广义 bent 函数和虚二次域理想类数*

冯克勤
(中国科学技术大学研究生院,信息安全国家实验室,北京 100039)

摘要 建立了广义 bent 函数和虚二次域理想类群的联系. 由此得到关于广义 bent 函数不存在性的一些新结果.

关键词 广义 bent 函数 虚二次域

设 q 和 n 为正整数,$q=2$, $\mathbb{Z}_q=\mathbb{Z}/q\mathbb{Z}$, $\zeta_q=e^{\frac{2\pi i}{q}}$. 函数 $f:\mathbb{Z}_q^n\to\mathbb{Z}_q$ 叫作类型$[n, q]$的广义 bent 函数,是指对每个 $y\in\mathbb{Z}_q^n$,

$$\left|\sum_{x\in\mathbb{Z}_q^n}\zeta_q^{f(x)-x\cdot y}\right|=q^{n/2}, \tag{1}$$

这里 $x\cdot y$ 是通常的向量内积. 广义 bent 函数用于多址通信和密码学等许多实际领域. 关于广义 bent 函数的基本性质和应用可参见文献[1]及其所附文献.

bent 函数(即 $q=2$ 的情形)由 Rothaus[2]于 1976 年提出,Kumar 等人[1]于 1985 年将其推广到一般 q 的情形. 对于 $q=2$ 的情形,Rothaus 证明了:类型为$[n, 2]$的 bent 函数存在当且仅当 n 为偶数,并且对所有正偶数 n 均构作出类型$[n, 2]$的 bent 函数. 文献[1]中对于偶数 n 或者 $q\not\equiv 2\pmod 4$的情形均构作出类型$[n, q]$的广义 bent 函数. 于是本文以下假设

$$n\text{ 为正奇数},q=2N,\ 2\nmid N\geqslant 3.$$

对于满足这个条件的 n 和 q,至今还没有构作出任何类型$[n, q]$的广义 bent 函数,但是已经得到在下列附加条件下的一些不存在性结果:

(A)[1] 存在正整数 s,使得

$$2^s\equiv -1\pmod N. \tag{2}$$

(B)[3] $(n, q)=(1, 14)$.

(C)[4] $n=1$, $N=p^l$, 其中 $l\geqslant 1$, p 为素数,

$$p\equiv 7\pmod 8,\ p\geqslant 23.$$

(D)[5] $n=1$, $N=p_1^{e_1}\cdots p_g^{e_g}$, 其中 $g\geqslant 1$, $p_1, \cdots, p_g$ 是不同的奇素数,$e_i\geqslant 1$ $(1\leqslant i\leqslant g)$,并且对每个 $i(1\leqslant i\leqslant g)$,存在 $s_i\geqslant 1$,使得

$$p_i^{s_i}\equiv -1\left(\bmod\frac{N}{p_i^{e_i}}\right).$$

2000-01-05 收稿
* 国家自然科学基金资助项目(批准号:19631100)

结果(D)是结果(B)和(C)的推广,因为由结果(D)可知对任意奇素数 p 和 $l\geqslant 1$,类型[1, $2p^l$]的广义 bent 函数均不存在. 本文将给出广义 bent 函数不存在性的一些新结果,其中 n 是大于 1 的奇数.

为了表明我们的结果(第 2 和 3 节)是新的,需要把满足条件(2)的 N 表示成更明显的形式. 文献[4]中已经给出这个明显形式. 简言之,设 $N=\prod_{i=1}^{g}p_i^{e_i}$,由中国剩余定理可知条件(2)相当于

$$2^s\equiv -1 \pmod{p_i^{e_i}}\ (1\leqslant i\leqslant g), \tag{3}$$

以 $I(p)$表示 2 模 p 乘法阶的偶数部分. 不难看出条件(3)等价于

$$I(p_i)\ (1\leqslant i\leqslant g)\text{ 是同样的偶数.} \tag{4}$$

当 $p\equiv 3, 5, 7 \pmod 8$时,易知 $I(p^e)$分别为 2, 4, 1. 于是(A)中条件(2)恰好相当于以下 5 种情形:

(A_1) $p_i\equiv 1 \pmod 8$ $(1\leqslant i\leqslant g)$, 并且 $I(p_i)$ $(1\leqslant i\leqslant g)$是同样的偶数.

(A_2) $p_i\equiv 3 \pmod 8$ $(1\leqslant i\leqslant g)$.

