学 术 论 文

类差分平衡函数的性质及其应用

张文英[1,2]，李世取[1]
（1. 郑州信息工程学院，郑州 450002；2. 济南陆军学院，济南 250029）

[摘要] 定义了布尔函数的类差分和类差分平衡函数，研究了类差分平衡函数的密码学性质以及构造方法。作为类差分平衡函数的应用，给出了 Z_4^2 上逻辑函数是完全非线性函数的充要条件，并在首先分析得到所有四元类差分平衡函数的基础上，编程搜索出 Z_4^2 上所有的完全非线性函数。

[关键词] Bent 函数；完全非线性函数；2 - 基展开；类差分；类自相关函数；类差分平衡函数
[中图分类号] TN918.1 [文献标识码] A [文章编号] 1009 - 1742 (2004) 03 - 0045 - 08

1 引言

由于具有抗差分攻击和最优仿射逼近的能力，以及具有最高的非线性度和高度的稳定性[1]，Bent 函数[2]在密码设计中发挥了重要作用，早在 1982 年，Olsen 和 Scholtz 就将用 Bent 函数构造的具有良好的自相关和互相关性质的二元序列用于码分多址通信系统中[3]，又如澳大利亚加密标准 HAVAL 算法[4]的设计中所用到的 5 个布尔函数无一例外都是由 Bent 函数演化而来。1990 年，K. Nyberg 把 Bent 函数的概念从二元域上的 n 维向量空间推广为素域 F_p 上的 n 维向量空间上的完全非线性函数，并研究了素域上完全非线性函数的密码性质及构造方法[5]。由于剩余类环中含有零因子，导致剩余类环上一大类逻辑函数（特别是可用常义下的多项式表示的函数）不是完全非线性函数[6]，这就给剩余类环上的完全非线性函数的研究带来了很大的困难，故迄今为止，关于剩余类环上完全非线性函数的存在性和构造研究的文献目前仍不多见。

众所周知，构造剩余类环上完全非线性函数是比较困难的，笔者在用 2 - 基分解的思想研究剩余类环上完全非线性函数新构造方法时，发现了一类新的布尔函数类，对这类函数做一种类似于“差分”的运算后可以得到平衡函数，于是定义了布尔函数的“类差分”和布尔函数中的类差分平衡函数，研究了类差分平衡函数的性质，给出了类差分平衡函数的一些构造方法。作为类差分平衡函数的重要应用，给出了 Z_4^2 上逻辑函数是完全非线性函数的充要条件，并在首先分析得到所有四元类差分平衡函数的基础上编程搜索出 Z_4^n 上所有的完全非线性函数。第 6 章中研究问题的思想和方法同样可以用于 Z_4^n 上弹性函数的研究。

将会看到，由于 Z_4^n 上完全非线性函数的 2 - 基分解式中的第一个分量都是类差分平衡函数，所以，研究类差分平衡函数对于 Z_4^n 上完全非线性函数的研究具有重要的指导意义。

2 基本概念

以 $GF(2)$ 表示二元域，记 $\Omega = GF^n(2)$，$\mathcal{F} = \{A : A \subset \Omega\}$，可测空间 $(\Omega, \mathcal{F})$ 上的概率测度 $P(\cdot)$ 满足

$$P\{(x_1, \cdots, x_n)\} \doteq 2^{-n},$$
$$(x_1, \cdots, x_n) \in \Omega = GF^n(2)。$$

又定义

$$X_k((x_1, \cdots, x_n)) = x_k,$$

[收稿日期] 2003 - 05 - 23；修回日期 2003 - 09 - 03
[作者简介] 张文英（1970 - ），女，山东鄄城县人，济南陆军学院讲师，郑州信息工程学院博士研究生

$(x_1,\cdots,x_n)\in\Omega=GF^n(2),1\leqslant k\leqslant n$，

易知 $X_1,X_2,\cdots,X_n$ 是概率空间$(\Omega,\mathcal{F},P)$上的 n 个相互独立的布尔随机变量，且满足

$$P\{X_k=0\}=P\{X_k=0\}=1/2,1\leqslant k\leqslant n。$$

从 $GF^n(2)$ 到 $GF(2)$ 的一个映射称为布尔函数，布尔函数 f 可以用关于 $x_1,\cdots,x_n$ 的多项式唯一表示，该多项式称为 f 的代数标准形，简记为 ANF[7]。f 的 ANF 中各单项式所含变元个数的最大值称为 f 的代数次数。如果 $GF^n(2)$ 中使得 $f(x)=1$ 的向量的个数为 2^{n-1}，则称 f 是平衡的。$GF^n(2)$ 中2个向量的点积记为 $\boldsymbol{w}\cdot\boldsymbol{x}$，布尔函数 f 的 Walsh 循环谱 $S_{(f)}(\boldsymbol{w})$[2]是定义在 $GF^n(2)$ 上的一个实值函数：

$$S_{(f)}(\boldsymbol{w})=2^{-n}\sum_{\boldsymbol{x}\in GF^n(2)}(-1)^{f(\boldsymbol{x})+\boldsymbol{w}\cdot\boldsymbol{x}},\quad \boldsymbol{w}\in GF^n(2)。\tag{1}$$

它反映了 f 与各个仿射函数的距离，分组密码中的线性攻击和流密码中的相关攻击都等价于寻找一个与给定布尔函数距离最近的仿射函数或线性函数。自相关函数 $r_f(s)$[2]也是定义在 $GF^n(2)$ 上的一个实值函数：

$$r_f(\boldsymbol{s})=2^{-n}\sum_{\boldsymbol{x}\in GF^n(2)}(-1)^{f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})},\boldsymbol{s}\in GF^n(2),$$

它反映了当输入改变量为 $\boldsymbol{s}$ 时的输出与原输出的符合优势，显然，$r_f(\boldsymbol{s})=0$ 等价于差分函数 $f(\boldsymbol{x}+\boldsymbol{s})+f(\boldsymbol{x})$ 平衡。布尔函数的 Walsh 循环谱与自相关函数之间有如下联系[8]：

$$[S_{(f)}(\boldsymbol{w})]^2=2^{-n}\sum_{\boldsymbol{s}\in GF^n(2)}r_f(\boldsymbol{s})(-1)^{\boldsymbol{w}-\boldsymbol{s}},\quad \boldsymbol{w}\in GF^n(2)。\tag{2}$$

如果对任意的 $\boldsymbol{w}\in GF^n(2)$ 都有 $[S_{(f)}(\boldsymbol{w})]^2=2^{-n}$（等价于对任意的 $0\neq\boldsymbol{s}\in GF^n(2)$，都有 $r_f(\boldsymbol{s})=0$），则称 f 是 Bent 函数。

