布尔函数非线性度的谱分析 [1]

武传坤

(西安电子科技大学应用数学系 西安 710071)

摘 要 任何一个密码系统都可以用一个非线性函数来描述。本文利用频谱技术研究了布尔函数的非线性度，以及布尔函数的某些运算对非线性度的影响，并指出这些结果在密码学中的应用。

关键词 布尔函数，非线性度，Walsh 谱，密码学

中图号 TN911.23

1 引 言

人们熟知，任何一个密码系统都可以用一个非线性函数来描述 [1]。由于布尔函数是设计流密码系统的主要工具，并且在分组密码和公钥密码的设计中有着越来越重要的应用，因此布尔函数的非线性度是衡量有关密码系统安全程度的重要标志。最近的研究 [2] 表明，线性逼近的方法对流密码系统的攻击已经构成威胁，因此研究布尔函数的非线性度是非常必要的。这一课题早已受到人们的重视 [3]，但研究得还不够深入，而且没能有效地利用有关数学工具。Walsh 变换和 Walsh 谱技术 [4] 是研究布尔函数非线性度的有效方法，我国已经把这种技术应用到非线性置换的构造中 [5]。本文的目的主要是利用 Walsh 谱技术研究布尔函数的非线性度以及布尔函数的某些运算对非线性度的影响。

2 布尔函数的 Walsh 变换和 Walsh 谱

记 GF(2) 为只含 0 与 1 的二元域。为书写方便，常把 GF(2) 上的 n 维向量 $x=(x_1,\cdots,x_n)$ 与一个二进制整数等同起来，即记为

$$x=(x_1,\cdots,x_n)=\sum_{i=1}^{n}x_i2^{n-i}. \tag{1}$$

这样，当和式从 0 变到 2^n-1 时，$x=(x_1,\cdots,x_n)$ 恰好取遍 $\mathrm{GF}^n(2)$ 上的所有向量。

定义 1 称 $\mathrm{GF}^n(2)\to\mathrm{GF}(2)$ 上的映射 f 为 n 个变元的布尔函数，记为 $f=(x_1,\cdots,x_n)$，简记为 $f(x)$。

记 $\omega,x\in\mathrm{GF}^n(2)$，定义实值函数

$$W_\omega(x)=(-1)^{\omega\cdot x} \tag{2}$$

[1] 1994-06-13 收到，1995-01-16 定稿

其中 $\omega \cdot x = \omega_1 x_1 \oplus \cdots \oplus \omega_n x_n$ 是向量 ω 与 x 的内积。容易验证下述性质成立：

(1) 对称性

$$W_\omega(x) = W_x(\omega); \tag{3a}$$

(2) 正交性

$$\sum_{\omega=0}^{2^n-1} W_\omega(x) W_\omega(t) = \begin{cases} 2^n, & \text{当 } x = t \text{ 时;} \\ 0, & \text{当 } x \neq t \text{ 时.} \end{cases} \tag{3b}$$

上述性质表明 (2) 式对所有 ω 和 x 构成正交函数系，称为 Walsh 正交函数系。由 (3b) 式立即可得

推论 1

$$\sum_{x=0}^{2^n-1} W_\omega(x) = \begin{cases} 2^n, & \text{当}\omega = 0\text{时;} \\ 0, & \text{当}\omega \neq 0\text{时.} \end{cases} \tag{3c}$$

定义 2 设 $f(x)$ 为 n 个变元的布尔函数，则 $f(x)$ 的 Walsh 变换定义为

$$S_f(\omega) = \sum_{x=0}^{2^n-1} f(x) W_\omega(x) = \sum_{x=0}^{2^n-1} f(x)(-1)^{\omega \cdot x}. \tag{4}$$

(4) 式对应的 Walsh 反变换表示为

$$f(x) = 2^{-n} \sum_{\omega=0}^{2^n-1} S_f(\omega)(-1)^{\omega \cdot x}. \tag{5}$$