(A_3) $p_i\equiv 5 \pmod 8$ $(1\leqslant i\leqslant g)$.

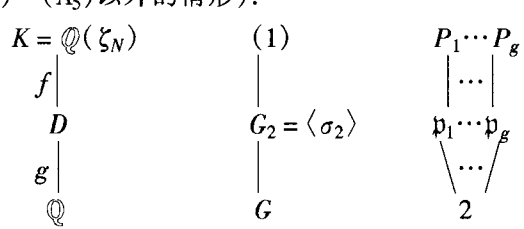
(A_4) $N=\prod_{i=1}^{l}p_i^{e_i}\cdot\prod_{j=1}^{s}p_j'^{f_j}$, $p_i\equiv 3 \pmod 8$ $(1\leqslant i\leqslant l)$, $p_j'\equiv 1 \pmod 8$ 并且 $I(p_j')=2$ $(1\leqslant j\leqslant s)$.

(A_5) $N=\prod_{i=1}^{l}p_i^{e_i}\cdot\prod_{j=1}^{s}p_j'^{f_j}$, $p_i\equiv 5 \pmod 8$ $(1\leqslant i\leqslant l)$, $p_j'\equiv 1 \pmod 8$ 并且 $I(p_j')=4$ $(1\leqslant j\leqslant s)$.

下面解释条件(2)的数论意义. 令 $K=\mathbb{Q}(\zeta_N)$, 其中 $\zeta_N=e^{\frac{2\pi i}{N}}$, 则 Galois 群 $G=\mathrm{Gal}(K/\mathbb{Q})$ 同构于$(\mathbb{Z}/N\mathbb{Z})^\times$:

$$G\xrightarrow{\sim}(\mathbb{Z}/N\mathbb{Z})^\times,\ \sigma_a\longmapsto a \pmod N,\ (a,N)=1, \tag{5}$$

其中 σ_a 是由$\sigma_a(\zeta_N)=\zeta_N^a$决定的自同构. 以 D 表示 2 在分圆域 K 中的分解域,$G_2=\mathrm{Gal}(K/D)$是 2 在 K 中的分解群,则 G_2 是由 σ_2 生成的循环群. 因此 $f=[K:D]=|G_2|$ 是 σ_2 在 G 中的阶,也就是 2 模 N 的乘法阶. 而 $g=[D:\mathbb{Q}]=\dfrac{\varphi(N)}{f}$, 其中 $\varphi(N)=[K:\mathbb{Q}]$是 Euler 函数. 对于代数数域 F,我们用 O_F 表示 F 的整数环,则 2 在分解域 D 中完全分解:$2O_D=\mathfrak{p}_1\cdots\mathfrak{p}_g$, 而每个 $\mathfrak{p}_i$ 在 K 中是惰性的,即 $\mathfrak{p}_iO_K=P_i$ 为 O_K 的素理想. 由同构(5)式可知,条件(2)相当于 σ_{-1} (复共轭自同构)属于群 $G_2=\langle\sigma_2\rangle$,这也相当于说 D 是实域,所以从下节起我们均考虑 D 不是实域的情形(即条件(A_1) ~ (A_5)以外的情形).



1　两个引理

本文以下采用如下的记号：

n，N 为正奇整数，$N\geqslant 3$，$q=2N$；$K=\mathbb{Q}(\zeta_N)$，$\zeta_N=e^{\frac{2\pi i}{N}}$；$G=\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_a \mid a\in(\mathbb{Z}/N\mathbb{Z})^\times\}$；$D$ 为 2 在 K 中的分解域；$G_2=\mathrm{Gal}(K/D)=\langle\sigma_2\rangle$ 为 2 在 K 中的分解群；$f=[K:D]=|G_2|$ 为 2 模 N 的乘法阶；O_F 为代数数域 F 的整数环；$g=[D:\mathbb{Q}]=\dfrac{\varphi(N)}{f}$ 为 2 在 O_K 和 O_D 中素理想因子的个数.

