2020 年 11 月 四川大学学报(自然科学版) Nov. 2020
第 57 卷 第 6 期 Journal of Sichuan University (Natural Science Edition) Vol. 57 No. 6

doi：10.3969/j.issn.0490-6756.2020.06.001

# 一类指数和的代数次数

陈 超[1]，彭国华[2]

(1. 中山大学数据科学与计算机学院；广州 510006；2. 四川大学数学学院，成都 610064)

**摘 要**：Wan 最近研究了指数和 $S_q(f)$ 的代数次数. 本文基于其结果研究了 $q=p^2$ 及 $p\equiv 1 \pmod 4$ 情形下的高斯和，得到了一类次数为 1 的高斯和 $S_q(x^d)$ 的两种可能取值. 本文还推广了 Myerson 在 1981 年提出的方法，进而得到了除 $d$ 为奇数的某些特定情形外所有高斯和代数次数的准确值.

**关键词**：指数和；高斯和；代数次数；有限域

**中图分类号**：O156.2 **文献标识码**：A **文章编号**：0490-6756(2020)06-1029-04

# Algebraic degrees of a class of exponential sums

*CHEN Chao*[1]，*PENG Guo-Hua*[2]

(1. School of Data and Computer Science, Sun Yat-Sen University, Guangzhou 510006, China;
2. School of Mathematics, Sichuan University, Chengdu 610064, China)

**Abstract**: Recently, Wan studied the algebraic degrees of the exponential sums $S_q(f)$ over a finite field $F_q$. In this article, based on Wan's results, we discuss the Gaussian sums in the case of $q=p^2$ and $p\equiv 1 \pmod 4$ and obtain that $S_q(x^d)$ has only two possible values, if it is of degree 1. Additionally, we generalize a method proposed by Myerson in 1981 and get all explicit values of the algebraic degrees of Gaussian sums in some special cases.

**Keywords**: Exponential sum; Gausssian sum; Algebraic degree; Finite field
(2010 MSC 11L05, 11T24)

## 1 引 言

设 $p$ 为奇素数，$q=p^r$，$\zeta_p$ 为一个 $p$ 次本原单位根. 以 $Tr$ 记从有限域 $F_q$ 到 $F_p$ 的迹映射，即 $Tr(x)=x+x^p+\cdots+x^{p^{r-1}}$. 本文讨论有限域 $F_q$ 上形如

$$S_q(f)=\sum_{x\in F_q}\zeta_p^{Tr(f(x))}$$

的指数和，其中 $f(x)\in F_q[x]$. 这类指数和不只有理论价值，在编码学[1-2]和密码学[3-5]方面也有重要应用.

由如上的指数和可得到分圆域 $\mathbf{Q}(\zeta_p)$ 中一个代数整数. 之前，对它们的研究主要集中在指数和的 $p$-adic 性质和 $|*|_\infty$ 性质[6-9]. 最近，以 Wan[10] 为代表的一些学者研究了这些代数整数的次数，即在 $\mathbf{Q}$ 上添加指数和作为代数单扩张，其扩张次数 $[\mathbf{Q}(S_q(f)):\mathbf{Q}]$ 的大小记为 $\deg S_q(f)=[\mathbf{Q}(S_q(f)):\mathbf{Q}]$. 对于一般的多项式 $f(x)\in F_q[x]$，要估计 $\deg S_q(f)$ 或得到 $\deg S_q(f)$ 的精确取值是非常困难的.

