# 有限域上的二次型表数

张　彬

(南京师范大学数学科学学院,江苏 南京 210023)

[摘要]　令 $F_q$ 为有限域,其中 $q=p^t$,$p$ 为奇素数,$t$ 为正整数. 设 $f(x_1,\cdots,x_n)$ 为 $F_q$ 上的 $n$ 元二次型,$\alpha\in F_q$,本文给出方程 $f(x_1,\cdots,x_n)=\alpha$ 在 $F_q$ 上的非零解数的具体公式.

[关键词]　有限域,$n$ 元二次型,二次型表数

[中图分类号]O156.5　[文献标志码]A　[文章编号]1001-4616(2013)02-0001-04

# The Number of Quadratic Forms Representations in Finite Fields

Zhang Bin

(School of Mathematical Sciences, Nanjing Normal University, Nanjing 210023, China)

**Abstract**: Let $q=p^t$, where $p$ is an odd prime number and $t$ is a positive integer. Let $F_q$ be a finite field with $q$ elements. In this note, for any $\alpha\in F_q$, we give a formula of the number of nonzero representations of $\alpha$ by a quadratic form $f(x_1,\cdots,x_n)$ in $F_q$.

**Key words**: finite fields, quadratic forms, the number of nonzero representations

设 $F$ 为一个域,一个系数在 $F$ 中的关于变量 $x_1,\cdots,x_n$ 的二次齐次多项式

$$f(x_1,\cdots,x_n)=\sum_{i,j=1}^{n}a_{ij}x_ix_j,$$

其中 $a_{ij}=a_{ji}$,称为域 $F$ 上的一个 $n$ 元二次型. 对称矩阵 $\boldsymbol{A}=(a_{ij})$ 称为二次型的矩阵,$\boldsymbol{A}$ 的秩称为二次型的秩. 行列式 $d=\det\boldsymbol{A}$ 称为二次型的行列式. 若行列式 $d=0$,则二次型 $f(x_1,\cdots,x_n)$ 称为退化的,否则二次型 $f(x_1,\cdots,x_n)$ 称为非退化的. 令 $\boldsymbol{X}=(x_1,\cdots,x_n)'$,则 $f(x_1,\cdots,x_n)=\boldsymbol{X}'\boldsymbol{A}\boldsymbol{X}$.

在本文中,我们一直假设 $F_q$ 为有限域,$F_q^*=F_q-\{0\}$,其中 $q=p^t$,$p$ 为奇素数,$t$ 为正整数. 首先对于非退化的 $n$ 元二次型 $f(x_1,\cdots,x_n)$,我们给出在有限域 $F_q$ 中方程 $f(x_1,\cdots,x_n)=0$ 的仅依赖于 $n$ 和其行列式 $d$ 的非零解数的具体公式,并由此给出二次型 $f$ 退化时的相应结论. 然后对于非退化的 $n$ 元二次型 $f(x_1,\cdots,x_n)$,给出在有限域 $F_q$ 中方程 $f(x_1,\cdots,x_n)=\alpha$,其中 $\alpha\in F_q^*$ 的解数,并由此给出二次型 $f$ 退化时的相应结论.

## 1　一些引理

在这一部分,我们给出本文涉及到的一些引理.

**定义 1**　域 $F$ 上的 $n\times n$ 阶矩阵 $\boldsymbol{A},\boldsymbol{B}$ 称为合同的,如果存在域 $F$ 上可逆的 $n\times n$ 阶矩阵 $\boldsymbol{C}$,使得

$$\boldsymbol{B}=\boldsymbol{C}'\boldsymbol{A}\boldsymbol{C}.$$

**定义 2**　两个 $n$ 元二次型 $f,g$ 称为等价的,如果它们的矩阵合同,记为 $f\sim g$.

**定义 3**　设 $f$ 为域 $F$ 上的一个 $n$ 元二次型,$\alpha\in F$,称二次型 $f$ 可以表 $\alpha$,或者 $\alpha$ 可以由 $f$ 表示,如果存在不全为 0 的数 $\alpha_1,\cdots,\alpha_n\in F$,使得 $f(\alpha_1,\cdots,\alpha_n)=\alpha$.

特别的,称二次型 $f$ 可以表 0,是指存在不全为 0 的数 $\alpha_1,\cdots,\alpha_n\in F$,使得 $f(\alpha_1,\cdots,\alpha_n)=0$.

