_a 和 χ_b 是不同的特征. 因此如果 b 遍历 \mathbb{F}_q 那就可以得到 q 个不同的加法特征.

另一方面, \mathbb{F}_q 有恰好 q 个特征, 因此已经找到了所有的 \mathbb{F}_q 的加法特征.

当 $b = 0$ 的时候, 就得到了平凡加法特征 χ_0 .

设 E 是 \mathbb{F}_q 的一个域扩张, χ_1 是 \mathbb{F}_q 的一个主加法特征, μ_1 是式 (6) 所定义的 E 的加法特征, Tr 为绝对迹 Tr_E .

那么 χ_1 和 μ_1 之间的关系为

$$\chi_1(Tr_{E/\mathbb{F}_q}(\beta)) = \mu_1(\beta), \beta \in E \quad (7)$$

其中 Tr_{E/\mathbb{F}_q} 是 E 到 \mathbb{F}_q 的迹函数. 这是由于

$$Tr_E(\beta) = Tr(Tr_{E/\mathbb{F}_q}(\beta)), \beta \in E$$

\mathbb{F}_q 的乘法群 \mathbb{F}_q^* 的特征被称为 \mathbb{F}_q 的乘法特征. 由于 \mathbb{F}_q^* 是循环群, 阶为 $q-1$, 所以它的特征很容易确定.

Theorem 5.8 Obtain Multiplicative Character

设 g 是一个确定的 \mathbb{F}_q 的本原元, 对于每个 $j = 0, 1, \dots, q-2$, 函数 ψ_j 定义了 \mathbb{F}_q 的乘法特征, 且每个乘法特征都可以如此获得.

其中

$$\psi_j(g^k) = e^{\frac{2\pi i}{q-1}jk}, k = 0, 1, \dots, q-2$$

证明: 由 Example 5.1 显然.

Corollary 5.9

\mathbb{F}_q 的乘法特征形成的群是阶为 $q-1$ 的循环群, 单位元是 ψ_0 .

证明: 对于每个 Theorem 5.8 中的特征 ψ_j , 如果 $\gcd(j, q-1) = 1$, 那么它就是这个群的生成元.

单位元显然是 ψ_0 .

Example 5.10 Quadratic Character

设 q 为奇数, η 是 \mathbb{F}_q^* 上的实值函数, 如果 c 是 \mathbb{F}_q^* 上元素的平方, 那么 $\eta(c) = 1$, 否则 $\eta(c) = -1$.

那么 η 是 \mathbb{F}_q 上的乘法特征. 这可以通过令 Theorem 5.8 中的 $j = (q-1)/2$ 从而得到.

特征 η 零化 \mathbb{F}_q^* 的包括所有平方元素的子群. 根据 Theorem 5.6 可以知道这是唯一一个满足这个条件的平凡特征.

这个特殊的特征 η 被称为 \mathbb{F}_q 的二次特征. 如果 q 是奇素数, 那么对于 $c \in \mathbb{F}_q^*$ 有 $\eta(c) = (\frac{c}{q})$, 这里的括号表示勒让德符号.

式 (3) 和 (4) 提到的正交关系在加法和乘法特征上也可以应用. 考虑加法特征, 用 Theorem 5.7 中的表示法, 即 $\chi_b(c) = \chi_1(bc)$, 那么对于加法特征 χ_a, χ_b 有

$$\sum_{c \in \mathbb{F}_q} \chi_a(c) \overline{\chi_b(c)} = \begin{cases} 0 & a \neq b \\ q & a = b \end{cases} \quad (8)$$

特别的

$$\sum_{c \in \mathbb{F}_q} \chi_a(c) = 0, a \neq 0 \quad (9)$$

此外, 对于元素 $c, d \in \mathbb{F}_q$ 有

$$\sum_{b \in \mathbb{F}_q} \chi_b(c) \overline{\chi_b(d)} = \begin{cases} 0 & c \neq d \\ q & c = d \end{cases} \quad (10)$$

类似的, 对于 \mathbb{F}_q 上的乘法特征 ψ 和 τ 有

$$\sum_{c \in \mathbb{F}_q^*} \chi(c) \overline{\tau(c)} = \begin{cases} 0 & \chi \neq \tau \\ 1 & \chi = \tau \end{cases} \quad (11)$$

特别的

$$\sum_{c \in \mathbb{F}_q^*} \chi(c) = 0, \chi \neq \chi_0 \tag{12}$$

对于元素 $c, d \in \mathbb{F}_q^*$, 有

$$\sum_{\psi} \psi(c) \overline{\psi(d)} = \begin{cases} 0 & c \neq d \\ 1 & c = d \end{cases} \tag{13}$$

和就被衍生到了所有 \mathbb{F}_q 的乘法特征上.

5.2 Gaussian Sum

设 ψ 和 χ 分别为 \mathbb{F}_q 的加法特征和乘法特征, 那么高斯和 $G(\psi, \chi)$ 定义为

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c) \chi(c)$$

显然这个式子的绝对值小于 $q - 1$, 但是总体来说这个式子不会这么大. 记 \mathbb{F}_q 的平凡乘法特征和平凡加法特征分别为 ψ_0 和 χ_0 .

Theorem 5.11 Value of Gaussian Sums

设 ψ 和 χ 分别是 \mathbb{F}_q 的乘法特征和加法特征, 那么高斯和 $G(\psi, \chi)$ 满足

$$G(\psi, \chi) = \begin{cases} q - 1 & \psi = \psi_0, \chi = \chi_0 \\ -1 & \psi = \psi_0, \chi \neq \chi_0 \\ 0 & \psi \neq \psi_0, \chi = \chi_0 \end{cases} \quad (14)$$

如果 $\chi \neq \chi_0, \psi \neq \psi_0$, 那么

$$|G(\psi, \chi)| = \sqrt{q} \quad (15)$$

证明: 第一个条件显然, 第三个条件根据式 (12) 显然.

对于第二个条件, 由式 (9) 可得

$$G(\psi_0, \chi) = \sum_{c \in \mathbb{F}_q^*} \chi(c) = \sum_{c \in \mathbb{F}_q} \chi(c) - \chi(0) = 0 - 1 = -1$$

如果 $\chi \neq \chi_0, \psi \neq \psi_0$, 那么

$$\begin{aligned} |G(\psi, \chi)|^2 &= \overline{G(\psi, \chi)} G(\psi, \chi) \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \overline{\psi(c) \chi(c)} \psi(c) \chi(c) \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \psi(c^{-1} c_1) \chi(c_1 - c) \end{aligned}$$

在内层求和的时候, 用 $c^{-1} c_1 = d$ 进行代换, 通过式 (12) 得到

$$\begin{aligned} |G(\psi, \chi)|^2 &= \sum_{c \in \mathbb{F}_q^*} \sum_{d \in \mathbb{F}_q^*} \psi(d) \chi(c(d - 1)) \\ &= \sum_{d \in \mathbb{F}_q^*} \psi(d) \left(\sum_{c \in \mathbb{F}_q} \chi(c(d - 1)) - \chi(0) \right) \\ &= \sum_{d \in \mathbb{F}_q^*} \psi(d) \sum_{c \in \mathbb{F}_q^*} \chi(c(d - 1)) \end{aligned}$$

根据式 (9), 如果 $d = 1$, 内层的和是 q , 否则是 0. 那么 $|G(\psi, \chi)| = \psi(1)q = q$. 所以式 (15) 得证.

Theorem 5.12 Gaussian Sums' Properties

对于域 \mathbb{F}_q , 高斯和满足下列性质:

(i) $G(\psi, \chi_{ab}) = \overline{\psi(a)}G(\psi, \chi_b)$ 对所有 $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ 成立.

(ii) $G(\psi, \bar{\chi}) = \psi(-1)G(\psi, \chi)$

(iii) $G(\bar{\psi}, \chi) = \psi(-1)\overline{G(\psi, \chi)}$

(iv) $G(\psi, \chi)G(\bar{\psi}, \chi) = \psi(-1)q$ 对所有 $\psi \neq \psi_0, \chi \neq \chi_0$ 成立

(v) $G(\psi^p, \chi_b) = G(\psi, \chi_{\sigma(b)})$ 对所有 $b \in \mathbb{F}_q$ 成立, 其中 p 是域 \mathbb{F}_q 的特征, $\sigma(b) = b^p$.

证明:

(i) 对于 $c \in \mathbb{F}_q$, 根据定义有 $\chi_{ab}(c) = \chi_1(abc) = \chi_b(ac)$. 所以

$$G(\psi, \chi_{ab}) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi_{ab}(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi_b(ac)$$

令 $d = ac$ 有

$$\begin{aligned} G(\psi, \chi_{ab}) &= \sum_{d \in \mathbb{F}_q^*} \psi(a^{-1}d)\chi_b(d) \\ &= \psi(a^{-1}) \sum_{d \in \mathbb{F}_q^*} \psi(d)\chi_b(d) \\ &= \overline{\psi(a)}G(\psi, \chi_b) \end{aligned}$$

(ii) 存在 $b \in \mathbb{F}_q$ 使得 $\chi = \chi_b$. 对于任意 $c \in \mathbb{F}_q$ 有 $\bar{\chi}(c) = \chi_b(-c) = \chi_{-b}(c)$. 因此由 (i), 令 $a = -1$, 注意到 $\psi(-1) = \pm 1$, 则有

$$G(\psi, \bar{\chi}) = G(\psi, \chi_{-b}) = \overline{\psi(-1)}G(\psi, \chi_b) = \psi(-1)G(\psi, \chi)$$

(iii) 根据 (ii)

$$G(\bar{\psi}, \chi) = \bar{\psi}(-1)G(\bar{\psi}, \bar{\chi}) = \psi(-1)\overline{G(\psi, \chi)}$$

(iv) 根据 (iii) 和式 (15) 有

$$G(\psi, \chi)G(\bar{\psi}, \chi) = \psi(-1)G(\psi, \chi)\overline{G(\psi, \chi)} = \psi(-1)|G(\psi, \chi)|^2 = \psi(-1)q$$

(v) 对于 $a \in \mathbb{F}_q$ 有 $Tr(a) = Tr(a^p)$. 那么就有 $\chi_1(a) = \chi_1(a^p)$. 因此对于 $c \in \mathbb{F}_q$ 就有 $\chi_b(c) = \chi_1(bc) = \chi_1(b^p c^p) = \chi_{\sigma(b)}(c^p)$.

从而

$$G(\psi^p, \chi_b) = \sum_{c \in \mathbb{F}_q^*} \psi^p(c)\chi_b(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c^p)\chi_{\sigma(b)}(c^p)$$

而 c^p 和 c 都可以遍历一遍 \mathbb{F}_q^* , 所以原式得证.

