具有线性结构的弹性函数非线性度的新上界

周 宇 肖国镇
(西安电子科技大学 ISN 国家重点实验室信息保密所 西安 710071)

摘 要 讨论了具有线性结构的弹性函数的两个指标:沃什谱和非线性度,得到了具有线性结构的布尔函数的一些性质。利用沃尔什变换和汉明重量的方法,发现了:如果 V 是 n 元布尔函数 $f(x)$ 的线性结构,那么得到 $f(x)$ 的沃尔什变换在 $F_2^n\backslash V^\perp$ 或 $V^\perp$ 为零这一事实,同时得到了一个布尔函数没有 $k(k\geqslant 0)$ 维线性结构的充分条件。最后,利用以上结果推出了具有线性结构的弹性函数的非线性度的上界表达式。

关键词 布尔函数,线性结构,弹性函数,非线性度
中图法分类号 TN918.1 **文献标识码** A

New Upper Bound on Nonlinearity of Resilient Function with Linear Structure

ZHOU Yu XIAO Guo-zhen
(Institute of Information Security, National Key Laboratory of ISN, Xidian University, Xi'an 710071, China)

Abstract The two criteria were discussed: the Walsh spectral and the nonlinearity of resilient functions with a linear structure, some properties of Boolean functions with linear structure were presented. By the methods of Walsh transform and Hamming weight, the fact that the Walsh transform of Boolean functions $f(x)$ with n variables are zero with respect to $F_2^n\backslash V^\perp$ or $V^\perp$, if V is a linear structure of $f(x)$, was found. A sufficient condition was derived to determine whether a Boolean function has no a linear structure with dimension $k(k\geqslant 0)$ or not. Finally, a new upper bound on nonlinearity of a resilient function with linear structure was deduced by using these results.

Keywords Boolean functions, Linear structure, Resilient functions, Nonlinearity

布尔函数的弹性和非线性度在流密码和分组密码中有很重要的应用,高非线性度能抵抗线性攻击[1],而弹性能抵抗相关攻击[2]。近来,文献[3]已经研究了非线性度和相关免疫的关系。进一步,Charpin 和 Pasalic 在文献[4]中得到对某些固定的 n(变元个数),d(代数次数)和 t(t 相关免疫),不可能构造没有线性结构的弹性函数,例如,若一个布尔函数满足 $n\geqslant 2^{2(n-t-\varepsilon-2)}$,其中 $\varepsilon=(n-t-2)/d$,则这个布尔函数一定具有线性结构。Canteaut 等人在文献[5]中也论述了布尔函数具有线性结构并不一定是坏事,且他们对具有线性结构 $k(k\leqslant 2)$的三谱值布尔函数非线性度得到了一些结果。在文献[6]中 Pasalic 考虑了一个 Maiorana- McFarland 类的子类来设计弹性函数,构造了代数次数高的向量弹性函数,但是这种构造方法在文献[7]中是用不交码给出的。

文中考虑了具有线性结构的布尔函数,得到了一个非线性度的新上界。为了得到此结果,首先将此类函数分成两类,给出了线性结构和平衡性及线性结构和沃什变换的关系。利用沃什变换和汉明重量得到:如果 V 是 n 元布尔函数 $f(x)$ 的线性结构,那么 $f(x)$ 的沃尔什变换在 $F_2^n\backslash V^\perp$ 或 $V^\perp$ 是零这一事实。同时得到了一个布尔函数没有 $k(k\geqslant 0)$ 维线性结构的充分条件。

1 预备知识

设 B_n 表示所有 n 元布尔函数的全体,因此 $f(x)\in B_n$:$F_2^n\to F_2$。布尔函数 $f(x_1,x_2,\cdots,x_n)$ 的真值表是通过输出的 2^n 向量来表示的,也就是,

$$f=[f(0,0,\cdots,0),f(0,0,\cdots,1),\cdots,f(1,1,\cdots,1)]$$

满足 $f(x)=1$ 的 $x=(x_1,x_2,\cdots,x_n)\in F_2^n$ 组成的集合称为支撑集,记为 $Supp(f)$。一个向量 $s\in F_2^n$ 的汉明重量是这个向量中 1 的个数,记为 $wt(s)$。n 元平衡的布尔函数的汉明重量为 $wt(f)=2^{n-1}$。