收稿日期:2012-09-17.
基金项目:国家自然科学基金(10971098).
通讯联系人:张彬,博士研究生,研究方向:代数数论. E-mail:zhangbin100902025@163.com

**引理1**　域 $F$ 上的任意一个 $n$ 元二次型均可以经过非退化线性替换转化为对角形 $d_1y_1^2+\cdots+d_ry_r^2$ 的形式,称为 $f$ 的标准型,其中 $d_1,\cdots,d_r\in F^*$,$r$ 为 $f$ 的秩.

**引理2**　若域 $F$ 上的两个 $n$ 元二次型等价,则它们的行列式相差 $F$ 上的一个非0平方因子.

**引理3**　设 $f,g$ 是域 $F$ 上的两个 $n$ 元二次型. 如果 $f\sim g,\alpha\in F$,那么 $\alpha$ 可以由 $f$ 表示当且仅当 $\alpha$ 可以由 $g$ 表示.

**定义4**　对任意的 $x\in F_q^*$,定义 $\delta(x)=1$,如果 $x\in(F_q^*)^2$;否则 $\delta(x)=-1$. 规定 $\delta(0)=0$.

**引理4**　若有限域 $F_q$ 上的一个非退化的 $n$ 元二次型 $f(x_1,\cdots,x_n)$ 可以表 $\alpha$,其中 $\alpha\in F_q^*$,则

$$f\sim\alpha y_1^2+g(y_2,\cdots,y_n),$$

其中 $g$ 是 $F_q$ 上的一个非退化的 $n-1$ 元二次型.

**证**　由于 $f(x_1,\cdots,x_n)$ 可以表 $\alpha$,所以存在不全为0的数 $\alpha_1,\cdots,\alpha_n\in F_q$,使得 $f(\alpha_1,\cdots,\alpha_n)=\alpha$. 设 $f$ 的矩阵为 $\boldsymbol{A}$. 任取一个非退化的 $n\times n$ 阶矩阵 $\boldsymbol{C}$ 满足条件:该矩阵的第一列是 $(\alpha_1,\cdots,\alpha_n)'$(容易取到). 令 $\boldsymbol{B}=\boldsymbol{C}'\boldsymbol{A}\boldsymbol{C}=(b_{ij})$,易知 $b_{11}=\alpha$. 作非退化线性替换 $\boldsymbol{X}=\boldsymbol{C}\boldsymbol{Z}$,可得

$$f\sim\alpha z_1^2+2\sum_{j=2}^n b_{1j}z_1z_j+\sum_{i=2}^n\sum_{j=2}^n b_{ij}z_iz_j=\alpha(z_1+\sum_{j=2}^n\alpha^{-1}b_{1j}z_j)^2-\alpha^{-1}(\sum_{j=2}^n b_{1j}z_j)^2+\sum_{i=2}^n\sum_{j=2}^n b_{ij}z_iz_j.$$

在上式中,令 $y_1=z_1+\sum\limits_{j=2}^n\alpha^{-1}b_{1j}z_j,y_k=z_k,k=2,\cdots,n$,这是一个非退化线性替换,因此

$$f\sim\alpha y_1^2+g(y_2,\cdots,y_n),$$

其中 $g(y_2,\cdots,y_n)=-\alpha^{-1}(\sum\limits_{j=2}^n b_{1j}y_j)^2+\sum\limits_{i=2}^n\sum\limits_{j=2}^n b_{ij}y_iy_j$ 是 $F_q$ 上的一个非退化的 $n-1$ 元二次型.

**引理5**　若有限域 $F_q$ 上的一个非退化的 $n$ 元二次型 $f(x_1,\cdots,x_n)$ 可以表0,则 $f(x_1,\cdots,x_n)$ 可以表 $F_q$ 上的所有元素.

**证**　由引理3,不妨设 $n$ 元二次型 $f(x_1,\cdots,x_n)=a_1x_1^2+\cdots+a_nx_n^2$,其中 $a_1,\cdots,a_n\in F_q^*$. 由于 $f(x_1,\cdots,x_n)$ 可以表0,所以存在不全为0的数 $\alpha_1,\cdots,\alpha_n\in F_q$,使得 $a_1\alpha_1^2+\cdots+a_n\alpha_n^2=0$. 令 $\gamma$ 为 $F_q$ 中的任意非0元,不妨设 $\alpha_1\neq0$,取 $x_1=\alpha_1(1+t),x_k=\alpha_k(1-t),k=2,\cdots,n$,其中参数 $t$ 待定. 代入方程

$$a_1x_1^2+\cdots+a_nx_n^2=\gamma,$$

后,有

$$2a_1\alpha_1^2t-2a_2\alpha_2^2t-\cdots-2a_n\alpha_n^2t=4a_1\alpha_1^2t=\gamma.$$