Remark 5.13 Value of $\psi(-1)$

在上面的定理里面, 考虑 $\psi(-1)$ 的值. 首先很显然的有 $\psi(-1) = \pm 1$.

设 m 是 ψ 的阶, 即 m 是满足 $\psi^m = \psi_0$ 的最小正整数. 那么因为 $\psi^{q-1} = \psi_0$ 可以得到 $m \mid q-1$.

ψ 的值是 m 次单位根, 具体的说, -1 这个值只会出现在 m 为偶数的时候出现. 如果 g 是 \mathbb{F}_q 的一个本原元, 那么 $\psi(g) = \zeta$, 其中 ζ 是 m 次本原根.

如果 m 是偶数, 那么 q 是奇数, 那么 $\psi(-1) = \psi(g^{(q-1)/2}) = \zeta^{(q-1)/2}$, 当且仅当 $(q-1)/2 \equiv m/2 \pmod{m}$ 即 $(q-1)/m$ 为奇数的时候值为 1. **因此 $\psi(-1) = -1$ 当且仅当 m 是偶数且 $(q-1)/m$ 为奇数.** 在其他情况下 $\psi(-1) = 1$.

Discussion B:

高斯和可以在很多情况下使用, 考虑下面的场景. 设 ψ 是 \mathbb{F}_q 的乘法特征, 那么根据式 (10) 对于所有 $c \in \mathbb{F}_q^*$ 有

$$\begin{aligned}\psi(c) &= \frac{1}{q} \sum_{d \in \mathbb{F}_q^*} \psi(d) \sum_{b \in \mathbb{F}_q} (\chi_b(c)) \overline{\chi_b(d)} \\ &= \frac{1}{q} \sum_{b \in \mathbb{F}_q} \chi_b(c) \sum_{d \in \mathbb{F}_q^*} \psi(d) \overline{\chi_b(d)}\end{aligned}$$

因此

$$\psi(c) = \frac{1}{q} \sum_{\chi} G(\psi, \bar{\chi}) \chi(c) \quad (16)$$

这个和就被扩展到了所有 \mathbb{F}_q 的加法特征上. 可以认为这是关于 \mathbb{F}_q 上的加法特征 ψ 的傅里叶展开, 高斯和在系数上出现.

类似的, 通过式 (13) 可以得到对于所有 $c \in \mathbb{F}_q^*$ 有

$$\chi(c) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \psi(c) \quad (17)$$

在进一步介绍高斯和的性质之前, 需要建立一些有用的原则. 设 Φ 表示 \mathbb{F}_q 上的首一多项式集合, λ 是 Φ 上的一个复值函数, 满足对于所有的 $g, h \in \Phi$ 有

$$\lambda(gh) = \lambda(g)\lambda(h) \quad (18)$$

且对于任意 $g \in \Phi$ 有 $|\lambda(g)| \leq 1$, 定义 $\lambda(1) = 1$.

注意, 这里的函数 λ 只是一个辅助函数, 只需要满足对于任意 $g \in \Phi$ 有 $|\lambda(g)| \leq 1$, $\lambda(1) = 1$ 且积性即可.

记 Φ_k 表示 Φ 中次数为 k 的多项式的集合, 考虑如下的幂级数

$$L(z) = \sum_{k=0}^{\infty} \left(\sum_{g \in \Phi_k} \lambda(g) \right) z^k \quad (19)$$

因为 Φ_k 上的多项式有 q^k 个, 所以 z^k 的系数的绝对值 $\leq q^k$. 所以这个幂级数在 $|z| < q^{-1}$ 时绝对收敛.

根据式 (18) 和多项式的唯一分解可以得到

$$\begin{aligned}
L(z) &= \sum_{g \in \Phi} \lambda(g) z^{\deg(g)} \\
&= \prod_f (1 + \lambda(f) z^{\deg(f)} + \lambda(f^2) z^{\deg(f^2)} + \dots) \\
&= \prod_f (1 + \lambda(f) z^{\deg(f)} + \lambda(f)^2 z^{2 \deg(f)} + \dots)
\end{aligned}$$

乘积遍历了所有 $\mathbb{F}_q[x]$ 上的首一不可约多项式 f . 那么就有

$$L(z) = \prod_f (1 - \lambda(f) z^{\deg(f)})^{-1}$$

两侧进行对数微分, 结果乘以 z 得到

$$z \frac{d \log L(z)}{dz} = \sum_f \frac{\lambda(f) \deg(f) z^{\deg(f)}}{1 - \lambda(f) z^{\deg(f)}}$$

把 $(1 - \lambda(f) z^{\deg(f)})^{-1}$ 扩展为几何级数, 有

$$\begin{aligned}
z \frac{d \log L(z)}{dz} &= \sum_f \lambda(f) \deg(f) z^{\deg(f)} (1 + \lambda(f) z^{\deg(f)} + \lambda(f)^2 z^{2 \deg(f)} + \dots) \\
&= \sum_f \deg(f) (\lambda(f) z^{\deg(f)} + \lambda(f)^2 z^{2 \deg(f)} + \lambda(f)^3 z^{3 \deg(f)} + \dots)
\end{aligned}$$

合并同类项得

$$z \frac{d \log L(z)}{dz} = \sum_{s=1}^{\infty} L_s z^s \quad (20)$$

其中

$$L_s = \sum_f \deg(f) \lambda(f)^{s / \deg(f)} \quad (21)$$

指数和就被拓展到了所有 $\mathbb{F}_q[x]$ 上满足 $\deg(f) \mid s$ 的所有首一不可约多项式 f 上了.

设存在一个正整数 t 对任意 $k > t$ 有

$$\sum_{g \in \Phi_k} \lambda(g) = 0 \quad (22)$$

那么 $L(z)$ 就是一个次数 $\leq t$ 的复多项式, 常数项是 1. 所以

$$L(z) = (1 - \omega_1 z)(1 - \omega_2 z) \dots (1 - \omega_t z) \quad (23)$$

其中 ω_i 都是复数. 所以就有

$$\begin{aligned}
z \frac{d \log L(z)}{dz} &= - \sum_{m=1}^t t \frac{\omega_m z}{1 - \omega_m z} \\
&= - \sum_{m=1}^t \omega_m z \sum_{j=0}^{\infty} \omega_m^j z^j \\
&= - \sum_{j=0}^{\infty} \left(\sum_{m=1}^t \omega_m^{j+1} \right) = - \sum_{s=1}^{\infty} \left(\sum_{m=1}^t \omega_m^s \right) z^s
\end{aligned}$$

和 (20) 对比后得到, 对于 $s \geq 1$ 有

$$L_s = -\omega_1^s - \omega_2^s - \dots - \omega_t^s \quad (24)$$

Theorem 5.14 Davenport-Hasse Theorem

设 χ 和 ψ 分别是 \mathbb{F}_q 的加法特征和乘法特征, 它们不全是平凡特征. 设 χ 和 ψ 被扩展为 χ' 和 ψ' 到 \mathbb{F}_q 的域扩张 E 上, $[E : \mathbb{F}_q = s]$. 那么

$$G(\psi', \chi') = (-1)^{s-1} G(\psi, \chi)^s$$

其中 $\chi'(\beta) = \chi(\text{Tr}_{E/\mathbb{F}_q}(\beta)), \beta \in E$. $\psi'(\beta) = \psi(N_{E/\mathbb{F}_q}(\beta)), \beta \in E^*$.

证明:

首先用 $\psi(0) = 0$ 扩展 ψ 的定义. 定义函数 λ , 首先 $\lambda(1) = 1$. 对于正次数多项式 $g \in \Phi$, $g(x) = x^k - c_1 x^{k-1} + \dots + (-1)^k c_k$, 令 $\lambda(g) = \psi(c_k) \psi(c_1)$. 那么显然 $\lambda(gh) = \lambda(g) \lambda(h)$.

对于 $k > 1$ 根据 c_1, c_k 的值划分 Φ_k . 在 Φ_k 中, 每个数对 (c_1, c_k) 都出现 q^{k-2} 次, 所以

$$\begin{aligned} \sum_{g \in \Phi_k} \lambda(g) &= q^{k-2} \sum_{c_1, c_k \in \mathbb{F}_q} \psi(c_k) \chi(c_1) \\ &= q^{k-2} \left(\sum_{c \in \mathbb{F}_q^*} \psi(c) \right) \left(\sum_{c \in \mathbb{F}_q} \chi(c) \right) \end{aligned}$$

由于 ψ 和 χ 有一个不是平凡的, 所以根据式 (9) 或 (12) 就可以得到对于 $k > 1$ 有

$$\sum_{g \in \Phi(k)} \lambda(g) = 0$$

所以式 (22) 在 $t = 1$ 下可以成立. 此外, Φ_1 包括了所有线性多项式 $x - c, c \in \mathbb{F}_q$, 所以

$$\sum_{g \in \Phi_1} \lambda(g) = \sum_{c \in \mathbb{F}_q} \psi(c) \chi(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c) \chi(c) = G(\psi, \chi)$$

因此根据式 (19) 有 $L(z) = 1 + G(\psi, \chi)z$, 因此根据 (23) 可以知道 $\omega_1 = -G(\psi, \chi)$. 那么根据式 (21) 和 λ 的积性, 就有

$$\begin{aligned} L_s &= \sum_f \deg(f) \lambda(f)^{s/\deg(f)} \\ &= \sum_f^* \deg(f) \lambda(f^{s/\deg(f)}) \end{aligned}$$

其中星号表示 $f(x) = x$ 被排除 (即 $c = 0$ 的情况) .

每个 f 在 E 上都有 $\deg(f)$ 个不同的非零根, 每个 f 的根 β 也是. 其中 \mathbb{F}_q 上的特征多项式为

$$f(x)^{s/\deg(f)} = x^s - c_1 x^{s-1} + \dots + (-1)^s c_s$$

其中 $c_1 = \text{Tr}_{E/\mathbb{F}_q}(\beta), c_s = N_{E/\mathbb{F}_q}(\beta)$. 因此

$$\begin{aligned} \lambda(f^{s/\deg(f)}) &= \psi(c_s) \chi(c_1) = \psi(N_{E/\mathbb{F}_q}(\beta)) \chi(\text{Tr}_{E/\mathbb{F}_q}(\beta)) \\ &= \psi'(\beta) \chi'(\beta) \end{aligned}$$

所以

$$L_s = \sum_f^* \deg(f) \lambda(f^{s/\deg(f)}) = \sum_f^* \sum_{\beta \in E, f(\beta)=0} \psi'(\beta) \chi'(\beta)$$

如果 f 遍历这个范围, 那么 β 就遍历 E^* 中的所有元素, 那么

$$L_s = \sum_{\beta \in E^*} \psi'(\beta) \chi'(\beta) = G(\psi', \chi')$$

然后根据式 (24) 就有

$$G(\psi', \chi') = -(-G(\psi, \chi))^s = (-1)^{s-1} G(\psi, \chi)^s$$

对于特殊的特征，对应的高斯和可以被计算出来.

