具有最优代数免疫度的 2^m 个变量的对称 Boolean 函数

廖群英^{①②*}, 冯克勤^②, 刘峰^②

① 四川师范大学数学与软件科学学院, 成都 610066;

② 清华大学数学科学系, 北京 100084

E-mail: liao_qunying@yahoo.com.cn, kfeng@math.tsinghua.edu.cn, fengliu@gmail.com

收稿日期: 2009-08-21; 接受日期: 2010-08-26; * 通信作者

国家自然科学基金重大项目 (批准号: 10990011)、教育部博士点专项基金 (批准号: 20095134120001) 和四川省教育厅重点项目 (批准号: 09ZA087) 联合资助

摘要 本文给出了 2^m 个变量的对称 Boolean 函数 f 具有最优代数免疫度 $AI_{2^m}(f) = 2^{m-1}$ 的一个充分必要条件. 由此得到一个递归公式, 从而构造出全部具有最优代数免疫度的 2^m 个变量的对称 Boolean 函数 ($m \geq 2$). 最后证明了这样的 Boolean 函数的个数为 $3 \cdot 2^m$.

关键词 对称 Boolean 函数 代数免疫度 密码学

MSC (2000) 主题分类 11T30, 11T55

1 引言

近年来, 流密码体制中提出一种成功的攻击方式 — 代数攻击^[1-5]. 为抵抗代数攻击, Meier 等^[5]、Batten^[6] 以及 Dalai 等^[7] 引进了 Boolean 函数的代数免疫度的概念. 几类代数免疫度大的 Boolean 函数可以很好的抵抗代数攻击^[5,7-9], 对称 Boolean 函数更得到了深入的研究^[10-12].

设 B_n 为全体 n 个变量的 Boolean 函数 $f = f(x_1, \dots, x_n) : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ 构成的函数环, SB_n 为全体 n 个变量的对称 Boolean 函数构成的集合. $f \in B_n$ 的代数免疫度 $AI_n(f)$ 定义为:

$$AI_n(f) = \min\{\deg g \mid 0 \neq g \in B_n, fg = 0 \text{ 或者 } (f+1)g = 0\},$$

其中 $\deg g$ 是把函数 g 表示为多项式

$$g(x_1, \dots, x_n) = \sum_{a=(a_1, \dots, a_n) \in \mathbb{F}_2^n} c(a)x_1^{a_1} \cdots x_n^{a_n} \quad (c(a) \in \mathbb{F}_2)$$

形式时的代数次数. 当 $g = 0$ 时, 规定 $\deg(0) = -\infty$. 由 $f(f+1) = f^2 + f = f + f = 0$ 可知 $AI_n(f) \leq \deg f$. 熟知, 对于任意的 $f \in B_n$, $AI_n(f) \leq \lfloor \frac{n+1}{2} \rfloor$ (参见文献 [7]).

任意对称 Boolean 函数 $f \in SB_n$ 均可唯一表示为

$$f = \sum_{i=0}^n \lambda_f(i) \sigma_i^{(n)} \quad (\lambda_f(i) \in \mathbb{F}_2),$$

引用格式: Liao Q Y, Feng K Q, Liu F. On 2^m -variable symmetric Boolean functions with maximum algebraic immunity 2^{m-1} (in Chinese). Sci Sin Math, 2010, 40(10): 929–942, doi: 10.1360/012009-617

其中 $\sigma_i^{(n)}$ 表示 n 个变量 $x_1, \dots, x_n$ 的 i 次初等对称多项式

$$\sigma_i^{(n)} = \sigma_i^{(n)}(x_1, \dots, x_n) = \sum_{1 \leq a_1 < \dots < a_i \leq n} x_{a_1} \cdots x_{a_i}.$$

另一方面, $f \in SB_n$ 也可唯一表示为向量值的形式:

$$v_f = (v_f(0), \dots, v_f(n)) \in \mathbb{F}_2^{n+1},$$

其中 $v_f(i)$ 为函数 f 在变量 $a \in \mathbb{F}_2^n$ 时的取值 $f(a)$, 其中 a 的 Hamming 重量为 i .

$\lambda_f = (\lambda_f(0), \dots, \lambda_f(n)) \in \mathbb{F}_2^{n+1}$ 与 $v_f = (v_f(0), \dots, v_f(n)) \in \mathbb{F}_2^{n+1}$ 之间的关系可由 Lucas 定理得到. 设整数 $a, b \geq 0$ 的 2-adic 展开式为

$$a = a_0 + a_1 2 + \dots + a_l 2^l, \quad b = b_0 + b_1 2 + \dots + b_l 2^l \quad (a_i, b_i \in \{0, 1\}).$$

若记 $a \preceq b$ 为 $a_i \leq b_i$ ($0 \leq i \leq l$), 则由 Lucas 定理可知

$$\binom{a}{b} = 1 \in \mathbb{F}_2 \Leftrightarrow b \preceq a. \quad (1.1)$$

因此, 对于 $f \in B_n$, 以及 Hamming 重量为 $w_H(v) = i$ ($0 \leq i \leq n$) 的向量 $v \in \mathbb{F}_2^n$, 有

$$v_f(i) = f(v) = \sum_{j=0}^n \lambda_f(j) \sigma_j^{(n)}(v) = \sum_{j=0}^n \lambda_f(j) \binom{i}{j} = \sum_{j=0, j \preceq i}^i \lambda_f(j). \quad (1.2)$$

再由逆变换可得

$$\lambda_f(i) = \sum_{j=0, j \preceq i}^i v_f(j). \quad (1.3)$$

进而, 若 $f \in SB_n$ 并且 $f \neq 0$, 则 $\deg f$ 为满足 $\lambda_f(i) \neq 0$ 的最大值 i .