由于 $F_q$ 的特征为奇素数,所以 $4a_1\alpha_1\neq0$. 令 $t=\dfrac{\gamma}{4a_1\alpha_1^2}$,则二次型 $f(x_1,\cdots,x_n)$ 可以表示 $\gamma$.

注记:该引理在文献[1]中的P. 393给出了证明.

**引理6**　设 $n\geqslant3$,若有限域 $F_q$ 上的一个非退化的 $n$ 元二次型 $f$ 可以表0,则

$$f\sim y_1y_2+g(y_3,\cdots,y_n),$$

其中 $g$ 是 $F_q$ 上的一个非退化的 $n-2$ 元二次型.

**证**　因为二次型 $f$ 可以表0,又 $1\in F_q$,所以根据引理5,可知 $f$ 可以表1. 从而由引理4可知

$$f\sim x_1^2+f_1(x_2,\cdots,x_n),$$

其中 $f_1$ 是 $F_q$ 上的一个非退化的 $n-1$ 元二次型. 故 $x_1^2+f_1(x_2,\cdots,x_n)$ 也可以表0,从而存在不全为0的数 $\beta_1,\beta_2,\cdots,\beta_n\in F_q$,使得 $f_1(\beta_2,\cdots,\beta_n)=-(\beta_1)^2$. 如果 $\beta_1\neq0$,则 $f_1$ 可以表 $-1$;如果 $\beta_1=0$,则 $f_1$ 可以表0,利用引理5,可知 $f_1$ 也可以表示 $-1$. 再利用引理4可知

$$f_1\sim-x_2^2+g(y_3,\cdots,y_n),$$

其中 $g$ 是 $F_q$ 上的一个非退化的 $n-2$ 元二次型. 从而

$$f\sim x_1^2-x_2^2+g(y_3,\cdots,y_n).$$

在上式中令 $x_1-x_2=y_1,x_1+x_2=y_2$,我们得到

$$f\sim y_1y_2+g(y_3,\cdots,y_n).$$

**引理7**　当 $n\geqslant3$ 时,有限域 $F_q$ 上的任意 $n$ 元二次型 $f(x_1,\cdots,x_n)$ 可以表0.

**证**　见文献[2]中的P. 6推论2.

**引理 8**　设$f(x_1,\cdots,x_n)$为有限域 $F_q$ 上的非退化的 $n$ 元二次型,令 $T_n$ 表示方程$f(x_1,\cdots,x_n)=0$ 在 $F_q$ 中的非零解数,那么

(1) $T_1=0$.

(2) $T_2=(q-1)(1+\delta(-d))$,其中 $d$ 为 $f$ 的行列式.

**证**　(1)当 $n=1$ 时,$f(x)=ax^2$. 因此 $T_1=0$.

(2)当 $n=2$ 时,由引理 3 可知不妨设$f(x_1,x_2)=a_1x_1^2+a_2x_2^2$,其中 $a_1,a_2\in F_q^*$,行列式 $d=a_1a_2$. 易知在 $F_q$ 中方程 $a_1x_1^2+a_2x_2^2=0$ 和 $a_1^2x_1^2+a_1a_2x_2^2=0$ 的非零解数相等,从而只需在 $F_q$ 中求方程

$$(a_1x_1)^2=-a_1a_2x_2^2$$

的非零解数. 该方程的非 0 解数为$(q-1)(1+\delta(-d))$. 所以 $T_2=(q-1)(1+\delta(-d))$,其中 $d=a_1a_2$.

## 2　主要定理

**定理 1**　设$f(x_1,\cdots,x_n)$为有限域 $F_q$ 上非退化的 $n$ 元二次型,行列式为 $d$,令 $T_n$ 表示在 $F_q$ 中方程 $f(x_1,\cdots,x_n)=0$ 的非零解数,则

(1)当 $n$ 为奇数时,$T_n=q^{n-1}-1$.