作变换 σ ： $f(x) \xrightarrow{\sigma} F(x) = (-1)^{f(x)}$ ，定义 $f(x)$ 的另一种 Walsh 变换为

$$S_{<f>}(\omega) = \sum_{x=0}^{2^n-1} \sigma(f(x)) W_\omega(x) = \sum_{x=0}^{2^n-1} (-1)^{f(x)+\omega \cdot x}. \tag{6}$$

称 $S_f(\omega)$(或 $S_{<f>}(\omega)$) 的值为布尔函数 $f(x)$ 的 Walsh 谱。注意到变换 σ 可用函数 $\sigma(Z) = 1 - 2Z$ 描述。将此关系代入 (6) 式得

$$S_{<f>}(\omega) = \begin{cases} 2^n - 2S_f(\omega), & \text{当}\omega = 0\text{时;} \\ -2S_f(\omega), & \text{当}\omega \neq 0\text{时.} \end{cases} \tag{7}$$

记 $W(f)$ 为布尔函数 $f(x)$ 的重量，即 $f(x)$ 的真值表中 1 的个数，则 (7) 式又可写为

$$S_{<f>}(\omega) = \begin{cases} 2^n - 2W(f), & \text{当}\omega = 0\text{时;} \\ -2S_f(\omega), & \text{当}\omega \neq 0\text{时.} \end{cases} \tag{8}$$

类似地，我们有

$$S_f(\omega) = \begin{cases} W(f), & \text{当}\omega = 0\text{时;} \\ -\dfrac{1}{2} S_{<f>}(\omega), & \text{当}\omega \neq 0\text{时.} \end{cases} \tag{9}$$

(8) 式与 (9) 式说明布尔函数的两种 Walsh 谱等价。

3 布尔函数非线性度的谱描述

定义 3　记 F_n 为所有 n 个变元的布尔函数构成的集合，L_n 为 F_n 中全体线性函数构成的集合。如果一个函数 $f(x) \in F_n$ 可表示为

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n, \tag{10}$$

其中 $a_i \in \mathrm{GF}(2)$, 符号 $\oplus$ 表示模 2 加，则称 $f(x)$ 为线性函数。（这里是与非线性度的概念相对应，有时 (10) 式所表示的函数亦称为仿射函数。）

定义 4　设 $f(x), g(x) \in F_n$ 。定义 $f(x)$ 与 $g(x)$ 之间的距离为它们真值表中对应分量的值不相同的分量的数目，表示为

$$d(f, g) = W(f \oplus g). \tag{11}$$

定义 5　设 $f(x) \in F_n$ 。定义 $f(x)$ 的非线性度 N_f 为 $f(x)$ 与所有 L_n 中线性函数间的最小距离，即

$$N_f = \min_{l \in L_n} d(f, l) = \min_{l \in L_n} W(f \oplus l). \tag{12}$$

$f(x)$ 的相对非线性度为

$$\overline{N}_f = N_f / 2^n. \tag{13}$$

下面我们将主要用 (6) 式所描述的 walsh 变换进行讨论。根据 (6) 式可得

$$W(f(x) \oplus \omega \cdot x) = (2^n - S_{<f>}(\omega))/2. \tag{14}$$

(14) 式表示的正是函数 $f(x)$ 与 $\omega \cdot x$ 之间的距离。类似地可以得到

$$W(f(x) \oplus \omega \cdot x \oplus 1) = (2^n + S_{<f>}(\omega))/2. \tag{15}$$

注意对任意线性函数 $l \in L_n$，总存在 $\omega \in \mathrm{GF}^n(2)$，使 $l = \omega \cdot x$(当常数项为 0 时) 或 $l = \omega \cdot x \oplus 1$ (当常数项为 1 时)。结合 (14)，(15) 和 (12) 式，可得

$$N_f = (2^n - \max_{\omega} |S_{<f>}(\omega)|)/2. \tag{16}$$

(16) 式就是布尔函数非线性度的频谱表示。根据 Parseval 方程 [6]