Theorem 5.15

设 \mathbb{F}_q 是一个有限域，其中 $q = p^s$, p 是奇素数， $s \in \mathbb{N}$.

设 η 是 \mathbb{F}_q 的二次特征， χ_1 是 \mathbb{F}_q 的主加法特征. 那么

$$G(\eta, \chi_1) = \begin{cases} (-1)^{s-1} \sqrt{q} & p \equiv 1 \pmod{4} \\ (-1)^{s-1} i^s \sqrt{q} & p \equiv 3 \pmod{4} \end{cases}$$

证明： $\bar{\eta} = \eta$, 根据 Theorem 5.12(iv) 可以得到 $G(\eta, \chi_1)^2 = \eta(-1)q$. 所以

$$G(\eta, \chi_1) = \begin{cases} \pm \sqrt{q} & q \equiv 1 \pmod{4} \\ \pm i \sqrt{q} & q \equiv 3 \pmod{4} \end{cases} \quad (25)$$

难点在于确定符号.

首先考虑 $s = 1$ 的情况. 设 V 是 \mathbb{F}_p^* 上所有复值函数的集合，这是一个 $p-1$ 维的复数上的向量空间.

通过 \mathbb{F}_p^* 上元素的特征函数 f_1, f_2, \dots, f_{p-1} 可以形成一组 V 的基，其中当 $c = j$ 的时候 $f_j(c) = 1$, 否则 $f_j(c) = 0$. 其中 $j = 1, 2, \dots, p-1$. 然后通过 (11) 式的正交关系可以得到 \mathbb{F}_p 上的乘法特征 $\psi_0, \psi_1, \dots, \psi_{p-2}$ 也是 V 的一组基. 设 $\zeta = e^{2\pi i/p}$, 定义一个 V 上的二元关系 T , 对于 $h \in V$, 对于任意的 $c = 1, 2, \dots, p-1$ 有

$$(Th)(c) = \sum_{k=1}^{p-1} \zeta^{ck} h(k) \quad (26)$$

那么根据 Theorem 5.12(i) 可以知道 $T\psi = G(\psi, \chi_1)\bar{\psi}$ 对于 \mathbb{F}_p 上的任意乘法特征 ψ 都成立. 由于对于平凡特征和二次特征有 $\psi = \bar{\psi}$. 所以基 $\psi_0, \psi_1, \dots, \psi_{p-2}$ 上的矩阵 T 有两个对角元素，即 $G(\psi_0, \chi_1) = -1$ 和 $G(\eta, \chi_1)$, 和矩阵

$$\begin{pmatrix} 0 & G(\bar{\psi}, \chi_1) \\ G(\psi, \chi_1) & 0 \end{pmatrix}$$

分别对应一对共轭特征 $\psi, \bar{\psi}$, 分别是非平凡的和非二次的. 如果要计算 T 的行列式，那根据 Theorem 5.12(iv) 每块的贡献为

$$-G(\psi, \chi_1)G(\bar{\psi}, \chi_1) = -\psi(-1)p$$

所以

$$\det(T) = -G(\eta, \chi_1)(-p)^{(p-3)/2} \prod_{j=1}^{(p-3)/2} \psi_j(-1) \quad (27)$$

注意到 $\psi_j(-1) = \psi_1^j(-1) = (-1)^j$, 所以

$$\prod_{j=1}^{(p-3)/2} \psi_j(-1) = (-1)^{1+2+\dots+(p-3)/2} = (-1)^{(p-1)(p-3)/8} \quad (28)$$

由于

$$i^{(p-1)^2/4} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ i & p \equiv 3 \pmod{4} \end{cases}$$

根据式 (25) 就有

$$G(\eta, \chi_1) = \pm i^{(p-1)^2/4} \sqrt{p} \quad (29)$$

联立式 (27), (28), (29) 得

$$\det(T) = \pm (-1)^{(p-1)/2} i^{(p-1)^2/4 + (p-1)(p-3)/4} p^{(p-2)/2} \quad (30)$$

下面使用矩阵 T 在基 f_1, f_2, \dots, f_{p-1} 上计算 $\det(T)$. 根据式 (26) 有

$$\begin{aligned} \det(T) &= \det((\zeta^{jk})_{1 \leq j, k \leq p-1}) = \det((\zeta^j \zeta^{j(k-1)})_{1 \leq j, k \leq p-1}) \\ &= \zeta^{1+2+\dots+(p-1)} \det((\zeta^{j(k-1)})_{1 \leq j, k \leq p-1}) \\ &= \det((\zeta^{j(k-1)})_{1 \leq j, k \leq p-1}) \end{aligned}$$

这是一个范德蒙行列式, 所以

$$\det(T) = \prod_{1 \leq m < n \leq p-1} (\zeta^n - \zeta^m)$$

由 $\delta = e^{\pi i/p}$ 得到

$$\begin{aligned} \det(T) &= \prod_{1 \leq m < n \leq p-1} (\delta^{2n} - \delta^{2m}) \\ &= \prod_{1 \leq m < n \leq p-1} \delta^{n+m} (\delta^{n-m} - \delta^{-(n-m)}) \\ &= \prod_{1 \leq m < n \leq p-1} \delta^{n+m} \prod_{1 \leq m < n \leq p-1} (2i \sin \frac{\pi(n-m)}{p}) \end{aligned}$$

由于

$$\begin{aligned} \sum_{1 \leq m < n \leq p-1} (n+m) &= \sum_{n=2}^{p-1} \sum_{m=1}^{n-1} (n+m) \\ &= \frac{3}{2} \sum_{n=2}^{p-1} n(n-1) = \frac{3}{2} \sum_{n=1}^{p-2} (n^2 + n) \\ &= \frac{p(p-1)(p-2)}{2} \end{aligned}$$

那么第一个乘积就等于

$$\delta^{p(p-1)(p-2)/2} = (-1)^{(p-1)(p-2)/2} = (-1)^{(p-1)/2}$$

此外

$$A = \prod_{1 \leq m < n \leq p-1} (2 \sin \frac{\pi(n-m)}{p}) > 0$$

因此

$$\det(T) = (-1)^{(p-1)/2} i^{(p-1)(p-2)/2} A$$

其中 $A > 0$. 对比式 (30) 可知正号在 (29) 式中恒成立, 所以这个定理对 $s = 1$ 成立.

根据 Theorem 5.14, 由于每个 \mathbb{F}_p 的主加法特征都可以通过式 (7) 扩展到 \mathbb{F}_q 上的主特征. 每个 \mathbb{F}_p 上的二次特征也可扩展到 \mathbb{F}_q 上的二次特征. 所以定理对于所有情况都是成立的.

下面再介绍一个计算高斯和的公式. 这个公式对于乘法特征的范围更宽, 但是对域有更严格的限制.

Theorem 5.16 Stickelberger's Theorem

设 q 是一个素数的幂, 设 ψ 是域 \mathbb{F}_{q^2} 的一个非平凡乘法特征, 这个域的特征是 $m, m \mid q+1$. 设 χ_1 是 \mathbb{F}_{q^2} 的主加法特征. 那么

$$G(\psi, \chi_1) = \begin{cases} q & m \text{ 是奇数或 } \frac{q+1}{m} \text{ 是偶数} \\ -q & m \text{ 是偶数且 } \frac{q+1}{m} \text{ 是奇数} \end{cases}$$

证明: 记 $E = \mathbb{F}_{q^2}, F = \mathbb{F}_q$. 设 γ 是 E 上的本原元, 令 $g = \gamma^{q+1}$. 那么有 $g^{q-1} = 1$, 从而 $g \in F$. 且 g 是 F 的本原元.

每个 $\alpha \in E^*$ 可以写成 $\alpha = g^j \gamma^k$ 的形式, 其中 $0 \leq j < q-1, 0 \leq k < q+1$. 由于 $\psi(g) = \psi^{q+1}(\gamma) = 1$, 那么就有

$$\begin{aligned} G(\psi, \chi_1) &= \sum_{j=0}^{q-2} \sum_{k=0}^q \psi(g^j \gamma^k) \chi_1(g^j \gamma^k) \\ &= \sum_{k=0}^q \psi^k(\gamma) \sum_{j=0}^{q-2} \chi_1(g^j \gamma^k) \\ &= \sum_{k=0}^q \psi^k(\gamma) \sum_{b \in F^*} \chi_1(b \gamma^k) \end{aligned} \quad (31)$$

若 τ_1 是 F 的主加法特征, 那么根据式 (7) 有 $\chi_1(b \gamma^k) = \tau_1(\text{Tr}_{E/F}(b \gamma^k))$. 因此根据式 (9) 有

$$\begin{aligned} \sum_{b \in F^*} \chi_1(b \gamma^k) &= \sum_{b \in F^*} \tau_1(b \text{Tr}_{E/F}(\gamma^k)) \\ &= \begin{cases} -1 & \text{Tr}_{E/F}(\gamma^k) \neq 0 \\ q-1 & \text{Tr}_{E/F}(\gamma^k) = 0 \end{cases} \end{aligned} \quad (32)$$

现在有 $\text{Tr}_{E/F}(\gamma^k) = \gamma^k + \gamma^{kq}$. 所以有

$$\text{Tr}_{E/F}(\gamma^k) = 0 \quad (33)$$

当且仅当 $\gamma^{k(q-1)} = -1$ 时成立. 如果 q 是奇数, 后面的条件等价于 $k = (q+1)/2$, 所以根据式 (32) 有

$$\sum_{b \in F^*} \chi_1(b \gamma^k) = \begin{cases} -1 & 0 \leq k < q+1, k \neq \frac{q+1}{2} \\ q-1 & k = \frac{q+1}{2} \end{cases}$$

联立式 (31), 因为 $\psi(\gamma) \neq 1, \psi^{q+1}(\gamma) = 1$ 所以有

$$\begin{aligned} G(\psi, \chi_1) &= - \sum_{k=0, k \neq (q+1)/2}^q \psi^k(\gamma) + (q-1) \psi^{(q+1)/2}(\gamma) \\ &= - \sum_{k=0}^q \psi^k(\gamma) + q \psi^{(q+1)/2}(\gamma) \\ &= q \psi^{(q+1)/2}(\gamma) \end{aligned}$$

所以当 $(q+1)/m$ 是偶数的时候, $\psi^{(q+1)/2}(\gamma) = 1$. 否则等于 -1 . 所以对于奇数 q 有

$$G(\psi, \chi_1) = \begin{cases} q & \frac{q+1}{m} \text{ 是偶数} \\ -q & \frac{q+1}{m} \text{ 是奇数} \end{cases} \quad (34)$$

如果 q 是偶数, 那么在式 (33) 的条件下, 这个条件等价于 $\gamma^{k(q-1)} = 1$, 当 $0 \leq k < q+1$ 的时候只有 $k=0$ 的时候满足, 那么根据式 (32) 就有

$$\sum_{b \in F^*} \chi_1(b \gamma^k) = \begin{cases} -1 & 1 \leq k \leq q \\ q-1 & k=0 \end{cases}$$

然后 (31) 式就为

$$G(\psi, \chi_1) = - \sum_{k=1}^q \psi^k(\gamma) + q - 1 = - \sum_{k=0}^q \psi^k(\gamma) + q = q$$

这个式子和 (34) 式成立，即表明原命题成立.