(2)当 $n$ 为偶数时,$T_n=q^{n-1}-1+(q-1)q^{\frac{n}{2}-1}\delta((-1)^{\frac{n}{2}}d)$.

**证**　当 $n=1$ 和 2 时,由引理 8 知定理成立. 下面考虑 $n\geqslant 3$ 时的情况,当$f(x_1,\cdots,x_n)$可以表 0 时,由引理 6 可知

$$f\sim y_1y_2+f_{n-2}(y_3,\cdots,y_n),$$

其中$f_{n-2}(y_3,\cdots,y_n)$是 $F_q$ 上的一个 $n-2$ 元非退化的二次型. 令 $T_{n-2}$表示在 $F_q$ 中方程$f_{n-2}(y_3,\cdots,y_n)=0$ 的非零解数,则

$$T_n=(2q-1)T_{n-2}+(q-1)(q^{n-2}-1-T_{n-2})+2(q-1),$$

即

$$T_n=qT_{n-2}+(q-1)(q^{n-2}+1).\tag{1}$$

(1)当 $n=2m+1(m\geqslant 1)$时,利用式(1)递归并结合引理 8(1)可得

$$T_{2m+1}=(q-1)(q^{2m-1}+1+q^{2m-2}+q+\cdots+q^m+q^{m-1})=q^{2m}-1.$$

(2)当 $n=2m(m\geqslant 2)$时,由引理 6 和引理 7 可知存在 $a,b\in F_q^*$,使得

$$f\sim y_1y_2+y_3y_4+\cdots+y_{2m-3}y_{2m-2}+ay_{2m-1}^2+by_{2m}^2.$$

易知上式右边的二次型的行列式为$(-\dfrac{1}{4})^{m-1}ab$,利用引理 2 可知,存在 $c\in F_q^*$,使得

$$d=(-\frac{1}{4})^{m-1}abc^2,$$

即

$$ab=(\frac{2^{m-1}}{c})^2(-1)^{m-1}d.$$

由引理 8 可得

$$T_2=(q-1)(1+\delta(-ab))=(q-1)(1+\delta((-1)^md)).$$

利用式(1)递归并结合上式可得

$$T_{2m}=(q-1)(q^{2m-2}+1+\cdots+q^{m-1}+q^{m-1}\delta((-1)^md))=q^{2m-1}-1+(q-1)q^{m-1}\delta((-1)^md).$$

这样就完成了证明.

注记:(1)当 $n$ 为奇数时,$T_n$ 的取值仅与 $n$ 有关;当 $n$ 为偶数时,$T_n$ 的取值仅与 $n$ 和$f(x_1,\cdots,x_n)$的行列式 $d$ 有关.

(2)文献[1]中 P. 9 习题 10 和习题 11,以及文献[3]中 P. 31 习题 13 均对有限域 $F_p$($p$ 为奇素数)给出了上述结论.

**推论 1**　若$f(x_1,\cdots,x_n)$为有限域 $F_q$ 上的秩为 $r(0<r\leqslant n)$的 $n$ 元二次型,那么存在非退化线性替换 $\boldsymbol{X}=\boldsymbol{CY}$,将 $f$ 变为标准型 $g(y_1,\cdots,y_r)=a_1y_1^2+\cdots+a_ry_r^2$,其中 $a_1,\cdots,a_r\in F_q^*$. 令 $T_r,R_n$ 分别表示在 $F_q$ 中方程

$g(y_1,\cdots,y_r)=0$ 和 $f(x_1,\cdots,x_n)=0$ 的非零解数,则

$$R_n=T_r q^{n-r}+q^{n-r}-1.$$

**证**　若 $f$ 的秩为 $r(0<r\leqslant n)$,则存在非退化线性替换 $\boldsymbol{X}=\boldsymbol{CY}$,使得

$$f\sim a_1y_1^2+\cdots+a_ry_r^2+0\cdot y_{r+1}^2+\cdots+0\cdot y_n^2,$$

其中 $a_1,\cdots,a_r\in F_q^*$. 从而我们有

$$R_n=T_r q^{n-r}+q^{n-r}-1.$$

注记:$F_q$ 上的 $n$ 元二次型 $f(x_1,\cdots,x_n)$ 的标准型是不唯一的,这与所做的非退化线性替换有关,即推论 2 中的 $g(y_1,\cdots,y_r)$ 的表达形式不唯一,但是不同形式之间是互相等价的,从而由引理 2 可知它们的行列式之间相差一个非 0 平方因子,由定义 4 中 $\delta(x)$ 的定义可知对结果不产生影响.

