doi:10.11959/j.issn.1000-436x.2016200

一类布尔函数的代数免疫度的下界

田叶[1]，张玉清[1,2]，胡予濮[1]，伍高飞[1]
(1. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 中国科学院大学国家计算机网络入侵防范中心，北京 101408)

摘 要：代数免疫度是衡量布尔函数抵抗代数攻击的重要指标。最近，Mesnager 等研究了布尔函数的零化子与函数所对应循环码最小距离之间的联系，代数免疫度的下界可以由对应的循环码的最小距离得到。解决了 Mesnager 提出的一个公开问题，给出了一类特定函数的零化子次数的下界，并得到一类布尔函数的代数免疫度的下界。
关键词：密码学；布尔函数；零化子；代数免疫度；循环码；最小距离
中图分类号：TN918 **文献标识码**：A

New bound of algebraic immunity of a class of Boolean function

TIAN Ye[1], ZHANG Yu-qing[1,2], HU Yu-pu[1], WU Gao-fei[1]
(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China)

Abstract: Algebraic immunity quantified the resistance of a Boolean function to the algebraic attack. Recently, Mesnager, et al showed that there were direct linked between the annihilators used in algebraic attacks and the coding theory. They showed that the lower bound of the algebraic immunity of Boolean functions could been derived from the minimum distance of the associated cyclic codes. An open problem proposed by Mesnager is settled with a detailed proof. Also, a lower bound of algebraic immunity of a class of Boolean functions will be introduced.
Key words: cryptography, Boolean functions, annihilators, algebraic immunity, cyclic code, minimum distance

1 引言

2003 年，Courtois 和 Meier[1]在欧洲密码学年会上提出了一种针对布尔函数的代数攻击方法，对基于线性反馈移位寄存器的流密码构成了极大的威胁，这种方法的主要原理是建立初始密钥和输出密钥流比特之间的代数方程，通过线性化方法求解该超定的多变元非线性方程组以得到初始密钥。为了衡量布尔函数抵抗代数攻击的能力，代数免疫的概念也随即被引出[1]。为了抵抗代数攻击[1~3]，流密码系统中使用的布尔函数需要尽可能具有高的代数免疫度。

国内外学者对具有最高代数免疫阶的布尔函数进行了深入的研究[1~13]。Courtois 和 Meier[1]证明了 n 元布尔函数的最大代数免疫度是 $\left\lceil \frac{n}{2} \right\rceil$，达到此上界的布尔函数称为具有最优代数免疫度的函数。Dalai[4]首次构造了偶数元的具有最优代数免疫的布尔函数。Carlet 和 Feng[6]构造了一类平衡的具有最优代数免疫度的布尔函数。2010 年，Rizomiliotis[7]给出了一个关于布尔函数具有最优代数免疫度的充要条件。最近，Mesnager[13]研究了布尔函数的零化子与循环码之间的关系，将对布尔函数零化子的研究转化为对所对应循环码的最小距离的研究，为

收稿日期：2016-05-11；**修回日期**：2016-08-24
基金项目：国家自然科学基金资助项目（No.61572460, No.61272481）；国家重点研究计划基金资助项目（No.2016YFB0800703）；国家发展改革委员会信息安全专项基金资助项目（No.(2012)1424）；国家 111 计划基金资助项目（No.B16037）
Foundation Items: The National Natural Science Foundation of China (No.61572460, No.61272481), The National Key Research and Development Project (No.2016YFB0800703), The National Information Security Special Projects of National Development, The Reform Commission of China (No.(2012)1424), China 111 Project (No.B16037)

研究布尔函数的代数免疫提供了一种新方法。

本文解决了 Mesnager 提出的一个公开问题，给出了一类特定函数的零化子的次数下界，并得到一类布尔函数的代数免疫度的下界。

2　预备知识

本节介绍将要用到的循环码和布尔函数相关的一些基础知识。

2.1　循环码

循环码是一类重要的线性码，在通信系统、存储设备中有着广泛的应用[14~19]。

设 n 为正整数，记 F_2 为含有 2 个元素的二元域，F_{2^n} 为 F_2 上的 n 维向量空间，F_{2^n} 为含有 2^n 个元素的有限域。

设 n、k、d 分别为正整数。记 C 是参数为 $[n,k,d]$ 的线性码，其中，码 C 的长度为 n，码 C 最小距离为 d，维数为 k。若对 C 中的任意码字进行循环移位后仍然是 C 的码字，则 C 称为循环码。

定理 1[14]　(BCH 界) α 为域 F_{2^n} 上的本原元。设 C 是循环码，其生成多项式为 $g(x)$，对于一些整数 $d\geqslant 0,\delta\geqslant 1$，满足

$$g(\alpha^b)=g(\alpha^{b+1})=\cdots=g(\alpha^{b+\delta-2})=0 \tag{1}$$

也就是说码 C 有（$\delta-1$）个 α 的相邻幂作为零点，则码 C 的最小距离 $d\geqslant\delta$。

2.2　布尔函数

在密码学中，最常用的表达布尔函数的形式是代数正规型(ANF)，表达式如式(2)所示。

$$f(x_1,x_2,\cdots,x_n)=\bigoplus_{u\in F_2^n}\alpha_u\left(\prod_{i=1}^{n}x_i^{u_i}\right) \tag{2}$$