对任意的 $\alpha=(\alpha_1,\cdots,\alpha_n)\in F_2^n$,$\varphi_\alpha(x_1,\cdots,x_n)=\sum_{i=1}^{n}\alpha_i x_i$,$f(x)$的沃什谱为

$$F(f+\varphi_\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+\varphi_\alpha(x)}$$

$f(x)$的非线性度 N_f 为

$$N_f=2^{n-1}-\frac{1}{2}\max_{\alpha\in F_2^n}|F(f+\varphi_\alpha)|$$

相关免疫函数和弹性函数是布尔函数的两个重要子类。肖和 Massey 在文献[8]中刻画了 $f(x)\in B_n$ 是相关免疫(CI)的充要条件:$f(x)\in B_n$ 是 CI(t)当且仅当对所有满足 $1\leqslant wt$

到稿日期:2008-07-01 返修日期:2008-10-06 本文受国家自然科学基金(60473028,60773003 和 60503010),陕西省自然科学基金(No. 2006F19)和信息安全国家重点实验室(中国科学院研究生院)开放课题(No. 03-06)资助。

周 宇 博士,主要研究方向为密码学与信息安全等,E-mail:zhouyu.zhy@tom.com;肖国镇 博士生导师,主要研究方向为密码学、信息安全与信息论等。

$(\alpha)\leqslant t$ 的 $\alpha\in F_2^n$，其沃什谱值 $F(f+\varphi_\alpha)=0$。如果 $f(x)$ 是平衡的，则 $F(f)=0$。平衡的 CI(t) 是 t-弹性函数。$f(x)$ 在 $\alpha\in F_2^n$ 处的差分 $D_\alpha f$ 定义为 $D_\alpha f(x)=f(x)+f(x+\alpha)$。若 $D_\alpha f$ 是常数，此时称 α 是 $f(x)$ 的线性结构。注意到 $f(x)$ 的所有线性结构组成一个空间，称为线性结构空间，记为 U_f。

对任意 F_2^n 的子空间 V，其对偶空间 $V^\perp$ 是对任意的 $x\in F_2^n$ 和 $y\in F_2^n$ 满足 $x\cdot y=0$ 的 y 的集合。下面引理揭示了沃什谱和相关谱的关系。

引理 1[5] 设 $f(x)\in B_n$，V 是 F_2^n 的维数为 k 的子空间，则 $\sum\limits_{\upsilon\in V}F^2(f+\varphi_\upsilon)=2^k\sum\limits_{u\in V^\perp}F(D_uf)$。

特别地，Sarkar 和 Maitra 在文献[3]中已经得到了布尔函数 $f(x)\in B_n$ 是 t-弹性函数沃什谱的关系：$F(f+\varphi_\alpha)\equiv 0 \pmod{2^{t+2}}$，其中 $\alpha\in F_2^n$。这个结果也被 Trannikov 在文献[9]中独立得到，同时被 Carlet 在文献[10]中改进为：$F(f+\varphi_\alpha)\equiv 0 \pmod{2^{t+2+\varepsilon}}$，其中 $\varepsilon=\lfloor(n-t-2)/d\rfloor$，$d$ 是代数次数，$\alpha\in F_2^n$。

2 具有线性结构的布尔函数的性质

这部分给出布尔函数的线性结构 U_f，支撑集 $Supp(f)$ 和 $\{\alpha\in F_2^n: F(f+\varphi_\alpha)=0\}$ 的关系。

为了方便，设 $\dim(U_f)=k$，记

$U_f^0=\{\alpha\in F_2^n: f(x+\alpha)+f(x)=0, \forall x\in F_2^n\}$，

$U_f^1=\{\alpha\in F_2^n: f(x+\alpha)+f(x)=1, \forall x\in F_2^n\}$。

则 $U_f=U_f^0\cup U_f^1$ 且 $U_f^0\cap U_f^1=\emptyset$。下面给出线性结构的一个性质。

引理 2[11] 设 $f(x)\in B_n$，U_f 是线性结构。若 $U_f^1\neq\emptyset$，则 $\#U_f^1=\#U_f^0$（$\#A$ 表示集合 A 的元素个数）。