如果存在类型$[n,\ q]$的广义 bent 函数，由条件(1)可知存在 $\xi\in O_K=\mathbb{Z}[\zeta_N]$，使得 $\xi\bar{\xi}=q^n=2^nN^m$，其中 $\bar{\xi}$ 为 ξ 的复共轭 $\sigma_{-1}(\xi)$. 本文采用的第 1 个引理为

引理 1.1[5]　设 $N=\prod_{i=1}^{g}p_i^{e_i}$，其中 $g\geqslant 1$，$p_1,\cdots,p_g$ 为不同的奇素数，$e_i\geqslant 1$ $(1\leqslant i\leqslant g)$，并且对每个 i $(1\leqslant i\leqslant g)$均存在正整数 s_i，使得

$$p_i^{s_i}\equiv -1\left(\mathrm{mod}\ \frac{N}{p_i^{e_i}}\right).$$

如果存在 $\xi\in O_K$，使得 $\xi\bar{\xi}=2^nN^m$，则存在 $\alpha\in O_K$，使得 $\alpha\bar{\alpha}=2^n$.

注 1.1　当 $g=1$(即 N 为奇素数的幂)时引理 1.1 中条件显然满足. 当 $g\geqslant 2$ 时，以 I_{ij} 表示 p_i 模 p_j 的乘法阶的偶数部分$(1\leqslant i\neq j\leqslant g)$，不难看出引理 1.1 中条件相当于：对每个 i $(1\leqslant i\leqslant g)$，$I_{ij}(1\leqslant j\leqslant g,\ j\neq i)$为相同的偶数(只依赖于 i).

本文采用的第 2 个引理是说：引理 1.1 中的 α 可在比 K 更小的子域中找到.

引理 1.2　若存在 $\alpha\in O_K$，使得 $\alpha\bar{\alpha}=2^n$，则存在 $\beta\in O_K$，使得 $\beta^2\in O_D$，$\beta\bar{\beta}=2^n$，其中 D 为 2 在 K 中的分解域. 进而若 $f=[K:D]$是奇数，则 $\beta\in O_D$.

证　按文献[4]中引理 2 的证明思想，但是加以简化. 由于 σ_2 固定 2 在 O_K 中的所有素理想因子，由 $\alpha\bar{\alpha}=2^n$ 可知 $\alpha O_K=\sigma_2(\alpha O_K)=\sigma_2(\alpha)O_K$. 于是 $\sigma_2(\alpha)=\alpha\varepsilon$，其中 ε 为 O_K 中单位. 对每个 $\sigma\in G$，

$$\sigma(\alpha)\overline{\sigma(\alpha)}=\sigma(\alpha\bar{\alpha})=2^n,\quad \sigma\sigma_2(\alpha)=\sigma(\alpha\varepsilon)=\sigma(\alpha)\sigma(\varepsilon),$$

因此

$$2^n=\sigma\sigma_2(\alpha)\overline{\sigma\sigma_2(\alpha)}=\sigma(\alpha\varepsilon)\overline{\sigma(\alpha\varepsilon)}=2^n\sigma(\varepsilon)\overline{\sigma(\varepsilon)},$$

于是$|\sigma(\varepsilon)|=1$ (对每个 $\sigma\in G$). 这表明 ε 是 K 中的单位根，即 $\varepsilon=\pm\delta$，其中 $\delta=\zeta_N^i$(对某个 $i\in\mathbb{Z}$). 令 $\beta=\alpha\delta^{-1}$，则 $\beta\bar{\beta}=\alpha\bar{\alpha}=2^n$，并且

$$\sigma_2(\beta)=\sigma_2(\alpha)\sigma_2(\delta)^{-1}=\alpha\varepsilon\delta^{-2}=\pm\alpha\delta^{-1}=\pm\beta,$$

于是 $\sigma_2(\beta^2)=\beta^2$，这表明 $\beta^2\in O_D$，进而 $D\subseteq D(\beta)\subseteq K$，并且$[D(\beta):D]\leqslant 2$. 如果 $f=[K:D]$为奇数，则 $D(\beta)=D$，从而 $\beta\in O_D$.

