Hamming 重量为 k 的布尔函数的全局特征和非线性度

周　宇[①]　王维琼[①②]　肖国镇[①]
[①](西安电子科技大学 ISN 综合业务网国家重点实验室　西安　710071)
[②](长安大学理学院　西安　710064)

摘　要：该文给出了布尔函数的自相关系数和互相关系数的一些性质，得到n元布尔函数$f(x)$满足t 阶扩散准则时，n，t 和Hamming重量$wt(f)$的制约关系，给出了任意Hamming重量为k的布尔函数的平方和指标下界表达式，推出了仅由布尔函数Hamming重量所确定的非线性度的上界表达式。这些结论推广了已有结果。

关键词：布尔函数；自相关系数；全局雪崩准则；非线性度
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2009)02-0435-04

Global Avalanche Characteristics and Nonlinearity of Boolean Function with the Hamming Weight k

Zhou Yu[①]　Wang Wei-qiong[①②]　Xiao Guo-zhen[①]
[①](*National Key Lab of Integrated Service Network*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*College of Science*, *Chang'an University*, *Xi'an* 710064, *China*)

Abstract: Some properties of autocorrelation coefficient and cross-correlation coefficient are given. The restricted relationship among n (n variables), $wt(f)$ (the Hamming weight of Boolean function $f(x)$) and t (t -th propagation criteria) was derived, then a lower bound on the sum-of-squares of any Boolean functions with Hamming weight k is concluded. Finally, the results generalized a upper bound on nonlinearity of Boolean function only depending on Hamming weight. This paper improved known results.

Key words: Boolean functions; Auto-correlation coefficient; Global Avalanche Characteristics (GAC); Nonlinearity

1　引言

非线性度和全局雪崩准则是密码函数的两大重要指标。非线性度是从复杂性角度，针对线性攻击提出的，而全局雪崩准则是为了克服严格雪崩准则和扩散准则在某些点的自相关值，使密码函数在整体上达到最优的一个衡量指标。所以，一个好的密码函数应该是非线性度高和全局雪崩指标低，对于平衡布尔函数和一些特殊的布尔函数国内外学者已经得到了一些全局雪崩指标和非线性度，但对于怎样利用汉明重量来刻画一般布尔函数的这些指标尚没有明确的结论。本文中将利用布尔函数的汉明重量和自相关系数来分析和推导全局雪崩准则和非线性度。

2　预备知识

设 B_n 表示所有 n 元布尔函数，　则 $f \in B_n : F_2^n \to F_2$，称 $[f(0,0,\cdots,0),\ f(0,0,\cdots,1),\cdots,f\ (1,1,\cdots,1)]$ 为 $f(x)$ 的真值表，$f(x)$ 的真值表中“1”的个数称为 $f(x)$ 的 Hamming 重量，记为 $wt(f)$。若 $wt(f)=2^{n-1}$，则称 $f(x)$ 为平衡的。

定义 1　设 $f(x)$，$g(x)$ 是 B_n 上的 n 元布尔函数，$\alpha \in F_2^n$，称 $\Delta_{f,g}(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+g(x+\alpha)}$ 为 $f(x)$，$g(x)$ 在 α 处的互相关系数。当 $f(x)=g(x)$ 时，称整数 $\Delta_{f,f}(\alpha)$ 为 $f(x)$ 在 α 处的自相关系数，简记为 $\Delta_f(\alpha)$。

定义 2　设 $f(x)$ 是 B_n 上的 n 元布尔函数，$\varphi_\omega(x)=\sum_{i=1}^{n}\omega_i x_i$，其中 $\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in F_2^n$，$x=(x_1,x_2,\cdots,x_n)\in F_2^n$，则 $f(x)$ 的 Walsh 谱为 $S_{(f)}(\omega)=\sum_{x\in F_2^n}(-1)^{f(x)+\varphi_\omega(x)}$。$f(x)$ 的非线性度定义为 $N_f=2^{n-1}-\frac{1}{2}\max_{\omega\in F_2^n}\left|S_{(f)}(\omega)\right|$。

