满足扩散准则的元素之集的性质

戚文峰,何德峰
(郑州信息工程大学信息工程学院应用数学系,河南郑州 450002)

摘 要: 设 $f(x)$ 是 V_n 上的布尔函数,本文研究了 $f(x)$ 的满足扩散准则的元素集合 R_f^c 的性质. 证明了,若 $\deg f(x) = n$,则 R_f^c 为空集. 对于所有的二次布尔函数而言,均有 R_f^c 中的元素个数大于等于 2^{n-1}. 还对一类函数的雪崩性质进行了讨论. 给出布尔函数不含有非零线性结构的充分必要条件是 ζ_f 中含有 n 个线性无关的元素,其中 $\zeta_f = \{(\alpha_i | \langle \zeta, l_i \rangle \neq 0, 0 \leq i \leq 2^n - 1\}$, l_i 为线性函数 $\phi_{\alpha_i} = \langle x, \alpha_i \rangle$ 的序列. 还给出了一种 2 阶扩散准则布尔函数的构造.

关键词: TN918.1 布尔函数; 扩散准则; 线性结构; 线性子空间
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2004) 02-0290-04

On the Avalanche Characteristics of the Boolean Function

QI Wen-feng, HE De-feng
(*Department of Applied Mathematics, Information Engineering University Zhengzhou, Henan* 450002, *China*)

Abstract: Let V be the space of dimension n over GF(2), $f(x)$ a boolean function on V. In this paper, the set U of the vectors satisfying the propagation criteria is discussed. If $\deg f(x) = n$, then U is an empty set. For all the functions of degree 2, U have at least half vectors of V. The avalanche characteristics of a class of functions is discussed. Boolean functions have no nonezero linear structure if and only if there are n linear independence vectors. Furthermore a construction of functions which satisfy propagation criteria of degree 2 is given.

Key words: boolean function; propagation criteria; linear structure; linear subspace

1 引言

设 V_n 表示 F_2 上 n 维向量空间,$f(x)$ 是 V_n 上的布尔函数,R_f^c 表示满足扩散准则的元素集合,R_f 表示不满足扩散准则的元素集合. 集合 R_f^c 和 R_f 的大小和元素分布情况对于函数的性质有很大的影响,R_f^c 中的元素越多则函数的雪崩性质越好,而且我们总是希望函数不含有非零线性结构. 本文研究了集合 R_f^c 的性质,并给出函数不含有非零线性结构的充分必要条件. 对于 V_n 上的布尔函数 $f(x) = f(x_1, x_2, \cdots, x_n)$, $\alpha \in V_n$,记

$$\zeta_f(\alpha) = ((-1)^{f(\alpha_0 + \alpha)}, (-1)^{f(\alpha_1 + \alpha)}, \cdots, (-1)^{f(\alpha_{2^n-1} + \alpha)})$$

其中 $\alpha_0 = (0,0,\cdots,0)$, $\alpha_1 = (0,0,\cdots,0,1)$, $\cdots$, $\alpha_{2^n-1} = (1,1,\cdots,1)$, $\zeta_f(\alpha_0)$ 简记为 ζ_f. 布尔函数的真值表中所含有的"1"元素的个数称为布尔函数的 hamming-重量,简记为 $wt(f)$. 设 $f(x)$ 是 V_n 上布尔函数,对 $\alpha \in V_n$,称 $\zeta_f(0)$ 与 $\zeta_f(\alpha)$ 的内积

$$\Delta_f(\alpha) = \langle \zeta_f(0), \zeta_f(\alpha) \rangle = \sum_{i=0}^{2^n-1} (-1)^{f(\alpha_i) \oplus f(\alpha_i \oplus \alpha)}$$

为 $f(x)$ 的自相关系数. 若 $|\Delta_f(\alpha)| = 2^n$,则称 α 为函数 $f(x)$ 的线性结构. 在不混淆的前提下,$\zeta_f(\alpha)$, $\Delta_f(\alpha)$ 简记为 $\zeta(\alpha)$, $\Delta(\alpha)$. 设 L 为布尔函数 $f(x)$ 的全部线性结构组成的集合,记

$$L_0 = \{\alpha | f(x) \oplus f(x \oplus \alpha) = 0, \alpha \in V_n\},$$

$$L_1 = \{\alpha | f(x) \oplus f(x \oplus \alpha) = 1, \alpha \in V_n\}$$

易知 $L = L_0 \cup L_1$,且 L 构成线性子空间,L_0 是 L 的子空间,L_1 是 L_0 的陪集.