下面给出一个高斯和的应用，尝试使用高斯和去证明二次互反律.

首先给出代数整数的定义：它是有理整数的推广。设 a 为复数，若存在系数为有理整数的首一多项式 $f(x)$ 使 $f(a) = 0$ ，则称 a 为代数整数。

Theorem 5.17 Law of Quadratic Reciprocity

对于任意不同的奇素数 p, r 有

$$\left(\frac{p}{r}\right)\left(\frac{r}{p}\right) = (-1)^{(p-1)(r-1)/4}$$

证明：

设 η 是 \mathbb{F}_p 的二次特征， χ_1 是 \mathbb{F}_p 的主加法特征，令 $G = G(\eta, \chi_1)$. 根据式 (25) 有 $G^2 = (-1)^{(p-1)/2} p = \bar{p}$, 所以

$$G^r = (G^2)^{(r-1)/2} G = \bar{p}^{(r-1)/2} G \quad (35)$$

设 R 表示代数整数环，即 R 里面包括了所有首一整系数多项式的复数根. 由于有限域的加法特征和乘法特征值都是复单位根，且每个复单位根都是代数整数，所以高斯和也是**代数整数**, 即 $G \in R$.

设 (r) 是 R 中由 r 生成的主理想，那么剩余类环 $R/(r)$ 的特征是 r . 所以有

$$G^r = \left(\sum_{c \in \mathbb{F}_p^*} \eta(c) \chi_1(c) \right)^r \equiv \sum_{c \in \mathbb{F}_p^*} \eta^r(c) \chi_1^r(c) \pmod{(r)}$$

那么根据 Theorem 5.12(i) 有

$$\sum_{c \in \mathbb{F}_p^*} \eta^r(c) \chi_1^r(c) = \sum_{c \in \mathbb{F}_p^*} \eta(c) \chi_r(c) = G(\eta, \chi_r) = \eta(r) G$$

所以

$$G^r \equiv \eta(r) G \pmod{(r)}$$

联立式 (35) 得

$$\bar{p}^{(r-1)/2} G \equiv \eta(r) G \pmod{(r)}$$

两边同时乘以 G

$$\bar{p}^{(r-1)/2} \bar{p} \equiv \eta(r) \bar{p} \pmod{(r)}$$

由于同余式两侧都是 \mathbb{Z} 中的元素，所以有

$$\bar{p}^{(r-1)/2} \bar{p} \equiv \eta(r) \bar{p} \pmod{r}$$

而 \bar{p} 和 r 互素，因此

$$\bar{p}^{(r-1)/2} \equiv \eta(r) \pmod{r}$$

而 $\bar{p} = (-1)^{(p-1)/2}p, p^{r-1} \equiv 1 \pmod{r}$. 两侧同乘 $p^{(r-1)/2}$ 得到

$$(-1)^{(p-1)(r-1)/4} \equiv p^{(r-1)/2} \eta(r) \pmod{r} \quad (36)$$

而 $p^{(r-1)/2} \equiv \pm 1 \pmod{r}$. 当且仅当 p 是 r 的二次剩余时成立. 因此

$$p^{(r-1)/2} \equiv \left(\frac{p}{r}\right) \pmod{r}$$

由于 $\eta(r) = \left(\frac{r}{p}\right)$. 由式 (36) 得

$$(-1)^{(p-1)(r-1)/4} \equiv \left(\frac{p}{r}\right) \left(\frac{r}{p}\right) \pmod{r}$$

但是等式两侧的值只能是 ± 1 . 且有 $r \geq 3$. 所以

$$(-1)^{(p-1)(r-1)/4} \equiv \left(\frac{p}{r}\right) \left(\frac{r}{p}\right)$$

原命题得证.

5.3 Jacobi Sum

设 λ 是 \mathbb{F}_q 的乘法特征, 定义在所有 \mathbb{F}_q 的非零元上. 定义当 λ 是平凡特征的时候 $\lambda(0) = 1$, 否则 $\lambda(0) = 0$. 那么

$$\sum_{c \in \mathbb{F}_q} \lambda(c) = \begin{cases} q & \lambda \text{ 是平凡特征} \\ 0 & \lambda \text{ 是非平凡特征} \end{cases} \quad (37)$$

此外, 对于 $a_1, a_2 \in \mathbb{F}_q$ 有 $\lambda(a_1 a_2) = \lambda(a_1) \lambda(a_2)$.

注意到, 令 $a_1 = a_2 = 1$, 可以知道 $\lambda(1) = \lambda(1) \lambda(1)$. 从而 $\lambda(1) = 1$. 如果 $a_1 = a_2 = -1$ 可知 $\lambda(-1)^2 = 1$, 即 $\lambda(-1) = \pm 1$.

设 $\lambda_1, \dots, \lambda_k$ 是 \mathbb{F}_q 的乘法特征, $a \in \mathbb{F}_q$ 已经确定. 定义和式

$$J_a(\lambda_1, \dots, \lambda_k) = \sum_{c_1 + \dots + c_k = a} \lambda_1(c_1) \dots \lambda_k(c_k)$$

这个和有 q^{k-1} 项. 如果 $a \neq 0$, 可以令 $c_i = ab_i$. 从而 $b_1 + \dots + b_k = 1$ 且

$$\begin{aligned} J_a(\lambda_1, \dots, \lambda_k) &= \sum_{b_1 + \dots + b_k = 1} \lambda_1(ab_1) \dots \lambda_k(ab_k) \\ &= \lambda_1(a) \dots \lambda_k(a) \sum_{b_1 + \dots + b_k = 1} \lambda_1(b_1) \dots \lambda_k(b_k) \\ &= (\lambda_1 \dots \lambda_k)(a) J_1(\lambda_1, \dots, \lambda_k) \end{aligned} \quad (38)$$

根据这个关系式, 我们只需要考虑 J_0 和 J_1 即可. 下面用略简洁的方法表示 J_1 .

Definition 5.18 Jacobi Sums

设 $\lambda_1, \dots, \lambda_k$ 是 \mathbb{F}_q 的乘法特征, 那么和式

$$J(\lambda_1, \dots, \lambda_k) = \sum_{c_1 + \dots + c_k = 1} \lambda_1(c_1) \dots \lambda_k(c_k)$$

被称为 \mathbb{F}_q 上的雅可比和. 这里的 J 相当于上面的 J_1 .

显然 $k = 1$ 的时候, $J(\lambda_1) = \lambda_1(1) = 1$. 这对任意的乘法特征都成立, 所以讨论雅可比和的时候只考虑 $k \geq 2$ 的情况.

同时根据定义不难发现在求雅可比和的时候, **和式的结果和乘法特征的顺序无关**.

Theorem 5.19 Value of J_1

设 \mathbb{F}_q 的乘法特征 $\lambda_1, \dots, \lambda_k$ 都是平凡特征, 那么

$$J(\lambda_1, \dots, \lambda_k) = J_0(\lambda_1, \dots, \lambda_k) = q^{k-1} \quad (39)$$

如果这些乘法特征不全为平凡特征, 那么

$$J(\lambda_1, \dots, \lambda_k) = J_0(\lambda_1, \dots, \lambda_k) = 0 \quad (40)$$

证明: 对于式 (39), 由于和式有 q^{k-1} 项, 若每个特征都是平凡特征, 那么和式的结果就是 q^{k-1} .

对于式 (40), 不妨设非平凡特征是 $\lambda_1, \dots, \lambda_h$, 平凡特征是 $\lambda_{h+1}, \dots, \lambda_k$. 其中 $1 \leq h \leq k-1$. 那么就有

$$\begin{aligned}
J(\lambda_1, \dots, \lambda_k) &= \sum_{c_1 + \dots + c_k = 1} \lambda_1(c_1) \dots \lambda_k(c_k) \\
&= \sum_{c_1 + \dots + c_h = 1} \lambda_1(c_1) \dots \lambda_h(c_h)
\end{aligned}$$

对于 $c_1, \dots, c_h \in \mathbb{F}_q$, 方程 $c_{h+1} + \dots + c_k = 1 - c_1 - \dots - c_h$ 有 q^{k-h-1} 组解 (c_{h+1}, \dots, c_k) . 因此根据式 (35) 有

$$\begin{aligned}
J(\lambda_1, \dots, \lambda_k) &= q^{k-h-1} \sum_{c_1 + \dots + c_h = 1} \lambda_1(c_1) \dots \lambda_h(c_h) \\
&= q^{k-h-1} \left(\sum_{c_1 \in \mathbb{F}_q} \lambda_1(c_1) \right) \dots \left(\sum_{c_h \in \mathbb{F}_q} \lambda_h(c_h) \right) \\
&= 0
\end{aligned}$$

Theorem 5.20 Value of J_0

设 $\lambda_1 \dots \lambda_k$ 是 \mathbb{F}_q 的乘法特征, λ_k 是非平凡特征, 那么如果所有特征都非平凡, 则有

$$J_0(\lambda_1, \dots, \lambda_k) = 0 \quad (41)$$

若 $\lambda_1 \dots \lambda_k$ 是平凡特征, 则有

$$J_0(\lambda_1, \dots, \lambda_k) = \lambda_k(-1)(q-1)J(\lambda_1, \dots, \lambda_{k-1}) \quad (42)$$

证明: $k=1$ 显然, 考虑 $k \geq 2$. 那么

$$\begin{aligned}
J_0(\lambda_1, \dots, \lambda_k) &= \sum_{a \in \mathbb{F}_q} \left(\sum_{c_1 + \dots + c_{k-1} = -a} \lambda_1(c_1) \dots \lambda_{k-1}(c_{k-1}) \right) \lambda_k(a) \\
&= \sum_{a \in \mathbb{F}_q} J_{-a}(\lambda_1, \dots, \lambda_{k-1}) \lambda_k(a)
\end{aligned}$$

由于 λ_k 非平凡, 所以有 $\lambda_k(0) = 0$. 所以根据式 (38) 就有

$$\begin{aligned}
J_0(\lambda_1, \dots, \lambda_k) &= \sum_{a \in \mathbb{F}_q^*} J_{-a}(\lambda_1, \dots, \lambda_{k-1}) \lambda_k(a) \\
&= J(\lambda_1, \dots, \lambda_{k-1}) \sum_{a \in \mathbb{F}_q^*} (\lambda_1 \dots \lambda_{k-1})(-a) \lambda_k(a) \\
&= (\lambda_1 \dots \lambda_{k-1})(-1) J(\lambda_1, \dots, \lambda_k) \sum_{a \in \mathbb{F}_q^*} (\lambda_1 \dots \lambda_k)(a)
\end{aligned}$$

如果 $\lambda_1 \dots \lambda_k$ 非平凡, 那么根据式 (12) 可以知道这个和为 0.