定义 3[1]　设 $f(x)$ 是 B_n 上的 n 元布尔函数，$\alpha\in F_2^n$，若 $\Delta_f(\alpha)=0$，即 $f(x)+f(x+\alpha)$ 是平衡的，则称 $f(x)$ 在 α 处满足扩散准则。如果对所有满足 $wt(\alpha)=1$ 的 α，$\Delta_f(\alpha)=0$，则称 $f(x)$ 满足严格雪崩准则(SAC)；如果对所有满足 $1\le wt(\alpha)\le t$ 的 α，$\Delta_f(\alpha)=0$，则称 $f(x)$ 满足 t 次扩散准则(PC(t))。

扩散准则在数据加密算法和 Hash 函数中是非常重要的概念，但是扩散准则仅仅是函数的局部性质，为了提高密码函数的全局特性，　Zhang 和 Zheng 在文献[2]中提出了密码

2007-08-03 收到，2007-12-24 改回
国家自然科学基金(60473028，60503010)资助课题

函数的全局雪崩准则(GAC)，用来克服 PC 在某些点上的自相关值，使得整体上达到最优。

定义 4[2] 设 $f(x)$ 是 B_n 上的 n 元布尔函数，称

$$\sigma_f=\sum_{\alpha\in F_2^n}\Delta_f^2(\alpha),\quad \Delta_f=\max_{\alpha\in F_2^n且\alpha\neq 0}\left|\Delta_f(\alpha)\right| \tag{1}$$

分别为 $f(x)$ 的平方和指标和绝对值指标。

Δ_f 和 σ_f 越小，$f(x)$ 的GAC性质越好。Zhang和Zheng[2]得到了这两个指标的上下界分别为 $2^{2n}\le\sigma_f\le 2^{3n}$，$0\le\Delta_f\le 2^n$。Bent函数[3]达到这两个指标的下界。Son[4]等得到 $n(n\ge 3)$ 元平衡布尔函数的两个指标下界，$\sigma_f\ge 2^{2n}+2^{n+3}$，$\Delta_f\ge 8$。Sung[5]等也得到了 n 元布尔函数 $f(x)$ 在 $A\subset F_2^n$（A 是 F_2^n 的一个子集)上的满足扩散时的平方和指标的下界。同时Stanica[6]等构造了一类GAC指标良好的 n 元平衡布尔函数。文献[7]中得到了两类平衡布尔函数，其中一类具有良好的非线性度 $N_f=2^{2k-1}-2^k+2^{k-2}(n=2k)$，其中 $\sigma_f=2^{4k}+2^{3k+2}+2^{3k}+2^{3k-2}$。

本文首先给出自相关系数和互相关系数的一些性质，由此得到布尔函数变元个数，扩散阶和汉明重量的制约关系，进而推出了由布尔函数的汉明重量所决定的平方和指标的下界表达式，最后得到了由布尔函数汉明重量所确定的非线性度的上界表达式。

3 结果

本文首先给出自相关系数与互相关系数的关系。由相关系数定义很容易得到：

性质 1 设 $f(x)$，$g(x)$ 是 B_n 上的 n 元布尔函数，则

(1) $\sum_{u\in F_2^n}(-1)^{g(u)}\Delta_f(u)=\sum_{v\in F_2^n}(-1)^{f(v)}\Delta_{f,g}(v)$；

(2) $\sum_{\alpha\in F_2^n}\Delta_{f,g}(\alpha)=(2^n-2wt(f))(2^n-2wt(g))$。

在性质 1 中，若 $f(x)=g(x)$，就有 $\sum_{\alpha\in F_2^n}\Delta_f(\alpha)=(2^n-2wt(f))^2$。特别地，$f(x)$ 是平衡函数的充要条件是 $\sum_{\alpha\in F_2^n}\Delta_f(\alpha)=0$。为了得出任意 Hamming 重量为 $k(k\ge 0)$ 的布尔函数的平方和指标的下界，由 $\Delta_f(\alpha)$ 的定义，很容易得到下面性质，此性质是后面的基础。