$$\sum_{\omega} S^2_{<f>}(\omega) = 2^{2n},$$

得到

$$2^n/2 \le \max_{\omega} |S_{<f>}(\omega)| \le 2^n. \tag{17}$$

代入 (16) 式可得

$$0 \le N_f \le 2^{n-1} - 2^{n/2-1}. \tag{18}$$

定理 1 设 $f(x)\in F_n$，则 $N_f=0$，当且仅当 $f\in L_n$。

定义 6 [7,p.426] 设 $f(x)\in F_n$，若对任意 $\omega\in \mathrm{GF}^n(2)$ 都有

$$S_{<f>}(\omega)=\pm 2^{n/2}. \tag{19}$$

则称 $f(x)$ 为 Bent 函数。

显然，只有当 n 为偶数时，才可能存在 Bent 函数。文献 [7] 给出了 Bent 函数的结构，并指出对任意偶数 $n\geq 2$，都存在 Bent 函数。根据不等式 (18) 式和定义 6 得

定理 2 设 $f(x)\in F_n$，则 $f(x)$ 为 Bent 函数。当且仅当 $f(x)$ 的非线性度达到最大值：$N_f=2^{n-1}-2^{n/2-1}$.

对 Bent 函数 $f(x)\in F_n$，容易证明下式成立：

$$\lim_{n\to\infty}\overline{N}_f=1/2. \tag{20}$$

(20) 式说明当用一个线性函数去近似一个 Bent 函数时，最佳逼近的复合率将随 n 的增大而趋于 $1/2$。

定义 7 设 $f(x)\in F_n$，若 $f(x)$ 真值表中 0 与 1 的个数相等，则称 $f(x)$ 是平衡的。

由 (8) 式和 (19) 式知，Bent 函数不是平衡函数，因此平衡函数达不到最大非线性度。对平衡函数的非线性度，我们有下面的猜想。

猜想 设 $f(x)\in F_n$ 是平衡函数，则有

$$0\leq N_f\leq\begin{cases}2^{n-1}-2^{(n-1)/2}, & \text{当}n\text{为奇数时;}\\ 2^{n-1}-2^{n/2}, & \text{当}n\text{为偶数时.}\end{cases} \tag{21}$$

(21) 式的上界都是可达的。例如当 n 为奇数时，取 $f(x)=b_1(x_1,\cdots,x_{n-1})\oplus x_n$；当 n 为偶数时，取 $g(x)=b_2(x_1,\cdots,x_{n-2})\oplus x_1\oplus x_n$，其中 b_1 和 b_2 分别是 $n-1$ 个变元和 $n-2$ 个变元的 Bent 函数。

4 布尔函数运算的非线性度

对于两个一般的布尔函数，我们很难确定它们的和和积的非线性度与原来函数非线性度的关系。但对特殊情况，我们得到一些结果。

定理 3 设 $f(x)\in F_n$，$l(x)\in F_n$，令 $g(x)=f(x)\oplus l(x)$，则 $N_g=N_f$。

定理 4 设 $f(x)\in F_n$，D 是 GF(2) 上的 $n\times n$ 阶非奇异 (可逆) 矩阵，$b\in \mathrm{GF}^n(2)$，令 $g(x)=f(xD\oplus b)$，则 $N_g=N_f$。

证明

$$S_{<g>}(\omega)=\sum_x(-1)^{g(x)+\omega\cdot x}=\sum_x(-1)^{f(xD+b)+\omega\cdot x}=\sum_y(-1)^{f(y)+\omega\cdot(y\oplus b)D^{-1}}\text{(其中}y=xD\oplus b)$$

$$=(-1)^{\omega\cdot bD^{-1}}\sum_y(-1)^{f(y)+\omega(D^T)^{-1}\cdot y}=(-1)^{\omega\cdot bD^{-1}}S_{<f>}(\omega(D^T)^{-1}).$$

由此得 $\max_\omega |S_{<g>}(\omega)| = \max_\omega |S_{<f>}(\omega)|$，根据 (16) 式即得 $N_g = N_f$.