3 类差分平衡函数及其性质

3.1 类差分函数与类自相关函数

在这节中 n 为正偶数。

定义1 设 $f(\boldsymbol{x}),\boldsymbol{x}=(x_1,\cdots,x_n)\in GF^n(2)$ 是布尔函数，对 $\boldsymbol{s}=(s_1,\cdots,s_n)\in GF^n(2)$，称

$$f(x_1+s_1,\ s_1x_1+x_2+s_2,\cdots,\ x_{n-1}+s_{n-1},\ s_{n-1}x_{n-1}+x_n+s_n)+f(x_1,\ x_2,\cdots,x_{n-1},\ x_n)$$

为 $f(\boldsymbol{x}),\boldsymbol{x}=(x_1,\cdots,x_n)\in GF^n(2)$ 在 $\boldsymbol{s}$ 点的类差分函数。

为了书写方便，记

$$\boldsymbol{x}\oplus\boldsymbol{s}=(x_1+s_1,\ s_1x_1+x_2+s_2,\cdots,\ x_{n-1}+s_{n-1},\ s_{n-1}x_{n-1}+x_n+s_n)。\tag{3}$$

注意：此处的 $\boldsymbol{x}\oplus\boldsymbol{s}$ 不同于通常意义下2个 n 维布尔向量之间的逐个比特模2加。

定义2 设 $f(\boldsymbol{x}),\boldsymbol{x}=(x_1,\cdots,x_n)\in GF^n(2)$ 是布尔函数，$\boldsymbol{x}\oplus\boldsymbol{s}$ 的定义如式(3)，称

$$\delta_f(\boldsymbol{s})=2^{-n}\sum_{\boldsymbol{x}\in GF^n(2)}(-1)^{f(\boldsymbol{x}\oplus\boldsymbol{s})+f(\boldsymbol{x})},\boldsymbol{s}\in GF^n(2),\quad \boldsymbol{s}=(s_1,\cdots,s_n)\in GF^n(2)\tag{4}$$

为 $f(x)$ 关于变量组$(x_1,\ x_2),\cdots,(x_{n-1},\ x_n)$ 的类自相关函数，简称为 $f(x)$ 的类自相关函数。

注1 $\delta_f(\boldsymbol{s})=0$ 的充要条件是类差分函数 $f(\boldsymbol{x}\oplus\boldsymbol{s})+f(\boldsymbol{x})$ 平衡。

注2 由于当 $\boldsymbol{s}$ 的下标为奇数的分量都是0，即 $\boldsymbol{s}$ 形如$(0,\ s_2,\cdots,\ 0,\ s_n)$时，

$$\boldsymbol{x}\oplus\boldsymbol{s}=(x_1,\ x_2+s_2,\cdots,x_{n-1},\ x_n+s_n)=\boldsymbol{x}+\boldsymbol{s}。$$

故此时有 $\delta_f(\boldsymbol{s})=r_f(\boldsymbol{s})$，其中 $r_f(\boldsymbol{s})$ 是布尔函数 $f(\boldsymbol{x})$ 自相关函数在 $\boldsymbol{s}=(0,\ s_2,\cdots,0,\ s_n)$ 处的函数值，特别地有 $\delta_f(0)=r_f(0)=0$。

另外 $\delta_f(\boldsymbol{s}),\boldsymbol{s}\in GF^n(2)$ 还有如下特点：

定理1 设 $f(\boldsymbol{x}),\boldsymbol{x}=(x_1,\cdots,x_n)\in GF^n(2)$ 是布尔函数，$\boldsymbol{e}_k\in GF^n(2)$ 是 n 维标准单位向量——只有第 k 分量是1的布尔向量，$1\leqslant k\leqslant n$，则

$$\delta_f(\boldsymbol{e}_i)=\delta_f(\boldsymbol{e}_i+\boldsymbol{e}_{i+1}),i=1,3,\cdots,n。$$

证明 只证 $\delta_f(\boldsymbol{e}_1)=\delta_f(\boldsymbol{e}_1+\boldsymbol{e}_2)$，其他类似可证。由式(4)容易得到

$$\delta_f(\boldsymbol{s})=2P\{f(\boldsymbol{X}\oplus\boldsymbol{s})+f(\boldsymbol{X})=0\}-1,\tag{5}$$

注意对任意的 $\boldsymbol{x}=(x_1,\cdots,x_n)\in GF^n(2)$，可有

$$f(x_1,\cdots,x_n)=x_1x_2h_0(x_3,\cdots,x_n)+x_1h_1\cdot(x_3,\cdots,x_n)+x_2h_2(x_3,\cdots,x_n)+h_3(x_3,\cdots,x_n),$$

其中 $h_i(x_3,\cdots,x_n),0\leqslant i\leqslant 3$ 是关于$(x_3,\cdots,x_n)$的 $n-2$ 元布尔函数，因而有

$$f(\boldsymbol{x}\oplus\boldsymbol{e}_1)+f(\boldsymbol{x})=x_2h_0+h_1+x_1h_2,$$

$$f(\boldsymbol{x}\oplus(\boldsymbol{e}_1+\boldsymbol{e}_2))+f(\boldsymbol{x})=(x_1+x_2+1)h_0+h_1+(x_1+1)h_2,$$

于是

$$\begin{aligned}P\{f(\boldsymbol{X}\oplus\boldsymbol{e}_1)+f(\boldsymbol{X})=0\}=&\\ P\{X_2h_0+h_1+X_1h_2=0,X_1=0,X_2=0\}+&\\ P\{X_2h_0+h_1+X_1h_2=0,X_1=1,X_2=0\}+&\\ P\{X_2h_0+h_1+X_1h_2=0,X_1=0,X_2=1\}+&\\ P\{X_2h_0+h_1+X_1h_2=0,X_1=1,X_2=1\}=&\\ [P\{h_1=0\}+P\{h_0+h_1=0\}+P\{h_1+h_2=0\}+&\end{aligned}$$

$$P\{h_0 + h_1 + h_2 = 0\}]/4,$$

类似可证

$$P\{f(\boldsymbol{X} \oplus (\boldsymbol{e}_1 + \boldsymbol{e}_2)) + f(\boldsymbol{X}) = 0\} =$$
$$P\{(X_1 + X_2 + 1)h_0 + h_1 + (X_1 + 1)h_2 = 0\} =$$
$$[P\{h_1 = 0\} + P\{h_0 + h_1 = 0\} + P\{h_1 + h_2 =$$
$$0\} + P\{h_0 + h_1 + h_2 = 0\}]/4,$$

所以，

$$P\{f(\boldsymbol{X} \oplus \boldsymbol{e}_1) + f(\boldsymbol{X}) = 0\} =$$
$$P\{f(\boldsymbol{X} \oplus (\boldsymbol{e}_1 + \boldsymbol{e}_2)) + f(\boldsymbol{X}) = 0\},$$

再由式 (5) 即知 $\delta_f(\boldsymbol{e}_1) = \delta_f(\boldsymbol{e}_1 + \boldsymbol{e}_2)$。