如果 $\lambda_1 \dots \lambda_k$ 是平凡特征, 那么最后的和为 $q-1$.

然后根据 $(\lambda_1 \dots \lambda_{k-1})(-1) = \overline{\lambda_k}(-1) = \lambda_k(-1)$. 原式成立.

Theorem 5.21 Connection between Jacobi Sums and Gauss Sums

设 $\lambda_1, \dots, \lambda_k$ 是 \mathbb{F}_q 的非平凡乘法特征, χ 是 \mathbb{F}_q 的非平凡加法特征, 那么如果 $\lambda_1 \dots \lambda_k$ 非平凡, 则

$$J(\lambda_1, \dots, \lambda_k) = \frac{G(\lambda_1, \chi) \dots G(\lambda_k, \chi)}{G(\lambda_1 \dots \lambda_k, \chi)} \quad (43)$$

若 $\lambda_1 \dots \lambda_k$ 平凡, 则

$$\begin{aligned}
J(\lambda_1, \dots, \lambda_k) &= -\lambda_k(-1) J(\lambda_1, \dots, \lambda_{k-1}) \\
&= -\frac{1}{q} G(\lambda_1, \chi) \dots G(\lambda_k, \chi)
\end{aligned} \quad (44)$$

证明: 由于每个乘法特征都非平凡, 所以 $\lambda_i(0) = 0$, 且

$$G(\lambda_i, \chi) = \sum_{c_i \in \mathbb{F}_q} \lambda_i(c_i) \chi(c_i)$$

因此

$$\begin{aligned} G(\lambda_1, \chi) \dots G(\lambda_k, \chi) &= \left(\sum_{c_1 \in \mathbb{F}_q} \lambda_1(c_1) \chi(c_1) \right) \dots \left(\sum_{c_k \in \mathbb{F}_q} \lambda_k(c_k) \chi(c_k) \right) \\ &= \sum_{c_1, \dots, c_k \in \mathbb{F}_q} \lambda_1(c_1) \dots \lambda_k(c_k) \chi(c_1 + \dots + c_k) \\ &= \sum_{a \in \mathbb{F}_q} \chi(a) \sum_{c_1 + \dots + c_k = a} \lambda_1(c_1) \dots \lambda_k(c_k) \\ &= \sum_{a \in \mathbb{F}_q} \chi(a) J_a(\lambda_1, \dots, \lambda_k) \end{aligned}$$

如果 $\lambda_1 \dots \lambda_k$ 非平凡, 那么 $J_0(\lambda_1, \dots, \lambda_k) = 0$. 根据式 (38) 就有

$$\begin{aligned} G(\lambda_1, \chi) \dots G(\lambda_k, \chi) &= J(\lambda_1, \dots, \lambda_k) \sum_{a \in \mathbb{F}_q^*} (\lambda_1 \dots \lambda_k)(a) \chi(a) \\ &= J(\lambda_1, \dots, \lambda_k) G(\lambda_1 \dots \lambda_k, \chi) \end{aligned}$$

由于 $\lambda_1 \dots \lambda_k$ 和 χ 都是非平凡特征, 所以 $G(\lambda_1 \dots \lambda_k, \chi) \neq 0$. 所以式 (43) 得证.

如果 $\lambda_1 \dots \lambda_k$ 平凡, 那么就有 $J_a(\lambda_1, \dots, \lambda_k) = J(\lambda_1, \dots, \lambda_k)$ 对于所有 $a \in \mathbb{F}_q^*$ 成立, 故根据式 (37) 有

$$\begin{aligned} J_0(\lambda_1, \dots, \lambda_k) + (q-1)J(\lambda_1, \dots, \lambda_k) &= \sum_{a \in \mathbb{F}_q} J_a(\lambda_1, \dots, \lambda_k) \\ &= \sum_{c_1, \dots, c_k \in \mathbb{F}_q} \lambda_1(c_1) \dots \lambda_k(c_k) \\ &= \left(\sum_{c_1 \in \mathbb{F}_q} \lambda_1(c_1) \right) \dots \left(\sum_{c_k \in \mathbb{F}_q} \lambda_k(c_k) \right) \\ &= 0 \end{aligned}$$

然后根据式 (42) 可知, 式 (44) 的第一个等号成立, 即

$$\begin{aligned} J(\lambda_1, \dots, \lambda_k) &= -(q-1)J_0(\lambda_1, \dots, \lambda_k) \\ &= -(q-1)\lambda_k(-1)(q-1)J(\lambda_1, \dots, \lambda_k) \\ &= -\lambda_k(-1)J(\lambda_1, \dots, \lambda_{k-1}) \end{aligned}$$

另外, 由于 $\lambda_1 \dots \lambda_{k-1}$ 是非平凡特征, 应用式 (43) 可得

$$\begin{aligned} \lambda_k(-1)J(\lambda_1, \dots, \lambda_{k-1}) &= \frac{\lambda_k(-1)G(\lambda_1, \chi) \dots G(\lambda_{k-1}, \chi)}{G(\lambda_1 \dots \lambda_{k-1}, \chi)} \\ &= \frac{\lambda_k(-1)G(\lambda_1, \chi) \dots G(\lambda_{k-1}, \chi)G(\lambda_k, \chi)}{G(\overline{\lambda_k}, \chi)G(\lambda_k, \chi)} \\ &= \frac{1}{q}G(\lambda_1, \chi) \dots G(\lambda_k, \chi) \end{aligned}$$

从而式 (44) 的第二个等号也成立. 最后一步等号成立是因为 **Theorem 5.12(iv)**, 即对于非平凡的加法特征 χ 和非平凡乘法特征 λ_k 有

$$G(\lambda_k, \chi)G(\overline{\lambda_k}, \chi) = \lambda_k(-1)q$$

直接代入上式可以知道等号成立.

Theorem 5.22 Value of J_1

设 $\lambda_1, \dots, \lambda_k$ 是 \mathbb{F}_q 的非平凡乘法特征, 那么如果 $\lambda_1 \dots \lambda_k$ 是非平凡的

$$|J(\lambda_1, \dots, \lambda_k)| = q^{(k-1)/2} \quad (45)$$

如果 $\lambda_1 \dots \lambda_k$ 是平凡的, 则

$$|J(\lambda_1, \dots, \lambda_k)| = q^{(k-2)/2} \quad (46)$$

证明: 对于非平凡乘法特征 ψ 和非平凡加法特征 χ 有 $|G(\psi, \chi)| = q^{1/2}$. 那么根据式 (43) 有

$$|J(\lambda_1, \dots, \lambda_k)| = \left| \frac{G(\lambda_1, \chi) \dots G(\lambda_k, \chi)}{G(\lambda_1 \dots \lambda_k, \chi)} \right| = \left| \frac{q^{k/2}}{q^{1/2}} \right| = q^{(k-1)/2}$$

所以式 (45) 成立.

如果 $\lambda_1 \dots \lambda_k$ 是平凡的, 则根据式 (44) 有

$$|J(\lambda_1, \dots, \lambda_k)| = \left| -\frac{1}{q} G(\lambda_1, \chi) \dots G(\lambda_k, \chi) \right| = \left| -\frac{1}{q} q^{k/2} \right| = q^{(k-2)/2}$$

所以式 (46) 成立.

Corollary 5.23

设 $\lambda_1, \dots, \lambda_k$ 是 \mathbb{F}_q 的非平凡乘法特征, 如果 $\lambda_1 \dots \lambda_k$ 是平凡的, 则有

$$|J_0(\lambda_1, \dots, \lambda_k)| = (q-1)q^{(k-2)/2}$$

证明: 根据式 (42) 和式 (45) 显然成立.

Example 5.24

用雅可比和证明二次互反律.

证明: 设 p 和 r 是不同的奇素数, η 和 χ_1 分别是 \mathbb{F}_p 的二次特征和主加法特征, 记 $G = G(\eta, \chi_1)$. 设 J 是 \mathbb{F}_p 上定义的雅可比和

$$J = \sum_{c_1 + \dots + c_r = 1} \eta(c_1) \dots \eta(c_r)$$

由于 η^{r+1} 是平凡特征, 继续记 $\bar{p} = (-1)^{(p-1)/2} p$, 那么根据式 (44) 就有

$$G^{r+1} = \eta(-1) p J = \bar{p} J$$

又因为 $\bar{p} = G^2$, 那么

$$G^{r+1} = (G^2)^{(r+1)/2} = \bar{p}^{(r+1)/2}$$

对比可得

$$J = \bar{p}^{(r-1)/2} \quad (47)$$

下面考虑 J 中的项. 由于 η 只能取值 $0, \pm 1$, 所以每个 J 的项都是整数. 如果每个 c_i 都相等的话, 那么相同的值等于 r^{-1} , 那么对应的 J 中的项的值就是 $\eta^r(r^{-1}) = \eta(r^{-1}) = \eta(r)$. 反过来如果不是每个 c_i 都相等, 那么 r 元组 (c_1, \dots, c_r) 就有 r 种不同取值构成循环. 对应的 J 中的项的值就有相同的值, 这些项的和模 r 就等于 0 了.

所以就有 $J \equiv \eta(r) \pmod{r}$. 联立式 (47) 就有

$$\bar{p}^{(r-1)/2} \equiv \eta(r) \pmod{r}$$

下面的证明过程和 Theorem 5.17 的剩余部分一致.

Example 5.25

用雅可比和证明: 每个模 4 余 1 的素数 p 都可以表示成两个整数的平方之和.

证明: 因为 $4 \mid p-1$, 所以根据 Corollary 5.9 可以得到存在一个 \mathbb{F}_p 上的阶为 4 的乘法特征 λ .

那么 λ 的取值只能是 $0, \pm 1, \pm i$. 所以就有 $\eta = \lambda^2$. 所以存在整数 A, B 使得

$$J(\lambda, \eta) = \sum_{c_1+c_2=1} = \lambda(c_1)\eta(c_2) = A + Bi$$

根据式 (45) 有

$$p = |J(\lambda, \eta)|^2 = A^2 + B^2$$

所以结论证毕. 模 4 余 3 的素数不能被表示成这种形式, 这是因为 A, B 的平方模 4 的值为 0 或 1, 所以 $A^2 + B^2$ 模 4 的值不可能是 3.