定义 设 $f(x)$ 是 V_n 上的布尔函数

(1) 若对于 $\alpha \in V_n$, $f(x) \oplus f(x \oplus \alpha)$ 是平衡的,则称 $f(x)$ 在 α 处满足扩散准则;

(2) 若对于任意 $\alpha \in V_n$ 且 $1 \leq wt(\alpha) \leq k$, $f(x) \oplus f(x \oplus \alpha)$ 都是平衡的,则称 $f(x)$ 为 k 阶扩散准则函数. 特别,1-阶扩散准则函数称为严格雪崩准则函数,简称 SAC.

定义 称 $F(w) = 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle w, x \rangle}$ 为布尔函数 $f(x)$ 的 wash-谱,其中 $w = (w_1, w_2, \cdots, w_n)$, $x = (x_1, x_2, \cdots, x_n)$, $\langle w, x \rangle$ 表示 w 与 x 内积. 若对任意 $w \in V_n$ 且 $1 \leq wt(w) \leq m$,有 $F(w) = 0$,则称 $f(x)$ 为 m-阶相关免疫函数,若对任意 $w \in V_n$ 且 $0 \leq wt(w) \leq m$,有 $F(w) = 0$,则称 $f(x)$ 为 m-resilient 函数.

设 $f(x)$ 是 V_n 上的布尔函数,定义 $R_f = \{\alpha_i | \Delta(\alpha_i) \neq 0, 0 \leq i \leq 2^n - 1\}$, $R_f^c = V_n - R_f$, $\zeta_f = \{\alpha_i | \langle \xi, l_i \rangle \neq 0, 0 \leq i \leq 2^n - 1\}$, 其中 l_i 为线性函数 $\phi_{\alpha_i} = \langle x, \alpha_i \rangle$ 的序列.

收稿日期:2002-05-22;修回日期:2002-10-06
基金项目:全国优秀博士学位论文专项基金(No. 200060);国家自然科学基金项目(No. 60373092)

2　R_f^c 的性质

设 $f(x)$ 是 V_n 上的布尔函数,集合 R_f^c 和 R_f 的大小和元素分布情况对于函数的性质有很大的影响, R_f^c 中的元素越多则函数的雪崩性质越好. 对这个集合的进一步认识将更好的推动对布尔函数构造和密码分析的研究,但是从整体上考虑这个集合是个比较困难的问题,本文从以下几个方面对这个集合进行了初步的研究.

引理 1[1]　设 $f(x)$ 是 V_n 上的布尔函数,则非退化条件下布尔函数的次数,Hamming 重量,非线性复杂度和满足扩散准则的元素个数不变.

引理 2　设 $f(x)$ 是 V_n 上的布尔函数,则 $wt(f)$ 为奇数当且仅当 $\deg f(x) = n$.

证明　设 $\phi = \{\alpha \mid f(\alpha) = 1$ 且 $g(\alpha) = 1\}$,则 $wt(f \oplus g) = wt(f) + wt(g) - 2|\phi|$,所以 $wt(f \oplus g)$ 为奇数当且仅当 $wt(f)$ 和 $wt(g)$ 中只有一个为奇数. 对于布尔函数 $f(x)$,可以表示为多项式的形式,而对于所有的单项式而言只有 $wt(x_1 x_2 \cdots x_n)$ 为奇数,所以 $wt(f)$ 为奇数当且仅当 $\deg f(x) = n$.

引理 3　设 $f(x)$ 是 V_n 上的布尔函数,若 $\deg f(x) = n$,则 R_f^c 中不含有重量为 1 的元素.