自相关函数和 Walsh 循环谱之间有关系式 (2)，那么类自相关函数和 Walsh 循环谱之间是否也有类似的关系？事实上只有在形如 $\boldsymbol{w} = (w_1, 0, \cdots, w_{n-1}, 0)$ 的点处类似的关系式才成立。

定理 2　设 $f(\boldsymbol{x}), \boldsymbol{x} \in GF^n(2)$ 是布尔函数，其类自相关函数和 Walsh 谱分别为 $\delta_f(\boldsymbol{s})$ 和 $S_{(f)}(\boldsymbol{w})$，则在形如 $\boldsymbol{w} = (w_1, 0, \cdots, w_{n-1}, 0)$ 的点处下列等式成立：

$$[S_{(f)}(\boldsymbol{w})]^2 = 2^{-n} \sum_{\boldsymbol{s} \in GF^n(2)} \delta_f(\boldsymbol{s})(-1)^{\boldsymbol{w} \cdot \boldsymbol{s}},$$
$$\boldsymbol{w} \in GF^n(2)。$$

证明　首先注意有

$$w_1 s_1 + w_2 s_2 + \cdots + w_n s_n = (w_1 + w_2 x_1) \cdot$$
$$(x_1 + s_1) + w_2(s_1 x_1 + x_2 + s_2) + \cdots +$$
$$(w_{n-1} + w_n x_{n-1})(x_{n-1} + s_{n-1}) + w_n(s_{n-1} x_{n-1} +$$
$$x_n + s_n) + (w_1 + w_2) x_1 + w_2 x_2 + \cdots +$$
$$(w_{n-1} + w_n) x_{n-1} + w_n x_n,$$

所以

$$f(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} +$$
$$s_{n-1}, s_{n-1} x_{n-1} + x_n + s_n) +$$
$$f(x_1, x_2, \cdots, x_{n-1}, x_n) + w_1 s_1 +$$
$$w_2 s_2 + \cdots + w_{n-1} s_{n-1} + w_n s_n =$$
$$f(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} +$$
$$s_{n-1}, s_{n-1} x_{n-1} + x_n + s_n) +$$
$$(w_1 + w_2 x_1)(x_1 + s_1) + w_2(s_1 x_1 + x_2 +$$
$$s_2) + \cdots + (w_{n-1} + w_n x_{n-1})(x_{n-1} +$$
$$s_{n-1}) + w_n(s_{n-1} x_{n-1} + x_n + s_n) +$$
$$f(x_1, x_2, \cdots, x_{n-1}, x_n) + (w_1 + w_2) x_1 +$$
$$w_2 x_2 + \cdots + (w_{n-1} + w_n) x_{n-1} + w_n x_n, \quad (6)$$

因而，对任意的 $\boldsymbol{w} \in GF^n(2)$，根据类自相关函数的定义及式 (6) 可得：

$$2^{-n} \sum_{\boldsymbol{s} \in GF^n(2)} \delta_f(\boldsymbol{s})(-1)^{\boldsymbol{w} \cdot \boldsymbol{s}} =$$
$$2^{-n} \sum_{\boldsymbol{s} \in GF^n(2)} \Big[\sum_{\boldsymbol{x} \in GF^n(2)} (-1)^{f(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} + s_{n-1}, s_{n-1} x_{n-1} + x_4 + s_n) + f(x_1, x_2, \cdots, x_{n-1}, x_n)} \Big] \cdot$$
$$(-1)^{w_1 s_1 + w_2 s_2 + \cdots + w_{n-1} s_{n-1} + w_n s_n} =$$
$$2^{-2n} \sum_{\boldsymbol{x} \in GF^n(2)} (-1)^{f(x_1, x_2, \cdots, x_{n-1}, x_n) + (w_1 + w_2) x_1 + w_2 x_2 + \cdots + (w_{n-1} + w_n) x_{n-1} + w_n x_n} \cdot$$
$$\Big[\sum_{\boldsymbol{s} \in GF^n(2)} (-1)^{f(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} + s_{n-1}, s_{n-1} x_{n-1} + x_n + s_n)} \cdot$$
$$(-1)^{(w_1 + w_2 x_1)(x_1 + s_1) + w_2(s_1 x_1 + x_2 + s_2) + \cdots + (w_{n-1} + w_n x_{n-1})(x_{n-1} + s_{n-1}) + w_n(s_{n-1} x_{n-1} + y_n + s_n)} \Big] =$$
$$2^{-n} \sum_{\boldsymbol{x} \in GF^n(2)} [(-1)^{f(x_1, x_2, \cdots, x_{n-1}, x_n) + (w_1 + w_2) x_1 + w_2 x_2 + \cdots + (w_{n-1} + w_n) x_{n-1} + w_n x_n} \cdot$$
$$S_{(f)}(w_1 + w_2 x_1, w_2, \cdots, w_{n-2}, w_{n-1} + w_n x_{n-1}, w_4)], \quad (7)$$

将定理题设条件 $w_2 = \cdots = w_{2k} = \cdots = w_n = 0$ 代入式 (7)，再用式(1) 即得

$$2^{-n} \sum_{\boldsymbol{s} \in GF^n(2)} \delta_f(\boldsymbol{s})(-1)^{\boldsymbol{w} \cdot \boldsymbol{s}} =$$
$$2^{-n} \sum_{\boldsymbol{x} \in GF^n(2)} [(-1)^{f(x_1, x_2, \cdots, x_n) + w_1 x_1 + w_2 x_2 + \cdots + w_n x_n} \cdot$$
$$S_{(f)}(\boldsymbol{w})] = [S_{(f)}(\boldsymbol{w})]^2。$$

3.2　类差分平衡函数

定义 3　设 $f(\boldsymbol{x}), \boldsymbol{x} \in GF^n(2)$ 是布尔函数，若对任意的 $0 \neq \boldsymbol{s} \in GF^n(2)$，类差分函数 $f(\boldsymbol{x} \oplus \boldsymbol{s}) + f(\boldsymbol{x})$，$\boldsymbol{x} \in GF^n(2)$ 都平衡，等价的就是 $\delta_f(\boldsymbol{s}) = 0$，则称 $f(\boldsymbol{x})$ 是关于变量组 $(x_1, x_2), \cdots, (x_{n-1}, x_n)$ 的类差分平衡函数。

根据类差分平衡函数的定义，可以验证 $x_1 x_2$，

$x_1x_4+x_2x_3$，$x_1x_6+x_2x_4+x_3x_5+x_1x_2x_3x_5$ 分别是二元、四元、六元类差分平衡函数，所以类差分平衡函数的存在性是勿庸置疑的。

由于布尔函数的许多密码学性质都可以通过其Walsh谱予以刻画，下面来考察类差分平衡函数的谱特征。由定理2可以得到类差分平衡函数的Walsh循环谱的取值有如下特点：