引理 2 表明布尔函数 $f(x)$ 的线性结构 $U_f=U_f^0\cup U_f^1$ 能被划分为两类：C(1)，$U_f^1=\emptyset$，也就是，对任意的 $\alpha\in U_f=U_f^0$ 有 $D_\alpha f=f(x+\alpha)+f(x)=0$；C(2)，$U_f^1\neq\emptyset$，也就是，对任意的 $\alpha\in U_f^0$ 有 $D_\alpha f=f(x+\alpha)+f(x)=0$，同时对任意的 $\alpha\in U_f^1$ 有 $D_\alpha f=f(x+\alpha)+f(x)=1$。

性质 1 设 $f(x)\in B_n$ 具有线性结构 $U_f=U_f^0\cup U_f^1$。若 $U_f^1\neq\emptyset$，则 $f(x)$ 是平衡的。

证明：由于 $U_f^1\neq\emptyset$，则存在某个 $\alpha\in U_f^1$ 满足 $D_\alpha f=f(x+\alpha)+f(x)=1$，因此有

$$2^n=wt(D_\alpha f)=wt(f(x))+wt(f(x+\alpha))-2wt(f(x)f(x+\alpha))$$

但

$$wt(f(x))=wt(f(x+\alpha))$$

且 $wt(f(x)f(x+\alpha))=0$，因此 $wt(f(x))=2^{n-1}$。

从线性结构的定义可知对任意的 $\alpha\in U_f$ 有 $D_\alpha f=f(x+\alpha)+f(x)=0$ 或 1，因此如果 $f(x)=1$，则 $f(x+\alpha)=1$ 或 0，如果 $f(x)=0$，则 $f(x+\alpha)=0$ 或 1，这也就表明 U_f 和 $Supp(f)$ 之间有某种联系，下一个定理揭示了线性结构和沃什谱为零的点的关系。

定理 1 设 $f(x)\in B_n$ 且 $U_f=U_f^1\cup U_f^0$ 是线性结构

1)若 $U_f^1=\emptyset$，则对于 $\alpha\in F_2^n\backslash U_f^\perp$，$F(f+\varphi_\alpha)=0$；

2)若 $U_f^1\neq\emptyset$，则对于 $\alpha\in U_f^\perp$，$F(f+\varphi_\alpha)=0$。

证明：注意到 U_f 是 F_2^n 的一个子空间，所以设 $\dim(U_f)=k$，

①如果 $U_f^1=\emptyset$。由引理 1 和线性结构的定义，可得到

$$\sum_{\alpha\in U_f^\perp}F^2(f+\varphi_\alpha)=2^{n-k}\sum_{\beta\in U_f}F(D_\beta f)=2^{n-k}\cdot 2^k\cdot 2^n=2^{2n}$$

同时，由 Parseval 等式，也可得到

$$\sum_{\alpha\in F_2^n}F^2(f+\varphi_\alpha)=\sum_{\alpha\in U_f^\perp}F^2(f+\varphi_\alpha)+\sum_{\alpha\in F_2^n\backslash U_f^\perp}F^2(f+\varphi_\alpha)=2^{2n}$$

因此 $\sum\limits_{\alpha\in F_2^n\backslash U_f^\perp}F^2(f+\varphi_\alpha)=0$，即结论成立。

②如果 $U_f^1\neq\emptyset$。由引理 1 和引理 2，得到

$$\sum_{\alpha\in U_f^\perp}F^2(f+\varphi_\alpha)=2^{n-k}\sum_{\beta\in U_f}F(D_\beta f)=$$