证明　令 $g_\alpha(x) = f(x) \oplus f(x \oplus \alpha)$,则 $\deg g_\alpha(x) \leq \deg f(x) - 1$. 因为 $f(x)$ 是 V_n 上的布尔函数,且 $\deg f(x) = n$,所以 $x_1 x_2 \cdots x_n$ 是 $f(x)$ 的一个单项式. 对于 $\alpha \in V_n$ 且 $wt(\alpha) = 1$,有 $g_\alpha(x)$ 是一个 $n-1$ 元布尔函数,且 $\deg g_\alpha(x) = n - 1$,由引理 2 可知 $wt(g_\alpha)$ 为奇数,非平衡,即 $\alpha \notin R_f^c$.

定理 1　设 $f(x)$ 是 V_n 上的布尔函数,若 $\deg f(x) = n$,则 R_f^c 为空集.

证明　若 R_f^c 非空,即存在一个元素 $\alpha \in R_f^c$. 设 $\beta \in V_n$ 且 $wt(\beta) = 1$,由线性代数可知存在一个非退化矩阵 A,满足 $\beta A = \alpha$. 令 $g(x) = f(xA)$,则 $\beta \in R_g^c$,由引理 1 可知 $g(x)$ 也是一个 n 次布尔函数,据引理 3 可知矛盾. 所以若 $\deg f(x) = n$,则 R_f^c 为空集.

引理 4[2]　设 $f(x)$ 是 V_n 上的布尔函数, A 是一个 n 阶 $(0,1)$ 非退化矩阵,若对于 A 的每一行 γ_i, $i = 1,2,\cdots,n$, $f(x) \oplus f(x \oplus \gamma_i)$ 都是平衡的,则 $\phi(x) = f(xA)$ 满足 SAC.

定理 2　对于函数 $f(x)$ 而言,若 $|R_f^c| \geq 2^{n-1}$,则函数在非退化条件下满足 SAC.

证明　因为 $|R_f^c| \geq 2^{n-1}$,所以集合 $\{0\} \cup R_f^c$ 中至少含有 $2^{n-1}+1$ 个元素,从而 $\{0\} \cup R_f^c$ 中必含有 n 个线性无关的元素,设为 $\gamma_0, \gamma_1, \cdots, \gamma_{n-1}$. 令 A 是以 $\gamma_0, \gamma_1, \cdots, \gamma_{n-1}$ 为行向量构成的矩阵,则由引理 4 可知, $\Phi(x) = f(xA)$ 满足 SAC.

引理 5[3]　设 ζ 是函数 $f(x)$ 的序列, H_n 为 Sylvester-Hadamard 矩阵, l_i 表示 H_n 的第 i 行, $0 \leq i \leq 2^n - 1$,则

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1}))\, H_n = (\langle \zeta, l_0 \rangle^2, \langle \zeta, l_1 \rangle^2), \cdots, \langle \zeta, l_{2^n-1} \rangle^2)$$

定理 3　对于所有的二次布尔函数,有 $|R_f^c| \geq 2^{2^n-1}$

证明　设 $f(x)$ 是任意二次布尔函数,对于任意的 $\alpha \in V_n$,令 $g_\alpha(x) = f(x) \oplus f(x \oplus \alpha)$,则 $\deg g_\alpha(x) \leq 1$,所以若 $g_\alpha(x)$ 不平衡,则必定为常数,即 α 为 $f(x)$ 的线性结构. 又因为全部的线性结构构成线性子空间,设维数为 k,若 $k < n$,则 $|R_f^c| \geq 2^{n-1}$. 若 $k = n$,分两种情况进行讨论:

(1) 若 L_1 为空集,即对任意的 $\alpha \in V_n$,有 $\Delta(\alpha) = 2^n$,由引理 5 可得

$$\langle \zeta, l_j \rangle^2 = \begin{cases} 2^{2n}, & j = 0 \\ 0, & j \neq 0 \end{cases}$$

l_i 是线性函数的序列,所以 $f(x)$ 是一常数函数,与题设矛盾.