性质 2 设 $f(x)$ 是 B_n 上的 n 元布尔函数，则 $\Delta_f(\alpha)=2^n-4wt(f)+4\left|C_\alpha\right|$（$\left|A\right|$ 表示集合 A 中元素的个数），$\alpha\in F_2^n$，其中 $C_\alpha=\{x\in F_2^n:f(x)=1,f(x+\alpha)=1\}$。

由于 $C_\alpha=\{x\in F_2^n:f(x)=1,f(x+\alpha)=1\}$，所以 $0\le\left|C_\alpha\right|\le wt(f)$。很显然存在 $\alpha\in F_2^n$ 使得 $\left|C_\alpha\right|=wt(f)$，因为当 $\alpha=0$（0 为零向量 $(0,\cdots,0)$）时就有 $\left|C_\alpha\right|=wt(f)$，所以 C_α 非空，而当 $\left|C_\alpha\right|\neq wt(f)$ 时，可知 $\left|C_\alpha\right|$ 为偶数，这是因为若 $\alpha\neq\beta\neq 0$ 且 $\beta\in C_\alpha$，则 $\alpha+\beta\in C_\alpha$。所以 $\left|C_\alpha\right|$ 为 $[0,wt(f))$ 中的偶数或 $\left|C_\alpha\right|=wt(f)$。这也就是说若 $wt(f)$ 为偶数时，$\left|C_\alpha\right|$ 全部为偶数，而当 $wt(f)$ 为奇数时，$\left|C_\alpha\right|$ 除等于 $wt(f)$ 是奇数外，其它都为偶数。所以由性质 2 很容易得到以下推论：

推论 1 设 $f(x)$ 是 B_n 上的 n 元布尔函数

(1) 若 $wt(f)\le 2^{n-2}$ 时，则对任意的 $\alpha\in F_2^n$，有 $2^n-4wt(f)\le\Delta_f(\alpha)\le 2^n$；

(2)若 $n(n\ge 3)$ 且 $wt(f)$ 为奇数，则对任意的 $\alpha\in F_2^n$，$f(x)$ 不满足扩散准则；

(3) $\sum_{\alpha\in F_2^n}\left|C_\alpha\right|=(wt(f))^2$。

在推论 1 的基础上，很容易得到 n 元布尔函数 $f(x)$ 满足 t 阶扩散准则时，n，$k=wt(f)$ 和 t 的制约关系。

定理 1 设 $f(x)$ 是 B_n 上的 $n(n\ge 3)$ 元布尔函数且其 Hamming 重量为 k。若 $f(x)$ 满足 t 阶扩散准则，则 $\frac{k^2-k}{k-2^{n-2}}\ge\sum_{i=1}^{t}\binom{n}{i}$。

证明 由于 $f(x)$ 满足 t 阶扩散准则，则对任意的 $\alpha\in F_2^n$ 且 $1\le wt(\alpha)\le t$，有 $\Delta_f(\alpha)=0$，即至少共有 $\sum_{i=1}^{t}\binom{n}{i}$ 个 α 使 $\Delta_f(\alpha)=0$，由性质 2 可知，此时对于满足 $1\le wt(\alpha)\le t$ 的 α，都有 $\left|C_\alpha\right|=k-2^{n-2}$，但由推论 1 得到 $\sum_{\alpha\in F_2^n}\left|C_\alpha\right|=k^2$，进而

$$\begin{aligned}k^2&=\sum_{\alpha\in F_2^n}\left|C_\alpha\right|\\&=\sum_{1\le wt(\alpha)\le t}\left|C_\alpha\right|+\sum_{wt(\alpha)=0}\left|C_\alpha\right|+\sum_{wt(\alpha)\ge t+1}\left|C_\alpha\right|\\&\ge\sum_{1\le wt(\alpha)\le t}\left|C_\alpha\right|+\sum_{wt(\alpha)=0}\left|C_\alpha\right|\\&=\sum_{i=1}^{t}\binom{n}{i}(k-2^{n-2})+k\end{aligned}\tag{2}$$