定理 5　设 $f(x), g(x) \in F_n$，定义 f 和 g 的卷积为 F_{n+1} 中的一个函数 φ: $\varphi = (1 \oplus x_{n+1})f \oplus x_{n+1}g$，则

$$N_\varphi \geq N_f + N_g. \tag{22}$$

证明　记 $x' = (x; x_{n+1})$, $\omega' = (\omega; \omega_{n+1})$，则

$$\begin{aligned} S_{<\varphi>}(\omega') &= \sum_{x'} (-1)^{\varphi(x')+\omega'\cdot x'} \\ &= \sum_{x_{n+1}=0} \sum_{x} (-1)^{f(x)+\omega\cdot x} + \sum_{x_{n+1}=1} \sum_{x} (-1)^{g(x)+\omega\cdot x+\omega_{n+1}} \\ &= S_{<f>}(\omega) + (-1)^{\omega_{n+1}} S_{<g>}(\omega). \end{aligned}$$

由此得 $\max_{\omega'} |S_{<\varphi>}(\omega')| \leq \max_\omega |S_{<f>}(\omega)| + \max_\omega |S_{<g>}(\omega)|$，代入 (16) 式即得所求结论。

证毕

定理 6　设 $f(x_1, \cdots, x_n) = f_1(x_1, \cdots, x_{n_1}) \oplus f_2(x_{n_1+1}, \cdots, x_n)$，简记为 $f(x) = f_1(\underline{x}_1) \oplus f_2(\underline{x}_2)$，记 $n_2 = n - n_1$，则

$$N_f = 2^{N_2} N_{f_1} + 2^{N_1} N_{f_2} - 2N_{f_1} N_{f_2} \geq 2N_{f_1} N_{f_2}. \tag{23}$$

证明

$$\begin{aligned} S_{<f>}(\omega) &= \sum_{x} (-1)^{f(x)+\omega\cdot x} = \sum_{\underline{x}_1} \sum_{\underline{x}_2} (-1)^{f_1(\underline{x}_1)+f_2(\underline{x}_2)+\underline{\omega}_1\cdot\underline{x}_1+\underline{\omega}_2\cdot\underline{x}_2} \\ &= \sum_{\underline{x}_1} (-1)^{f_1+\underline{\omega}_1\cdot\underline{x}_1} \sum_{\underline{x}_2} (-1)^{f_2+\underline{\omega}_2\cdot\underline{x}_2} = S_{<f_1>}(\underline{\omega}_1) \cdot S_{<f_2>}(\underline{\omega}_2). \end{aligned}$$

由此得到，对 $\omega = (\underline{\omega}_1; \underline{\omega}_2)$，当且仅当 $|S_{<f_1>}(\underline{\omega}_1)|$ 和 $|S_{<f_2>}(\underline{\omega}_2)|$ 同时取最大值时，$|S_{<f>}(\omega)|$ 才取得最大值。由 (16) 式得

$$\begin{aligned} N_f &= \frac{1}{2}(2^n - |S_{<f>}(\omega)|) \\ &= \frac{1}{2}(2^n - 2^{n_2}|S_{<f_1>}(\underline{\omega}_1)| + 2^{n_2}|S_{<f_1>}(\underline{\omega}_1)| - |S_{<f_1>}(\underline{\omega}_1)||S_{<f_2>}(\underline{\omega}_2)|) \\ &= 2^{n_2}(2^{n_1} - |S_{<f_1>}(\underline{\omega}_1)|)/2 + |S_{<f_1>}(\underline{\omega}_1)|(2^{n_2} - |S_{<f_2>}(\underline{\omega}_2)|)/2 \\ &= 2^{n_2} N_{f_1} + |S_{<f_1>}(\underline{\omega}_1)| N_{f_2}. \end{aligned}$$

将 $|S_{<f_1>}(\underline{\omega}_1)| = 2^{n_1} - 2N_{f_1}$ 代入上式，得 $N_f = 2^{n_2} N_{f_1} + 2^{n_1} N_{f_2} - 2N_{f_1} N_{f_2}$.　　证毕

推论 2　设 $f(x_1, \cdots, x_n) = f_1(x_1, \cdots, x_{n_1}) \oplus f_2(x_{n_1+1}, \cdots, x_n)$，则当且仅当 f_1 和 f_2 都为 Bent 函数时，f 才为 Bent 函数。