(2) 若 L_1 为非空集合,不妨设 $\Delta(\alpha_i) = 2^n$, $\Delta(\alpha_j) = -2^n$,由引理 5 可得

$$\langle \zeta, l_{2^{n-1}} \rangle^2 = \begin{cases} 2^{2n}, & j = 2^{n-1} \\ 0, & j \neq 2^{n-1} \end{cases}$$

所以 $f(x)$ 为一个线性函数,与题设矛盾.

故 $k \neq n$,即对于所有的二次布尔函数,有 $|R_f^c| = 2^{n-1}$.

推论 1　在非退化条件下,所有的二次布尔函数都满足 SAC.

推论 2　对于所有的 3 元布尔函数,若 R_f^c 非空,则 $|R_f^c| \geq 4$.

证明　设 $f(x)$ 是任意 3 元布尔函数,则 $\deg f(x) \leq 3$. 对于 $\deg f(x) \leq 2$ 的函数,由定理 3 可知,结论成立. 若 $\deg f(x) = 3$,由定理 1 可知, R_f^c 为空集,结论成立.

定理 4　若 4 次布尔函数 $f(x)$ 满足下列条件

(1) $f(x)$ 中任何一个 2 次项是某个 4 次项的因子,并且任何 3 次项也是某个 4 次项的因子.

(2) 单项式 $x_i x_j x_k$ 出现在所有的 4 次项当中.

(3) 设在 4 次项中出现的除 x_i, x_j, x_k 之外的变量为 $y_0, \cdots, y_k$. 若存在一个 s,使 $x_i x_j y_s$ 或 $x_i y_s$ 出现,那么对于所有的 $m, 0 \leq m \leq k$, $x_i x_j y_m$ 或 $x_i y_m$ 均出现. 那么元素 $\alpha = (0, \cdots, 1, 0, \cdots, 1, 0, \cdots, 1, 0, \cdots, 0)$ 不属于 R_f^c,其中 $x_i = x_j = x_k = 1$, $x_t = 0$, $t \neq i, j, k$.

证明　设 $g_\alpha(x) = f(x) \oplus f(x \oplus \alpha)$.

若 $x_i x_j x_k$ 出现可记为

$$g_\alpha(x) = g(x_i, x_j, x_k)(y_0 \oplus \cdots \oplus y_k) \oplus h(x_i, x_j, x_k)$$

若 $x_i x_j x_k$ 不出现则可记为

$$g_\alpha(x) = g(x_i, x_j, x_k)(y_0 \oplus \cdots \oplus y_k \oplus 1) \oplus h(x_i, x_j, x_k)$$

其中 $g(x_i, x_j, x_k) = (x_i x_j \oplus x_j x_k \oplus x_i x_k) \oplus g_0(x_i, x_j, x_k)$, $g_0(x_i, x_j, x_k)$, $h(x_i, x_j, x_k)$ 为常数或是一次函数,仅考虑第一种情况,第二种情况类似可以考虑.

考虑 2 次项,若 $x_i x_j, x_j x_k, x_i x_k$ 全不出现或是全都出现,则 $h(x_i, x_j, x_k)$ 为常数,否则为只有两个变元的 1 次退化函数.

考虑 3 次项,若 $x_i x_j y_s, x_j x_k y_s, x_i x_k y_s$ 全不出现或全都出现,则 $g_0(x_i, x_j, x_k) = x_i \oplus x_j \oplus x_k \oplus 1$ 或 $x_i \oplus x_j \oplus x_k$. 否则 $g_0(x_i, x_j, x_k)$ 为只有一个变元的退化函数.

下面考察 $g_\alpha(x)$ 的平衡性,若 $y_0 \oplus \cdots \oplus y_k = 0$,则 $g_\alpha(x) = h(x_i, x_j, x_k)$,若 $y_0 \oplus \cdots \oplus y_k \oplus 1$,则 $g_\alpha(x) = (x_i x_j \oplus x_j x_k \oplus x_i x_k) \oplus g_0(x_i, x_j, x_k) \oplus h(x_i, x_j, x_k)$.