引理 1.1^[13] 设 $l \geq 1, f \in SB_n$. 若 $\deg f < 2^l$, 则 v_f 的周期为 2^l , 即对于任意的 $i, 0 \leq i \leq n - 2^l, v_f(i) = v_f(i + 2^l)$.

文献 [13] 中证明了: 对于任意的奇数 $n \geq 3$, 具有最大代数免疫度 $\frac{n+1}{2}$ 的 n 个变量对称 Boolean 函数只有两个: f 和 $f+1$. 其中 f 由下式给出:

$$v_f(i) = \begin{cases} 0, & 0 \leq i \leq \frac{n-1}{2}, \\ 1, & \frac{n+1}{2} \leq i \leq n. \end{cases}$$

另一方面, 当 n 为偶数时, 已经找到许多 n 元对称 Boolean 函数, 其代数免疫度达到最大值 $AI_n(f) = \frac{n}{2}$, 给出这种函数的几个必要条件^[5,7,10]. 能否完全确定全部偶数个变量的具有最大代数免疫度的对称 Boolean 函数仍然是一个尚未解决的公开问题.

本文对于 $n = 2^m$ 的情形解决这个问题. 通过给出集合

$$A(m) = \left\{ f \in SB_n \mid AI_n(f) = \frac{n}{2} \right\} \quad (n = 2^m)$$

的一个良好特性, 得到由 $A(m-1)$ 计算 $A(m)$ 的一个简单的递归公式, 并由此决定了 $A(m)$ 的大小 (本文的定理 3.2). 从而完全确定了具有最优代数免疫度的全部 2^m 个变量的对称 Boolean 函数及其计数.

2 $AI_n(f) \geq d$ 的对称 Boolean 函数 $f \in SB_n$ 的一般性质

设 $n \geq 2, N = \{0, 1, \dots, n\}$. 对任意 $d, 1 \leq d \leq [\frac{n+1}{2}]$, 本节给出对称 Boolean 函数 $f \in SB_n$ 的代数免疫度满足 $AI_n(f) \geq d$ 的一个判别准则. 为此, 首先引进如下概念.

定义 2.1 定义 Boolean 函数 $f \in B_n$ 的重量支撑为

$$WS(f) = \{i \in N \mid \text{存在 } a \in \mathbb{F}_2^n, w_H(a) = i \text{ 使得 } f(a) = 1\},$$

其中 $w_H(a) = \#\{l \mid 1 \leq l \leq n, a_l = 1\}$ 为向量 $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$ 的 Hamming 重量. 容易看出: 当 f 为对称函数时, $WS(f) = \{i \mid 0 \leq i \leq n, v_f(i) = 1\}$.

对于 Boolean 函数 $f \in SB_n, g \in B_n$, 由定义 2.1 易知:

$$\begin{aligned} fg = 0 &\Leftrightarrow \text{如果存在 } a \in \mathbb{F}_2^n, w_H(a) = i \text{ 使得 } g(a) = 1, \text{ 则 } v_f(i) = 0 \\ &\Leftrightarrow WS(g) \subseteq \overline{WS(f)}, \end{aligned}$$

其中 $\overline{WS(f)} = N \setminus WS(f)$ 表示集合 $WS(f)$ 在 $N = \{0, 1, \dots, n\}$ 中的补集. 类似可得

$$(f+1)g = 0 \Leftrightarrow WS(g) \subseteq \overline{WS(f+1)} = WS(f).$$

由此, 可得如下引理:

引理 2.2 设 $n \geq 2, 1 \leq d \leq [\frac{n+1}{2}], f \in SB_n$. 则对任意的 $g \in B_n, 0 \leq \deg g \leq d-1$, 有

$$AI_n(f) \geq d \Leftrightarrow WS(g) \not\subseteq WS(f) \text{ 并且 } WS(g) \not\subseteq \overline{WS(f)}.$$

下面的引理 2.3 表明引理 2.2 中的函数 g 可以只由 B_n 的某个特定子集合决定.

引理 2.3 设 $n \geq 2, f \in SB_n, 0 \neq g \in B_n$. 若 $fg = 0$, 则存在 $0 \neq g' \in B_n, \deg g' \leq \deg g$ 使得 $fg' = 0$ 且 g' 有以下特定形式:

$$g'(x_1, \dots, x_n) = p_b(x_1, \dots, x_{2b})h(x_{2b+1}, \dots, x_n),$$

其中 $0 \leq b \leq \frac{n}{2}, h \in SB_{n-2b}$,

$$p_b(x_1, \dots, x_{2b}) = (x_1 + x_2)(x_3 + x_4) \cdots (x_{2b-1} + x_{2b}). \quad (2.1)$$

证明 设 Σ_n 为集合 $\{1, 2, \dots, n\}$ 上的置换群. 对每个置换 $\sigma \in \Sigma_n$ 以及 $g \in B_n$, 定义 $g^\sigma(x_1, \dots, x_n) = g(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. 对于任意的 $i, j, 1 \leq i < j \leq n$, 令

$$X_{(i,j)} = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{j-1}, x_{j+1}, \dots, x_n),$$

则

$$g = g(x_1, \dots, x_n) = g_0(X_{(i,j)}) + x_i g_1(X_{(i,j)}) + x_j g_2(X_{(i,j)}) + x_i x_j g_3(X_{(i,j)}).$$