其中，“$\oplus$”表示 F_2 上的加，$\alpha_u\in F_2$，$u=(u_1,u_2,\cdots,u_n)$，函数 $f(x)$ 的代数次数定义为代数正规型中系数不为零的次数最高的乘积项中变元的个数，即 $\max\{wt(u)|\alpha_u\neq 0\}$，记为 $\deg f$。代数次数小于等于 1 的布尔函数称为仿射函数。

n 元布尔函数的支撑集定义为 $\mathrm{supp}\{f\}=\{x\in F_2^n|f(x)=1\}$。函数 f 的汉明重量 $wt(f)$ 等于其支撑集中的元素个数。如果 $wt(f)=2^{n-1}$，则函数 f 称为平衡函数。2 个 n 元布尔函数 f 和 g 之间的汉明距离为 $wt(f\oplus g)$。n 元布尔函数 f 的非线性度 $nl(f)$ 是函数 f 与所有的 n 元仿射函数之间的汉明距离的最小值。

布尔函数 $f(x)$ 也可以看成是从 F_{2^n} 到 F_2 的一个映射，它可以唯一地表示为

$$f(x)=\sum_{i=0}^{2^n-1}\lambda_i x^i \tag{3}$$

其中，对于 $i\in\{1,\cdots,2^n-2\}$，$\lambda_{2i\bmod(2^n-1)}=\lambda_i^2$，并且 $\lambda_0,\lambda_{2^n-1}\in F_2$。函数的代数次数为 $\max\limits_{\lambda_i\neq 0}wt_2(i)$，其中，$wt_2(i)$ 为 i 的二进制表达式中 1 的个数。

定义 1[1]　令 $f(x)\in F_{2^n}$，如果存在一个非零的函数 $g(x)\in F_{2^n}$，使 $f(x)g(x)=0$，那么称 $g(x)$ 是 $f(x)$ 的零化子。函数 $f(x)$ 的代数免疫度 $AI(f)$ 定义为 $f(x)$ 与 $f(x)+1$ 的零化子的最小次数。

本文标记 $MDA(f)$ 为函数 f 的零化子的最小次数，$MDA(f+1)$ 为函数 $f+1$ 的零化子的最小次数。因此 $f(x)$ 的代数免疫度可以记为

$$AI(f)=\min(MDA(f),MDA(f+1)) \tag{4}$$

3　主要结果

布尔函数在编码理论中具有重要的作用[13,20~22]。例如一类著名的二元码 Reed-Muller 码就可以通过布尔函数获得。最近，Mesnager 等[13]把对布尔函数零化子的研究转化为对循环码的研究，为研究代数免疫提供了一种新方法。本节详细介绍了 Mesnager 提出的公开问题的具体方法。首先介绍一些关于循环码和代数免疫关系的已有的结论，更多的细节见文献[13]。

定义 2[13]　记 S 为 F_{2^n} 的一个子集，任意 $x\in S$ 时，记 $C(S)$ 为所有 $F_{2^n}^{2^n}$ 中满足 $\sum\limits_{i=0}^{2^n-1}\mu_i x^i=0$ 的 $(\mu_0,\mu_1,\cdots,\mu_{2^n-1})$ 的集合，$\widehat{C}(S)$ 为所有满足 $\sum\limits_{i=1}^{2^n-1}\mu_i x^i=0$ 的 $(\mu_1,\mu_2,\cdots,\mu_{2^n-1})$ 的集合。

推论 1[13]　记 $S\subset F_{2^n}$，则 $C(S)$ 为长度为 2^n 的线性码，$\widehat{C}(S)$ 为长度 2^n-1 的循环码。

记 $g:F_{2^n}\to F_2$ 为 F_{2^n} 上布尔函数 f 的零化子，$g(x)$ 可以表示为 $g(x)=\sum\limits_{i=0}^{2^n-1}\mu_i x^i$，其中，对于 $i\in\{1,2,\cdots,2^n-2\}$，$\mu_{2i}=\mu_i^2$，$\mu_0,\mu_{2^n-1}\in F_2$。根据零化子的定义，当任意 $x\in\mathrm{supp}(f)$，$g(x)=\sum\limits_{i=0}^{2^n-1}\mu_i x^i=0$。当 $f(0)=1$ 时，$g(0)=0$，$\mu_0=0$，$g(x)=$

$\mu_0+\sum_{i=1}^{2^n-1}\mu_i x^i=\sum_{i=1}^{2^n-1}\mu_i x^i=0$。因此，$(\mu_1,\mu_2,\cdots,\mu_{2^n-1})$为$\widehat{C}(\mathrm{supp}(f))$的一个码字。记$\hat{g}(x)=\sum_{i=1}^{2^n-1}\mu_i x^i=0$。但并不是$\widehat{C}(\mathrm{supp}(f))$中的每一个码字都能对应函数 f 的一个零化子。本文记 B 为$(\mu_0,\mu_1,\cdots,\mu_{2^n-1})$的集合，其中，$(\mu_0,\mu_1,\cdots,\mu_{2^n-1})\in F_2\times F_{2^n}^{2^n-2}\times F_2$，且满足$i\in\{1,2,\cdots,2^n-2\}$时，$\mu_{2i}=\mu_i^2$，$\mu_0,\mu_{2^n-1}\in F_2$。