定理3 若 $f(\boldsymbol{x}),\boldsymbol{x}\in GF^n(2)$ 是类差分平衡函数，则一定有

$$[S_{(f)}(w_1,0,\cdots,w_{n-1},0)]^2=2^{-n},$$

$$(w_1,w_3,\cdots,w_{n-1})\in GF^{n/2}(2)。$$

证明 因为 $f(\boldsymbol{x})$ 是类差分平衡函数，故对任一 $0\neq \boldsymbol{s}\in GF^n(2)$，都有 $\delta_f(\boldsymbol{s})=0$，且 $\delta_f(0)=1$，由定理2即知，当 $\boldsymbol{w}=(w_1,0,\cdots,w_{n-1},0)$ 时有

$$[S_{(f)}(\boldsymbol{w})]^2=2^{-n}\sum_{\boldsymbol{s}\in GF^n(2)}\delta_f(\boldsymbol{s})(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}}=$$

$$2^{-n}\Big[1+\sum_{0\neq \boldsymbol{s}\in GF^n(2)}\delta_f(\boldsymbol{s})(-1)^{\boldsymbol{w}\cdot\boldsymbol{s}}\Big]=2^{-n}。$$

定理4 若 $f(\boldsymbol{x}),\boldsymbol{x}\in GF^n(2)$ 是类差分平衡函数，则其常义下的自相关函数 $r_f(\boldsymbol{s})$ 满足

$$r_f(0,s_2,\cdots,0,s_n)=0,(s_2,s_4,\cdots,s_{n-2})\in GF^{n/2}(2)。$$

证明 由前述关于类自相关函数定义的注2即得。

众所周知，n 元Bent函数的代数次数至多可达到 $n/2$，即在 n 元Bent函数的多项式表达式中代数次数大于 $n/2$ 的单项式的系数都是0，然而对于类差分平衡函数可以得到下面的结论：

定理5 若 $f(\boldsymbol{x}),\boldsymbol{x}=(x_1,\cdots,x_n)\in GF^n(2)$ 是类差分平衡函数，则当 $n\geqslant 4$ 时，$f(\boldsymbol{x})$ 的ANF中不含有以 $x_2x_4\cdots x_n$ 作为因式的单项式。

证明 设 $i_1,i_2,\cdots,i_k$ 是奇数，且 $1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_k\leqslant n-1$，记

$$\bar{S}_{2,4,\cdots n,i_1,\cdots,i_k}=\{\boldsymbol{x}=(x_1,x_2,\cdots,x_n):$$

$$x_2=x_4=\cdots=x_n=x_{i_1}=\cdots=x_{i_k}=0,$$

$$x_j\in GF(2),j\in\{\{1,2,\cdots,n\}\setminus\{2,4,\cdots,$$

$$n,i_1,i_2,\cdots,i_k\}\},$$

则由文献[1]中“定理7.2.5”及定理3知，$f(\boldsymbol{x})$ 的多项式表示式中单项式 $x_2x_4\cdots x_nx_{i_1}\cdots x_{i_k}$ 的系数

$$a_{24\cdots ni_1\cdots i_k}=\left|\frac{2^{n/2+k}}{2}\Big[1-\sum_{\boldsymbol{w}\in\bar{S}_{24\cdots ni_1i_2\cdots i_r}}S_{(f)}(\boldsymbol{w})\Big]\right|=$$

$$\Big[\frac{2^{n/2+k}}{2}\Big(1-\sum_{\boldsymbol{w}\in\bar{S}_{24\cdots ni_1i_2\cdots i_r}}(\pm 2^{-n/2})\Big)\Big]_{\mathrm{mod}2}=$$

$$\Big[2^{n/2+k-1}-2^{k-1}\sum_{\boldsymbol{w}\in\bar{S}_{24\cdots ni_1i\setminus -2\cdots i_r}}(\pm 1)\Big]_{\mathrm{mod}2},$$

而当 $k=1$ 时，$a_{24\cdots ni_1}=\Big[2^{n/2}-\sum_{\boldsymbol{w}\in\bar{S}_{24\cdots ni_1i_2\cdots i_r}}(\pm 1)\Big]_{\mathrm{mod}2}$，由 $n\geqslant 4$ 得 $2^{n/2}=0_{\mathrm{mod}2}$ 且 $|\bar{S}_{24\cdots ni_1}|=2^{n/2-1}$ 是偶数，故和式 $\sum_{\boldsymbol{w}\in\bar{S}_{24\cdots ni_1}}(\pm 1)$ 中+1和-1的个数有相同的奇偶性，从而 $\sum_{\boldsymbol{w}\in\bar{S}_{24\cdots ni_1}}(\pm 1)=0_{\mathrm{mod}2}$，所以 $a_{24\cdots ni_1\cdots i_k}=0$，故定理结论成立。

例如，四元类差分平衡函数的多项式表达式中不含有 $x_1x_2x_4$，$x_2x_3x_4$，$x_1x_2x_3x_4$ 六元类差分平衡函数的多项式表达式中不含有 $x_1x_2x_4x_6$，$x_2x_3x_4x_6$，$x_2x_4x_5x_6$，$x_1x_2x_3x_4x_6$，$x_1x_2x_4x_5x_6$ $x_2x_3x_4x_5x_6$，$x_1x_2x_3x_4x_5x_6$ 等，所以定理5为确定类差分平衡函数的多项式表达式提供了一定的理论依据。

4 类差分平衡函数与Bent函数的关系

由于布尔函数的类差分和差分的运算法则不同，所以类差分平衡函数和Bent函数这2个概念是有区别的，例如类差分平衡函数 $x_1x_6+x_2x_4+x_3x_5+x_1x_2x_3x_5$ 就不是Bent函数，而四元Bent函数 $x_1x_2+x_3x_4+x_2x_4$ 等也不是类差分平衡函数。但类差分平衡函数与Bent函数也有一些相同的地方，例如在形如 $(w_1,0,\cdots,w_{n-1},0)$ 点的循环谱的二次方都是 2^{-n}，在形如 $(0,s_2,\cdots,0,s_n)$ 的点处的差分都平衡等。因此类差分平衡函数与Bent函数是交集非空的2个不同的函数类。关于二者的联系，有下面的定理：

定理6 代数次数为2的类差分平衡函数都是Bent函数。

证明 由于代数次数为2的布尔函数都是部分Bent函数[8]，因部分Bent函数的循环谱的二次方最多取2个不同的值0和 2^{-n+r}，$1\leqslant r\leqslant n$，再由定理3知道，代数次数为2的类差分平衡函数的循环谱的二次方有一部分是 2^{-n}。再由能量守恒定理[7]知此类函数在所有点处循环谱的二次方都必须是 2^{-n}。所以代数次数为2的类差分平衡函数都是Bent函数。