唯一剩下的素数为 $p = 2$ 显然可以表示成两个整数的平方之和, 即 $2 = 1^2 + 1^2$.

Theorem 5.26

设 $\lambda_1, \dots, \lambda_k$ 是 \mathbb{F}_q 的乘法特征, 这些特征不全为平凡特征. 设 \mathbb{F}_q 及其域扩张 E . 且 $[E : \mathbb{F}_q] = s$. 那么这些乘法特征可以被扩展为 $\lambda'_1, \lambda'_2, \dots, \lambda'_k$. 则有

$$J(\lambda'_1, \dots, \lambda'_k) = (-1)^{(s-1)(k-1)} J(\lambda_1, \dots, \lambda_k)^s \quad (48)$$

证明: 显然特征扩展后不影响其平凡/非平凡的性质. 因此, 如果某些特征是平凡特征, 那根据式 (40) 可知式子两侧都等于 0, 从而相等. 如果所有的特征都是非平凡特征且其乘积也非平凡, 考虑 \mathbb{F}_q 上的一个加法特征 χ . 那么根据式 (43) 和 Theorem 5.14 就可以得到

$$\begin{aligned} J(\lambda'_1, \dots, \lambda'_k) &= \frac{G(\lambda'_1, \chi') \dots G(\lambda'_k, \chi')}{G(\lambda'_1 \dots \lambda'_k, \chi')} \\ &= \frac{(-1)^{s-1} G(\lambda_1, \chi)^s \dots (-1)^{s-1} G(\lambda_k, \chi)^s}{(-1)^{s-1} G(\lambda_1 \dots \lambda_k, \chi)^s} \\ &= (-1)^{(s-1)(k-1)} J(\lambda_1, \dots, \lambda_k)^s \end{aligned}$$

如果所有特征都是非平凡特征且乘积为平凡特征, 那么根据式 (44) 和 Theorem 5.14 就可以得到

$$\begin{aligned}
J(\lambda'_1, \dots, \lambda'_k) &= -\frac{1}{q^s} G(\lambda'_1, \chi') \dots G(\lambda'_k, \chi') \\
&= -\frac{1}{q^s} (-1)^{(s-1)k} G(\lambda_1, \chi)^s \dots G(\lambda_k, \chi)^s \\
&= (-1)^{(s-1)k} (-1)^{-(s-1)} \left(-\frac{1}{q} G(\lambda_1, \chi) \dots G(\lambda_k, \chi)\right)^s \\
&= (-1)^{(s-1)(k-1)} J(\lambda_1, \dots, \lambda_k)^s
\end{aligned}$$

综上, 结论成立.

对于 $k = 2$ 的情况有特殊的结论, 这种也是雅可比和被应用最多的情况.

Theorem 5.27

设 λ 是 \mathbb{F}_q 上的阶为 $m \geq 2$ 的乘法特征, χ 是 \mathbb{F}_q 上的非平凡加法特征, 那么

$$G(\lambda, \chi)^m = \lambda(-1)qJ(\lambda, \lambda)J(\lambda, \lambda^2) \dots J(\lambda, \lambda^{m-2}) \quad (49)$$

证明: 考虑 $m \geq 3$. 根据式 (43), 对于 $1 \leq j \leq m-2$ 有

$$\frac{G(\lambda, \chi)G(\lambda^j, \chi)}{G(\lambda^{j+1}, \chi)} = J(\lambda, \lambda^j)$$

对这 $m-2$ 个等式做积有

$$\frac{G(\lambda, \chi)^{m-1}}{G(\lambda^{m-1}, \chi)} = J(\lambda, \lambda)J(\lambda, \lambda^2) \dots J(\lambda, \lambda^{m-2}) \quad (50)$$

由于 λ^m 是平凡特征, 那么 $\lambda^{m-1} = \bar{\lambda}$, 从而根据 Theorem 5.12(iv) 有

$$G(\lambda, \chi)G(\lambda^{m-1}, \chi) = \lambda(-1)q \quad (51)$$

把式 (50), (51) 两侧相乘就得到了结果.

当 $m = 2$ 的时候, 右侧的 J 都不存在, 从而直接得到了式 (51). 从而结论成立.

在 $k = 2$ 的时候, 可以和高斯和存在关系.

Theorem 5.28 Davenport-Hasse Relation

设 λ, ψ 是 \mathbb{F}_q 的乘法特征, λ 的阶为 $m \geq 2$, ψ^m 是非平凡特征, χ_b 是 \mathbb{F}_q 的非平凡加法特征. 那么

$$\frac{G(\psi, \chi_b)^m}{G(\psi^m, \chi_{mb})} = \prod_{j=1}^{m-1} J(\psi, \lambda^j)$$

Corollary 5.29

设 λ, ψ 是 \mathbb{F}_q 的乘法特征, λ 的阶为 $m \geq 2$, ψ^m 是非平凡特征, χ_b 是 \mathbb{F}_q 的非平凡加法特征.

那么当 m 是奇数的时候

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = q^{(m-1)/2} G(\psi^m, \chi_{mb}) \quad (52)$$

当 m 是偶数的时候

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = (-1)^{(q-1)(m-2)/8} q^{(m-2)/2} G(\eta, \chi_b) G(\psi^m, \chi_{mb}) \quad (53)$$

其中 η 是 \mathbb{F}_q 的二次特征.

下面给出基于 Theorem 5.28 的证明.

证明: 首先, $(\psi\lambda^j)^m = \psi^m \lambda^{jm} = \psi^m$ 不是平凡特征, 可以得到 $\psi\lambda^j$ 也是非平凡特征. 所以对 Theorem 5.28 应用 (43) 式得

$$\frac{G(\psi, \chi_b)^m}{G(\psi^m, \chi_{mb})} = \prod_{j=1}^{m-1} \frac{G(\psi, \chi_b) G(\lambda^j, \chi_b)}{G(\psi\lambda^j, \chi_b)} = G(\psi, \chi_b)^{m-1} \prod_{j=1}^{m-1} \frac{G(\lambda^j, \chi_b)}{G(\psi\lambda^j, \chi_b)}$$

整理得

$$\prod_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = G(\psi^m, \chi_{mb}) \prod_{j=1}^{m-1} G(\lambda^j, \chi_b) \quad (54)$$

当 m 是奇数时, 有

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = \prod_{j=1}^{(m-1)/2} G(\lambda^j, \chi_b) G(\lambda^{m-j}, \chi_b)$$

因为 λ^m 是平凡特征, 所以 $\lambda^{m-j} = \overline{\lambda^j}$. 所以根据 Theorem 5.12(iv) 得

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = q^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \lambda^j (-1)$$

因为 m 是奇数, 所以 $\lambda(-1) = 1$. 所以

$$\prod_{j=1}^{m-1} G(\lambda^j, \chi_b) = q^{(m-1)/2}$$

代入 (54) 式得到 (52) 式成立.

当 m 是偶数时, 同理可以得到

$$\begin{aligned} \prod_{j=1}^{m-1} G(\lambda^j, \chi_b) &= G(\lambda^{m/2}, \chi_b) \prod_{j=1}^{(m-2)/2} G(\lambda^j, \chi_b) G(\lambda^{m-j}, \chi_b) \\ &= G(\eta, \chi_b) \prod_{j=1}^{(m-2)/2} G(\lambda^j, \chi_b) G(\overline{\lambda^j}, \chi_b) \\ &= q^{(m-2)/2} G(\eta, \chi_b) \prod_{j=1}^{(m-2)/2} \lambda^j (-1) \end{aligned}$$

根据 Remark 5.13 可知当 $(q-1)/m$ 为偶数的时候 $\lambda(-1) = 1$, 否则为 -1 . 即 $\lambda(-1) = (-1)^{(q-1)/m}$. 代入上式可得

$$\begin{aligned} \prod_{j=1}^{m-1} G(\lambda^j, \chi_b) &= q^{(m-2)/2} G(\eta, \chi_b) \prod_{j=1}^{(m-2)/2} (-1)^{j(q-1)/m} \\ &= q^{(m-2)/2} G(\eta, \chi_b) (-1)^{(q-1)(m-2)/8} \end{aligned}$$

代入 (54) 式可得 (53) 式成立. 证毕.

回头看 Theorem 5.28 的证明, 这个需要通过代数数论的方法去证明, 这里两种额外满足不同条件情况下的初等证明.

Discussion 5.29(I) Proof of Theorem 5.28 when $\psi = \eta$

第一种是 $\psi = \eta$ 的情况, 从而有 m 和 q 都是奇数.

因此 Theorem 5.28 和式 (52) 等价, 只需要证明 (52) 式成立即可.

考虑 (52) 式左侧

$$\begin{aligned}\prod_{j=0}^{m-1} G(\eta\lambda^j, \chi_b) &= G(\eta, \chi_b) \prod_{j=1}^{m-1} G(\eta\lambda^j, \chi_b) G(\eta\lambda^{m-j}, \chi_b) \\ &= G(\eta, \chi_b) \prod_{j=1}^{m-1} G(\eta\lambda^j, \chi_b) G(\overline{\eta\lambda^j}, \chi_b) \\ &= G(\eta, \chi_b) q^{(m-1)/2} \prod_{j=1}^{(m-1)/2} (\eta\lambda^j)(-1)\end{aligned}$$

这个时候 $\lambda(-1) = 1, \eta(-1) = (-1)^{(q-1)/2}$, 从而

$$\prod_{j=0}^{m-1} G(\eta\lambda^j, \chi_b) = q^{(m-1)/2} (-1)^{(q-1)(m-1)/4} G(\eta, \chi_b)$$

考虑 (52) 式右侧

$$q^{(m-1)/2} G(\eta^m, \chi_{mb}) = q^{(m-1)/2} G(\eta, \chi_{mb}) = q^{(m-1)/2} \eta(m) G(\eta, \chi_b)$$

上式第二个等号根据 Theorem 5.12(i) 成立. 对比左侧和右侧, 只需要证明

$$\eta(m) = (-1)^{(q-1)(m-1)/4} \quad (55)$$

设 p 是域 \mathbb{F}_q 的特征, $q = p^s$. \mathbb{F}_q 上的二次特征 η 可以通过 \mathbb{F}_p 上的二次特征 η_p 扩展得到, 所以

$$\eta(m) = \eta_p(N_{\mathbb{F}_q/\mathbb{F}_p}(m)) = \eta_p(m^s)$$

设 $m = r_1 \dots r_t$, 其中 r_i 是不等于 p 的奇素数, 因为 $m \mid q-1$ 所以 $r_i \neq p$. 又因为 $\eta(r_i) = (\frac{r_i}{p})$

$$\eta(m) = [\eta_p(r_1) \dots \eta_p(r_t)]^s = [(\frac{r_1}{p}) \dots (\frac{r_t}{p})]^s$$