推论 2[13] 布尔函数 $f:F_{2^n}\to F_2$ 且满足 $f(0)=1$，那么集合$\widehat{C}(\mathrm{supp}(f))\cap B$与函数 f 的零化子一一对应。

记 $S_f=\mathrm{supp}(f)\cap F_{2^n}^*$，于是当 $f(0)=1$ 时，$\mathrm{supp}(f)=\{0\}\cup S_f$；当 $f(0)=0$时，$\mathrm{supp}(f)=S_f$。记 $S_{1+f}=\{x\in F_{2^n}^*\,|\,1+f(x)=1\}$，对于 $x\in S_{1+f}$，记$\widehat{C}(S_{1+f})$为满足$\hat{g}(x)=\sum_{i=1}^{2^n-1}\mu_i x^i=0$的集合$(\mu_1,\mu_2,\cdots,\mu_{2^n-1})$。

定理 2[13] 设函数 $f:F_{2^n}\to F_2$ 满足 $f(0)=1$，记 δ 为 $\widehat{C}(S_f)$ 的最小距离。设 d 为满足不等式$\sum_{i=1}^{d}\binom{n}{i}\geqslant\delta$的最小正整数，则 $MDA(f)\geqslant d$。

定理 3[13] 设函数 $f:F_{2^n}\to F_2$ 满足 $f(0)=0$，记 δ 为 $\widehat{C}(S_f)$ 的最小距离。设 d 为满足不等式$\sum_{i=1}^{d}\binom{n}{i}\geqslant\delta$的最小正整数，则 $MDA(f)\geqslant d-1$。

定理 4[13] 设函数$f:F_{2^n}\to F_2$，记δ为$\widehat{C}(S_f)$的最小距离，记δ'为$\widehat{C}(S_{1+f})$的最小距离。p 为满足不等式$\sum_{i=1}^{p}\binom{n}{i}\geqslant\delta$的最小正整数，$p'$为满足不等式$\sum_{i=1}^{p'}\binom{n}{i}\geqslant\delta'$的最小正整数。因此，集合 S_f 对应的布尔函数的代数免疫度 $AI(f)$ 具有如下的下界。

1) 如果 $f(0)=1$，则 $AI(f)\geqslant\min(p,p'-1)$。

2) 如果 $f(0)=0$，则 $AI(f)\geqslant\min(p-1,p')$。

设 b 和 δ 为 2 个非负整数。记 $V(\alpha,b,\delta-1)=\{\alpha^b,\alpha^{b+1},\cdots,\alpha^{b+\delta-2}\}$，其中，$\alpha$ 为 F_{2^n} 中的一个本原元，记 $N=2^n-1$。

文献[13]提出的公开问题具体描述如下，给定布尔函数 $f:F_{2^n}\to F_2$，t、b、k、δ 均为正整数，m 为与 N 互素的正整数，设集合 S_f 为

$$S_f=V(\alpha,b,\delta-1)\cup V(\alpha,b+m,\delta-1)\cup\cdots\cup V(\alpha,b+km,\delta-1)$$

那么就存在函数 1+f 的零化子的最小次数的下界如何表示的问题。

注：当 $m\leqslant\delta-2$ 时，$V(\alpha,b,\delta-1)\cup V(\alpha,b+m,\delta-1)\cup\cdots\cup V(\alpha,b+km,\delta-1)=V(\alpha,b,km+\delta-1)$。下文，只考虑 $m>\delta-2$ 的情形。

为了解决这个问题，首先对文献[13]中的定理进行完善得到定理 5。

定理 5 布尔函数 $f:F_{2^n}\to F_2$，假设

$$S_f=V(\alpha,b,\delta-1)$$

于是有：

1) 当 $f(0)=1$时，$MDA(f)\geqslant p$；

2) 当 $f(0)=0$时，$MDA(f)\geqslant p-1$。

其中，p 是满足不等式$\sum_{i=1}^{p}\binom{n}{i}\geqslant\delta$的最小正整数。

证明 根据定义有

$$S_f=V(\alpha,b,\delta-1)=\{\alpha^b,\alpha^{b+1},\cdots,\alpha^{b+\delta-2}\}$$

当$x\in S_f$且$f(0)=1$时，$\hat{g}(x)=\sum_{i=1}^{2^n-1}\mu_i x^i=0$，即$\widehat{C}(S_f)$含有$(\delta-1)$个$\alpha$的相邻幂作为零元，根据定理 1 得到$\widehat{C}(S_f)$的最小距离大于$\delta-1$，即$\widehat{C}(S_f)$的最小距离至少为$\delta$。再由定理 3 和定理 4，便可以推导出定理 5，完成了证明。

定理 6 对文献[13]中的定理进行了完善。

定理 6 布尔函数 $f:F_{2^n}\to F_2$，t、b、k、δ均为正整数，m 为与 N 互素的正整数，假设

$$S_f=V(\alpha,b,\delta-1)\cup V(\alpha,b+m,\delta-1)\cup\cdots\cup V(\alpha,b+km,\delta-1)$$