若 $g_1(X_{(i,j)}) = g_2(X_{(i,j)}) (1 \leq i < j \leq n)$, 则对任意的 $\sigma = (ij)$, 均有 $g^\sigma = g$. 注意到群 Σ_n 是由全体对换 $(ij) (1 \leq i < j \leq n)$ 所生成的, 故 g 为对称函数, 此时结论自明. 否则, 必存在置换 $\sigma = (ij) (1 \leq i < j \leq n)$ 使 $g_1(X_{(i,j)}) \neq g_2(X_{(i,j)})$ 成立. 于是可选取置换 $\tau \in \Sigma_n$ 使得 $\tau(i) = (1, i)(2, j)$, 从而有

$$g^\tau = g_0(x_3, \dots, x_n) + x_1 g_1(x_3, \dots, x_n) + x_2 g_2(x_3, \dots, x_n) + x_1 x_2 g_3(x_3, \dots, x_n),$$

以及 $g_1(x_3, \dots, x_n) \neq g_2(x_3, \dots, x_n)$. 特别的, 若取 $\sigma = (12)$, 则

$$\begin{aligned} g^\tau + g^{\tau\sigma} &= (x_1 + x_2)(g_1(x_3, \dots, x_n) + g_2(x_3, \dots, x_n)) \neq 0, \\ \deg(g_1 + g_2) &\leq \max\{\deg g_1, \deg g_2\} \leq \deg g - 1. \end{aligned}$$

于是

$$\begin{aligned} f(g^\tau + g^{\tau\sigma}) &= f^\tau g^\tau + f^{\tau\sigma} g^{\tau\sigma} \quad (f \text{ 为对称函数}) \\ &= (fg)^\tau + (fg)^{\tau\sigma} = 0. \end{aligned}$$

若 $h = g_1(x_3, \dots, x_n) + g_2(x_3, \dots, x_n) \in B_{n-2}$ 为对称函数, 则结论得证. 否则我们可以重复上述证明, 即可得到引理. $\square$

设 $n \geq 2, 1 \leq d \leq \lfloor \frac{n+1}{2} \rfloor, 0 \leq b \leq d-1$. 令

$$\begin{aligned} G(n, d, b) &= \{p_b(x_1, \dots, x_{2b})h(x_{2b+1}, \dots, x_n) : h \in SB_{n-2b}, 0 \leq \deg h \leq d-1-b\}, \\ G(n, d) &= \bigcup_{b=0}^{d-1} G(n, d, b), \\ WS(n, d, b) &= \{WS(g) : g \in G(n, d, b)\}, \\ WS(n, d) &= \bigcup_{b=0}^{d-1} WS(n, d, b) = \{WS(g) : g \in G(n, d)\}. \end{aligned} \tag{2.2}$$

设 $g \in B_n$, 则 $WS(g)$ 是 $N = \{0, 1, \dots, n\}$ 的一个子集族 $WS(g) = \{i_1, \dots, i_l\}$. 为方便, 本文简记为 $WS(g) = (i_1, \dots, i_l)$ 或者 $(i_1 \cdots i_l)$. 于是 $WS(n, d, b)$ (以及 $WS(n, d)$) 为 N 的一个子集族. 对于 $f \in SB_n$, 由引理 2.2 和引理 2.3 可知:

$$\begin{aligned} AI_n(f) \geq d &\Leftrightarrow \text{对所有的 } g \in G(n, d), WS(g) \not\subseteq WS(f) \text{ 并且 } WS(g) \not\subseteq \overline{WS(f)} \\ &\Leftrightarrow \text{对所有的 } A \in WS(n, d), A \not\subseteq WS(f) \text{ 且 } A \not\subseteq \overline{WS(f)} \\ &\Leftrightarrow \text{对所有的 } A \in WS(n, d), \text{映射 } v_f : N \rightarrow \mathbb{F}_2, i \mapsto v_f(i) (0 \leq i \leq n) \text{ 在集合 } A \text{ 上的限制非常值映射} \\ &\Leftrightarrow \text{对所有的 } A = (i_1, \dots, i_l) \in WS(n, d), (v_f(i_1), \dots, v_f(i_l)) \neq (0, \dots, 0), (1, \dots, 1). \end{aligned}$$

进而, 如果 $f \in SB_n$ 满足条件:

$$\text{对 } N \text{ 的某个子集 } A, A \not\subseteq WS(f) \text{ 且 } A \not\subseteq \overline{WS(f)},$$

则对任何子集 $A' \supseteq A$, 均有

$$A' \not\subseteq WS(f) \text{ 且 } A' \not\subseteq \overline{WS(f)}.$$

因此, 我们只需考虑偏序集合 $(WS(n, d), \subseteq)$ 中的所有极小元即可. 设 $WS_{\min}(n, d)$ 为 $(WS(n, d), \subseteq)$ 中全体极小元之集. 我们有对称 Boolean 函数 f 的代数免疫度满足 $AI_n(f) \geq d$ 的如下判别准则.

定理 2.4 设 $n \geq 2, 1 \leq d \leq \lfloor \frac{n+1}{2} \rfloor, f \in SB_n$. 则下述 3 条彼此等价:

- (1) $AI_n(f) \geq d$;
- (2) 对任意的 $A \in WS_{\min}(n, d), A \not\subseteq WS(f)$ 并且 $A \not\subseteq \overline{WS(f)}$;

(3) 对于任意的 $A \in WS_{\min}(n, d)$, 映射

$$v_f : N \rightarrow \mathbb{F}_2, \quad i \mapsto v_f(i)$$

在集合 A 上的限制非常值映射. 换言之, 对任意的 $A = (i_1, \dots, i_l) \in WS_{\min}(n, d)$,

$$(v_f(i_1), \dots, v_f(i_l)) \neq (0, \dots, 0), (1, \dots, 1).$$

因此我们的问题转化为:

(*) 对于 $n \geq 2, 1 \leq d \leq [\frac{n+1}{2}]$, 如何决定集合 $WS_{\min}(n, d)$?