当 $f(x)=x^d$，$d\mid(q-1)$ 时，如上的指数和就是经典的高斯和. 19 世纪初，高斯应用初等方法

**收稿日期**：2020-04-13
**基金项目**：国家自然科学基金(11171150)
**作者简介**：陈超(1995—)，四川广元人，博士研究生，主要研究方向为数论及其应用. E-mail：812042210@qq.com
**通讯作者**：彭国华. E-mail：peng@scu.edu.cn

给出了 $q=p$(即 $r=1$) 情形的结论. 高斯证明，当 $d\mid(p-1)$时 $\deg S_p(x^d)=d$. 1981 年,Myerson[11] 研究了 $r>1$ 的情形并得到:如果 $d\mid(p-1)$且 $\gcd(d,r)=1$，那么 $\deg S_q(x^d)=d$. Wan[10] 最近推广了这一结论，得到：如果 $d\mid(p-1)$,那么 $\deg S_q(x^d)=\frac{d}{\gcd(d,r)}$. 同时，他应用 Galois 理论还证明：如果 $d\mid\frac{q-1}{p-1}$，则 $\deg S_q(x^d)=1$，即 $S_q(x^d)$是有理数.

本文基于 Wan 的结果讨论了 $r=2,p\equiv1(\bmod 4)$的情形，得到:若 $d\mid(p+1)$，则 $S_q(x^d)$仅有两种可能取值(定理 2.2，推论 2.4). 在此基础上，我们拓展了 Myerson 提出的方法，得到某些情形下 $S_q(x^d)$代数次数的精确值(定理 3.5),推广了 Wan 的部分结论.

## 2 高斯和

以下设 $p$ 为奇素数，$q=p^r$. 设 $\zeta_p=\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}}$ 为一个 $p$ 次本原单位根,$\mathbf{Q}(\zeta_p)$为 $p$ 次分圆域. 对于 $q-1$ 的正因子 $d$，定义高斯和

$$S_q(x^d)=\sum_{x\in F_q}\zeta_p^{\mathrm{Tr}(x^d)}\in\mathbf{Z}(\zeta_p).$$

对于代数数 $\alpha$,定义 $\alpha$ 的代数次数为 $\deg\alpha=[\mathbf{Q}(\alpha):\mathbf{Q}]$，即在 $\mathbf{Q}$ 上添加 $\alpha$ 所得代数数域的扩张次数. 本文主要考虑高斯和 $S_q(x^d)$的代数次数，即 $\deg S_q(x^d)=[\mathbf{Q}(S_q(x^d)):\mathbf{Q}]$的大小.

若 $d=1$，利用 Tr 的满同态性质可得

$$S_q(x)=p^{r-1}\sum_{k=0}^{p-1}\zeta_p^k=0.$$

当 $d=2$ 时，高斯已得到

$$S_p(x^2)=\sqrt{(-1)^{\frac{p-1}{2}}p},$$

再由 Hasse-Davenport 定理可知

$$-S_q(x^2)=(-S_p(x^2))^r=\left(-\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^r \tag{1}$$

故

$$\deg S_q(x^2)=\begin{cases}1, & 若\ 2\mid r,\\ 2, & 若\ 2\nmid r.\end{cases}$$

最近，Wan[10] 利用 Galois 理论得到如下结果.

**定理 2.1** 若 $d\mid\frac{q-1}{p-1}$，则 $\deg S_q(x^d)=1$.

由 Wan 的结论可知，当 $d\mid\frac{q-1}{p-1}$时，$S_q(x^d)$的值是一个有理整数，但其精确值并不容易确定. 对于 $r=2$ 情形，我们将得到

**定理 2.2** 若 $d\mid(p+1)$，则 $S_{p^2}(x^d)=-p$ 或 $(d-1)p$.

为了证明定理 2.2，我们需要如下引理.

**引理 2.3**[12] 设 $\chi$ 为 $F_q$ 一个非平凡的加法特征，$n$ 为正整数，$e=\gcd(n,q-1)$. 对任意的 $a$，$b\in F_q$，$a\neq0$，有

$$\left|\sum_{c\in F_q}\chi(ac^n+b)\right|\leqslant(e-1)\sqrt{q}.$$

定理 2.2 的证明 对 $k=0,1,\cdots,p-1$,令

$$N_k=|\{x\in F_{p^2}\mid\mathrm{Tr}(x^d)\equiv k(\bmod p)\}|.$$

则

$$S_{p^2}(x^d)=\sum_{x\in F_{p^2}}\zeta_p^{\mathrm{Tr}(x^d)}=N_0+N_1\zeta_p+\cdots+N_{p-1}\zeta_p^{p-1}.$$