于是有：

1) 当 $f(0)=1$时，$MDA(f)\geqslant p$；

2) 当 $f(0)=0$时，$MDA(f)\geqslant p-1$。

其中，p 是满足不等式$\sum_{i=1}^{p}\binom{n}{i}\geqslant\delta+k$ 的最小正整数。

证明 根据 S_f 的定义，可得

$$\begin{cases}V(\alpha,b,\delta-1)=\{\alpha^b,\alpha^{b+1},\cdots,\alpha^{b+\delta-2}\}\\ V(\alpha,b+m,\delta-1)=\{\alpha^{b+m},\cdots,\alpha^{b+m+\delta-2}\}\\ \quad\vdots\qquad\qquad\vdots\\ V(\alpha,b+2m,\delta-1)=\{\alpha^{b+2m},\cdots,\alpha^{b+2m+\delta-2}\}\\ V(\alpha,b+km,\delta-1)=\{\alpha^{b+km},\cdots,\alpha^{b+km+\delta-2}\}\end{cases}\tag{5}$$

设集合 U 为 S_f 中 α 的所有指数的集合，即式(5)中 α 的所有指数的集合。

设整数 $d_0=k+\delta$，假设 $\widehat{C}(S_f)$ 中含有重量 ω 小于 d_0 的码字，即 $\omega<k+\delta$。由于 $\widehat{C}(S_f)$ 为循环码，某一重量为 ω 的码字可以表示为下面的码多项式 $T(x)=1+\sum_{i=1}^{\omega-1}\gamma_i x^{s_i}$，其中，$\gamma_i\in F_{2^n}$，$0<s_i<N$。

设 $X_i=\alpha^{s_i}$，$P_j=\sum_{i=1}^{\omega-1}\gamma_i X_i^j=\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}$，$j\in U$。

而 $T(\alpha^j)=1+\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}=1+P_j=0$，所以 $P_j=-1$。

设 $\phi(x)=\phi_1(x)\phi_2(x)$，其中，

$$\phi_1(x)=\prod_{i_1=1}^{k}(x-X_{i_1}^m)=x^k+\phi_1^{(1)}x^{k-1}+\cdots+\phi_{k-1}^{(1)}x^1+\phi_k^{(1)} \tag{6}$$

$$\phi_2(x)=\prod_{i_2=k+1}^{\omega}(x-X_{i_2})=x^{\omega-k-1}+\phi_1^{(2)}x^{\omega-k-2}+\cdots+\phi_{\omega-k-2}^{(2)}x+\phi_{\omega-k-1}^{(2)} \tag{7}$$

因为 $(m,N)=1$，$s_i\neq 0$，所以 $X_{i_1}^m\neq 1$，$X_{i_2}\neq 1$，$\phi(1)=\phi_1(1)\phi_2(1)\neq 0$。

构造如下的等式 $\bar{Z}$

$$\begin{aligned}\bar{Z}=&(P_{b+km+(\omega-k-1)}+\phi_1^{(1)}P_{b+(k-1)m+(\omega-k-1)}+\cdots+\\&\phi_k^{(1)}P_{b+(\omega-k-1)})+\phi_1^{(2)}(P_{b+km+(w-k-2)}+\\&\phi_1^{(1)}P_{b+(k-1)m+(w-k-2)}+\cdots+\phi_k^{(1)}P_{b+(w-k-2)})+\cdots+\\&\phi_{\omega-k-1}^{(2)}(P_{b+km}+\phi_1^{(1)}P_{b+(k-1)m}+\cdots+\phi_k^{(1)}P_b)\end{aligned} \tag{8}$$

将 $P_j=\sum_{i=1}^{\omega-1}\gamma_i X_i^j=\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}$ 代入式(8)，对式(8)进行化简，得到

$$\begin{aligned}\bar{Z}&=\sum_{i=1}^{\omega}\gamma_i X_i^b\phi_1(X_i^m)\phi_2(X_i)\\&=\sum_{i=1}^{\omega}\gamma_i X_i^b\left(\prod_{i_1=1}^{k}(X_i^m-X_{i_1}^m)\prod_{i_2=k+1}^{\omega}(X_i-X_{i_2})\right)\\&=\left(\sum_{i=1}^{k}\gamma_i X_i^b+\sum_{i=k+1}^{\omega}\gamma_i X_i^b\right)\phi_1(X_i^m)\phi_2(X_i)\\&=0\end{aligned} \tag{9}$$

当 $j\in U$，$P_j=-1$，前面假设 $\omega<k+\delta$，所以 $\omega-k-1<\delta-1$，因此式(8)可以转化为

$$\begin{aligned}\bar{Z}&=(-1-\phi_1^{(1)}-\cdots-\phi_k^{(1)})+\phi_1^{(2)}(-1-\phi_1^{(1)}-\cdots-\phi_k^{(1)})+\\&\quad\cdots+\phi_{\omega-k-1}^{(2)}(-1-\phi_1^{(1)}-\cdots-\phi_k^{(1)})\\&=-\phi_1(1)\phi_2(1)\\&=-\phi(1)\end{aligned} \tag{10}$$

结合式(9)和式(10)，可以得出 $\phi(1)=0$，然而与 $\phi(1)\neq 0$ 是矛盾的。因此，假设 $\omega<k+\delta$ 是错误的，从而 $\omega\geqslant k+\delta$，也就是说 $\widehat{C}(S_f)$ 中不存在任何重量 ω 小于 $k+\delta$ 的码字，即 $\widehat{C}(S_f)$ 的最小距离至少为 $k+\delta$。