证明　记 $N_2 = n - n_1$，若 f_1 和 f_2 都为 Bent 函数，则 $N_f = 2^{n_2}(2^{n_1} - 2^{n_1/2-1}) + 2^{n_1}(2^{n_2-1} - 2^{n_2/2-1}) - 2^{n_1-1} - 2^{n_1/2-1})(2^{n_2-1} - 2^{n_2/2-1}) = 2^{n-1} - 2^{n/2-1}$。根据定理 2 知，$f$ 为 Bent 函数。

反之，由 $N_f = 2^{n_1}N_{f_2} + (2^{n_2} - 2N_{f_2})N_{f_1}$ 和 $N_{f_2} < 2^{N_2-1}$ 知，当 N_{f_2} 固定而 N_{f_1} 变小时，N_f 亦变小。同样，由 $N_f = 2^{n_2}N_{f_1} + (2^{n_1} - 2N_{f_1})N_{f_2}$ 和 $N_{f_1} < 2^{N_1-1}$ 知，N_{f_2} 变小时，N_f 亦变小。因此只要 f_1 和 f_2 中有一个不是 Bent 函数，则 $N_f < 2^{n-1} - 2^{n/2-1}$，即 f 也不是 Bent 函数。 证毕

定理 7 设 $f(x_1, \cdots, x_n) = f_1(x_1, \cdots, x_{n_1}) \cdot f_2(x_{n_1+1}, \cdots, x_n)$，简记为 $f(x) = f_1(\underline{x}_1)f_2(\underline{x}_2)$，则

$$N_f \geq N_{f_1}N_{f_2}. \tag{24}$$

为证明定理 7，先给出一个引理。

引理 1 设 $f(x) \in F_n$，则

$$N_f \leq W(f) \leq 2^n - N_f. \tag{25}$$

证明 根据定义 5，有 $N_f \leq W(f)$。由 (16) 式得

$$N_f = \frac{1}{2}(2^n - \max_{\omega}|S_{<f>}(\omega)|) \leq \frac{1}{2}(2^n - |S_{<f>}(0)|).$$

(1) 当 $W(f) \geq 2^{n-1}$ 时，$S_{<f>}(0) = 2^n - 2W(f) \leq 0$，故

$$N_f \leq (2^n + 2^n - 2W(f))/2 = 2^n - W(f).$$

(2) 当 $W(f) < 2^{n-1}$ 时，令 $g = 1 + f$，则有 $W(g) = 2^n - W(f) > 2^{n-1}$，故有 $N_g \leq 2^n - W(g)$。但由定理 3 知 $N_g = N_f$，因此 $N_f \leq (2^n - W(g)) < (2^n - W(f))$. 综上即得 (25) 式。 证毕

定理 7 的证明 记 $n_2 = n - n_1$，由 (3c) 式得

$$\begin{aligned}
S_{<f>}(\omega) &= \sum_{x}(-1)^{f_1f_2+\omega\cdot x} \\
&= \sum_{\underline{x}_1}\sum_{\underline{x}_2}(-1)^{f_1f_2+\underline{\omega}_1\cdot\underline{x}_1+\underline{\omega}_2\cdot\underline{x}_2} \\
&= \sum_{f_1=1}(-1)^{\underline{\omega}_1\cdot\underline{x}_1}\sum_{\underline{x}_2}(-1)^{f_2+\underline{\omega}_2\cdot\underline{x}_2} + \sum_{f_1=0}(-1)^{\underline{\omega}_1\cdot\underline{x}_1}\sum_{\underline{x}_2}(-1)^{\underline{\omega}_2\cdot\underline{x}_2} \\
&= \sum_{\underline{x}_1}f_1(\underline{x}_1)(-1)^{\underline{\omega}_1\cdot\underline{x}_1}\sum_{\underline{x}_2}(-1)^{f_2+\underline{\omega}_2\cdot\underline{x}_2} + \sum_{\underline{x}_1}(f(\underline{x}_1)\oplus 1)(-1)^{\underline{\omega}_1\cdot\underline{x}_1}\sum_{\underline{x}_2}(-1)^{\underline{\omega}_2\cdot\underline{x}_2} \\
&= \begin{cases} S_{f_1}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2) + 2^{n_2}S_{f_1\oplus 1}(\omega_1), & \text{当}\underline{\omega}_2 = 0\text{时;} \\ S_{f_1}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2) & \text{当}\underline{\omega}_2 \neq 0\text{时.} \end{cases}
\end{aligned} \tag{26}$$