下面的定理7可以用来判定Bent函数何时是类差分平衡函数。

定理7 若 $f(\boldsymbol{x}),\boldsymbol{x}\in GF^n(2)$ 是Bent函数，

且其循环谱满足：对任意的

$$\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in GF^n(2) \text{ 和}$$

$$(w_1, w_3, \cdots, w_{n-1}) \in GF^{n/2}(2),$$

都成立

$$S_{(f)}(w_1 + w_2x_1, w_2, \cdots, w_{n-1} + w_nx_1, w_n) = (-1)^{w_2x_1+\cdots+w_nx_{n-1}} S_{(f)}(w_1, w_2, \cdots, w_{n-1}, w_n), \tag{8}$$

则 $f(\boldsymbol{x}), \boldsymbol{x} \in GF^n(2)$ 是类差分平衡函数。

证明　这是因为一方面由 $f(\boldsymbol{x})$ 是 Bent 函数知

$$\sum_{w \in GF^4(2)} [S_{(f)}(w_1, w_2, \cdots, w_{n-1}, w_n)]^2 \cdot (-1)^{w_1s_1+w_2s_2+\cdots+w_{n-1}s_{n-1}+w_ns_n} = \begin{cases} 1, s = 0, \\ 0, s \neq 0, \end{cases}$$

另一方面根据式 (7) 和式(8) 又有

$$\sum_{w \in GF^n(2)} [S_{(f)}(w_1, w_2, \cdots, w_{n-1}, w_n)]^2 (-1)^{w_1s_1+w_2s_2+\cdots+w_{n-1}s_{n-1}+w_ns_n} =$$

$$\sum_{w \in GF^n(2)} 2^{-n} \sum_{x \in GF^n(2)} [(-1)^{f(x_1, x_2, \cdots, x_{n-1}, x_n)+w_1x_1+w_2x_2+\cdots+w_{n-1}x_{n-1}+w_nx_n} S_{(f)}(w_1, w_2, \cdots, w_{n-1}, w_n)] \cdot (-1)^{w_1s_1+w_2s_2+\cdots+w_{n-1}s_{n-1}+w_ns_n} =$$

$$\sum_{w \in GF^n(2)} 2^{-n} \sum_{x \in GF^n(2)} [(-1)^{f(x_1, x_2, \cdots, x_{n-1}, x_n)+(w_1+w_2)x_1+w_2x_2+\cdots+(w_{n-3}+w_n)x_{n-1}+w_nx_n} \cdot S_{(f)}(w_1 + w_2x_1, w_2, \cdots, w_{n-1} + w_nx_{n-1}, w_n)](-1)^{w_1s_1+w_2s_2+\cdots+w_{n-1}s_{n-1}+w_ns_n} =$$

$$2^{-n} \sum_{w \in GF^n(2)} \sum_{v \in GF^n(2)} \delta_f(\boldsymbol{v}) \cdot (-1)^{w_1v_1+w_2v_2+\cdots+w_{n-1}v_{n-1}+w_nv_n} (-1)^{w_1s_1+w_2s_2+\cdots+w_{n-1}s_{n-1}+w_ns_n} =$$

$$2^{-n} \sum_{v \in GF^n(2)} \delta_f(\boldsymbol{v}) \sum_{w \in GF^n(2)} (-1)^{w_1(v_1+s_1)+w_2(v_2+s_2)+\cdots+w_{n-1}(v_{n-1}+s_{n-1})+w_n(v_n+s_n)} = \delta_f(\boldsymbol{s}),$$

因而有

$$\delta_f(\boldsymbol{s}) = \begin{cases} 1, s = 0, \\ 0, s \neq 0, \end{cases}$$

即 $f(\boldsymbol{x})$ 是类差分平衡函数。

满足定理 7 中条件的 Bent 函数是存在的，例如 $f(x, y) = xy, x, y \in GF(2)$ 便是一类。

5　类差分平衡函数的构造

定理 8　形如

$$f(\boldsymbol{x}) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + g(x_1, x_3, \cdots, x_{n-1}), (x_1, \cdots, x_n) \in GF^n(2) \tag{9}$$

的布尔函数都是关于变量组 $(x_1, x_2), \cdots, (x_{n-1}, x_n)$ 的类差分平衡函数，其中 $g(x_1, x_3, \cdots, x_{n-1}), (x_1, x_3, \cdots, x_{n-1}) \in GF^{n/2}(2)$ 是关于变元 $(x_1, x_3, \cdots, x_{n-1})$ 的任一布尔函数。

证明　因为形如式 (9) 的布尔函数都是 Bent 函数[2]，且对任意的 $\boldsymbol{s} \in GF^{n/2}(2)$，都有

$$f(\boldsymbol{x} \oplus \boldsymbol{s}) + f(\boldsymbol{x}) = f(\boldsymbol{x} + \boldsymbol{s}) + f(\boldsymbol{x}), \boldsymbol{x} \in GF^n(2)$$

所以对于任意的 $0 \neq \boldsymbol{s} \in GF^n(2)$，都有 $\delta_f(\boldsymbol{s}) = r_f(\boldsymbol{s}) = 0$。

引理 1　设 $f_i(\boldsymbol{x}^{(i)}), \boldsymbol{x}^{(i)}, \in GF^{n_i}(2), 1 \leqslant i \leqslant k$ 都是布尔函数，$\boldsymbol{x}^{(i)} \in GF^{n_i}(2)$，$\boldsymbol{x} = (\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)}, \cdots, \boldsymbol{x}^{(k)})$，$f(\boldsymbol{x}) = f_1(\boldsymbol{x}^{(1)} + f_2(\boldsymbol{x}^{(2)}) + \cdots + f_k(\boldsymbol{x}^{(k)})$，$\boldsymbol{s}^{(i)} \in GF^{n_i}(2)$，$\boldsymbol{s} = (\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \cdots, \boldsymbol{s}^{(k)})$，$\delta_f(\boldsymbol{s})$ 是 $f(\boldsymbol{x})$ 的类自相关函数，则有

$$\delta_f(\boldsymbol{s}) = \prod_{i=1}^{k} \delta_{f_i}(\boldsymbol{s}^{(i)})。$$

证明　为记号简单，仅证 $k = 2$ 时结论成立：记 $\boldsymbol{s} = (\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}) \in GF^{n_1+n_2}(2)$，其中 $\boldsymbol{s}^{(1)} \in GF^{n_1}(2), \boldsymbol{s}^{(2)} \in GF^{n_2}(2)$，则由类自相关函数的定义知

$$\delta_f(\boldsymbol{s}) = 2^{-n} \sum_{x \in GF^n(2)} (-1)^{f(x \oplus s)+f(x)} =$$

$$2^{-(n_1+n_2)} \sum_{x^{(1)} \in GF^{n_1}(2)} \sum_{x^{(2)} \in GF^{n_2}(2)} (-1)^{f_1(x^{(1)} \oplus s^{(1)})+f_2(x^{(2)} \oplus s^{(2)})+f_1(x^{(1)})+f_2(x^{(2)})} =$$

$$2^{-(n_1+n_2)} \sum_{x^{(1)} \in GF^n(2)} (-1)^{f_1(x^{(1)} \oplus s^{(1)})+f_1(x^{(1)})} \sum_{x^{(2)} \in GF^n(2)} (-1)^{f_2(x^{(2)} \oplus s^{(2)})+f_2(x^{(2)})} = \delta_{f_1}(\boldsymbol{s}^{(1)}) \delta_{f_2}(\boldsymbol{s}^{(2)})。$$