由定理 2.1 可知 $S_{p^2}(x^d)\in\mathbf{Z}$. 由于 $1,\zeta_p,\cdots,\zeta_p^{p-2}$ 在 $\mathbf{Z}$ 上线性独立且 $\zeta_p^{p-1}=-1-\zeta_p-\cdots-\zeta_p^{p-2}$，由上式可推出 $N_1=N_2=\cdots=N_{p-1}$,且

$$S_{p^2}(x^d)=N_0-N_1 \tag{2}$$

又

$$p^2=N_0+N_1+\cdots+N_{p-1} \tag{3}$$

故

$$S_{p^2}(x^d)=mp \tag{4}$$

其中 $m=\frac{N_0-p}{p-1}\in\mathbf{Z}$. 取定乘法群 $F_{p^2}^*$ 的一个本原元 $g$. 若 $\mathrm{Tr}(x^d)\equiv k(\bmod p)$,则 $\mathrm{Tr}((g^{\frac{q-1}{d}i}x)^d)\equiv k(\bmod p)$对所有 $i=0,1,\cdots,d-1$ 成立. 注意到 $\mathrm{Tr}(0)=0$,故 $N_0\equiv1(\bmod d)$. 于是 $m\equiv-1(\bmod d)$. 注意到 $N_0\geqslant1$ 及 $\chi(x)=\zeta_p^{\mathrm{Tr}(x)}$ 是 $F_{p^2}$ 上的加法特征,由引理 2.3 可得

$$-p\leqslant S_{p^2}(x^d)\leqslant(d-1)p.$$

于是 $-1\leqslant m\leqslant d-1$. 因而 $m=-1$ 或者 $m=d-1$. 所以 $S_{p^2}(x^d)=-p$ 或 $S_{p^2}(x^d)=(d-1)p$. 证毕.

对于一些特殊情况，我们还可以得到 $S_{p^2}(x^d)$ 的精确值.

**推论 2.4** 设 $p\equiv1(\bmod 4)$. 若 $2\mid d\mid(p+1)$，则 $S_{p^2}(x^d)=-p$.

证明 由(1)式可知 $S_{p^2}(x^2)=-p$. 再由(4)式可得当 $d=2$ 时 $N_0=1$. 这表明 $\mathrm{Tr}(x^2)=0\in F_p$ 当且仅当 $x=0\in F_{p^2}$. 若 $\mathrm{Tr}(x^d)=0\in F_p$,则 $\mathrm{Tr}((x^{\frac{d}{2}})^2)=0$,故 $x=0$,即 $N_0=1$. 由(4)式可知 $S_{p^2}(x^d)=-p$. 证毕.

## 3　高斯和的代数次数

为方便讨论，我们引入一些记号.

对于 $q-1$ 的因子 $d$，令 $d^*=\frac{q-1}{d}$. 则 $dd^*=q-1$. 由于 $F_q^*$ 为 $q-1$ 阶循环群，它有唯一的 $d^*$ 阶循环群，记为 $H_{d^*}$. 固定循环群 $F_q^*$ 的一个生成元 $g$. 易见

$$H_{d^*}=(F_q^*)^d=\{g^{di}\mid i=0,1,\cdots,d^*-1\}=\langle g^d\rangle.$$

对于 $k=0,1,\cdots,d-1$，定义

$$\eta_d(k)=\sum_{x\in g^kH_{d^*}}\zeta_p^{\mathrm{Tr}(x)},$$

$$\varphi_d(x)=\prod_{k=0}^{d-1}(x-\eta_d(k)).$$

考虑 $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ 在 $\varphi_d(x)$ 上的作用便知 $\varphi_d(x)\in\mathbf{Z}[x]$. 利用 $S_q(x^d)$ 的定义即得 $S_q(x^d)=d\eta_d(0)+1$. 对于代数数 $\alpha$，我们知道 $\deg\alpha=[\mathbf{Q}(\alpha):\mathbf{Q}]$. 故

**引理 3.1**　$\deg S_q(x^d)=\deg\eta_d(0)$.

关于多项式 $\varphi_d(x)$，Myerson[11] 证明了如下定理.