如果 $h(x_i, x_j, x_k)$ 为常数,不妨设为 1,则无论 $g_0(x_i, x_j, x_k)$ 为何种情况, $wt(g_\alpha) > 2^{n-1}$, $g_\alpha(x)$ 为非平衡的.

如果 $h(x_i, x_j, x_k)$ 为含有 2 个变元的退化函数,则 $y_0 \oplus \cdots \oplus y_k = 0$ 时,平衡;$y_0 \oplus \cdots \oplus y_k = 1$ 时,无论 $g_0(x_i, x_j, x_k)$ 为何种情况,$g_0(x_i, x_j, x_k) \oplus h(x_i, x_j, x_k)$ 不可能为常数或只含有 2 个变元的退化函数. 而对于 $g_\alpha(x)$,只有 $g_0(x_i, x_j, x_k) \oplus h(x_i, x_j, x_k)$ 为常数或只含有 2 个变元时才是平衡的,所以 $g_\alpha(x)$ 非平衡.

综上可得,α 不属于 R_f^c.

3 f(x) 含有非零线性结构的判别条件

引理 6[1] 设 ζ 是函数 $f(x)$ 的序列,l_i 是线性函数 $\varphi_i = \langle \alpha_i, x \rangle$ 的序列,$0 \le i \le 2^n - 1$,则 $\sum_{i=0}^{2^n-1} \langle \zeta, l_i \rangle^2 = 2^{2n}$.

定理 5 设 $f(x)$ 是 V_n 上的布尔函数,则 $f(x)$ 含有非零线性结构的充分必要条件是存在 $\alpha_i \neq 0$,使 ζ_f 包含于 $\{0, \alpha_i\}^\perp$.

证明 "充分性",由

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1}))\, H_n = (\langle \zeta, l_0 \rangle^2, \langle \zeta, l_1 \rangle^2, \cdots, \langle \zeta, l_{2^n-1} \rangle^2)$$

可得

$$2^n (\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})) = (\langle \zeta, l_0 \rangle^2, \langle \zeta, l_1 \rangle^2, \cdots, \langle \zeta, l_{2^n-1} \rangle^2)\, H_n$$

因为 ζ_f 包含于 $\{0, \alpha_i\}^\perp$,所以对于 H_n 的第 a_i 列,用 T 表示,则

$$(\langle \zeta, l_0 \rangle^2, \langle \zeta, l_1 \rangle^2, \cdots, \langle \zeta, l_{2^n-1} \rangle^2)\, T = 2^{2n}$$

即 $\Delta(\alpha_i) = 2^n$,α_i 为函数 $f(x)$ 的一个线性结构.

"必要性",$f(x)$ 含有非零线性结构,则存在 $\alpha_i \neq 0$,有 $\Delta(\alpha_i) = 2^n$,设 H_n 的第 α_i 列为 T, 由

$$2^n (\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})) = (\langle \zeta, l_0 \rangle^2, \langle \zeta, l_1 \rangle^2, \cdots, \langle \zeta, l_{2^n-1} \rangle^2)\, H_n$$

可得

$$(\langle \zeta, l_0 \rangle^2, \langle \zeta, l_1 \rangle^2, \cdots, \langle \zeta, l_{2^n-1} \rangle^2)\, T = 2^{2n}$$

又因为 $\sum_{i=0}^{2^n-1} \langle \zeta, l_i \rangle^2 = 2^{2n}$,所以 ζ_f 包含于 $\{0, \alpha_i\}^\perp$.

推论 3 对于函数 $f(x)$,若 $|\zeta_f| \ge 2^{n-1}$,则 $f(x)$ 不含有非零线性结构.

定理 6 若 ζ_f 构成 k 维线性子空间,则函数 $f(x)$ 含有 2^{n-k} 个线性结构.

证明 由引理 6 和 Hadmard-矩阵的性质简单可得.