再根据定理 2 和定理 3，得到定理 6，即完成了证明。

定理 7 给出公开问题的答案，并利用证明定理 6 的方法对其进行证明。

定理 7　布尔函数 $f:F_{2^n}\to F_2$，t,b,k,δ 均为正整数，m 为与 N 互素的正整数，假设

$$S_f=V(\alpha,b,\delta-1)\cup V(\alpha,b+m,\delta-1)\cup\cdots\cup V(\alpha,b+km,\delta-1)$$

于是有如下情况。

1) 当 $m(1+k)<2^n-1$ 时

① 如果 $f(0)=1$，则 $MDA(1+f)\geqslant p$；

② 如果 $f(0)=0$，则 $MDA(1+f)\geqslant p-1$。

其中，p 满足不等式 $\sum_{i=1}^{p}\binom{n}{i}\geqslant k+m-\delta+2$ 的最小正整数。

2) 当 $m(1+k)\geqslant 2^n$ 时

① 如果 $f(0)=1$，则 $MDA(1+f)\geqslant p$；

② 如果 $f(0)=0$，则 $MDA(1+f)\geqslant p-1$。

其中，p 是满足不等式 $\sum_{i=1}^{p}\binom{n}{i}\geqslant k+m-\delta+1$ 的最小正整数。

证明　由 S_f 的定义可得

$$\begin{aligned}S_{1+f}=&\{1,\alpha,\alpha^2,\cdots,\alpha^{b-1},\alpha^{b+\delta-1},\\&\cdots,\alpha^{b+m-1},\alpha^{b+m+\delta-1},\cdots,\alpha^{b+2m-1},\\&\cdots,\alpha^{b+km-1},\alpha^{b+km+\delta-1},\cdots,\alpha^{2^n-2}\}\\=&V_0\cup V_1\cup V_2\cup\cdots\cup V_{k-1}\cup\Omega\end{aligned} \tag{11}$$

其中，

$$\begin{aligned}V_0&=\{\alpha^{b+\delta-1},\alpha^{b+\delta},\cdots,\alpha^{b+m-1}\}\\&=\{\alpha^{b+\delta-1},\alpha^{b+\delta},\cdots,\alpha^{b+\delta-1+(m-\delta)}\}\\&=V(\alpha,b+\delta-1,m-\delta+1)\end{aligned} \tag{12}$$

$$\begin{aligned}V_1&=\{\alpha^{b+m+\delta-1},\alpha^{b+m+\delta},\cdots,\alpha^{b+2m-1}\}\\&=\{\alpha^{b+m+\delta-1},\alpha^{b+m+\delta},\cdots,\alpha^{b+m+\delta-1+(m-\delta)}\}\\&=V(\alpha,b+m+\delta-1,m-\delta+1)\end{aligned} \tag{13}$$

$$\begin{aligned}V_2&=\left\{\alpha^{b+2m+\delta-1},\alpha^{b+2m+\delta},\cdots,\alpha^{b+3m-1}\right\}\\&=\left\{\alpha^{b+2m+\delta-1},\alpha^{b+2m+\delta},\cdots,\alpha^{b+2m+\delta-1+(m-\delta)}\right\}\\&=V\left(\alpha,b+2m+\delta-1,m-\delta+1\right)\end{aligned}\tag{14}$$

$$\vdots$$

$$\begin{aligned}V_{k-1}&=\left\{\alpha^{b+(k-1)m+\delta-1},\alpha^{b+(k-1)m+\delta},\cdots,\alpha^{b+km-1}\right\}\\&=\left\{\alpha^{b+(k-1)m+\delta-1},\alpha^{b+(k-1)m+\delta},\cdots,\alpha^{b+(k-1)m+\delta-1+(m-\delta)}\right\}\\&=V\left(\alpha,b+(k-1)m+\delta-1,m-\delta+1\right)\end{aligned}\tag{15}$$

$$\begin{aligned}\Omega&=\left\{\alpha^{b+km+\delta-1},\alpha^{b+km+\delta},\cdots,\alpha^{2^n-2},1,\alpha,\cdots,\alpha^{b-1}\right\}\\&=\left\{\alpha^{b+km+\delta-1},\cdots,\alpha^{2^n-2},\alpha^{2^n-1},\alpha^{2^n},\cdots,\alpha^{2^n-1+b-1}\right\}\\&=\left\{\alpha^{b+km+\delta-1},\cdots,\alpha^{2^n},\cdots,\alpha^{b+km+\delta-1+\left(2^n-km-\delta-1\right)}\right\}\\&=V\left(\alpha,b+km+\delta-1,2^n-km-\delta\right)\end{aligned}\tag{16}$$

设集合 U 为 S_{1+f} 中 α 的所有指数的集合，即式(12)~式(16)中 α 的所有指数的集合。

如果 $2^n-km-\delta=m-\delta+1$，则 $2^n-1=m(1+k)$，这与 $(m,2^n-1)=1$ 矛盾，所以 $2^n-1\neq m(1+k)$。