所以结论成立。 证毕

特别地，对于 $n(n\ge 3)$ 元平衡布尔函数来说有 $2^n-2\ge\sum_{i=1}^{t}\binom{n}{i}$，也就是说 $n(n\ge 3)$ 元平衡布尔函数最多满足 $n-1$ 阶扩散准则。文献[8]通过特征矩阵刻画了 $n(n\ge 3)$ 元布尔函数在某一点满足扩散准则的充要条件，而定理 1 表明，扩散集的元素个数和变元数之间存在着制约关系，也就是说，若 $n(n\ge 3)$ 元布尔函数在一个集合 $A\subset F_2^n$ 上满足扩散准则时，就有 $\frac{k^2-k}{k-2^{n-2}}\ge\left|A\right|$。

引理 1[4]　设 $X_i \in Z$，$i=1,2,\cdots,n$ 且 $\sum_{i=1}^{n} X_i = X$，则

$$\sum_{i=1}^{n}(X_i)^2 \geq 2X\left\lfloor\frac{X}{n}\right\rfloor - n\left\lfloor\frac{X}{n}\right\rfloor^2 + X - n\left\lfloor\frac{X}{n}\right\rfloor \tag{3}$$

定理 2　设 $f(x)$ 是 B_n 上的 n 元布尔函数，记 $wt(f)=k$ 和 $\left\lfloor\frac{k(k-1)}{2(2^n-1)}\right\rfloor = t$，则

$$\sum_{\alpha\in F_2^n}|C_\alpha|^2 \geq k^2 + 4k(k-1)t - 4(2^n-1)t^2 + 2k(k-1) - 4(2^n-1)t \tag{4}$$

证明　设 $\mathrm{Supp}(f)=\{x\in F_2^n : f(x)=1\}$，则 $|\mathrm{Supp}(f)| = wt(f)=k$，由于 $C_\alpha = \{x\in F_2^n : f(x)=1, f(x+\alpha)=1\}$，所以

$$\begin{aligned}\sum_{\alpha\in F_2^n}|C_\alpha|^2 &= \sum_{\alpha\in F_2^n}\left(\sum_{x\in F_2^n} f(x)f(x+\alpha)\right)^2\\ &= \sum_{x\in F_2^n}\left(f^2(x)\sum_{\alpha\in F_2^n} f^2(x+\alpha)\right) + 2\sum_{i<j} f(x_i)f(x_j)\sum_{\alpha\in F_2^n} f(x_i+\alpha)f(x_j+\alpha)\\ &= k^2 + 2\sum_{i<j,x_i,x_j\in\mathrm{Supp}(f)}\sum_{\alpha\in F_2^n} f(x_i+\alpha)f(x_j+\alpha)\\ &= k^2 + 2\sum_{\substack{i<j,x_i,x_j\in\mathrm{Supp}(f)\\ x_i+x_j=x_1}}\sum_{\alpha\in F_2^n} f(x_i+\alpha)f(x_j+\alpha)\\ &\quad + 2\sum_{\substack{i<j,x_i,x_j\in\mathrm{Supp}(f)\\ x_i+x_j=x_2}}\sum_{\alpha\in F_2^n} f(x_i+\alpha)f(x_j+\alpha) + \cdots\\ &\quad + 2\sum_{\substack{i<j,x_i,x_j\in\mathrm{Supp}(f)\\ x_i+x_j=x_{2^n-1}}}\sum_{\alpha\in F_2^n} f(x_i+\alpha)f(x_j+\alpha)\end{aligned}$$