由引理1不难得到下面的类差分平衡函数的构造方法：

定理9 设 $f_i(\boldsymbol{x}^{(i)}), \boldsymbol{x}^{(i)} \in \in GF^{n_i}(2), 1 \leqslant i \leqslant k$ 都是布尔函数，则

$$f_1(\boldsymbol{x}^{(1)}) + f_2(\boldsymbol{x}^{(2)}) + \cdots + f_k(\boldsymbol{x}^{(k)}),$$
$$\boldsymbol{x}^{(i)} \in GF^{n_i}(2), 1 \leqslant i \leqslant k$$

是类差分平衡函数的充分必要条件是 $f_i(\boldsymbol{x}^{(i)}), \boldsymbol{x}^{(i)} \in GF^{n_i}(2), 1 \leqslant i \leqslant k$ 都是类差分平衡函数。

证明 充分性显然。

必要性 设 $f_1(\boldsymbol{x}^{(1)}) + f_2(\boldsymbol{x}^{(2)}) + \cdots + f_k(\boldsymbol{x}^{(k)}), \boldsymbol{x}^{(i)} \in GF^{n_i}(2)$ 是类差分平衡函数，由引理1，对任意的 $0 \neq \boldsymbol{s} = (\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \cdots, \boldsymbol{s}^{(k)})$，都有

$$\delta_{f_1+f_2+\cdots+f_k}(\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \cdots, \boldsymbol{s}^{(k)}) =$$
$$\delta_{f_1}(\boldsymbol{s}^{(1)})\delta_{f_2}(\boldsymbol{s}^{(2)})\cdots\delta_{f_k}(\boldsymbol{s}^{(k)}) = 0,$$

特别取 $\boldsymbol{s}^{(1)} \neq 0$，而 $\boldsymbol{s}^{(i)} = 0$，$2 \leqslant i \leqslant k$，即知

$$\delta_{f_1+f_2+\cdots+f_k}(\boldsymbol{s}^{(1)}, 0, \cdots, 0) =$$
$$\delta_{f_1}(\boldsymbol{s}^{(1)})\delta_{f_2}(0)\cdots\delta f_k(0) = 0,$$

因 $\delta_{f_i}(0) = 1, 2 \leqslant i \leqslant k$，故对任意的 $\boldsymbol{s}^{(1)} \neq 0$，$\delta_{f_1}(\boldsymbol{s}^{(1)}) = 0$，可见 $f_1(\boldsymbol{x}^{(1)})$ 是类差分平衡函数，同理可知，$f_i(\boldsymbol{x}^{(i)}), 1 \leqslant i \leqslant k$ 都是类差分平衡函数。

在构造密码函数时，总希望所构造的函数具有较高的代数次数和不要过于简单的代数结构形式，而由定理9所构造的布尔函数的代数次数不会超过2个函数的代数次数的最大值，结构形式也过于简单，为了构造具有较高代数次数，代数形式稍微复杂的密码函数，有必要去寻求其他的构造方法，定理10将给出一种新的构造方法，这里处理问题的思想方法不同于 Rothous 在文献［2］中所给出的 Bent 的经典构造法。

定理10 设 $f_i(\boldsymbol{x}^{(i)}), \boldsymbol{x}^{(i)} \in GF^{n_i}(2), i = 1, 2$ 都是类差分平衡函数，若存在 $h_i(\boldsymbol{x}^{(i)}), i = 1, 2$ 使得 $f_i(\boldsymbol{x}^{(i)}) + h_i(\boldsymbol{x}^{(i)}), i = 1, 2$ 也都是类差分平衡函数，则下述函数是类差分平衡函数：

$$f_1(\boldsymbol{x}^{(1)}) + f_2(\boldsymbol{x}^{(2)}) + h_1(\boldsymbol{x}^{(1)}) + h_2(\boldsymbol{x}^{(2)}),$$
$$\boldsymbol{x}^{(i)} \in GF^{n_i}(2), i = 1, 2。$$

用与文献［6］中定理1.11完全相同的方法可证定理10（证明略）。下面仅举一例说明其应用。

例 设 $f_1(\boldsymbol{x}^{(1)}) = x_1x_2 + x_1x_5 + x_1x_6 + x_2x_3 + x_2x_6 + x_4x_6 + x_2x_3x_4 + x_1x_3x_4x_5$，$f_2(\boldsymbol{x}^{(2)}) = x_7$，$h_1(\boldsymbol{x}^{(1)}) = x_1x_6 + x_2x_4 + x_3x_5 + x_1x_2x_3x_5$，$h_2(\boldsymbol{x}^{(2)}) = x_7x_8$，则上述函数满足定理10的条件，故 $f_1(\boldsymbol{x}^{(1)}) + f_2(\boldsymbol{x}^{(2)}) + h_1(\boldsymbol{x}^{(1)})h_2(\boldsymbol{x}^{(2)})$ 是代数次数为5的类差分平衡函数。

6 类差分平衡函数的应用

下面给出类差分平衡函数在 Z_4 上完全非线性函数构造中的应用。

定义4[5] 称 n 元 m 值逻辑函数 $f(\boldsymbol{y}), \boldsymbol{y} \in Z_m^n$ 为完全非线性函数，如果对任意的 $\boldsymbol{v} \in Z_m^n \setminus \{0\}$，差分函数 $f(\boldsymbol{y}+\boldsymbol{v}) - f(\boldsymbol{y}), \boldsymbol{y} \in Z_m^n$ 在 Z_m 上取值都是均匀的，即

$$|\{y : f(\boldsymbol{y}+\boldsymbol{v}) - f(\boldsymbol{y}) = i,$$
$$\boldsymbol{y} \in Z_m^n\}| = m^{n-1}, i \in Z_m。$$

因在 Z_4 上完全非线性函数的概念中涉及到变元之间以及逻辑函数之间的模4加法、减法运算，故先给出2－基分解意义下各个变量 $y_i \in Z_4$，$1 \leqslant i \leqslant n$ 及函数 f 的2－基分解表示：

当 $y_1 \in Z_4$ 时，y_1 可以分解表示为

$$y_1 = x_1 + 2x_2, (x_1, x_2) \in GF^2(2) =$$
$$\{(0,0), (1,0), (0,1), (1,1)\},$$