根据二次互反律

$$\begin{aligned}\eta(m) &= [(\frac{p}{r_1})(-1)^{(p-1)(r_1-1)/4} \dots (\frac{p}{r_t})(-1)^{(p-1)(r_t-1)/4}] \\ &= (\frac{q}{r_1}) \dots (\frac{q}{r_t}) [(-1)^{us}]^{(p-1)/2}\end{aligned} \quad (*)$$

其中

$$u = \frac{r_1-1}{2} + \dots + \frac{r_t-1}{2}$$

注意到

$$\frac{q-1}{p-1} = p^{s-1} + p^{s-2} + \dots + 1 \equiv s \pmod{2}$$

此外, 对于两个奇整数 v, w 有

$$\frac{vw-1}{2} - \frac{v}{2} - \frac{w}{2} = \frac{(v-1)(w-1)}{2} \equiv 0 \pmod{2}$$

所以

$$\frac{v-1}{2} + \frac{w-1}{2} \equiv \frac{(v-1)(w-1)}{2} \pmod{2}$$

从而

$$u = \frac{r_1-1}{2} + \dots + \frac{r_t-1}{2} \equiv \frac{r_1 \dots r_t - 1}{2} \equiv \frac{m-1}{2} \pmod{2}$$

所以

$$us \equiv \frac{m-1}{2} \frac{q-1}{p-1} \pmod{2}$$

代入 (*) 式得到

$$\eta(m) = \left(\frac{q}{r_1}\right) \dots \left(\frac{q}{r_t}\right) (-1)^{(q-1)(m-1)/4}$$

由于 $q \equiv 1 \pmod{m}$ 意味着 $q \equiv 1 \pmod{r_i}$. 所以就有对于任意 $1 \leq i \leq t$ 有

$$\left(\frac{q}{r_i}\right) = 1$$

所以式子 (55) 成立, 即式 (52) 成立, 原定理成立.

Discussion 5.29(II) Proof of Theorem 5.28 when m is the power of 2

第二种是 m 是 2 的幂的情况.

首先考虑 $m = 2$. 那么 λ 就是二次特征 η . 且 q 是奇数. 那么有

$$\begin{aligned} \frac{G(\psi, \chi_b)^2}{G(\psi^2, \chi_{2b})} &= \frac{G(\psi, \chi_b)^2}{\psi(4)G(\psi^2, \chi_b)} \\ &= \psi(4)J(\psi, \psi) \\ &= \psi(4) \sum_{c_1+c_2=1} \psi(c_1)\psi(c_2) \\ &= \psi(4) \sum_{c \in \mathbb{F}_q} \psi(c - c^2) \end{aligned}$$

对于一个确定的 $d \in \mathbb{F}_q$, 如果 $1 - 4d$ 是某个 \mathbb{F}_q^* 中元素的平方, 方程 $x - x^2 = d$ 在 \mathbb{F}_q 上有两根, 如果 $1 - 4d = 0$, 则方程只有一个根, 如果 $1 - 4d$ 不是某个 \mathbb{F}_q 中元素的平方, 则方程没有根. 从而可以得到方程解的个数为 $1 + \eta(1 - 4d)$. 所以

$$\begin{aligned} \frac{G(\psi, \chi_b)^2}{G(\psi^2, \chi_{2b})} &= \psi(4) \sum_{d \in \mathbb{F}_q} (1 + \eta(1 - 4d))\psi(d) \\ &= \psi(4) \sum_{d \in \mathbb{F}_q} \psi(d) + \sum_{d \in \mathbb{F}_q} \psi(4d)\eta(1 - 4d) \\ &= J(\psi, \eta) \end{aligned}$$

最后一步是因为式 (37), 即对于非平凡乘法特征 ψ 有 $\sum_{c \in \mathbb{F}_q} \lambda(c) = 0$.

所以对于 $m = 2$ 的情况得证.

下面考虑 $m \geq 4$ 且是 2 的幂的情况. 定理和式 (53) 等价, 假设对所有更小的 2 的幂次这个式子都成立. 考虑对 $m/2$ 应用这个关系, 就有

$$\begin{aligned}
\sum_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) &= \sum_{j=0}^{(m/2)-1} G(\psi\lambda^{2j}, \chi_b) \sum_{j=0}^{(m/2)-1} G(\psi\lambda\lambda^{2j}, \chi_b) \\
&= (-1)^{(q-1)(m-1)/16} q^{(m-4)/4} G(\eta, \chi_b) G(\psi^{m/2}, \chi_{(m/2)b}) \\
&\quad \cdot (-1)^{(q-1)(m-1)/16} q^{(m-4)/4} G(\eta, \chi_b) G(\psi^{m/2}\eta, \chi_{(m/2)b}) \\
&= q^{(m-4)/2} G(\eta, \chi_b)^2 G(\psi^{m/2}, \chi_{(m/2)b}) G(\psi^{m/2}\eta, \chi_{(m/2)b})
\end{aligned}$$

第二个求和是把 $\psi\lambda$ 看成一个整体, $(\psi\lambda)^{m/2} = \psi^{m/2}\lambda^{m/2} = \psi^{m/2}\eta$. 从而这个式子成立.

而 $G(\eta, \chi_b)^2 = \eta(-1)q, \eta(-1) = (-1)^{(q-1)/2}$, 所以

$$\sum_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = (-1)^{(q-1)/2} q^{(m-2)/2} G(\psi^{m/2}, \chi_{(m/2)b}) G(\psi^{m/2}\eta, \chi_{(m/2)b})$$

把 $m = 2$ 代入式 (53), 得到

$$G(\psi^{m/2}, \chi_{(m/2)b}) G(\psi^{m/2}\eta, \chi_{(m/2)b}) = G(\eta, \chi_{(m/2)b}) G(\psi^m, \chi_{mb})$$

所以

$$\sum_{j=0}^{m-1} G(\psi\lambda^j, \chi_b) = (-1)^{(q-1)/2} q^{(m-2)/2} \eta\left(\frac{m}{2}\right) G(\eta, \chi_b) G(\psi^m, \chi_{mb}) \quad (56)$$

下面去确定 $\eta(2)$ 的值, 由于 $q^2 \equiv 1 \pmod{8}$, 所以存在一个 $\mathbb{F}_{q^2}^*$ 的 8 阶元 γ . 那么 $\gamma^4 = -1$, 从而 $(\gamma + \gamma^{-1})^2 = \gamma^{-2}(\gamma^4 + 1) + 2 = 2$. 因此 2 是平方元素当且仅当 $\gamma + \gamma^{-1} \in \mathbb{F}_q$. 即当且仅当 $(\gamma + \gamma^{-1})^q = \gamma + \gamma^{-1}$.

即当且仅当 $\gamma^q + \gamma^{-q} = \gamma + \gamma^{-1}$. 即 $(\gamma^{q+1} - 1)(\gamma^{q-1} - 1) = 0$. 即 $\gamma^{q+1} = 1$ 或 $\gamma^{q-1} = 1$.

又因为 γ 是 8 阶元, 所以 $\eta(2) = 1$ 当且仅当 q 模 8 等于 ± 1 .

为了求 $\eta(m/2)$ 的值, 注意到 $m \geq 8$, 所以 $q \equiv 1 \pmod{8}$, 从而 $\eta(m/2) = 1$. 如果 $m = 4$ 那么 $\eta(2)$ 在 q 模 8 等于 1 的时候为 1, 在 q 模 8 等于 5 的之后为 -1 . 所以对于所有的情况可以写成

$$\eta\left(\frac{m}{2}\right) = (-1)^{(q-1)(m-6)/8}$$

代入 (56) 式即得 (53) 式, 故原命题成立.

5.4 Character Sums with Polynomial Arguments

设 χ 是 \mathbb{F}_q 上的非平凡加法特征, $f \in \mathbb{F}_q[x]$ 是正次数多项式, 考虑和式

$$\sum_{c \in \mathbb{F}_q} \chi(f(c))$$

这个和式被称为威尔和(Weil Sums).

计算这个指数和非常困难, 通常是去求该指数和的绝对值. 但是在某些情况下, 这个值可以进行处理.

第一种情况是在 f 为二项式的时候进行处理.

Theorem 5.30 Weil Sums in Binomial

设 χ 是 \mathbb{F}_q 上的非平凡加法特征, $n \in \mathbb{N}$, λ 是 \mathbb{F}_q 上的乘法特征, 阶为 $d = \gcd(n, q-1)$, 那么对于任意的 $a, b \in \mathbb{F}_q, a \neq 0$ 有

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = \chi(b) \sum_{j=1}^{d-1} \bar{\lambda}^j(a) G(\lambda^j, \chi)$$

证明: 设 τ 是 \mathbb{F}_q 上的非平凡加法特征, 且对于 $c \in \mathbb{F}_q$ 有 $\tau(c) = \chi(ac)$. 那么

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = \chi(b) \sum_{c \in \mathbb{F}_q} \chi(ac^n) = \chi(b) \sum_{c \in \mathbb{F}_q} \tau(c^n) \quad (57)$$

根据 (17) 式对于 $c \in \mathbb{F}_q^*$ 有

$$\tau(c^n) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \tau) \psi(c^n)$$

因此

$$\sum_{c \in \mathbb{F}_q} \tau(c^n) = \tau(0) + \sum_{c \in \mathbb{F}_q^*} \tau(c^n) = 1 + \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \tau) \sum_{c \in \mathbb{F}_q^*} \psi^n(c)$$

根据式 (12), 最后一个和式在 ψ^n 是平凡特征时等于 $q-1$, 否则等于 0. ψ^n 是平凡特征等价于 ψ 的阶整除 d .

由于 $\bar{\lambda}$ 的阶是 d , 阶可以整除 d 的特征 ψ 可以表示为 $\psi = \bar{\lambda}^j$, 其中 $j = 0, 1, \dots, d-1$. 所以

$$\sum_{c \in \mathbb{F}_q} \tau(c^n) = 1 + \sum_{j=0}^{d-1} G(\lambda^j, \tau) = \sum_{j=1}^{d-1} G(\lambda^j, \tau)$$

最后一个等号是因为当 λ 是平凡乘法特征, τ 是非平凡加法特征时, $G(\lambda, \tau) = -1$. 即式 (14).

然后根据 Theorem 5.12(i) 和式 (57) 可得结论.