$$2^{n-k}(2^{k-1}\cdot 2^n-2^{k-1}\cdot 2^n)=0$$

因此，$\sum\limits_{\alpha\in U_f^\perp}F^2(f+\varphi_\alpha)=0$，即结论成立。

换句话说，如果 $U_f^1=\emptyset$，则 $f(x)$ 在 $\alpha\in F_2^n\backslash U_f^\perp$ 上是相关免疫(CI)的；如果 $U_f^1\neq\emptyset$，则 $f(x)$ 在 $U_f^\perp$ 上是相关免疫的。相反，定理 1 暗示了如果 $f(x)$ 在 V 或者 $F_2^n\backslash V$（V 是 F_2^n 的子空间）上是相关免疫的，则 $f(x)$ 可能在 $V^\perp$ 上具有线性结构，也就是，如果要知道 $f(x)$ 是否具有线性结构时，仅仅考虑 $f(x)$ 在 V 或者 $F_2^n\backslash V$ 上的相关免疫是不够的，还必须验证 $f(x)$ 在 $V^\perp$ 上的情况。因此在研究 $f(x)$ 在 V 或者 $F_2^n\backslash V$ 上的相关免疫性时也得考虑 $f(x)$ 在其对偶空间 $V^\perp$ 的性质，这对以后构造性质量好的弹性函数很重要。

推论 1 设 $f(x)\in B_n$ 和 $Z_f=\{\alpha\in F_2^n\mid F(f+\varphi_\alpha)=0\}$。若 $\#Z_f\leqslant\min\{2^{n-k}-1, 2^n-2^{n-k}-1\}$，则 $f(x)$ 没有维数为 k（$k\geqslant 1$）的线性结构。

证明：由定理 1 可知如果 $D_\alpha f$ 在 U_f 上是常数 U_f，其中 $\dim(U_f)=k$，则集合 Z_f 包含 $U_f^\perp$ 或者 $F_2^n\backslash U_f^\perp$。因此当 $f(x)$ 具有维数为 k 的线性结构时，Z_f 的大小一定不小于 2^{n-k} 或者 2^n-2^{n-k}。

Canteaut 等人在文献[5]中仅仅得到了 $k=1$ 时，集合 Z_f 的大小不超过 $2^{n-1}-1$，在这里推论 1 将此推广到了任意的 k，得到了更一般的结果。

3 具有线性结构的弹性函数非线性度的新上界

利用前面的结论得到具有线性结构的弹性函数非线性度的新上界。

定理 2 设 $f(x)$ 是代数次数为 $d(d\geqslant 2)$ 的 t-弹性函数，U_f 是维数 $\dim(U_f)=k$ 的线性结构，$\varepsilon=\lfloor(n-t-2)/d\rfloor$。

1)若 $f(x)$ 在 U_f 上具有第一类线性结构，则 $N_f\leqslant 2^{n-1}-l\cdot 2^{t+2+\varepsilon}$，其中 l 是所有满足 $2^{2n-2(t+2+\varepsilon)}\leqslant i^2(2^{n-k}-2)$ 的 i 中最小的；

2)若 $f(x)$ 在 U_f 上具有第二类线性结构，则 $N_f\leqslant 2^{n-1}-l\cdot 2^{t+2+\varepsilon}$，其中 l 是所有满足 $2^{2n-2(t+2+\varepsilon)}\leqslant i^2(2^n-2^{n-k}-1)$ 的 i 中最小的。

证明：1)由定理 1 和 Parseval 等式，由于对任意的 $\alpha\in F_2^n\backslash U_f^\perp$，有 $F(f+\varphi_\alpha)=0$，因此 $\sum\limits_{\alpha\in U_f^\perp}F^2(f+\varphi_\alpha)=2^{2n}$。另外，对任意的 t-弹性函数有：$F(f+\varphi_\alpha)\equiv 0 \pmod{2^{t+2+\varepsilon}}$，其中 $\alpha\in F_2^n$。因此得到对任意的 $\alpha\in U_f$，存在整数 i 满足 $0\leqslant i^2\leqslant 2^{2n-2(t+2+\varepsilon)}$ 和 $F^2(f+\varphi_\alpha)=i^2 2^{2(t+2+\varepsilon)}$。紧接着对每个 i 定义 λ_i

$$\lambda_i=\#\{\alpha\in U_f^\perp: |F(f+\varphi_\alpha)|=i2^{t+2+\varepsilon}\}$$