2　$N=p^l$，$p\equiv 7\ (\mathrm{mod}\ 8)$的情形

如果存在类型$[n,\ 2p^l]$的广义 bent 函数，由条件(1)可知存在 $\xi\in O_K$，使得 $\xi\bar{\xi}=(2p^l)^n$，再由引理 1.1 可知存在 $\alpha\in O_K$，使得 $\alpha\bar{\alpha}=2^n$. 当 $p\equiv 7\ (\mathrm{mod}\ 8)$时，$\left(\dfrac{2}{p}\right)=1$，从而 f 和 $s=\dfrac{g}{2}$

$=\dfrac{\varphi(p^l)}{2f}$均为奇数. 由引理1.2可知存在$\beta\in O_D$,使得$\beta\bar{\beta}=2^n$. 文献[4]中引理3声称这样的$\beta$可以取成$D$的虚二次子域$\mathbb{Q}(\sqrt{-p})$中的整数,但是其证明似乎有问题. 我们知道2在$\mathbb{Q}(\sqrt{-p})$中分解成两个不同素理想乘积: $2=\mathfrak{p}\bar{\mathfrak{p}}$, 而$\mathfrak{p}$和$\bar{\mathfrak{p}}$在$D$中也完全分解为

$$\mathfrak{p}O_D = \mathfrak{p}_1\cdots\mathfrak{p}_s,\ \bar{\mathfrak{p}}O_D = \bar{\mathfrak{p}}_1\cdots\bar{\mathfrak{p}}_s \quad \left(s=\frac{g}{2}\right).$$

问题在于$\mathrm{Gal}(D/\mathbb{Q})$的生成元在集合$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_s,\bar{\mathfrak{p}}_1,\cdots,\bar{\mathfrak{p}}_s\}$上的作用为循环置换$(\mathfrak{p}_1\bar{\mathfrak{p}}_t\mathfrak{p}_2\bar{\mathfrak{p}}_{t+1}\cdots\mathfrak{p}_s\bar{\mathfrak{p}}_{t-1})\left(t=\dfrac{s+3}{2}\right)$, 而不是像文献[4]引理3证明中所说的为循环置换$(\mathfrak{p}_1\cdots\mathfrak{p}_s\bar{\mathfrak{p}}_1\cdots\bar{\mathfrak{p}}_s)$, 所以文献[4]中关于类型$[1,2p^l]$的广义bent函数不存在性(即前述结果(C))的证明似乎是不完全的. 文献[5]中补救了这个欠缺,对于条件(1)作进一步分析之后得到结果(D),而结果(C)是它的特殊情形. 我们现在对于$n>1$的情形得到关于广义bent函数不存在性的新结果.

定理2.1 设$N=p^l$,其中$l\geqslant 1$, p为素数并且$p\equiv 7\pmod 8$. 记f为2模p^l的乘法阶,$s=\dfrac{g}{2}=\dfrac{\varphi(p^l)}{2f}$(于是$f$和$s$均为奇数). 令$m$是使方程$x^2+py^2=2^{m+2}$有整数解$(x,y)$的最小奇整数, 则对正奇整数$n$, 当$n<\dfrac{m}{s}$时不存在类型$[n,2p^l]$的广义bent函数.

证 如果存在类型$[n,2p^l]$的广义bent函数,由定理2.1前面所述,可知存在$\beta\in O_D$, 使得$\beta\bar{\beta}=2^n$. 令$E=\mathbb{Q}(\sqrt{-p})$, 则$[D:E]=\dfrac{g}{2}=s$. 令$\gamma=N_{D/E}(\beta)\in O_E$, 则$\gamma\bar{\gamma}=N_{D/E}(\beta\bar{\beta})=2^{sn}$. 由于$O_E=\mathbb{Z}\left[\dfrac{1+\sqrt{-p}}{2}\right]$,可知$\gamma=\dfrac{1}{2}(A+B\sqrt{-p})$, 其中$A$, $B\in\mathbb{Z}$. 于是$A^2+pB^2=4\gamma\bar{\gamma}=2^{sn+2}$. 由$sn$为奇数和$m$的定义可知$m\leqslant sn$. 这就表明当$n<\dfrac{m}{s}$时不存在类型$[n,2p^l]$的广义bent函数.

注2.1 (i) 设p是固定的奇素数. 对每个$l\geqslant 1$, 以f_l表示2模p^l的乘法阶,$g_l=\dfrac{\varphi(p^l)}{f_l}$. 不难看出,若$2^{p-1}\not\equiv 1\pmod{p^2}$, 则$f_l=p^{l-1}f_1$, $g_l=\dfrac{\varphi(p^l)}{f_l}=g_1$. 熟知在$p<6\cdot 10^9$当中除了$p=1\,093$和$3\,511$之外均满足$2^{p-1}\not\equiv 1\pmod{p^2}$(参见文献[6]), 所以对于$p<6\cdot 10^9$, $p\neq 1\,093$, $3\,511$的情形只需计算g_1.