**定理 3.2**　令 $\delta=\gcd(d,\frac{q-1}{p-1})$. 则 $\varphi_d(x)$ 在 $\mathbf{Z}$ 上有分解 $\varphi_d(x)=\prod_{k=0}^{\delta-1}\varphi_d^{(k)}(x)$，

$$\varphi_d^{(k)}(x)=\prod_{i=0}^{\frac{d}{\delta}-1}(x-\eta_d(k+\delta i))\in\mathbf{Z}[x]\qquad(5)$$

或者不可约，或者是某个多项式的完全方幂，其中 $k=0,1,\cdots,\delta-1$.

为了得到高斯和的次数，我们先证明两个引理.

首先，由于 $\eta_l(0)=\sum_{x\in H_{l^*}}\zeta_p^{\mathrm{Tr}(x)}$ 且有陪集分解 $H_{l^*}=\bigcup_{i=0}^{k-1}g^{li}H_{(kl)^*}$. 所以有

**引理 3.3**　若 $kl\mid(q-1)$，则

$$\eta_l(0)=\eta_{kl}(0)+\eta_{kl}(l)+\cdots+\eta_{kl}((k-1)l).$$

**引理 3.4**　若 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是 $\mathbf{Z}$ 上多项式的 $k$ 次方，则 $k\mid\gcd(a_{n-1},n)$.

**证明**　设

$$x^n+a_{n-1}x^{n-1}+\cdots+a_0=(x^l+b_{l-1}x^{l-1}+\cdots+b_0)^k.$$

比较等式两边 $x^{n-1}$ 的系数可得 $a_{n-1}=kb_{l-1}$，故 $k\mid a_{n-1}$. 显然 $k\mid n$，所以 $k\mid\gcd(n,a_{n-1})$. 证毕.

由引理 3.4，若 $\varphi_d(x)$ 的因子 $\varphi_d^{(0)}(x)$ 的次高项系数与 $\frac{d}{\delta}$ 互素，则 $\varphi_d^{(0)}(x)$ 不会是 $\mathbf{Z}$ 上一个多项式的方幂. 再由定理 3.2 便知 $\varphi_d^{(0)}(x)$ 不可约，它就是 $\eta_d(0)$ 的极小多项式. 从而 $\deg S_q(x^d)=\deg\eta_d(0)=\frac{d}{\delta}$.

以下讨论 $r=2$ 情形. 设 $p\equiv1\pmod 4$ 且 $d\mid(p^2-1)$. 令 $\delta=\gcd(p+1,d)$. 由定理 3.2，$\frac{d}{\delta}$ 次多项式 $\varphi_d^{(0)}(x)=\prod_{i=0}^{\frac{d}{\delta}-1}(x-\eta_d(\delta i))$ 或者不可约，或者是某个多项式的完全方幂. 由引理 3.3 知 $\varphi_d^{(0)}(x)$ 的次高项的系数为

$$-\sum_{i=0}^{\frac{d}{\delta}-1}\eta_d(\delta i)=-\eta_\delta(0)=\frac{1-S_{p^2}(x^\delta)}{\delta}.$$

由定理 2.2 可知 $S_{p^2}(x^\delta)=-p$ 或 $(\delta-1)p$.