这时得到（$c=2^{2n-2(t+2+\varepsilon)}$）

$$\sum_{i=1}^{c}\lambda_i i^2 2^{2(t+2+\varepsilon)}=2^{2n}, \text{i. e.}, \sum_{i=1}^{c}\lambda_i i^2=2^{2n-2(t+2+\varepsilon)}$$

另一方面，对每个 $\alpha\in U_f^\perp$，考察非零 $F(f+\varphi_\alpha)$ 的个数 Λ。

由于 $f(x)$ 是 t-弹性函数，则 $F(f)=0$，因此 $\Lambda<2^{n-k}-1$，也就是，$\Lambda\leqslant 2^{n-k}-2$。所以存在满足 $2^{2n-2(t+2+\varepsilon)}=\sum_{j=1}^{c}\lambda_i j^2\leqslant\Lambda i^2\leqslant i^2(2^{n-k}-2)$ 的整数 i。

因此，可以定义 l 为满足 $2^{2n-2(t+2+\varepsilon)}\leqslant i^2(2^{n-k}-2)$ 的最小 i。这时能保证对某个 $\alpha\in U_f$ 使得 $|F(f+\varphi_\alpha)|\geqslant l2^{t+2+\varepsilon}$。所以就证明了沃什谱的绝对值最小值为 $l2^{t+2+\varepsilon}$，等价于，$N_f\leqslant 2^{n-1}-l\cdot 2^{t+2+\varepsilon}$。

2)利用 1)的方法就能得到 2)的结果。

结束语 文中得到了具有线性结构的布尔函数的一些性质。找到了此类函数的一个事实：若 V 是布尔函数的线性结构，则 $f(x)$ 的沃什谱值在 $F_2^n\backslash V^\perp$ 或者 $V^\perp$ 上为零。同时得到布尔函数没有 $k(k\geqslant 0)$ 线性结构的充分条件，最后给出了具有线性结构的弹性函数的非线性度的新上界。这些结果将为以后设计性质良好的弹性函数提供依据。

参 考 文 献

[1] Yan Matsui M. Linear cryptanalysis method for DES cipher[C] // Advances in Cryptology-Eurocrypt'93, LNCS. 1994, 765: 386-397

[2] Siegenthaler T. Decrypting a class of stream ciphers using ciphertexts only[J]. IEEE Transactions on Computers, 1985, 34 (1): 81-85

[3] Sarkar P, Maitra M. Nonlinearity bounds and constructions of resilient Boolean functions[C] // Advances in cryptology Eurocrypt'2000, LNCS. Springer-Verlag, 2000, 1809: 515-532

[4] Charpin P, Pasalic E. On propagation characteristics of resilient functions[C] // Advances in Cryptology-SAC' 2002, LNCS. Springer-Verlag, 2003, 2595: 175-195

[5] Canteaut A, Carlet C, Charpin P, et al. On cryptographic properties of the cosets of R(1, m)[J]. IEEE Transactions on Information Theory, 2001, 47: 1494-1513

[6] Pasalic E. Maiorana - McFarland class : degree optimization and algebraic properties[J]. IEEE Transactions on Information Theory, 2006, 52(10): 4581-4594

[7] Charpin P, Psaslic E. Highly nonlinear resilient functions th - rough disjoint codes in projective spaces[J]. Designs, Codes and Cryptology, 2005, 37(2): 319-346

[8] Xiao Guozhen, Massey J L. A spectral characterization of correlation immune combining function[J]. IEEE Transactions on Information Theory, 1988, 34(5): 569-571

[9] Tarannikov Y. On resilient Boolean functions with maximal possible nonlinearity[C] // Proceedings of Indocrypt 2000, LNCS. Spring- Verlag, 2000, 1977: 19-30

[10] Carlet C. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions[C] // Sequences and their Applications-SETA 2001(Discrete Mathematics and Theoretical Compute Science). Berlin: Springer-Verlag, 2001: 131-144

[11] 温巧燕，钮心忻，杨义先. 现代密码学中的布尔函数[M]. 北京：科学出版社，2000: 13-14

(上接第 81 页)