一般情形下, 要确定集合 $WS_{\min}(n, d)$ 很困难. 本文给出一个计算 $WS_{\min}(n, d)$ 的一般公式, 并由此决定了集合 $WS_{\min}(2^m, 2^{m-1})$ ($m \geq 1$), 从而得到代数免疫度达到最大值 $AI(f) = 2^{m-1}$ 的全部 2^m 个变量的对称 Boolean 函数 $f \in SB_n$.

为此, 我们首先给出计算 $WS_{\min}(n, d)$ 的一个递归公式. 设 S 为 $N = \{0, 1, \dots, n\}$ 的一个子集族, 记 $S_{\min}$ 为偏序集 $(S, \subseteq)$ 中全体极小元之集. 对每个 $b \in N$, 记

$$S + b = \{A + b : A \in S\}.$$

引理 2.5 设 $n \geq 2, 1 \leq d \leq [\frac{n+1}{2}], 0 \leq b \leq d-1$. 则对于任意的 $i, 1 \leq i \leq d-1$, 我们有

$$WS_{\min}(n, d) = \left(\bigcup_{b=0}^{i-1} (WS_{\min}(n-2b, d-b, 0) + b) \cup (WS_{\min}(n-2i, d-i) + i) \right)_{\min}.$$

特别的, 当 $m \geq 2$ 时,

$$WS_{\min}(2^m, 2^{m-1}) = \left(\bigcup_{b=0}^{2^{m-2}-1} (WS_{\min}(2^m-2b, 2^{m-1}-b, 0) + b) \cup (WS_{\min}(2^{m-1}, 2^{m-2}) + 2^{m-2}) \right)_{\min}.$$

引理的证明 由 $WS_{\min}(n, d)$ 以及 $WS(n, d)$ 的定义, 可知

$$\begin{aligned} WS(n, d, b) &= \left\{ WS(g) : g = h_b p_b \left| \begin{array}{l} p_b = (x_1 + x_2) \cdots (x_{2b-1} + x_{2b}), \\ h_{n-2b}(x_{2b+1}, \dots, x_n) \in SB_{n-2b}, \\ 0 \leq \deg h_b < d-b-1 \end{array} \right. \right\} \\ &= \{WS(h) + b : h \in SB_{n-2b}, 0 \leq \deg h \leq d-b-1\} \quad (\text{因为 } WS(p_b) = \{b\}) \\ &= WS(n-2b, d-b, 0) + b. \end{aligned}$$

于是对任意的 $i, 1 \leq i \leq d-1$, 我们有

$$\begin{aligned} WS(n, d) &= \bigcup_{b=0}^{d-1} WS(n, d, b) = \left(\bigcup_{b=0}^{i-1} WS(n, d, b) \right) \cup \left(\bigcup_{b=i}^{d-1} WS(n, d, b) \right) \\ &= \left(\bigcup_{b=0}^{i-1} (WS(n-2b, d-b, 0) + b) \right) \cup \left(\bigcup_{b=0}^{d-i-1} (WS(n-2i, d-i, b) + i) \right) \\ &= \left(\bigcup_{b=0}^{i-1} (WS(n-2b, d-b, 0) + b) \right) \cup (WS(n-2i, d-i) + i). \end{aligned}$$

上式两边同时取极小元即得引理 2.5. □

由引理 2.5, 问题 (*) 归结于: 对任意的 $d, 1 \leq d \leq [\frac{n+1}{2}]$, 如何求集合 $WS_{\min}(n, d, 0)$? 其中

$$WS(n, d, 0) = \{WS(h) : h \in SB_n, 0 \leq \deg h \leq d-1\} = \{WS(h) : h \in G(n, d, 0)\}.$$

注意到集合 $\{h \in SB_n : \deg h \leq d-1\}$ 为 SB_n 的 d 维 $\mathbb{F}_2$ 向量空间, 从而每个 $h \in G(n, d, 0)$ 均可唯一表示为

$$h = h(x_1, \dots, x_n) = \sum_{i=0}^{d-1} \lambda_h(i) \sigma_i \quad (\lambda_h(i) \in \mathbb{F}_2).$$

由变换公式 (1.2) 和 (1.3), $v_h(0), \dots, v_h(d-1)$ 与 $\lambda_h(0), \dots, \lambda_h(d-1)$ 有如下对应关系:

$$\lambda_h(i) = \sum_{j=0, j \preceq i}^{d-1} v_h(j), \quad v_h(i) = \sum_{j=0, j \preceq i}^{d-1} \lambda_h(j),$$

即映射 $(v_h(0), \dots, v_h(d-1)) \mapsto (\lambda_h(0), \dots, \lambda_h(d-1))$ 为 $\mathbb{F}_2^d$ 上的双射. 现在取向量空间 $\mathbb{F}_2^d$ 上的一组标准基底:

$$e_0 = (1, 0, \dots, 0), \quad e_1 = (0, 1, \dots, 0), \quad \dots, \quad e_{d-1} = (0, 0, \dots, 1) \in \mathbb{F}_2^d. \quad (2.3)$$