定理 7 函数 $f(x)$ 不含有非零线性结构的充分必要条件是 ζ_f 中含有 n 个线性无关的元素.

证明 "充分性",ζ_f 中含有 n 个线性无关的元素,不妨设为 $\alpha_{2^0}, \cdots, \alpha_{2^{n-1}}$. 假设函数含有非零线性结构 α_i,由定理 5 可知,ζ_f 包含在 $\{0, \alpha_i\}^\perp$ 中,所以 $\alpha_{2^0}, \cdots, \alpha_{2^{n-1}}$ 均属于 $\{0, \alpha_i\}^\perp$,这是不可能的,所以函数不含有非零线性结构.

"必要性",假设 ζ_f 中含有的线性无关元素的最大个数小于 n,则 ζ_f 包含在一个 $n-1$ 维线性子空间中,由定理 6 可知,函数至少含有 2 个线性结构,必定含有一个非零的线性结构,矛盾.

4 二阶扩散准则布尔函数的构造

引理 7[4] 对于任意的 $s, t \in Z^+$,$t < s < 2^t$,存在 s 个非 0 元素 $\beta_0, \beta_1, \cdots, \beta_{s-1} \in V_t$,使得向量 $\Phi(y) = (\varphi_{\beta_0}(y), \varphi_{\beta_1}(y), \cdots, \varphi_{\beta_{s-1}}(y))$ 满足对任意 $\beta \in V_t$,$\beta \neq 0$,向量 $\Phi(\beta) = (\varphi_{\beta_0}(\beta), \varphi_{\beta_1}(\beta), \cdots, \varphi_{\beta_{s-1}}(\beta))$ 中即含有 0 元又含有 1 元,其中 $\varphi_{\beta_1}(y) = \langle \beta_i, y \rangle$.

引理 8[5] 设 $f(x, y) = f_1(x) \oplus f_2(y)$,若 $f_1(x)$ 或 $f_2(y)$ 平衡,则 $f(x, y)$ 为平衡函数.

定理 8 设 $s, t \in Z^+$,$t < s < 2^t$,$x \in V_s$,$y \in V_t$,则 $F(x, y) = x\Phi(y) \oplus g(y)$ 是 2-阶扩散准则函数,其中 $\Phi(y)$ 满足引理 7 中的条件,$g(y)$ 是 V_t 上的任意函数.

证明 对于任意的 $\alpha \in V_s$,$\beta \in V_t$ 且 $wt(\alpha, \beta) \le 2$.

$$\begin{aligned} &F(x, y) \oplus F(x \oplus \alpha, y \oplus \beta) \\ &= x\Phi(y) \oplus g(y) \oplus (x \oplus \alpha)\Phi(y \oplus \beta) \oplus g(y \oplus \beta) \\ &= x(\Phi(y) \oplus \Phi(y \oplus \beta)) \oplus \alpha\Phi(y \oplus \beta) \oplus g(y) \oplus g(y \oplus \beta) \end{aligned}$$

若 $\beta = 0$,则 $0 < wt(\alpha) \le 2$. 此时 $F(x, y) \oplus (F(x \oplus \alpha, y \oplus \beta) = \alpha\Phi(y)$,由引理 7 的证明过程可以知道 $\Phi(y)$ 是由互不相同的线性函数构成,故 $\alpha\Phi(y)$ 平衡.

若 $\beta \neq 0$,因为 $\Phi(y)$ 是由互不相同的线性函数构成,$\Phi(y) \oplus \Phi(y \oplus \beta) = \Phi(\beta)$. 此时 $F(x, y) \oplus F(x \oplus \alpha, y \oplus \beta) = x\Phi(\beta) \oplus g(y) \oplus g(y \oplus \beta)$,由引理 7 可知 $\Phi(\beta)$ 为非 0 向量,所以 $F(x, y) \oplus F(x \oplus \alpha, y \oplus \beta)$ 平衡.

由上面可知 $F(x, y)$ 是 2-阶扩散准则函数.