当 $d$ 为偶数时，$2\mid\delta$. 由推论 2.4 知 $S_{p^2}(x^\delta)=-p$，故 $\varphi_d^{(0)}(x)$ 的次高项的系数为 $\frac{p+1}{\delta}$. 然而 $\gcd(\frac{p+1}{\delta},\frac{d}{\delta})=1$，由引理 3.4 和定理 3.2 可知 $\varphi_d^{(0)}(x)$ 是一个 $\frac{d}{\delta}$ 次不可约多项式. 故 $\eta_d(0)$ 的代数次数为 $\frac{d}{\delta}$. 再由引理 3.1 即得

$$\deg S_{p^2}(x^d)=\frac{d}{\gcd(d,p+1)}.$$

当 $d$ 为奇数时，$d$ 可以唯一分解成 $d=\delta m$，其中 $\delta=\gcd(d,p+1)$，$m=\gcd(d,p-1)$ 且 $\delta$ 与 $m$ 互素. 若 $S_{p^2}(x^\delta)=-p$，则 $\varphi_d^{(0)}(x)$ 的次高项的系数为 $\frac{p+1}{\delta}$，从而

$$\deg S_{p^2}(x^d)=\frac{d}{\gcd(d,p+1)}.$$

若 $S_{p^2}(x^\delta)=(\delta-1)p$，则 $\varphi_d^{(0)}(x)$ 的次高项的系数为 $-\frac{\delta p-p-1}{\delta}$. 由于

$$\gcd(\frac{\delta p-p-1}{\delta},\frac{d}{\delta})=\gcd(\frac{\delta p-p-1}{\delta},m)=\gcd(\delta p-p-1,m)=\gcd(\delta-2,m).$$

因此当 $\gcd(\delta-2,m)=1$ 时，同样可以得到 $\deg S_{p^2}(x^d)=\frac{d}{\gcd(d,p+1)}$.

综上，我们有定理 3.5.

**定理 3.5**　设 $p\equiv1\pmod 4$，$d\mid(p^2-1)$. 若 $d$ 为偶数或 $d$ 为奇数且 $\gcd(d,p+1)-2$ 与 $\gcd(d,p-1)$ 互素，则

$$\deg S_{p^2}(x^d)=\frac{d}{\gcd(d,p+1)}.$$

## 参考文献:


[1] Eric F. Weight of duals of BCH codes and exponential sums [J]. Finite Fields Th App, 2003, 9: 1.

[2] Marcel V. Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes [J]. J Number Theory, 1995, 55: 145.

[3] Castro F N, Medina L A. Modular periodicity of exponential sums of symmetric Boolean functions [J]. Discrete Appl Math, 2017, 217: 455.

[4] Mesnager S. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials [J]. IEEE T Inform Theory, 2011, 57: 5996.

[5] Niederreiter H, Winterhof A. Exponential sums for nonlinear recurring sequences [J]. Finite Fields Th App, 2008, 14: 59.

[6] Shparlinski I. On sums of Kloosterman and Gauss sums [J]. T Am Math Soc, 2019, 371: 8679.

[7] Mohammadi A. Improved bounds on Gauss sums in arbitrary finite fields [J]. Int J Number Theory, 2019, 15: 2027.

[8] Wan D. Variation of *p*-adic Newton polygons for L-functions of exponential sums [J]. Asian J Math, 2004, 8: 427.

[9] Sperber S. On the p-adic theory of exponential sums [J]. Am J Math, 1986, 108: 255.

[10] Wan D. Algebraic theory of exponential sums over finite fields [EB/OL]. https://www.math.uci.deu/~dwan/Wan-HIT-2019.pdf.

[11] Myerson G. Period polynomials and Gauss sums for finite fields [J]. Acta Arith, 1981, 39: 251.

[12] Lidl R, Niederreiter H. Finite Fields [M]. New York: Addision-Wesley, 1983.



**引用本文格式:**

中 文:陈超,彭国华. 一类指数和的代数次数[J]. 四川大学学报:自然科学版,2020,57:1029.

英 文:Chen C, Peng G H. Algebraic degrees of a class of exponential sums [J]. J Sichuan Univ: Nat Sci Ed, 2020, 57: 1029.