设 $h_t \in G(n, d, 0)$ 且 $(v_{h_t}(0), \dots, v_{h_t}(d-1)) = e_t$. 则 $\{h_0, \dots, h_{d-1}\}$ 为向量空间 $G(n, d, 0) \cup \{0\}$ 的一组基底. 于是当 $j \geq d$ 时,

$$0 = \lambda_{h_t}(j) = \sum_{i=0, i \preceq j}^j v_{h_t}(i).$$

而当 $d \leq j \leq n$ 时, $v_{h_t}(j)$ 有递归计算公式:

$$v_{h_t}(j) = \sum_{i=0, i \prec j}^j \lambda_{h_t}(i). \quad (2.4)$$

最后, 对于 $h, h' \in G(n, d, 0)$, 由映射 $v : G(n, d, 0) \rightarrow \mathbb{F}_2^{n+1}, h \mapsto v_h$ 的线性性可得:

$$v_{h+h'} = (v_{h+h'}(0), \dots, v_{h+h'}(n)) = v_h + v_{h'} \in \mathbb{F}_2^{n+1}.$$

因为 $WS(h) = \{i \mid v_h(i) = 1, i \in \{0, 1, 2, \dots, d-1\}\}$, 故

$$WS(h+h') = WS(h) \triangle WS(h'),$$

其中 $A \triangle B$ 表示集合 $N = \{0, 1, \dots, n\}$ 的两个子集合 A, B 的对称差

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

由此可得到集合 $WS(n, d, 0)$ 的如下刻画.

定理 2.6 设 $n \geq 2, 1 \leq d \leq [\frac{n+1}{2}], \{e_0, \dots, e_{d-1}\}$ 为 $\mathbb{F}_2^d$ 中由式 (2.3) 给出的标准基底. 若 $h_t \in G(n, d, 0)$ 且

$$(v_{h_t}(0), \dots, v_{h_t}(d-1)) = e_t \quad (0 \leq t \leq d-1),$$

则

$$WS(n, d, 0) = \{WS(h_{i_1}) \triangle \dots \triangle WS(h_{i_l}) : \emptyset \neq \{i_1, \dots, i_l\} \subseteq \{0, 1, \dots, d-1\}\}.$$

当 d 为 2 的方幂时, 由定理 2.6 容易决定集合 $WS_{\min}(n, d, 0)$. 我们先给出一个具体例子, 其在后面的证明中要用到.

引理 2.7 设 $d = 2^l (l \geq 1), n = 2d$. 则

$$WS_{\min}(2^{l+1}, 2^l, 0) = \{(0, 2^l, 2^{l+1}), (1, 2^l + 1), (2, 2^l + 2), \dots, (2^l - 1, 2^{l+1} - 1)\}.$$

证明 设 $e_t (0 \leq t \leq d-1)$ 为 $\mathbb{F}_2^d$ 上由式 (2.3) 给出的标准基底, $h_t \in G(2^{l+1}, 2^l, 0)$ 并且 $(v_{h_t}(0), \dots, v_{h_t}(d-1)) = e_t (0 \leq t \leq d-1)$. 由 $\deg h_t \leq d-1 = 2^l - 1$ 以及引理 1.1, 可知向量 $(v_{h_t}(0), \dots, v_{h_t}(2^{l+1}))$ 的周期为 2^l . 于是

$$\begin{aligned} WS(h_0) &= (0, 2^l, 2^{l+1}) \quad (\text{因为 } (v_{h_0}(0), \dots, v_{h_0}(d-1)) = (1, 0, \dots, 0)), \\ WS(h_t) &= (t, t + 2^l) \quad (1 \leq t \leq d-1). \end{aligned}$$

注意到 $WS(h_t) (0 \leq t \leq d-1)$ 两两无交, 于是他们的对称差等于他们的并集合. 因此集合 $WS(2^{l+1}, 2^l, 0)$ 的全体极小元之集恰为 $WS(h_t) (0 \leq t \leq d-1)$. 即

$$\begin{aligned} WS(2^{l+1}, 2^l, 0) &= \{WS(h_t) : 0 \leq t \leq d-1\} \\ &= \{(0, 2^l, 2^{l+1})\} \cup \{(t, t + 2^l) : 1 \leq t \leq 2^l - 1\}. \end{aligned}$$

从而由引理 2.5 可知: 当 $m \geq 2$ 时,

$$WS_{\min}(2^m, 2^{m-1}) = \left(\bigcup_{b=0}^{2^{m-2}-1} (WS_{\min}(2^m - 2b, 2^{m-1} - b, 0) + b) \cup (WS_{\min}(2^{m-1}, 2^{m-2}) + 2^{m-2}) \right)_{\min}.$$

上述等式右边取 $b = 0$ 立得引理 2.7. □

在第 3 节中将证明: 若 $1 \leq b \leq 2^{m-2} - 1$, 则 $WS_{\min}(2^m - 2b, 2^{m-1} - b, 0) + \{b\}$ 中每一个元素都包含集合 $WS_{\min}(2^m, 2^{m-1}, 0) \cup (WS_{\min}(2^{m-1}, 2^{m-2}) + 2^{m-2})$ 中的元素, 从而有递归公式

$$WS_{\min}(2^m, 2^{m-1}) = (WS_{\min}(2^m, 2^{m-1}, 0) \cup (WS_{\min}(2^{m-1}, 2^{m-2}) + 2^{m-2}))_{\min}.$$

对任意的 $m \geq 2$, 由此公式即可决定集合 $WS_{\min}(2^m, 2^{m-1})$. 再由定理 2.4, 我们就可以确定全部具有最优代数免疫度的 2^m 个变量的对称 Boolean 函数.