(ii) 定理2.1中m的定义是初等的,但是它有代数数论意义. 由于m是使$x^2+py^2=2^{m+2}$有整数解$(x,y)=(A,B)$的最小奇数,可知A和B均为奇数. 于是$\delta=\dfrac{1}{2}(A+B\sqrt{-p})\in O_E$,并且$\delta\bar{\delta}=2^m$. 由$2O_E=\mathfrak{p}\bar{\mathfrak{p}}$和$m$的最小性可知$\delta O_E=\mathfrak{p}^m$或$\bar{\mathfrak{p}}^m$,所以$m$即是理想类$[\mathfrak{p}]$在$E=\mathbb{Q}(\sqrt{-p})$的理想类群中的阶. 特别地,$m$是$E$的理想类数$h(-p)$的因子. 由Gauss亏格理论知$h(-p)$为奇数. 另一方面,由$2^{m+2}=A^2+pB^2>p$可得到下界$m>\dfrac{\log p}{\log 2}-2$. 特别当$p\geqslant 23$时,$m\geqslant 3$. 所以当$h(-p)$是素数时,$m=h(-p)$. 虚二次域类数可查文献[7]中的类数表.

由以上考查可知，定理 2.1 有如下推论：

推论 2.1　设 $p\equiv 7 \pmod 8$，$p\geqslant 23$，$2^{p-1}\not\equiv 1 \pmod{p^2}$并且 2 模 p 的乘法阶为 $\frac{p-1}{2}$，则当正奇数 n 小于定理 2.1 中定义的 m 时，对每个 $l\geqslant 1$ 均不存在类型$[n, 2p^l]$的广义 bent 函数.

推论 2.2　设 $p\equiv 7 \pmod 8$，$p\geqslant 23$，$2^{p-1}\not\equiv 1 \pmod{p^2}$并且 $h(-p)$为素数. 以 f 表示 2 模 p 的乘法阶，$s=\frac{p-1}{2f}$，则当 $2\nmid n<\frac{h(-p)}{s}$时，对每个 $l\geqslant 1$ 均不存在类型$[n, 2p^l]$的广义 bent 函数.

例 1　$p=47, 71, 79, 103, 191$ 和 199 满足推论 2.1 中条件(即 $s=1$)，对其中前 5 个素数 p，$h(-p)$分别为素数 5, 7, 5, 5, 13，于是 $m=h(-p)$. 由推论 2.2 知对每个 $l\geqslant 1$，类型$[3, 2\cdot 47^l]$，$[3, 2\cdot 71^l]$，$[5, 2\cdot 71^l]$，$[3, 2\cdot 79^l]$，$[3, 2\cdot 103^l]$和$[n, 2\cdot 191^l]$ $(n=3, 5, 7, 9, 11)$的广义 bent 函数均不存在. 对于 $p=199$，可算出 $s=1$，$h(-199)=9$. 由于 $m\mid 9$ 并且 $m>\frac{\log 199}{\log 2}-2>3$，可知 $m=9$，从而类型为$[n, 2\cdot 199^l]$ $(l\geqslant 1,\ n=3, 5, 7)$的广义 bent 函数均不存在($n=1$ 的情形为已知结果).

3　$N=p^lp'^{l'}$的情形

本节考虑 $N=p^lp'^{l'}$的情形，其中 l，$l'\geqslant 1$，p 和 p'是不同的奇素数，并且不属于情形$(A_1)\sim(A_5)$. 但是我们假设 N 满足引理 1.1 中所述条件，即存在正整数 s 和 s'，使得

$$p^s\equiv -1 \pmod{p'^{l'}},\quad p'^{s'}\equiv -1 \pmod{p^l},$$

易知这相当于条件

(*)　p 模 p' 的乘法阶和 p' 模 p 的乘法阶均为偶数.

定理 3.1　设 $N=p^lp'^{l'}$，其中 l，$l'\geqslant 1$，$p\equiv 3 \pmod 4$，$p'\equiv 5 \pmod 8$，并且素数 p 和 p'满足条件(*)$\left(\text{易知这相当于}\left(\frac{p}{p'}\right)=-1\right)$. 记 f 为 2 模 N 的乘法阶，$\varphi(N)=fg$，则 g 为偶数，$s=g/2$ 为奇数.