其意义是

$$y_1 = 0 \Leftrightarrow (x_1, x_2) = (0,0),$$
$$y_1 = 1 \Leftrightarrow (x_1, x_2) = (1,0),$$
$$y_1 = 2 \Leftrightarrow (x_1, x_2) = (0,1),$$
$$y_1 = 3 \Leftrightarrow (x_1, x_2) = (1,1),$$

称 $y_1 = (x_1, x_2)$ 为 y 的2－基分解。由此不难知道，当 $v_1 \in Z_4$ 的2－基分解为 $v_1 = (s_1, s_2)$ 时，y_1 和 v_1 在 Z_4 中的“和” $y_1 + v_1$ 的2－基分解即为

$$y_1 + v_1 = (x_1s_1, s_1x_1 + x_2 + s_2)。$$

在2－基分解的意义下，Z_4^n 上的四值逻辑函数 $f(y_1, y_2, \cdots, y_n)$ 就可以表示为

$$f(y_1, y_2, \cdots, y_n) = f_1(y_1, y_2, \cdots, y_n) +$$
$$2f_2(y_1, y_2, \cdots, y_n), (y_1, y_2, \cdots, y_n) \in Z_4^n,$$

其中 $f_1(y_1, y_2, \cdots, y_n), f_2(y_1, y_2, \cdots, y_n)$ 都是定义在 Z_4^n 上的逻辑函数，又因为存在 Z_4^n 到 $GF^{2n}(2)$ 的一一映射

$$\boldsymbol{y} = (y_1, y_2, \cdots, y_n) \in Z_4^n \mapsto \boldsymbol{x} =$$
$$(x_1, x_2, x_3, x_4, \cdots, x_{2n-1}, x_{2n})$$

所以可将定义在 Z_4^n 上的逻辑函数 $f_1(\boldsymbol{y})$，$f_2(\boldsymbol{y}), \boldsymbol{y} \in Z_4^n$ 分别转化为 $2n$ 元布尔函数

$$(f_1(x_1, x_2, x_3, x_4, \cdots, x_{2n-1}, x_{2n}),$$

$$f_2(x_1, x_2, x_3, x_4, \cdots, x_{2n-1}, x_{2n})),$$

对于 $a = a_1 + 2a_2$，$b = b_1 + 2b_2 \in Z_4$，易知 a 和 b 在 Z_4 中的“差” $a - b$ 的 2 - 基分解为

$$a - b = a + 3b = (a_1 + b_1)_{\text{mod2}} + 2[(a_1 b_1 + a_2 + b_2)_{\text{mod2}}], \quad (10)$$

由式 (10) 知，在上述意义下，对 $\boldsymbol{v} \in Z_4^n$，Z_4^n 上的 4 值逻辑函数 $f(\boldsymbol{y})$，$\boldsymbol{y} \in Z_4^n$ 的差分函数

$$f(\boldsymbol{y} + \boldsymbol{v}) - f(\boldsymbol{y}),\ \boldsymbol{y} \in Z_4^n。$$

可如下转换

$$f(\boldsymbol{y} + \boldsymbol{v}) - f(\boldsymbol{y}) = [f_1(\boldsymbol{y} + \boldsymbol{v}) + f_1(\boldsymbol{y})]_{\text{mod2}} + 2\{[f_2(\boldsymbol{y} + \boldsymbol{v}) + f_2(\boldsymbol{y}) + f_1(\boldsymbol{y}) + f_1(\boldsymbol{y} + \boldsymbol{v})\, f_1(\boldsymbol{y})]_{\text{mod2}}\}, \quad (11)$$

再将 $\boldsymbol{y} + \boldsymbol{v}$，$\boldsymbol{y}$ 都用 2 - 基分解表示可得到

$$f(\boldsymbol{y} + \boldsymbol{v}) - f(\boldsymbol{y}) = [f_1(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} + s_{n-1}, s_{n-1} x_{n-1} + x_n + s_n) + f_1(x)]_{\text{mod2}} + 2[f_1(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} + s_{n-1}, s_{n-1} x_{n-1} + x_n + s_n) f_1(x) + f_1(x) + f_2(x_1 + s_1, s_1 x_1 + x_2 + s_2, \cdots, x_{n-1} + s_{n-1}, s_{n-1} x_{n-1} + x_n + s_n) + f_2(x)]_{\text{mod2}} = [f_1(\boldsymbol{x} \oplus \boldsymbol{s}) + f_1(\boldsymbol{x})]_{\text{mod2}} + 2\{[f_2(\boldsymbol{x} \oplus \boldsymbol{s}) + f_2(\boldsymbol{x}) + f_1(\boldsymbol{x}) + f_1(\boldsymbol{x} \oplus \boldsymbol{s})\, f_1(\boldsymbol{x})]_{\text{mod2}}\}, \quad (12)$$

其中

$$\boldsymbol{y} = (y_1, y_2, \cdots, y_n) \in Z_4^n \mid\!\rightarrow \boldsymbol{x} = (x_1, x_2, x_3, x_4, \cdots, x_{2n-1}, x_{2n}) \in GF^{2n}(2),$$

$$\boldsymbol{v} = (v_1, v_2, \cdots, v_n) \in Z_4^n \mid\!\rightarrow \boldsymbol{s} = (s_1, s_2, s_3, s_4, \cdots, s_{2n-1}, s_{2n}) \in GF^{2n}(2)。$$

运用式 (11) 和式(12) 及相关知识可以得到如下定理：

定理 11　4 值逻辑函数 $f(\boldsymbol{y}), \boldsymbol{y} \in Z_4^n$ 为完全非线性函数的充要条件是对任意的

$$0 \neq (v_1, \cdots, v_n) = (s_1 + 2s_2, \cdots, s_{2n-1} + 2s_{2n}) \in Z_4^n,$$

差分函数 $f(\boldsymbol{y} + \boldsymbol{v}) - f(\boldsymbol{y})$ 的 2 - 基分解表示式 (11) 中的 2 值布尔函数

$$f_1(\boldsymbol{y} + \boldsymbol{v}) + f_1(\boldsymbol{y}), f_2(\boldsymbol{y} + \boldsymbol{v}) + f_2(\boldsymbol{y}) + f_1(\boldsymbol{y}) + f_1(\boldsymbol{y} + \boldsymbol{v}) f_1(\boldsymbol{y})$$

都平衡，等价的就是式(12) 中的 $2n$ 元布尔函数

$$f_1(\boldsymbol{x} \oplus \boldsymbol{s}) + f_1(\boldsymbol{x}),$$

$$f_2(\boldsymbol{x} \oplus \boldsymbol{s}) + f_2(\boldsymbol{x}) + f_1(\boldsymbol{x}) + f_1(\boldsymbol{x} \oplus \boldsymbol{s}) f_1(\boldsymbol{x})$$