3 主要结果

在给出集合 $WS_{\min}(2^m, 2^{m-1})$ 的准确公式之前, 我们先计算 $m = 1, 2$ 和 3 的情形.

当 $m = 1$ 时, $G(2, 1) = \{h \in SB_2 \mid \deg h = 0\}$ 中只有一个函数 $h \equiv 1$. 于是

$$WS(2, 1) = \{(0, 1, 2)\}.$$

当 $m = 2$ 时, 由引理 2.5 和 2.7 可知

$$\begin{aligned} WS_{\min}(4, 2) &= (WS_{\min}(4, 2, 0) \cup (WS_{\min}(2, 1) + 1))_{\min} \\ &= \{(0, 2, 4), (1, 3), (1, 2, 3)\}_{\min} = \{(0, 2, 4), (1, 3)\}. \end{aligned}$$

当 $m = 3$ 时, 同样由引理 2.5 和 2.7 可得

$$\begin{aligned} WS_{\min}(8, 4) &= (WS_{\min}(8, 4, 0) \cup (WS_{\min}(6, 3, 0) + 1) \cup (WS_{\min}(4, 2) + 2))_{\min} \\ &= (\{(0, 4, 8), (1, 5), (2, 6), (3, 7)\} \cup \{(2, 4, 6), (3, 5)\} \cup (WS_{\min}(6, 3, 0) + 1))_{\min} \\ &= (\{(0, 4, 8), (1, 5), (2, 6), (3, 7), (3, 5)\} \cup (WS_{\min}(6, 3, 0) + 1))_{\min}. \end{aligned} \quad (3.1)$$

现在利用定理 2.6 来计算集合 $WS_{\min}(6, 3, 0)$. 设 $h_t \in SB_6$ ($0 \leq t \leq 2$) 且

$$\begin{aligned} (v_{h_0}(0), v_{h_0}(1), v_{h_0}(2)) &= (1, 0, 0), \\ (v_{h_1}(0), v_{h_1}(1), v_{h_1}(2)) &= (0, 1, 0), \\ (v_{h_2}(0), v_{h_2}(1), v_{h_2}(2)) &= (0, 0, 1). \end{aligned}$$

若 $3 \leq j \leq 6$, 则由公式 (2.4) 可计算出 $v_{h_t}(j)$:

$$\begin{aligned} v_{h_0} &= (v_{h_0}(0), \dots, v_{h_0}(6)) = (1, 0, 0, 1, 1, 0, 0), \\ v_{h_1} &= (0, 1, 0, 1, 0, 1, 0), \quad v_{h_2} = (0, 0, 1, 1, 0, 0, 1). \end{aligned}$$

从而

$$WS(h_0) = (0, 3, 4), \quad WS(h_1) = (1, 3, 5), \quad WS(h_2) = (2, 3, 6).$$

再由定理 2.6 可知:

$$\begin{aligned} WS_{\min}(6, 3, 0) + 1 &= \{(0, 3, 4), (1, 3, 5), (2, 3, 6), (0, 1, 4, 5), (0, 2, 4, 6), (1, 2, 5, 6), (0, 1, 2, 3, 4, 5, 6)\}_{\min} + 1 \\ &= \{(1, 4, 5), (2, 4, 6), (3, 4, 7), (1, 2, 5, 6), (1, 3, 5, 7), (2, 3, 6, 7)\}. \end{aligned}$$

故 $WS_{\min}(6, 3, 0) + 1$ 的每个元素均包含了下述集合中的元素:

$$\{(0, 4, 8), (1, 5), (2, 6), (3, 7), (3, 5)\}.$$

于是由 (3.1) 立得

$$WS_{\min}(8, 4) = \{(0, 4, 8), (1, 5), (2, 6), (3, 7), (3, 5)\}.$$

现在我们证明本文的主要结果.

定理 3.1 设 $m \geq 2, n = 2^m$, 则

(1) 集合 $WS_{\min}(2^m, 2^{m-1})$ 等于

$$S'(m) = \{(0, 2^{m-1}, 2^m)\} \cup \{(2^{m-1} + i_t - 2^t, 2^{m-1} + i_t) : 1 \leq t \leq m-1, 1 \leq i_t \leq 2^t - 1\}.$$

(2) 设 $f \in SB_n$, 则 $AI_n(f) = \frac{n}{2}$ 当且仅当 $v_f = (v_f(0), \dots, v_f(n)) \in \mathbb{F}_2^{n+1}$ 满足下述两个条件:

(2.1) 对任意的 $1 \leq t \leq m-1, 1 \leq i_t \leq 2^t - 1, v_f(2^{m-1} + i_t - 2^t) = v_f(2^{m-1} + i_t) + 1$.

(2.2) $(v_f(0), v_f(2^{m-1}), v_f(2^m)) \neq (0, 0, 0), (1, 1, 1)$.