(ⅰ) 若 $p\equiv 3 \pmod 8$，记 $E=\mathbb{Q}(\sqrt{-pp'})$，则 $2O_E=P\bar{P}$，其中 P 和 $\bar{P}$ 是 O_E 中不同素理想. 以 m 表示使方程 $p'y^2+pz^2=2^{m+2}$有整数解(y, z)的最小正整数，则 m 为奇数并且理想类$[P]$在 E 的类群中的阶为 $2m$. 如果奇数 n 小于 m/s，则不存在类型$[n, 2N]$的广义 bent 函数.

(ⅱ) 若 $p\equiv 7 \pmod 8$，记 $E=\mathbb{Q}(\sqrt{-p})$，则 $2O_E=P\bar{P}$. 以 m 表示使方程 $x^2+pz^2=2^{m+2}$有整数解(x, z)的最小正奇数，则 m 是理想类$[P]$在 E 的类群中的阶. 如果奇数 n 小于 m/s，则不存在类型$[n, 2N]$的广义 bent 函数.

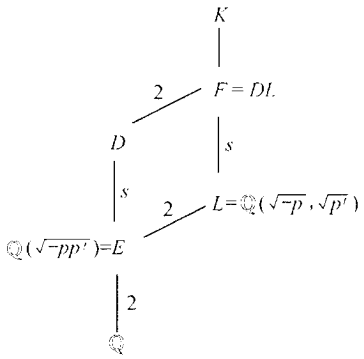
证　由条件 $p\equiv 3 \pmod 4$和 $p'\equiv 5 \pmod 8$可知，2 模 p^l 和$p'^{l'}$的乘法阶分别为 t 和 $4t'$，其中 t'为奇数. 于是 $f=[t, 4t']=4a$，a 为奇数，由此可知 $s=\frac{g}{2}=\frac{\varphi(N)}{2f}$为奇数. 以 D 表示 2 在 $K=\mathbb{Q}(\zeta_N)$中的分解域，则$[D:\mathbb{Q}]=g=2s$.

如果存在类型$[n, 2N]$的广义 bent 函数(其中 n 为正奇数)，则存在 $\xi\in O_K$，使得 $\xi\bar{\xi}=$

$(2N)^n$. 由于 N 满足条件(*),根据引理1.1可知存在 $\alpha\in O_K$,使得 $\alpha\bar{\alpha}=2^n$. 再由引理1.2可知存在 $\beta\in O_K$,$\beta^2\in O_D$,使得 $\beta\bar{\beta}=2^n$.

(ⅰ) 设 $p\equiv 3\pmod 8$. 由2在 $E=\mathbb{Q}(\sqrt{-pp'})$中的分解可知,$E\subset D$ 并且$[D:E]=s$. 由 $\beta^2\in O_D$ 可知β 属于D 在K 中的唯一的二次扩域F,域 F Galois 对应于 G 中由$\sigma_2^2=\sigma_4$ 生成的循环子群,由此可知 $L=\mathbb{Q}(\sqrt{-p},\sqrt{p'})$是 F 的子域并且 $F=DL$, $[F:L]=s$. 令 $\gamma=N_{F/L}(\beta)\in O_L$,则

$$\gamma\bar{\gamma}=N_{F/L}(\beta\bar{\beta})=N_{F/L}(2^n)=2^{ns},$$
$$\gamma^2=N_{F/L}(\beta^2)=N_{D/E}(\beta^2)\in O_E.$$



熟知 O_L 有整基$\left\{1,\ \alpha=\dfrac{1+\sqrt{p'}}{2},\ \beta=\dfrac{1+\sqrt{-p}}{2},\ \alpha\beta\right\}$(例如可见文献[8]p. 52,习题42(d)),所以

$$\gamma=A+B\alpha+C\beta+D\alpha\beta\quad(A,B,C,D\in\mathbb{Z})$$
$$=\frac{1}{4}(X+Y\sqrt{p'}+Z\sqrt{-p}+W\sqrt{-pp'}),$$