**定理 2**　设 $f(x_1,\cdots,x_n)$ 为有限域 $F_q$ 上非退化的 $n$ 元二次型,行列式为 $d$,对任意的 $\alpha\in F_q^*$,令 $Q_n$ 表示在 $F_q$ 中方程 $f(x_1,\cdots,x_n)=\alpha$ 的解数,则

(1) 当 $n$ 为奇数时,$Q_n=q^{n-1}+q^{\frac{n-1}{2}}\delta((-1)^{\frac{n-1}{2}}\alpha d)$.

(2) 当 $n$ 为偶数时,$Q_n=q^{n-1}-q^{\frac{n}{2}-1}\delta((-1)^{\frac{n}{2}}d)$.

**证**　令 $g(x_1,\cdots,x_n,x_{n+1})=f(x_1,\cdots,x_n)-\alpha x_{n+1}^2$,由 $f(x_1,\cdots,x_n)$ 为有限域 $F_q$ 上的非退化的 $n$ 元二次型,$\alpha\in F_q^*$,可知 $g(x_1,\cdots,x_n,x_{n+1})$ 是 $F_q$ 上非退化的 $n+1$ 元二次型. 令 $T_{n+1},T_n$ 分别表示在 $F_q$ 上方程 $g(x_1,\cdots,x_n,x_{n+1})=0$ 和 $f(x_1,\cdots,x_n)=0$ 的非零解数,则

$$Q_n=\frac{T_{n+1}-T_n}{q-1}.\tag{2}$$

由式(2),并利用定理 1 可得

(1) 当 $n=2m+1(m\geqslant 0)$ 时,

$$Q_{2m+1}=\frac{T_{2m+2}-T_{2m+1}}{q-1}=\frac{q^{2m+1}-1+(q-1)q^m\delta((-1)^{m+2}\alpha d)-q^{2m}+1}{q-1}=q^{2m}+q^m\delta((-1)^m\alpha d).$$

(2) 当 $n=2m(m\geqslant 1)$ 时,

$$Q_{2m}=\frac{T_{2m+1}-T_{2m}}{q-1}=\frac{q^{2m}-1-q^{2m-1}+1-(q-1)q^{m-1}\delta((-1)^m d)}{q-1}=q^{2m-1}-q^{m-1}\delta((-1)^m d).$$

这就完成了证明.

**推论 2**　若 $f(x_1,\cdots,x_n)$ 为有限域 $F_q$ 上的秩为 $r(0<r\leqslant n)$ 的 $n$ 元二次型,那么存在非退化线性替换 $\boldsymbol{X}=\boldsymbol{CY}$,将 $f$ 变为标准型 $g(y_1,\cdots,y_r)=a_1y_1^2+\cdots+a_ry_r^2$,其中 $a_1,\cdots,a_r\in F_q^*$. 对任意的 $\alpha\in F_q^*$,令 $Q_r,P_n$ 分别表示在 $F_q$ 中方程 $g(y_1,\cdots,y_r)=\alpha$ 和 $f(x_1,\cdots,x_n)=\alpha$ 的解数,则

$$P_n=Q_rq^{n-r}.$$

**证**　若 $f$ 的秩为 $r(0<r\leqslant n)$,则存在非退化线性替换 $\boldsymbol{X}=\boldsymbol{CY}$,使得

$$f\sim a_1y_1^2+\cdots+a_ry_r^2+0\cdot y_{r+1}^2+\cdots+0\cdot y_n^2,$$

其中 $a_1,\cdots,a_r\in F_q^*$. 从而

$$P_n=Q_rq^{n-r}.$$

**致谢**　在本文的写作过程中,我的导师纪春岗教授给予了悉心的指导,在此向纪老师表示衷心的感谢!

## [参考文献]


[1] Borevich Z I,Shafarevich I R. Number Theory[M]. New York:Academic Press,Inc,1966.

[2] Serre J P. A Course in Arithmetic[M]. New York:Springer-Verlag,1973.

[3] Cassels J W S. Rational Quadratic Forms[M]. London:Academic Press,Inc,1978.


[责任编辑:丁　蓉]