下面分 2 种情况考虑。

1) 当 $m(1+k)<2^n-1$ 时，设整数 $d_0=k+m-\delta+2$，假设 $\widehat{C}(S_{1+f})$ 中含有重量 ω 小于 d_0 的码字，即 $\omega<k+m-\delta+2$。令 $T(x)=1+\sum_{i=1}^{\omega-1}\gamma_i x^{s_i}$ 为某一重量为 ω 的码字的码多项式，其中，$\gamma_i\in F_{2^n}$，$0<s_i<N$。

设 $X_i=\alpha^{s_i}$，$P_j=\sum_{i=1}^{\omega-1}\gamma_i X_i^j=\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}$，当 $j\in U$ 时，$T(\alpha^j)=1+\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}=1+P_j=0$，所以 $P_j=-1$。

设 $\phi(x)=\phi_1(x)\phi_2(x)$，其中，

$$\phi_1(x)=\prod_{i_1=1}^{k}(x-X_{i_1}^m)=x^k+\phi_1^{(1)}x^{k-1}+\cdots+\phi_{k-1}^{(1)}x^1+\phi_k^{(1)}\tag{17}$$

$$\begin{aligned}\phi_2(x)=\prod_{i_2=k+1}^{\omega}(x-X_{i_2})=x^{\omega-k-1}+\\\phi_1^{(2)}x^{\omega-k-2}+\cdots+\phi_{\omega-k-2}^{(2)}x+\phi_{\omega-k-1}^{(2)}\end{aligned}\tag{18}$$

因为 $s_i\neq 0$，$(m,N)=1$，所以 $X_{i_1}^m\neq 1$，$X_{i_2}\neq 1$，$\phi(1)=\phi_1(1)\phi_2(1)\neq 0$。

令整数 $l=b+\delta-1$，构造等式 $\bar{Z}$ 为

$$\begin{aligned}\bar{Z}=&(P_{l+km+(\omega-k-1)}+\phi_1^{(1)}P_{l+(k-1)m+(\omega-k-1)}+\cdots+\\&\phi_k^{(1)}P_{l+(\omega-k-1)})+\phi_1^{(2)}(P_{l+km+(w-k-2)}+\\&\phi_1^{(1)}P_{l+(k-1)m+(w-k-2)}+\cdots+\phi_k^{(1)}P_{l+(w-k-2)})+\cdots+\\&\phi_{\omega-k-1}^{(2)}(P_{l+km}+\phi_1^{(1)}P_{l+(k-1)m}+\cdots+\phi_k^{(1)}P_l)\end{aligned}\tag{19}$$

将 $P_j=\sum_{i=1}^{\omega-1}\gamma_i X_i^j=\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}$ 代入式(19)，得到

$$\begin{aligned}\bar{Z}&=\sum_{i=1}^{\omega}\gamma_i X_i^b\phi_1(X_i^m)\phi_2(X_i)\\&=\sum_{i=1}^{\omega}\gamma_i X_i^l\left(\prod_{i_1=1}^{k}(X_i^m-X_{i_1}^m)\prod_{i_2=k+1}^{\omega}(X_i-X_{i_2})\right)\\&=0\end{aligned}\tag{20}$$

前面假设 $\omega<k+m-\delta+2$，即 $\omega-k-1<m-\delta+1$，并且当 $j\in U$，$P_j=-1$，所以式(19)也可以转化成式(21)。

$$\begin{aligned}\bar{Z}&=(-1-\phi_1^{(1)}-\cdots-\phi_k^{(1)})+\phi_1^{(2)}(-1-\phi_1^{(1)}-\cdots-\phi_k^{(1)})+\\&\quad\cdots+\phi_{\omega-k-1}^{(2)}(-1-\phi_1^{(1)}-\cdots-\phi_k^{(1)})\\&=-\phi_1(1)\phi_1(1)\\&=-\phi(1)\end{aligned}\tag{21}$$

结合式(20)和式(21)，可以得出 $\phi(1)=0$，然而与 $\phi(1)\neq 0$ 是矛盾的。因此，假设 $\omega<k+m-\delta+2$ 是错误的，从而 $\omega\geqslant k+m-\delta+2$，也就是说 $\widehat{C}(S_{1+f})$ 中不存在任何重量 ω 小于 $k+m-\delta+2$ 的码字，即 $\widehat{C}(S_{1+f})$ 的最小距离至少为 $k+m-\delta+2$。

2) 当 $m(1+k)\geqslant 2^n$ 时，设整数 $d_0=k+m-\delta+1$，假设 $\widehat{C}(S_{1+f})$ 中含有重量 ω 小于 d_0 的码字，即 $\omega<k+m-\delta+1$。令 $T(x)=1+\sum_{i=1}^{\omega-1}\gamma_i x^{s_i}$ 为某一重量为 ω 的码字的码多项式，其中，$\gamma_i\in F_{2^n}$，$0<s_i<N$。

设 $X_i=\alpha^{s_i}$，$P_j=\sum_{i=1}^{\omega-1}\gamma_i X_i^j=\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}$，当 $j\in U$ 时，$T(\alpha^j)=1+\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}=1+P_j=0$，所以 $P_j=-1$。