其中 $X=4A+2B+2C+D$, $Y=2B+D$, $Z=2C+D$ 和 $W=D$ 满足

$$X\equiv Y\equiv Z\equiv W\pmod 2,\quad X+W\equiv Y+Z\pmod 4. \tag{6}$$

而

$$2^{ns+4}=16\gamma\bar{\gamma}=X^2+p'Y^2+pZ^2+pp'W^2+2(XY+pZW)\sqrt{p'},$$

于是

$$X^2+p'Y^2+pZ^2+pp'W^2=2^{ns+4},\tag{7}$$
$$XY=-pZW,$$

注意 $\gamma^2\in O_E=\mathbb{Z}\left[\dfrac{1+\sqrt{-pp'}}{2}\right]$. 如果 $\gamma\in O_E$, 则 $Y=Z=0$, 于是 $X^2+pp'W^2=2^{ns+4}$. 由于 ns 为奇数,由此方程模 p 得到$\left(\dfrac{2}{p}\right)=1$, 这与 $p\equiv 3\pmod 8$矛盾. 因此 $\gamma\notin O_E$ 而$\gamma\in O_L$. 所以 $L=E(\gamma)$, $\gamma^2\in O_E$, 记 σ 为 $\mathrm{Gal}(L/E)$的非恒等自同构,则 $\sigma(\gamma)=-\gamma$, 即 $X-Y\sqrt{p'}-Z\sqrt{-p}+W\sqrt{-pp'}=-X-Y\sqrt{p'}-Z\sqrt{-p}-W\sqrt{-pp'}$, 于是 $X=W=0$. 这时由同余式(6)可知 Y 和 Z 均为偶数. 记 $y=\dfrac{Y}{2}$, $z=\dfrac{Z}{2}$, 则(7)式变为

$$p'y^2 + pz^2 = 2^{ns+2}. \tag{8}$$

以 m 表示方程 $p'y^2 + pz^2 = 2^{m+2}$ 有整数解 $(y, z) = (a, b)$ 的最小正整数，则 $-1 = \left(\frac{p'}{p}\right) = \left(\frac{2}{p}\right)^m = (-1)^m$，可知 m 为奇数. 由 m 的最小性可知 a 和 b 均为奇数，而

$$2^m p = \left(\frac{bp + a\sqrt{-pp'}}{2}\right)\left(\frac{bp - a\sqrt{-pp'}}{2}\right).$$

由于 $2O_E = P\bar{P}$，$pO_E = P'^2$，再由 m 的最小性可知

$$\left(\frac{bp + a\sqrt{-pp'}}{2}\right) O_E = P^m P' \text{ 或 } \bar{P}^m P'.$$

于是 $[P]^m[P'] = 1$. 熟知 $[P']$ 是二阶元素，从而 $[P]$ 的阶为 $2m$. 由(8)式和 m 的定义可知 $sn \geqslant m$. 因此当 $2\nmid n < \frac{m}{s}$ 时，不存在类型 $[n, 2N]$ 的广义 bent 函数.

(ⅱ) 再考虑 $p \equiv 7 \pmod 8$. 这时取 $E = \mathbb{Q}(\sqrt{-p})$. 如前推理可知存在

$$\gamma = \frac{1}{4}(X + Y\sqrt{p'} + Z\sqrt{-p} + W\sqrt{-pp'}) \in O_L,$$

$$\gamma^2 \in O_E = \mathbb{Z}\left[\frac{1 + \sqrt{-p}}{2}\right],\ \gamma\bar{\gamma} = 2^{ns},$$

如果 $\gamma \notin O_E$，则 $L = E(\gamma)$，$\gamma^2 \in O_E$，可知 $X = Z = 0$，于是 $2^{ns+4} = p'(Y^2 + pW^2)$，这不可能. 所以 $\gamma \in O_E$，即 $Y = W = 0$，$X^2 + pZ^2 = 2^{ns+4}$，$X \equiv Z \equiv 0 \pmod 2$. 令 $x = \frac{X}{2}$，$z = \frac{Z}{2}$，则

$$x^2 + pz^2 = 2^{ns+2}. \tag{9}$$

以 m 表示使 $x^2 + pz^2 = 2^{m+2}$ 有整数解 $(x, z) = (a, c)$ 的最小正奇数，则 a 和 c 均为奇数并且 $\left(\frac{a + c\sqrt{-p}}{2}\right)\left(\frac{a - c\sqrt{-p}}{2}\right) = 2^m$. 由 $2O_E = P\bar{P}$ 和 m 的最小性可知 $\left(\frac{a + c\sqrt{-p}}{2}\right) O_E = P^m$ 或 $\bar{P}^m$，并且 m 为 $[P]$ 的阶. 由(9)式和 m 的最小性可知 $ns \geqslant m$. 所以当 $2\nmid n < \frac{m}{s}$ 时不存在类型 $[n, 2N]$ 的广义 bent 函数.