证明 (1) 由前面的例子可知 $m = 2$ 时, $WS_{\min}(2^m, 2^{m-1}) = S'(m)$ 成立. 现在假设 $m \geq 3$ 时 $WS_{\min}(2^{m-1}, 2^{m-2}) = S'(m-1)$ 成立. 由引理 2.5,

$$WS_{\min}(2^m, 2^{m-1}) = \left(\bigcup_{b=1}^{2^{m-2}-1} (WS_{\min}(2^m - 2b, 2^{m-1} - b, 0) + b) \cup M(m) \right)_{\min}, \quad (3.2)$$

其中

$$M(m) = (WS_{\min}(2^m, 2^{m-1}, 0) \cup (WS_{\min}(2^{m-1}, 2^{m-2}) + 2^{m-2}))_{\min}. \quad (3.3)$$

于是由假设可得

$$\begin{aligned} & WS_{\min}(2^{m-1}, 2^{m-2}) + 2^{m-2} \\ &= S'(m-1) + 2^{m-2} \\ &= \{(0, 2^{m-2}, 2^{m-1})\} \cup \{(2^{m-2} + i_t - 2^t, 2^{m-2} + i_t) : 1 \leq t \leq m-2, 1 \leq i_t \leq 2^t - 1\} + 2^{m-2} \\ &= \{(2^{m-2}, 2^{m-1}, 2^{m-1} + 2^{m-2})\} \\ &\quad \cup \{(2^{m-1} + i_t - 2^t, 2^{m-1} + i_t) : 1 \leq t \leq m-2, 1 \leq i_t \leq 2^t - 1\}. \end{aligned} \quad (3.4)$$

再由引理 2.7,

$$WS_{\min}(2^m, 2^{m-1}, 0) = \{(0, 2^{m-1}, 2^m)\} \cup \{(i, i + 2^{m-1}) : 1 \leq i \leq 2^{m-1} - 1\}. \quad (3.5)$$

注意到 $S'(m-1) + 2^{m-2}$ 中的元素 $(2^{m-2}, 2^{m-1}, 2^{m-1} + 2^{m-2})$ 包含 $WS_{\min}(2^m, 2^{m-1}, 0)$ 中的元素 $(2^{m-2}, 2^{m-1}, 2^{m-2})$. 于是由 (3.3)–(3.5) 式可知 $M(m) = S'(m)$. 再由式 (3.2) 知欲证 $WS_{\min}(2^m, 2^{m-1}) = S'(m)$, 只需证明如下论断.

论断 设 $m \geq 3, 1 \leq b \leq 2^{m-2} - 1, WS_{\min}(2^m - 2b, 2^{m-1} - b, 0) + b$ 的每个元素都至少包含 $S'(m)$ 中一个元素.

上述论断的证明请见本文的附录. 这样就完成了 (1) 的证明.

(2) 由 (1) 和定理 2.4(3) 立得 (2). □

设 $m \geq 1, n = 2^m$. 记 $A(m)$ 为具有最大代数免疫度的 n 个变量的全体对称 Boolean 函数之集:

$$A(m) = \left\{ f \in SB_n : AI_n(f) = \frac{n}{2} \right\}.$$

由定理 3.1 可得到由 $A(m)$ 计算 $A(m+1)$ 的一个递归公式, 从而可由此确定具有最大代数免疫度的 2^m 变量的全部对称 Boolean 函数的个数 $|A(m)|$.

定理 3.2 设 $m \geq 1, n = 2^m$.

(1) 对任意的 $f^{(m)} \in A(m)$, 如下定义 $f^{(m+1)} \in SB_{2^{m+1}}$:

i	0	1	$\dots$	$2^{m-1} - 1$
$v_{f^{(m+1)}}(i)$	$v_{f^{(m)}}(0)$	$v_{f^{(m)}}(1)$	$\dots$	$v_{f^{(m)}}(2^{m-1} - 1)$
i	2^{m-1}	$2^{m-1} + 1$	$\dots$	$2^m - 1$
$v_{f^{(m+1)}}(i)$	d	$v_{f^{(m)}}(1)$	$\dots$	$v_{f^{(m)}}(2^{m-1} - 1)$
i	2^m	$2^m + 1$	$\dots$	$3 \cdot 2^{m-1} - 1$
$v_{f^{(m+1)}}(i)$	$v_{f^{(m)}}(2^{m-1})$	$v_{f^{(m)}}(2^{m-1} + 1)$	$\dots$	$v_{f^{(m)}}(2^m - 1)$
i	$3 \cdot 2^{m-1}$	$3 \cdot 2^{m-1} + 1$	$\dots$	$2^{m+1} - 1$
$v_{f^{(m+1)}}(i)$	$d + 1$	$v_{f^{(m)}}(2^{m-1} + 1)$	$\dots$	$v_{f^{(m)}}(2^m - 1)$
				$v_{f^{(m)}}(2^m)$

其中 $d \in \mathbb{F}_2$. 则 $f^{(m+1)} \in A(m+1)$, 并且 $A(m+1)$ 中的全体函数均可由此给出.

(2) 对任意的 $m \geq 1, |A(m)| = 3 \cdot 2^m$.

证明 (1) 由定理 3.1 可知 $f \in A(m+1)$, 并且 f 满足下列条件:

$$(m+1): \begin{cases} v_f(2^m + i_t - 2^t) = v_f(2^m + i_t) + 1, & 1 \leq t \leq m, 1 \leq i_t \leq 2^t - 1, \\ (v_f(0), v_f(2^m), v_f(2^{m+1})) \neq (0, 0, 0), (1, 1, 1). \end{cases}$$

现在如下定义函数 $f' \in SB_{2^m}$:

$$\begin{aligned} v_{f'}(i) &= v_f(i), & 1 \leq i \leq 2^{m-1} - 1, \\ v_{f'}(i) &= v_f(i - 2^{m-1}), & 2^{m-1} + 1 \leq i \leq 2^m - 1, \\ (v_{f'}(0), v_{f'}(2^{m-1}), v_{f'}(2^m)) &= (v_f(0), v_f(2^m), v_f(2^{m+1})). \end{aligned}$$

容易证明函数 $f' \in A(m)$ 满足条件:

$$(m): \begin{cases} v_{f'}(2^{m-1} + i_t - 2^t) = v_{f'}(2^{m-1} + i_t) + 1, & 1 \leq t \leq m-1, 1 \leq i_t \leq 2^t - 1, \\ (v_{f'}(0), v_{f'}(2^{m-1}), v_{f'}(2^m)) \neq (0, 0, 0), (1, 1, 1). \end{cases}$$

反过来, 若 $f^{(m)} \in A(m)$, 并且 $v_{f^{(m)}}$ 满足条件 (m), 易知 (1) 中定义的函数 $f^{(m+1)}$ 也适合条件 (m+1), 从而 $f^{(m+1)} \in A(m+1)$. 这就证明了 (1).