其中 $x_1,x_2,\cdots,x_{2^n-1}\in F_2^n$，为此可以定义新的集合 $Y_c = \{(x_l,x_m)\in \mathrm{Supp}(f)\times\mathrm{Supp}(f) \mid l<m且x_l+x_m=x_c\}$，其中 $c=1,2,\cdots,2^n-1$。由于 $x_l+x_m=(x_l+\alpha)+(x_m+\alpha)$，如果 $x_l+x_m\in Y_c$ 且 $f(x_l+\alpha)f(x_m+\alpha)=1$，则 $(x_l+\alpha,x_m+\alpha)\in Y_c$ 或者 $(x_m+\alpha,x_l+\alpha)\in Y_c$，因此当 $c=1$ 时，有

$$\sum_{\substack{i<j,x_i,x_j\in\mathrm{Supp}(f)\\ x_i+x_j=x_1}}\sum_{\alpha\in F_2^n} f(x_i+\alpha)f(x_j+\alpha) = \sum_{\substack{i<j,x_i,x_j\in\mathrm{Supp}(f)\\ x_i+x_j=x_1}}\sum_{\substack{x_l+\alpha,x_m+\alpha\in\mathrm{Supp}(f)\\ x_i+\alpha+x_j+\alpha=x_1}} 1 = 2|Y_1|^2$$

依此类推可计算 $c=2,\cdots,2^n-1$，进而就有 $\sum_{\alpha\in F_2^n}|C_\alpha|^2 = k^2 + 4\sum_{c=1}^{2^n-1}|Y_c|^2$。

但是由 Y_c 的定义可知 $\sum_{c=1}^{2^n-1}|Y_c| = \frac{k(k-1)}{2}$，利用引理 1，令 $\left\lfloor\frac{k(k-1)}{2(2^n-1)}\right\rfloor = t$，有 $\sum_{c=1}^{2^n-1}|Y_c|^2 \geq k(k-1)t - (2^n-1)t^2 + \frac{k(k-1)}{2} - (2^n-1)t$。所以结论成立。　证毕

定理 3　设 $f(x)$ 是 B_n 上的 n 元布尔函数，记 $wt(f)=k$ 和 $\left\lfloor\frac{k(k-1)}{2(2^n-1)}\right\rfloor = t$，则

$$\begin{aligned}\sigma_f \geq\ & 2^{3n} + 3\cdot 2^{n+3}k^2 - 2^{2n+3}k - 32\cdot k^3 + 16\cdot k^2\\ & + 2^5[(2t+1)(k^2-k) - (2^{n+1}-2)(t^2+t)]\end{aligned} \tag{5}$$

证明　利用性质 2 和推论 1 可知

$$\begin{aligned}\sigma_f &= \sum_{\alpha\in F_2^n}\Delta_f^2(\alpha) = \sum_{\alpha\in F_2^n}\left(2^n - 4k + 4|C_\alpha|\right)^2\\ &= \sum_{\alpha\in F_2^n}\left(2^{2n} + 16k^2 - 8k2^n - 32|C_\alpha| + 8\cdot 2^n|C_\alpha| + 16|C_\alpha|^2\right)\\ &= 2^{3n} + 16k^2 2^n - 8k2^{2n} - (32 - 8\cdot 2^n)k^2 + 16\sum_{\alpha\in F_2^n}|C_\alpha|^2\end{aligned}$$

利用引理 2 可知结论成立。　证毕

在定理 3 中若 $k=2^{n-1}$ 时，有 $\left\lfloor\frac{k(k-1)}{2(2^n-1)}\right\rfloor = \left\lfloor 2^{n-3} - \frac{2^{n-3}}{2^n-1}\right\rfloor = 2^{n-3}-1$，进而根据定理 3 就有 $\sigma_f \geq 2^{2n} + 2^{n+3}(n\geq 3)$，这时就与文献[4]中的结论一致。另一方面，文献[4]中是针对平衡布尔函数，而本文得到的是任意 Hamming 重量为 k 的布尔函数的 σ_f 下界，所以本文的结论推广了文献[4]中的结果，使得仅从 Hamming 重量角度方面就可以给出 σ_f 的下界。