设 $\phi(x)=\phi_1(x)\phi_2(x)$，其中，

$$\phi_1(x)=\prod_{i_1=1}^{k-1}(x-X_{i_1}^m)=x^{k-1}+\phi_1^{(1)}x^{k-2}+\cdots+\phi_{k-2}^{(1)}x^1+\phi_{k-1}^{(1)}\tag{22}$$

$$\phi_2(x)=\prod_{i_2=k}^{\omega}(x-X_{i_2})=x^{\omega-k}+\phi_1^{(2)}x^{\omega-k-1}+\cdots+\phi_{\omega-k-1}^{(2)}x+\phi_{\omega-k}^{(2)} \tag{23}$$

因为 $s_i\neq 0$，$(m,N)=1$，所以 $X_{i_1}^m\neq 1$，$X_{i_2}\neq 1$，$\phi(1)=\phi_1(1)\phi_2(1)\neq 0$。

令整数 $l=b+\delta-1$，构造如下的等式 $\overline{Z}$。

$$\begin{aligned}\overline{Z}=&(P_{l+(k-1)m+(\omega-k)}+\phi_1^{(1)}P_{l+(k-2)m+(\omega-k)}+\cdots+\\&\phi_{k-1}^{(1)}P_{l+(\omega-k)})+\phi_1^{(2)}(P_{l+(k-1)m+(w-k-1)}+\\&\phi_1^{(1)}P_{l+(k-2)m+(w-k-1)}+\cdots+\phi_{k-1}^{(1)}P_{l+(w-k-1)})+\cdots+\\&\phi_{\omega-k}^{(2)}(P_{l+(k-1)m}+\phi_1^{(1)}P_{l+(k-2)m}+\cdots+\phi_{k-1}^{(1)}P_l)\end{aligned} \tag{24}$$

将 $P_j=\sum_{i=1}^{\omega-1}\gamma_i X_i^j=\sum_{i=1}^{\omega-1}\gamma_i\alpha^{js_i}$ 代入式(24)，对式(24)进行化简，得到式(25)。

$$\begin{aligned}\overline{Z}&=\sum_{i=1}^{\omega}\gamma_i X_i^b\phi_1(X_i^m)\phi_2(X_i)\\&=\sum_{i=1}^{\omega}\gamma_i X_i^l\left(\prod_{i_1=1}^{k-1}(X_i^m-X_{i_1}^m)\prod_{i_2=k}^{\omega}(X_i-X_{i_2})\right)\\&=0\end{aligned} \tag{25}$$

前面假设 $\omega<k+m-\delta+1$，即 $\omega-k-1<m-\delta$，当 $j\in U$，$P_j=-1$，所以式(24)可以转化成式(26)。

$$\begin{aligned}\overline{Z}=&(-1-\phi_1^{(1)}-\cdots-\phi_{k-1}^{(1)})+\\&\phi_1^{(2)}(-1-\phi_1^{(1)}-\cdots-\phi(1))+\cdots+\\&\phi_{\omega-k}^{(2)}(-1-\phi_1^{(1)}-\cdots-\phi_{k-1}^{(1)})\\=&-\phi_1(1)\phi_1(1)\\=&-\phi(1)\end{aligned} \tag{26}$$

结合式(25)和式(26)，可以得出 $\phi(1)=0$，然而与前面 $\phi(1)\neq 0$ 是矛盾的。因此假设 $\omega<k+m-\delta+1$ 是错误的，也就是说 $\widehat{C}(S_{1+f})$ 中不存在任何重量 ω 小于 $k+m-\delta+1$ 的码字，即 $\widehat{C}(S_{1+f})$ 的最小距离至少为 $k+m-\delta+1$。再根据定理 2 和定理 3，就得到了定理 7。

结合布尔函数的代数免疫度的定义 $AI(f)=\min(MDA(f),MDA(1+f))$ 以及定理 6 和定理 7，本文得到了一类布尔函数的代数免疫度的一个下界。

定理 8　函数 $f:F_{2^n}\to F_2$，t、b、k、δ 均为正整数，m 为与 N 互素的正整数，假设

$$\begin{aligned}S_f=&V(\alpha,b,\delta-1)\cup V(\alpha,b+m,\delta-1)\cup\\&\cdots\cup V(\alpha,b+km,\delta-1)\end{aligned}$$

于是有如下情况。

1) 当 $m(1+k)<2^n-1$ 时

① 如果 $f(0)=0$，则 $AI(f)\geqslant\min(p,\hat{p}-1)$；

② 如果 $f(0)=1$，则 $AI(f)\geqslant\min(p-1,\hat{p})$。

其中，p 是满足不等式 $\sum_{i=1}^{p}\binom{n}{i}\geqslant\delta+k$ 的最小正整数，$\hat{p}$ 是满足不等式 $\sum_{i=1}^{\hat{p}}\binom{n}{i}\geqslant k+m-\delta+2$ 的最小正整数。

2) 当 $m(1+k)\geqslant 2^n$ 时

① 如果 $f(0)=0$，则 $AI(f)\geqslant\min(p,\hat{p}-1)$；

② 如果 $f(0)=1$，则 $AI(f)\geqslant\min(p-1,\hat{p})$。

其中，p 是满足不等式 $\sum_{i=1}^{p}\binom{n}{i}\geqslant\delta+k$ 的最小正整数，$\hat{p}$ 是满足不等式 $\sum_{i=1}^{\hat{p}}\binom{n}{i}\geqslant k+m-\delta+1$ 的最小正整数。