注意到

$$\begin{aligned}
S_{f_1\oplus 1}(\underline{\omega}_1) &= \sum_{\underline{x}_1}(f(\underline{x}_1)\oplus 1)(-1)^{\underline{\omega}_1\cdot\underline{x}_1} \\
&= \sum_{\underline{x}_1}(-1)^{\underline{\omega}_1\cdot\underline{x}_1} - \sum_{\underline{x}_1}f_1(\underline{x}_1)(-1)^{\underline{\omega}_1\cdot\underline{x}_1} \\
&= \begin{cases} 2^{n_1} - S_{f_1}(\underline{\omega}_1), & \text{当}\underline{\omega}_1 = 0\text{时;} \\ -S_{f_1}(\underline{\omega}_1), & \text{当}\underline{\omega}_1 \neq 0\text{时.} \end{cases}
\end{aligned}$$

而

$$S_{f_1}(\underline{\omega}_1)=\begin{cases}(2^{n_1}-S_{<f_1>}(\underline{\omega}_1))/2, & \text{当}\underline{\omega}_1=0\text{时};\\ -S_{<f_1>}(\underline{\omega}_1)/2, & \text{当}\underline{\omega}_1\neq 0\text{时}.\end{cases}$$

代入 (26) 式并整理得

$$S_{<f>}(\omega)=\begin{cases}2^{n-1}+2^{n_1-1}S_{<f_2>}(\underline{\omega}_2)+2^{n_2-1}S_{<f_1>}(\underline{\omega}_1)\\ \quad -\dfrac{1}{2}S_{<f_1>}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2), & \text{当}\underline{\omega}_1=0,\underline{\omega}_2=0\text{时};\quad (27a)\\ 2^{n_2-1}S_{<f_1>}(\underline{\omega}_1)-\dfrac{1}{2}S_{<f_1>}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2), & \text{当}\underline{\omega}_1\neq 0,\underline{\omega}_2=0\text{时};\quad (27b)\\ 2^{n_1-1}S_{<f_2>}(\underline{\omega}_2)-\dfrac{1}{2}S_{<f_1>}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2), & \text{当}\underline{\omega}_1=0,\underline{\omega}_2\neq 0\text{时};\quad (27c)\\ -\dfrac{1}{2}S_{<f_1>}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2), & \text{当}\underline{\omega}_1\neq 0,\underline{\omega}_2\neq 0\text{时};\quad (27d)\end{cases}$$

假设某个 $\omega=(\underline{\omega}_1;\underline{\omega}_2)$ 使 $|S_{<f>}(\omega)|$ 取得最大值。下面分几种情况讨论 $f(x)$ 的非线性度 N_f 。

(1) 当 $\underline{\omega}_1=0,\underline{\omega}_2=0$ 时， $S_{<f_1>}(\underline{\omega}_1)=2^{n_1}-2W(f_1)$， $S_{<f_2>}(\underline{\omega}_2)=2^{n_2}-2W(f_2)$，代入 (27a) 式得 $S_{<f>}(\omega)=2^n-2W(f_1)W(f_2)$.

(a) 当 $W(f_1)W(f_2)\le 2^{n_1}$ 时， $N_f=(2^n-|S_{<f>}(\omega)|)/2=W(f_1)W(f_2)$，根据引理 1，有 $N_f\ge N_{f_1}N_{f_2}$.