也不会受到影响。而且由于有些针对 HTTP 的攻击会导致系统的可用性严重偏离系统正常使用时的状态，很可能会被其它代理如可用性检测代理检测到，所以在少量检测代理失效时，增加的漏警率会很小，即：$\omega_{MD}R_{MD}(\breve{\Sigma}_{AIIDS})-\omega_{MD}R_{MD}(\breve{\Sigma}_{AIIDS})$ 很小；而当少量检测代理失效时，由它们所引起的虚警会消失，同时它们产生的抑制虚警的能力也会消失，两种作用相抵消，使得增加的虚警率比较小，即：$\omega_{FD}R_{FD}(\breve{\Sigma}_{AIIDS})-\omega_{FD}R_{FD}(\Sigma_{AIIDS})$ 比较小，因此能够满足：

$$\frac{DA(\breve{\Sigma}_{AIIDS})-DA(\Sigma_{AIIDS})}{DA(\Sigma_{AIIDS})}$$

$$=\frac{\omega_{MD}R_{MD}(\breve{\Sigma}_{AIIDS})+\omega_{FD}R_{FD}(\breve{\Sigma}_{AIIDS})-\omega_{MD}R_{MD}(\Sigma_{AIIDS})-\omega_{FD}R_{FD}(\Sigma_{AIIDS})}{\omega_{MD}R_{MD}(\Sigma_{AIIDS})+\omega_{FD}R_{FD}(\Sigma_{AIIDS})}\leqslant\Gamma$$

所以 Σ_{AIIDS} 具有健壮性。

4.4 自适应性

基于自然免疫系统克隆选择的启发，在 Σ_{AIIDS} 利用规则优化组件使得检测器的规则集合能够根据当前的入侵自动调节，经常能够检测到攻击的规则具有更高的适应度，而在一定时间范围内，很少或根本没有检测到入侵的规则具有更低的适应度，最终将会被移出常用规则库，这样就会使得当前规则库中的规则能够更好地适应它所经常遇到的攻击。基于免疫机理的入侵检测系统 Σ_{AIIDS} 大量采用异常检测方法检测攻击，而规则优化组件对通过异常检测检测到的攻击能够提取其特征形成新的滥用检测规则，从而当这些入侵再次出现时能够直接通过规则匹配来检测到。由于优化组件提取已知入侵的特征形成新的滥用检测规则，当相同入侵再次出现时，Σ_{AIIDS} 能够直接通过滥用检测规则检测到，从而减少了异常检测所需的时间和资源，因此满足入侵检测系统的自适应性的第二和第三个条件。由于经过一段时间，规则库中的规则都是具有较高适应度的，使得此时的检测系统比原系统有更强的检测能力，因此满足入侵检测系统的自适应性的第一个条件。因此可以得出 Σ_{AIIDS} 具有自适应性的结论。

结束语 本文用四元组定义了自然免疫系统和入侵检测系统的数学模型，并给出了入侵检测系统检测性能、健壮性、自适应性以及动态防护性等概念的数学描述，基于自然免疫系统的多层次性、多样性、独特性、协同性、动态性、分布性和克隆选择等机理提出基于免疫机理的入侵检测系统 AIIDS 的总体设计。我们已经根据该设计用 c 语言实现了 AIIDS 的原型，并对一些标准入侵检测数据以及自己收集到的数据进行了实验，实验结果[5]证实了 AIIDS 检测的有效性。

参 考 文 献

[1] Axelsson S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection[J]. ACM Transactions on Information and System Security, 2000, 3(3): 186-205

[2] Hofmeyr S A. An Interpretative Introduction to the Immune System[M] // I. Cohen, L. Segel, eds. Design Principles for the Immune System and other Distributed Autonomous Systems. Oxford University Press, 2000

[3] Forrest S, Hofmeyr S, Somayaji A. Computer Immunology[J]. Communications of the ACM, 1997, 40(10): 88-96

[4] Hofmeyr S A. A Immunological Model of Distributed Detection and its Application to Computer Security[D]. Department of Computer Sciences, University of New Mexico, Albuquerque, NM, April 1999.

[5] 闫巧，江勇，吴建平. 基于免疫机理的网络入侵检测系统的抗体生成与检测组件[J]. 计算机学报，2005, 28(10): 1601-1607