推论 4 若定理 8 中的 $t = s$,设 $\beta_0, \beta_1, \cdots, \beta_{s-1}$ 为 V_s 的一组基,则 $F(x, y) = x\Phi(y) \oplus g(y)$ 是 2-阶扩散准则函数.

证明 因为 $\beta_0, \beta_1, \cdots, \beta_{s-1}$ 为 V_s 的一组基,故对任意 $\beta \in V_t$,$\beta \neq 0$,向量 $\Phi(\beta) = (\varphi_{\beta_0}(\beta), \varphi_{\beta_1}(\beta), \cdots, \varphi_{\beta_{s-1}}(\beta))$ 为非 0 向量,同定理 8 可知,$F(x, y) = x((y) \oplus g(y)$ 是 2-阶扩散准则函数.

推论 5 定理 8 中构造的函数 $F(x, y) = x\Phi(y) \oplus g(y)$ 或是 Bent-函数或是满足 2 阶扩散准则的部分 Bent-函数.

证明 由定理 8 可得函数 $F(x, y)$ 满足 2 阶扩散准则.

对于任意的 $\alpha \in V_s$,$\beta \in V_t$ 且 $0 < wt(\alpha, \beta) \le n$

$$\begin{aligned} &F(x, y) \oplus F(x \oplus \alpha, y \oplus \beta) \\ &= x\Phi(y) \oplus g(y) \oplus (x \oplus \alpha)\Phi(y \oplus \beta) \oplus g(y \oplus \beta) \\ &= x(\Phi(y) \oplus \Phi(y \oplus \beta)) \oplus \alpha\Phi(y \oplus \beta) \oplus g(y) \oplus g(y \oplus \beta) \end{aligned}$$

若 $\beta = 0$,则 $0 < wt(\alpha) \le n$,由引理 7 的证明过程可以知道 $\Phi(y)$ 是由互不相同的线性函数构成,故 $\alpha\Phi(y)$ 为平衡函数或 0. 如果 $\alpha\Phi(y)$ 为 0,则元素 $(\alpha, 0)$ 为线性结构;如果 $\alpha\Phi(y)$ 平衡,则元素 $(\alpha, 0)$ 满足扩散准则.

若 $\beta \neq 0$,同定理 8 可知 $F(x, y) \oplus F(x \oplus \alpha, y \oplus \beta)$ 平衡,元素 (α, β) 满足扩散准则.

所以 $F(x, y) = x\Phi(y) \oplus g(y)$ 或是 Bent-函数或是满足 2 阶扩散准则的部分 Bent-函数.

参考文献:

[1] J Seberry, X M Zhang, Y Zheng. Nonlinearity and propagarion charac-

teristics of balanced boolean functions[J]. Information and Comprtation ,1995 ,119(1) :1 - 13.

[2] J Seberry ,X M Zhang ,Y Zheng. Improving the strict avalanche characteristics of cryptographic functions[J]. Information Processing Letters , 1994 ,50 :37 - 41.

[3] C Carlet. Partially-Bent Function ,Designs ,Codes ,Crytography[M]. 1993. 3. 135 - 145.

[4] Y Zheng ,X M Zhang. Plateaued functions[A]. Advances in Cryptology ICIC '99[C]. LNCS 1726 ,Springer Verlag ,New York ,1999. 284 - 300.

[5] J Seberry ,X M Zhang. Highly nonlinear 0-1balanced functions satisfying strict avalanche criterion[A]. Advances in Cryptology-AUSCRYPT' 92[C] ,LNCS718. Spring-Verlag ,New York ,1993. 145 - 155.

作者简介:

戚文峰　男,1963 年 7 月生于浙江宁波,1997 在信息工程学院获密码学博士学位,获 2000 年度全国优秀博士学位论文,现为郑州信息工程大学教授,博士生导师,主要研究领域为密码学与信息安全,目前已在国内外发表论文 30 余篇. Email :wenfeng. qi @263. net

何德峰　男,1976 年 10 月生于山东青岛,现为郑州信息工程大学密码学硕士研究生,主要研究领域为密码理论.