都平衡。

证明　必要性显然。充分性由定理的假设及文献 [6] 中的“引理 6.2” 即得。

注 3　由定理 11 的结论知，若记 n 元四值完全非线性函数 $f(y_1, y_2, \cdots, y_n)$ 的“2 - 基分解”为

$$f(y_1, \cdots, y_n) = f_1(x_1 + 2x_2, \cdots, x_{2n-1} + 2x_{2n}) + 2f_2(x_1 + 2x_2, \cdots, x_{2n-1} + 2x_{2n}) = (f_1(x_1, x_2, \cdots, x_{2n-1}, x_{2n}), f_2(x_1, x_2, \cdots, x_{2n-1}, x_{2n})),$$

则作为关于 $(x_1, x_2, \cdots, x_{2n-1}, x_{2n})$ 的布尔函数

$$f_1(x) = f_1(x_1, x_2, \cdots, x_{2n-1}, x_{2n})$$

一定是关于变量组 $(x_1, x_2), \cdots, (x_{2n-1}, x_{2n})$ 的类差分平衡函数。

根据定理 11 若想构造 Z_4^n 上的完全非线性函数，只须先构造一个 $2n$ 元类差分平衡函数 f_1；再根据 $f_2(\boldsymbol{x} \oplus \boldsymbol{s}) + f_2(\boldsymbol{x}) + f_1(\boldsymbol{x}) + f_1(\boldsymbol{x} \oplus \boldsymbol{s}) \cdot f_1(\boldsymbol{x})$ 平衡的要求寻找 f_2 即可，基于此，在首先分析得到所有 4 元类差分平衡函数的基础上，可编程搜索出 Z_4^2 上所有的完全非线性函数，具体做法是：

假设 $f_1(\boldsymbol{x})$，$f_2(\boldsymbol{x})$ 的常数项为 0。首先通过理论分析找到所有的四元类差分平衡函数，共 192 个，然后对于每个四元类差分平衡函数 $f_1(\boldsymbol{x})$，通过上机搜索找到与上述各四元类差分平衡函数做成二元四值完全非线性函数的四元布尔函数 $f_2(\boldsymbol{x})$，共得到16 384个二元四值完全非线性函数。另外，可以证明完全非线性函数的 2 个分量函数中的任意一个分量加 1 后所得到的新的函数仍然是完全非线性函数，所以二元四值完全非线性函数的总个数为 $16\,384 \times 4 = 65\,536$。这个搜索过程在 Pentium (Ⅳ) 计算机上用不到 2 h 的时间便全部完成，而若直接按照真值表穷尽搜索所有的二元四值完全非线性函数，搜索量是 4^{16}，如果没有快速算法这个计算量在普通计算机上实施起来是比较困难的，可见类差分平衡函数的研究是很有意义的。下面给出用这种方法得到的 2 个二元四值完全非线性函数：

$$g(y_1, y_2) = (x_1 x_2 + x_3 x_4)_{\text{mod2}} + 2(x_4 + x_1 x_4 + x_2 x_3 + x_1 x_3 x_4)_{\text{mod2}};$$

$$h(y_1, y_2) = (x_1 x_2 + x_3 x_4)_{\text{mod2}} + 2(x_2 + x_4 + x_1 x_4 + x_2 x_3 + x_3 x_4)_{\text{mod2}}。$$

7　结语

笔者提出了类差分平衡函数的概念，讨论了类

差分平衡函数的性质及其在剩余类环上的完全非线性函数研究中的应用。因为完全非线性函数的直和仍然是完全非线性函数，所以 Z_4 上关于任意正偶数个变量的完全非线性函数都存在，并且上面得到的二元四值完全非线性函数可以大量构造。

计算表明，当 $m>2$ 时，环 Z_{2^m} 上的完全非线性函数的2-基分解意义下的第一个分量函数的形式和性质与类差分平衡函数相似，故类差分平衡函数的研究对环上的完全非线性函数的研究也有重要的指导意义；另外，用2-基分解的方法研究环上的问题，这一思想还可用于一般剩余类环 Z_{p^m}（p 是大于2的素数）上该类逻辑函数的研究中。

关于类差分平衡函数的研究仍然有许多遗留问题，比如类差分平衡函数是否像 Bent 函数那样非退化？其谱特征和自相关特征为何？笔者曾经计算了大量的六元类差分平衡函数的 Walsh 谱及自相关函数值，发现这些六元类差分平衡函数都是非退化的，其 Walsh 谱至多取下述5个值：0，$\pm 2^{-3}$，$\pm 2^{-2}$，其自相关函数在非零点至多取下述3个值：0，$\pm 2^{-2}$。由此猜测 n 元类差分平衡函数的 Walsh 谱取值可能比较均匀；自相关函数在非零点的绝对值也比较均匀。故类差分平衡函数除去可用于构造 Z_4^n 上的完全非线性函数外，也许其自身在密码设计中还能有直接应用。

参考文献

[1] 丁存生，肖国镇. 流密码学及其应用 [M]. 北京：国防工业出版社，1994

[2] Rothous O S. On bent functions [J]. J Comb Theory, 1976, 20A: 300～305

[3] Olsen J D, Scholtz R A, Welch L R. Bent-function sequences [J]. IEEE Trans Information Theory, 1982, IT-28: 858～864

[4] Zheng Y L, Josef P, Jennifer S. HAVAL-A one way hashing algorithm with variable length output [A]. Advances in Crytology-AUSCRYPT'92 [C], Springer-Verlag, 1993. 83～104

[5] Nyberg K. Constructions of bent functions and difference sets [A]. Advances in Cryptology-EUROCRYPT' [C], Springer-Verlag, 1990. 151～160

[6] 李世取，曾本胜，廉玉忠，等. 密码学中的逻辑函数 [M]. 北京：中软电子出版社，2003

[7] Williams F J M, Slone N J A. The Theory of Error Correcting Codes [M]. North Holland, 1977

[8] Carlet C. Partially-bent functions [A]. Advances in Cryptology-CRYPTO'92 [C], Springer-Verlag, 1993. 280～291

Analogue Difference Balanced Function and Its Applications

Zhang Wenying[1,2], Li Shiqu[1]

(1. *Institute of Information Engineering, Information Engineering University, Zhengzhou* 450002, *China*; 2. *Ji'nan Army Academy, Ji'nan* 250029, *China*)

[**Abstract**] This paper presents the concept of analogous difference of Boolean function, and call the Boolean function an analogue difference balanced function if whose analogous difference is balanced at any nonzero point. The aim of this paper is to study their cryptographic properties and construction methods. Making use of analogue bent functions, the paper proposes an efficient and sufficient condition for a logical function defined on Z_4^n to be perfect nonlinear, and get all perfect nonlinear functions defined on Z_4^2.

[**Key words**] Bent function; perfect nonlinear function; 2-radical expansion; analogue difference; analogue auto-correlation function; analogue difference balanced function