注 3.1　当 $p \equiv 3 \pmod 8$ 时，熟知 $E = \mathbb{Q}(\sqrt{-pp'})$ 的理想类数 $h(-pp') = 2t$，其中 t 为奇数. 由于 m 是 $h(-pp')$ 的奇因子，所以若 t 为素数，则 $m = t = h(-pp')/2$. 当 $p \equiv 7 \pmod 8$ 并且 $p \geqslant 23$ 时，$1 < m \mid h(-p)$. 特别若 $h(-p)$ 为素数，则 $m = h(-p)$.

例 2　表 1 列出的 (p, p') $(p \equiv 3 \pmod 8,\ p' \equiv 5 \pmod 8)$ 满足条件 $(*)$ $\left(\text{这相当于}\left(\frac{p'}{p}\right) = -1\right)$. 表内同样列出 s 和 $h(-pp')$ 的值. 当 $h(-pp')/2$ 为素数时 $m = h(-pp')/2$. 否则用 m 的定义决定 m(它是 $h(-pp')/2$ 的因子).

根据定理 3.1 可知对所有 l，$l' \geqslant 1$，不存在类型 $[3, 2\cdot 43^l \cdot 29^{l'}]$ 和 $[3, 2\cdot 43^l \cdot 61^{l'}]$ 的广义 bent 函数. 对其余情形均有 $s = 1$，从而当 $2\nmid n < m$ 时不存在类型 $[n, 2p^l p'^{l'}]$ 的广义 bent 函数 ($n = 1$ 的情形为文献[5]中已知结果).

表1

(p, p')	s	$h(-pp')$	m	(p, p')	s	$h(-pp')$	m
(67,5)	1	18	9	(59,37)	1	42	21
(83,5)	1	10	5	(3,53)	1	10	5
(11,13)	1	10	5	(19,53)	1	30	15
(59,13)	1	22	11	(67,53)	1	58	29
(67,13)	1	22	11	(83,53)	1	50	25
(83,13)	1	34	17	(11,61)	1	30	15
(11,29)	1	10	5	(43,61)	3	22	11
(19,29)	1	26	13	(59,61)	1	66	33
(43,29)	3	26	13	(67,61)	1	30	5
(19,37)	1	14	7				

例3 表2列出的(p, p') ($p\equiv 7 \pmod 8$, $p'\equiv 5 \pmod 8$)满足条件$(*)\left(\text{即}\left(\frac{p}{p'}\right)=-1\right)$. 对所有情形 $s=1$, 并且 $h(-p)$为素数,于是 $m=h(-p)$.

表2

(p, p')	(47, 5),(47, 13),(47,29)	(71, 13),(71,53),(71,61)	(79,29),(79,37),(79,53),(79,61)
$m=h(-p)$	5	7	5

由定理3.1可知对于 $N=p^{l}\cdot p'^{l'}$(其中 l, $l'\geqslant 1$ 而(p, p')如表2所示),当 $2\nmid n<h(-p)$ 时不存在类型$[n, 2N]$的广义 bent 函数($n=1$ 的情形为文献[5]中已知结果).

参 考 文 献

1 Kumar P V, Scholtz R A, Welch L R. Generalized bent functions and their properties. J of Comb Theory (A), 1985, 40: 90~107

2 Rothaus O S. On bent functions. J Comb Theory (A), 1976, 20: 300~305

3 Pei D. On non-existance of generalized bent functions. In: LN in Pure and Applied Math, Vol 141. New York: Dekker, 1993. 165~172

4 Akyildiz E, Guloglu I S, Ikeda M. A note of generalized bent functions. J of Pure and Applied Alg, 1996, 106: 1~9

5 Ikeda M. A remark on the non-existance of generalized bent functions. In: Number Theory and its Applications (Ankara, 1996). LN in Pure and Appl Math, Vol 204. New York: Dekker, 1999. 109~119

6 Ribenboim P. The Book of Prime Number Records. 2nd ed. New York: Springer-Verlag, 1989

7 Wada H, Saito M. A Table of Ideal Class Group of Imaginary Quadratic Fields. Sophia Kokyuroku in Math, Vol 28. Tokyo: Sophia Univ, 1988

8 Marcus D A. Number Fields. New York: Springer-Verlag, 1977