(b) 当 $W(f_1)W(f_2)>2^{n-1}$ 时，由引理 1，得

$$N_f=(2^n-|S_{<f>}(\omega)|)/2=2^n-W(f_1)W(f_2)\ge 2^n-(2^{n_1}-N_{f_1})(2^{n_2}-N_{f_2})=2^{n_2}N_{f_1}+2^{n_1}N_{f_2}-N_{f_1}N_{f_2}.$$

因 $N_{f_1}<2^{n_1-1}$, $N_{f_2}<2^{n_2-1}$，故得 $N_f\ge 3N_{f_1}N_{f_2}$ 。

(2) 当 $\underline{\omega}_1\neq 0$, $\underline{\omega}_2=0$ 时，

$$S_{<f>}(\omega)=S_{<f_1>}(\underline{\omega}_1)(2^{n_2}-S_{<f>}(\underline{\omega}_2))/2=S_{<f_1>}(\underline{\omega}_1)W(f_2),$$

$$\begin{aligned}N_f&=(2^n-|S_{<f>}(\omega)|)/2=(2^n-W(f_2)|S_{<f_1>}(\underline{\omega}_1)|)/2\\&=2^{n-1}-2^{n_1-1}W(f_2)+W(f_2)(2^{n_1}-|S_{<f_1>}(\underline{\omega}_1)|)/2\ge 2^{n-1}-2^{n_1-1}W(f_2)+W(f_2)N_{f_1}\\&=2^{n-1}-(2^{n_1-1}-N_{f_1})W(f_2)\qquad(\because N_{f_1}<2^{n_1-1},W(f_2)\ge 2^{n_2}-N_{f_2})\\&\ge 2^{n-1}(2^{n_1-1}-N_{f_1})(2^{n_2-1}-N_{f_2})=2^{n_1-1}N_{f_2}+(2^{n_2}-N_{f_2})N_{f_1}\ge 2N_{f_1}N_{f_1}.\end{aligned}$$

(3) 当 $\underline{\omega}_1=0$, $\underline{\omega}_2\neq 0$ 时，类似于情形 (2) 可证得 $N_f\ge 2N_{f_1}N_{f_2}$.

(4) 当 $\underline{\omega}_1\neq 0$, $\underline{\omega}_2\neq 0$ 时， $S_{<f>}(\omega)=-S_{<f_1>}(\underline{\omega}_1)S_{<f_2>}(\underline{\omega}_2)/2$，则当且仅当 $|S_{<f_1>}(\underline{\omega}_1)|$ 和 $|S_{<f_2>}(\underline{\omega}_2)|$ 都取得最大值时， $|S_{<f>}(\omega)|$ 才取得最大值。类似于定理 6 的证明，得

$$\begin{aligned}N_f&=(2^n-|S_{<f>}(\omega)|)/2=(2^n-\frac{1}{2}|S_{<f_1>}(\underline{\omega}_1)||S_{<f_2>}(\underline{\omega}_2)|)/2\\&=2^{n-2}+2^{n_2-2}(2^{n_1}-|S_{<f_1>}(\underline{\omega}_1)|)+|S_{<f_1>}(\underline{\omega}_1)|(2^{n_2}-|S_{<f_2>}(\underline{\omega}_2)|)/4\\&\ge 2^{n-2}+2^{n_2-2}N_{f_1}+|S_{<f_1>}(\underline{\omega}_1)|N_{f_2}/4.\end{aligned}$$

由 $N_{f_1}=(2^{n_1}-|S_{<f_1>}(\underline{\omega}_1)|)/2$ 得，$|S_{<f_1>}(\underline{\omega}_1)| \quad 2^{n_1}-2N_{f_1}$，代入上式得 $N_f \geq 2^{n-2}+2^{n_2-2}N_{f_1}+2^{n_1-2}N_{f_2}-N_{f_1}N_{f_2}/2$。注意 $N_{f_1}<2^{n_1-1}$，$N_{f_2}<2^{n_2-1}$，因此 $N_f \geq 3N_{f_1}N_{f_2}/2$。综上所证即知 (24) 式成立。 证毕