4　结束语

布尔函数在密码学中有着重要的作用。一个好的布尔函数需要具有高的代数免疫度以抵抗代数攻击。如何构造具有高的代数免疫度的布尔函数仍然是一个重要的问题。本文主要研究了布尔函数零化子与循环码最小距离之间的关系，解决了 Mesnager 提出的一个公开问题，即给出特定布尔函数的零化子次数的下界，并且给出了一类布尔函数的代数免疫度的下界。在未来的工作中，考虑利用一些具有优良性质的循环码来构造具有最优代数免疫度的布尔函数是非常有意义的。

参考文献：

[1] COURTOIS N, MEIER W. Algebraic attacks on stream ciphers with linear feedback[C]//Cryptology-Eurocrypt 2003, LNCS 2656. Berlin: Springer-Verlag, 2003: 345-359.

[2] ARMKNECHT F, KRAUSE M.Algebraic attacks on combiners with memory[C]//Cryptology-Crypto. 2003: 162-175.

[3] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[C]//Cryptology -Eurocrypt 2004, LNCS 3027. 2004: 474-491.

[4] DALAI D, MAITRA S, SARKAR S. Cryptographically significant Boolean functions:construction and analysis in terms of algebraic immunity[J]. Fast Software Encryption , 2005, 3557:98-111.

[5] CARLET C, DALAI D, GUPTA C. Algebraic immunity for cryptographically significant Boolean function: analysis and construction[J]. IEEE Transactions on Information Theory, 2006, 52(7):3105-3121.

[6] CARLET C, FENG K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks

and good nonlinearity[C]//Cryptology-Asiacrypt 2008, LNCS 5350. 2008, 5350:425-440.

[7] RIZOMILIOTIS P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation[J]. IEEE Trans Information Theory, 2010, 56(8):4014-4024.

[8] TU Z, DENG Y. A conjecture on binary string and its applications on constructing Boolean functions of optimal algebraic immunity [J]. Designs Codes and Cryptography, 2011, 60(1): 1-14.

[9] HELLESTH T, RONJOM S. Simplifying algebraic attacks with univariate analysis[C]//Information Theory and Applications Workshop (ITA). 2011:1-7.

[10] TANG D, CARLET C, TANG X. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks[J]. IEEE Trans Inf Theory, 2013, 59(59):653-664.

[11] LIN J, WANG M, LI Y. On annihilators in fewer variables:basic theory and applications[J]. Chinese Journal of Electronics, 2013, 22(3): 489-494.

[12] 欧智慧，赵亚群，李旭．一类密码函数的构造与分析[J].通信学报,2013, 4(4): 106-113.
OU Z H, ZHAO Y Q, LI X. Construction and analysis of one class of cryptographic functions[J]. Journal on Communications, 2013, 34(4): 106-113.

[13] MESNAGER S. A note on linear codes and algebraic immunity of Boolean Functions[C]//21st International Symposium on Mathematical Theory of Networks and Systems. 2014.

[14] MACWILLIAMS F,SLOANE N. The theory of error-correcting Codes[M]. North-Holland Mathematical Library. Amsterdam, The Netherlands: North-Holland, 1977.

[15] HUFFMAN W, PLESS V. Fundamentals of error-correcting codes[M]. Cambridge, UK: Cambridge Univ. Press, 2003.

[16] BETTI E, SALA M. A new bound for the minimum distance of a cyclic code from its defining set[J].IEEE Trans Information Theory, 2006, 52(8):3700-3706.

[17] BETTEN A, BRAUN M, FRIPERTINGER H. Error- correcting linear codes[M]. Berlin,Germany: Springer- Verlag, 2006.

[18] GAO J, HU Y, LI X. Linear span of the optimal frequency hopping sequences from irreducible cyclic Codes[J]. Chinese Journal of Electronics, 2015, 24(4): 818-823.

[19] DING C, DU X, ZHOU A. The bose and minimum distance of a class of BCH codes[J]. IEEE Trans Information Theory, 2015, 61(5): 2351- 2356.

[20] FENG X,GONG G. On algebraic immunity of trace inverse functions on finite fields of characteristic two[J]. Journal of Systems Science and Complexity, 2016, 29(1):272-288.

[21] WU D,QI W. On the spectral immunity of periodic sequences restricted to binary annihilators[J]. Designs Codes and Cryptography, 2016, 78(2):533-545.

[22] DING C.A construction of binary linear codes from Boolean functions[J]. Discrete Mathematics, 2016, 339(9): 2288-2303.

作者简介：

田叶（1987-），女，山西平遥人，西安电子科技大学博士生，主要研究方向为布尔函数、序列密码的分析与构造。

张玉清（1966-），男，陕西宝鸡人，博士，中国科学院大学教授、博士生导师，主要研究方向为网络与信息系统安全。

胡予濮（1955-），男，河南濮阳人，西安电子科技大学教授、博士生导师，主要研究方向为序列密码与分组密码、网络安全协议的设计与分析。

伍高飞（1987-），男，河南灵宝人，西安电子科技大学博士生，主要研究方向为序列设计和密码学。