考虑和式

$$\sum_{c \in \mathbb{F}_q^*} \chi(c^n)$$

这个式子实际上是跑了 d 次由 c^d 所生成的子群, 即

$$\sum_{c \in \mathbb{F}_q^*} \chi(c^n) = d \sum_{c \in \langle c^d \rangle} \chi(c)$$

等式右侧的求和部分我们称之为**高斯周期**.

其中

$$\mathbb{F}_q^* = \langle c^d \rangle \cup c_1 \langle c^d \rangle \cup c_2 \langle c^d \rangle \cup \dots \cup c_{d-1} \langle c^d \rangle$$

是一个陪集分解形式.

Corollary 5.31

设 χ 是 \mathbb{F}_q 的非平凡加法特征, $\gcd(n, q-1) = 1$, 那么对于任意 $a, b \in \mathbb{F}_q, a \neq 0$ 有

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = 0$$

可以由上面的定理直接得到.

也可以由高斯周期得到. 这个情况可知 $d = 1$. 也就是说 $ac^n + b$ 和 c 一样跑遍整个 \mathbb{F}_q . 所以这个和式很自然等于 0.

Theorem 5.32

设 χ 是 \mathbb{F}_q 的非平凡加法特征, $n \in \mathbb{N}, d = \gcd(n, q-1)$. 那么对于任意 $a, b \in \mathbb{F}_q, a \neq 0$ 有

$$|\sum_{c \in \mathbb{F}_q} \chi(ac^n + b)| \leq (d-1)\sqrt{q}$$

证明: 根据式 (15) 可知, 对于非平凡加法特征 χ 和非平凡乘法特征 ψ 有 $|G(\psi, \chi)| = \sqrt{q}$. 所以根据 Theorem 5.30 得证.

Theorem 5.33 Weil Sums when $n = 2$ and q is odd

设 χ 是 \mathbb{F}_q 的非平凡加法特征, q 是奇数, 设 $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x], a_2 \neq 0$. 那么

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \chi(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G(\eta, \chi)$$

其中 η 是 \mathbb{F}_q 上的二次特征.

证明: 对 $f(c)$ 配方, 对于 $c \in \mathbb{F}_q$ 有

$$f(c) = a_2c^2 + a_1c + a_0 = a_2(c + a_1(2a_2)^{-1})^2 + a_0 - a_1^2(4a_2)^{-1}$$

令 $c_1 = c + a_1(2a_2)^{-1}, b = a_0 - a_1^2(4a_2)^{-1}$, 则根据 Theorem 5.30 有

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \sum_{c_1 \in \mathbb{F}_q} \chi(a_2c_1^2 + b) = \chi(b)\eta(a_2)G(\eta, \chi)$$

Theorem 5.34 Weil Sums in p-Affine Polynomial

设 \mathbb{F}_q 的特征为 p , 设 p -仿射多项式

$$f(x) = a_r x^{p^r} + a_{r-1} x^{p^{r-1}} + \dots + a_1 x^p + a_0 x + a$$

设 $b \in \mathbb{F}_q^*$, χ_b 是 \mathbb{F}_q 的非平凡加法特征, 定义为 $\chi_b(c) = \chi_1(bc)$. 那么

$$\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) = \begin{cases} \chi_b(a)q & ba^r + b^p a_{r-1}^p + \dots + b^{p^{r-1}} a_1^{p^{r-1}} + b^{p^r} a_0^{p^r} = 0 \\ 0 & otherwise \end{cases}$$

证明: 首先有

$$\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) = \chi_b(a) \sum_{c \in \mathbb{F}_q} \chi_1(L(c))$$

其中

$$L(x) = ba_r x^{p^r} + ba_{r-1} x^{p^{r-1}} + \dots + ba_1 x^p + ba_0 x$$

也是一个 p -仿射多项式. 令 $\tau(c) = \chi_1(L(c))$, $c \in \mathbb{F}_q$. 那么 τ 也是 \mathbb{F}_q 上的加法特征. 因此

$$\sum_{c \in \mathbb{F}_q} \chi_1(L(c)) = \sum_{c \in \mathbb{F}_q} \tau(c) = \begin{cases} q & \tau \text{ 是平凡特征} \\ 0 & otherwise \end{cases}$$

下面求 τ 是平凡特征的条件. 令 $q = p^s$, Tr 是 \mathbb{F}_q 到 \mathbb{F}_p 的绝对迹函数. 根据式 (6) 可得到 τ 是平凡特征当且仅当对于任意 $c \in \mathbb{F}_q$

$$Tr(L(c)) = \sum_{j=0}^{s-1} L(c)p^j = 0$$

这个式子等价于

$$\sum_{j=0}^{s-1} L(x)p^j \equiv 0 \pmod{(x^q - x)} \quad (58)$$

而

$$\sum_{j=0}^{s-1} L(x)p^j = \sum_{j=0}^{s-1} \left(\sum_{i=0}^r ba_i x^{p^i} \right) p^j = \sum_{j=0}^{s-1} \sum_{i=0}^r b^{p^j} a_i^{p^j} x^{p^{i+j}}$$

当 $m \equiv n \pmod{s}$ 的时候, 对于任意 $c \in \mathbb{F}_q$ 有 $c^{p^m} = c^{p^n}$, 且 $x^{p^m} \equiv x^{p^n} \pmod{(x^q - x)}$. 所以

$$\sum_{j=0}^{s-1} L(x)p^j \equiv \sum_{k=0}^{s-1} \left(\sum_{i=0}^r b^{p^{k-i}} a_i^{p^{k-i}} \right) x^{p^k} \pmod{(x^q - x)}$$

上一步的外层求和是枚举余数, 然后对照发现 $i+j$ 和 k 同余, 从而 j 和 $k-i$ 同余.

那么 (58) 式等价于对于任意的 $k = 0, 1, \dots, s-1$ 有

$$\sum_{i=0}^r b^{p^{k-i}} a_i^{p^{k-i}} = 0$$

当且仅当

$$\sum_{i=0}^r b^{p^{r-i}} a_i^{p^{r-i}} = \left(\sum_{i=0}^r b^{p^{k-i}} a_i^{p^{k-i}} \right) p^{r-k} = 0$$

时成立, 所以原式证毕.

Corollary 5.35

设 $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$, $a_2 \neq 0$. q 是偶数. 设 $b \in \mathbb{F}_q^*$, χ_b 是 \mathbb{F}_q 的非平凡加法特征, 定义为 $\chi_b(c) = \chi_1(bc)$. 那么

$$\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) = \begin{cases} \chi_b(a_0)q & a_2 = ba_1^2 \\ 0 & otherwise \end{cases}$$

Theorem 5.36

设 $f \in \mathbb{F}_q[x]$ 是次数为 $n \geq 2$ 的多项式, $\gcd(n, q) = 1$, 设 χ 是 \mathbb{F}_q 上的非平凡加法特征.

那么存在复数 $\omega_1, \dots, \omega_{n-1}$, 它们只和 f 和 χ 有关, 且对于任意正整数 s 有

$$\sum_{\gamma \in \mathbb{F}_{q^s}} \chi^{(s)}(f(\gamma)) = -\omega_1^s - \dots - \omega_{n-1}^s$$

Theorem 5.37

Theorem 5.36 中的所有复数 $\omega_1, \dots, \omega_{n-1}$ 的绝对值都是 \sqrt{q} .

Theorem 5.38 Weil's Theorem

设 $f \in \mathbb{F}_q[x]$ 是次数为 $n \geq 1$ 的多项式, $\gcd(n, q) = 1$, 设 χ 是 \mathbb{F}_q 上的非平凡加法特征. 那么

$$|\sum_{c \in \mathbb{F}_q} \chi(f(c))| \leq (n-1)\sqrt{q}$$

证明: $n = 1$ 情况是显然的.

对于 $n = 2$ 应用 Theorem 5.36 可以得到

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = -\omega_1 - \dots - \omega_{n-1}$$

然后根据 Theorem 5.37 就可以知道原式得证.

在 $\gcd(n, q) > 1$ 的情况下, 需要有一些关于 f 的限制使得 Weil's Theorem 仍然成立. 考虑 $p \mid \deg(f)$ 的情况, 其中 p 是域 \mathbb{F}_q 的特征. 例如 $f(x) = x^p - x, \chi = \chi_1$. 那么根据绝对迹函数的性质有 $\chi_1(f(c)) = 1$ 对任意 $c \in \mathbb{F}_q$ 都成立, 从而在 $q \geq p^2$ 的时候 Weil's Theorem 不成立.

更一般的, 对于任意 $f = g^p - g + b$ 这个定理仍然不成立. 其中 $g \in \mathbb{F}_q[x], b \in \mathbb{F}_q$.

如果 f 不是这个形式的话, 这个定理在 $\gcd(n, q) > 1$ 的情况仍然是成立的.

Theorem 5.39

设 ψ 是 \mathbb{F}_q 上阶为 $m > 1$ 的乘法特征, $f \in \mathbb{F}_q[x]$ 是正次数首一多项式, 且不是任意多项式的 m 次幂.

令 d 为 f 在它自己在 \mathbb{F}_q 的分裂域上的不同根的个数, 设 $d \geq 2$. 那么存在复数 $\omega_1, \dots, \omega_{d-1}$, 它们只和 f 和 ψ 有关, 且对于任意正整数 s 有

$$\sum_{\gamma \in \mathbb{F}_{q^s}} \psi^{(s)}(f(\gamma)) = -\omega_1^s - \dots - \omega_{d-1}^s$$

Theorem 5.40

Theorem 5.39 中的所有复数 $\omega_1, \dots, \omega_{d-1}$ 的绝对值都是 \sqrt{q} .

Theorem 5.41

设 ψ 是 \mathbb{F}_q 上阶为 $m > 1$ 的乘法特征, $f \in \mathbb{F}_q[x]$ 是正次数首一多项式, 且不是任意多项式的 m 次幂.

令 d 为 f 在它自己在 \mathbb{F}_q 的分裂域上的不同根的个数, 那么对于任意的 $a \in \mathbb{F}_q$ 都有

$$\left| \sum_{c \in \mathbb{F}_q} \psi(af(c)) \right| \leq (d-1)\sqrt{q}$$

证明: $d = 1$ 显然, 考虑 $d = 2$.

根据 Theorem 5.39

$$\sum_{c \in \mathbb{F}_q} \psi(af(c)) = \psi(a) \sum_{c \in \mathbb{F}_q} \psi(f(c)) = -\psi(a)(\omega_1 + \dots + \omega_{d-1})$$

从而根据 Theorem 5.40 可以知道上式成立.

5.5 Further Results on Character Sums

Definition 5.42 Kloosterman Sum

设 χ 是 \mathbb{F}_q 上的非平凡加法特征, 设 $a, b \in \mathbb{F}_q$. 定义和式

$$K(\chi; a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1})$$

这个和式被称为克洛斯特曼和.