对于特定的布尔函数的非线性度，已经有好多结果，如文献[7]和文献[9]，而在文献[10]中给出通过线性码去构造 n-输入 m-输出的高非线性布尔函数，在下面将从 Hamming 重量角度给出非线性度。

引理 2[4]　设 $f(x)$ 是 B_n 上的 n 元布尔函数，则 $N_f \leq 2^{n-1} - \frac{1}{2}2^{-\frac{n}{2}}\sqrt{\sigma_f}$。

若记在定理 2 中得到的界为 $\overline{\sigma}_f$，则在引理 2 的基础上，就得到仅由布尔函数 Hamming 重量所确定的非线性度上界的表达式。

推论 2　设 $f(x)$ 是 B_n 上的 n 元布尔函数，则 $N_f \leq 2^{n-1} - \frac{1}{2}2^{-\frac{n}{2}}\sqrt{\overline{\sigma}_f}$。

4　结束语

本文讨论了自相关系数和互相关系数的一些性质，在此基础上得到了 n 元布尔函数 $f(x)$ 满足 t 阶扩散准则时，n (变元个数)，t 和 $wt(f)$ 的制约关系，进而给出了任意Hamming重量为 k 的布尔函数的平方和指标下界表达式，此结论推广了Son等人在文献[4]中的结果，使得具有一定的普遍性，由此推出了仅由布尔函数的Hamming重量所确定的非线性度的上界表达式。

参 考 文 献

[1]　Preneel B, Leekwijck W V, Linden L V, Govaerts R, and

Vandewalle J. Propagation characteristics of Boolean functions [C]. Advances in Cryptology-EuroCrypt'90, Spring, Berlin, 1991: 161–173.

[2] Zhang X M and Zheng Y L. GAC-the criterion for global avalanche characteristics of cryptographic functions [J]. *Journal of Universal Computer Science*. 1995, 1(5): 320–337.

[3] Rothaus O S. On "bent" functions [J]. *Journal of Combinatorial Theory*, 1976, 20(A): 300–305.

[4] Son J J, Lim J I, Chee S, and Sung S H. Global avalanche characteristics and nonlinearity of balanced Boolean function [J]. *Information Processing Letters*, 1998, 65: 139–144.

[5] Sung S H, Chee S, and Park C. Global avalanche characteristics and propagation criterion of balanced Boolean functions [J]. *Information Processing Letters*, 1999, 69: 21–24.

[6] Stanica P and Sung S H. Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics [J]. *Information Processing Letters*, 2001, 79: 167–172.

[7] Ren Kui, Park Jaemin, and Kim Kwangjo. On the construction of cryptographically strong Boolean with desirable trade-off [J]. *Journal of Zhejiang University Science*, 2005, 6(5): 358–364.

[8] 郭锦辉, 李世取. 布尔函数扩散性的矩阵刻画[J]. 电子与信息学报, 2006, 28(4): 712–716.
Guo Jin-hui and Li Shi-qu. Matrix description on propagation characteristic of Boolean function [J]. *Journal of Electronics & Information Technology*, 2006, 28(4): 712–716.

[9] Carlet C. The complexity of Boolean functions from cryptographic viewpoint[J], http:// drops.dagstuhl.de/opus /volltexte/2006/604.

[10] 常祖领, 陈鲁生, 符方伟. 高非线性度n-输入m-输出布尔函数的一般构造方法(英文)[J]. 南开大学学报(自然科学版), 2005, 38(3): 29–33.
Chang Zu-ling, Chen Lu-sheng, and Fu Fang-wei. Generalized construction of n-input m-output Boolean functions with high nonlinearity[J]. *Acta Scientiarun Naturaltium Universitatis Nankaiensis*, 2005, 38(3): 29–33.

周 宇： 男，1980 年生，博士生，研究方向为密码函数和序列密码.

王维琼： 女，1978 年生，讲师，研究方向为密码函数和数字签名.

肖国镇： 男，1934 年生，教授，博士生导师，研究方向包含信息论、编码学和密码学.