定理 8 设 $f(x)\in F_n$，定义 $f_0(x_1,\cdots,x_{n-1})=f(x_1,\cdots,x_{n-1},0)$，$f_1(x_1,\cdots,x_{n-1})=f(x_1,\cdots,x_{n-1},1)$，则有

$$N_f \geq N_{f_0}+N_{f_1}. \tag{28}$$

证明 记 $\underline{x}_1=(x_1,\cdots,x_{n-1})$，$(\underline{\omega}_1)=(\omega_1,\cdots,\omega_{n-1})$，则

$$\begin{aligned}
S_{<f>}(\omega) &= \sum_{x}(-1)^{f(x)+\omega\cdot x} \\
&= \sum_{x_n=0}\sum_{\underline{x}_1}(-1)^{f_0+\underline{\omega}_1\cdot\underline{x}_1}+\sum_{x_n=1}\sum_{\underline{x}_1}(-1)^{f_1+\underline{\omega}_1\cdot\underline{x}_1+\omega_n} \\
&= \begin{cases} S_{<f_0>}(\underline{\omega}_1)+S_{<f_1>}(\underline{\omega}_1), & \text{当}\omega_n=0\text{时;} \\ S_{<f_0>}(\underline{\omega}_1)-S_{<f_1>}(\underline{\omega}_1), & \text{当}\omega_n=1\text{时.} \end{cases}
\end{aligned}$$

由此得 $\max_{\omega}|S_{<f>}(\omega)|\leq\max_{\underline{\omega}_1}|S_{<f_0>}(\underline{\omega}_1)|+\max_{\underline{\omega}_1}|S_{<f_1>}(\underline{\omega}_1)|$，因此

$$\begin{aligned}
N_f &= (2^n-\max_{\omega}|S_{<f>}(\omega)|)/2 \\
&\geq (2^{n-1}-\max_{\underline{\omega}_1}|S_{<f_0>}(\underline{\omega}_1)|)/2+(2^{n-1}-\max_{\underline{\omega}_1}|S_{<f_1>}(\underline{\omega}_1)|)/2 \\
&= N_{f_0}+N_{f_1}. \qquad \text{证毕}
\end{aligned}$$

5 结 论

布尔函数的非线性度通过频谱技术可以较为直观地描述出来。本文通过频谱技术研究了一般布尔函数的非线性度和布尔函数的某些运算对非线性度的影响。这些结果对于密码设计将有一定参考价值。对某些特殊函数的非线性度，如相关免疫函数的非线性度，项数受限和重量受限的布尔函数的非线性度，布尔函数非线性度分布等问题都可利用频谱技术进行讨论，这类问题我们将在以后作进一步研究。

参 考 文 献

[1] Diffie W, Hellman M E. Proc. IEEE, 1979, 67(3): 397–427.

[2] Ding C, *et al.* The Stability Theory of Stream Ciphers. Berlin: Springer-Verag, 1991, Chapter 3.

[3] Pieprzyk J, Finkelstein G. IEE Proc.-E, 1988, 135(6): 325–335.

[4] Karpovsky M G. Finite Orthogonal Series in the Design of Digital Devices. New York: John Wiely & Sons, 1976, Chapter 1.

[5] 武传坤，王新梅. 科学通报，1992, 37(12): 1147–1150.

[6] Titsworth R C. Correlation Properties of Cyclic Sequences: [thesis]. Pasadena, California: California Insitute of Technology, 1963, 160–170.

[7] MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes. North-Holland: 1977, Vol. II, 426–432.

SPECTRAL ANALYSIS ON THE NONLINEARITY OF BOOLEAN FUNCTIONS

Wu Chuankun

(*Xidian University, Xi'an* 710071)

Abstract It is well known that any cryptographic system can be described by a nonlinear function. This paper studies the nonlinearity of Boolean functions and the effect of certain operations on the nonlinearity of Boolean functions by using the spectral techniques. Finally, the applicability of the results to the cryptography is indicated.

Key words Boolean function, Nonlinearity, Walsh spectrum, Cryptography

武传坤：男，1964 年生，副教授，从事应用数学和密码学的教学和研究工作。感兴趣的领域有密码体制设计和分析、认证理论和实现、离散数学等.