(2) 由 d 的取值为 0 或 1, 可知 $A(m)$ 到 $A(m+1)$ 上的映射 $f^{(m)} \mapsto f^{(m+1)}$ 为 2 对 1 的映射. 于是对任意的 $m \geq 1, |A(m+1)| = 2|A(m)|$. 又

$$A(1) = \{h \in SB_2 : AI(h) = 1\} = \{h \in SB_2 : 1 \leq \deg h \leq 2\} = \{h \in SB_2 : h \neq 0, 1\},$$

即 $|A(1)| = |SB_2| - 2 = 2^3 - 2 = 6$. 从而对任意的 $m \geq 1, |A(m)| = 3 \cdot 2^m$. □

参考文献

- 1 Armknecht F. Improving fast algebraic attacks. In: FSE 2004. LNCS 3017. Berlin: Springer-Verlag, 2004, 65–82
- 2 Armknecht F, et al. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In: EUROCRYPT 2006. LNCS 4004. Berlin: Springer-Verlag, 2006, 147–164
- 3 Courtois N. Fast algebraic attacks on stream ciphers with linear feedback. In: CRYPTO 2003. LNCS 2729. Berlin: Springer-Verlag, 2003, 176–194
- 4 Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback. In: EUROCRYPT 2003. LNCS 2656. Berlin: Springer-Verlag, 2003, 345–359
- 5 Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions. In: EUROCRYPT 2004. LNCS 3027. Berlin: Springer-Verlag, 2004, 474–491
- 6 Batten L M. Algebraic attack over $GF(q)$. In: INDOCRYPT 2004. LNCS 3348. Berlin: Springer-Verlag, 2004, 84–91
- 7 Dalai D K, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Des Codes Cryptogr, to appear
- 8 Carlet C, Dalai D K, Gupta K C, et al. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans Inform Theory, 2006, 52: 3105–3121
- 9 Dalai D K, Gupta K C, Maitra S. Results on algebraic immunity for cryptographically significant Boolean functions. In: INDOCRYPT 2004. LNCS 3348. Berlin: Springer-Verlag, 2004, 92–106
- 10 Braeken A, Preneel B. On the algebraic immunity of symmetric Boolean functions. In: INDOCRYPT 2005. LNCS 3797. Berlin: Springer-Verlag, 2005, 35–48
- 11 Qu L J, Li C, Feng K Q. A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variable. IEEE Trans Inform Theory, 2007, 53: 2908–2910

- 12 Qu L J, Feng K Q, Liu F, et al. Constructing symmetric Boolean functions with maximum algebraic immunity. IEEE Trans Inform Theory, 2007, 55: 2406–2412
- 13 Cantean C, Videan M. Symmetric Boolean functions, IEEE Trans Inform Theory, 2005, 51: 2791–2811

附录

现在我们来证明定理 3.1 中的论断. 该论断可以等价的叙述为:

定理 A.1 设 $m \geq 3, 1 \leq b \leq 2^{m-2} - 1, h = h(x) \in SB_{2^m-2b}$, 且 $0 \leq \deg h \leq 2^{m-1} - b - 1$. 则存在 t $1 \leq t \leq m-1$ 以及 $i_t, i_t + b \geq 1$ 使得 $v_h(2^{m-1} + i_t - 2^t) = v_h(2^{m-1} + i_t) = 1$.

为证明此定理, 先证明如下引理.

引理 A.2 设 $n \geq 2, f(x) \in \mathbb{F}_2[x], 0 \leq \deg f \leq n$. 若 $(1+x)^n f(x) = \sum_{j=0}^{2n} a_j x^j \in \mathbb{F}_2[x]$, 则存在 $l \geq 1, \lambda \geq 0$ 使得 $\lambda + 2^l \geq n$ 并且 $a_\lambda = a_{\lambda+2^l} = 1$.

证明 首先证明引理 A.2 当 $n = 2$ 和 3 时成立.

当 $n = 2$ 时,

$$\begin{aligned} \sum_{j=0}^4 a_j x^j &= (1+x^2)(A_0 + A_1 x + A_2 x^2) \quad ((0,0,0) \neq (A_0, A_1, A_2) \in \mathbb{F}_2^3) \\ &= (A_0 + (A_0 + A_2)x^2 + A_2 x^4) + (A_1 x + A_1 x^3). \end{aligned}$$

若 $A_1 = 1$, 则 $a_1 = a_3 = 1$. 否则 $(A_0, A_2) \neq (0,0)$, 此时 Hamming 重量 $w_H(A_0, A_0 + A_2, A_2) = 2$. 从而 $(a_0, a_2), (a_2, a_4)$ 以及 (a_0, a_4) 中必有一个为 $(1,1)$. 即引理 A.2 当 $n = 2$ 时成立.

当 $n = 3$ 时,

$$\begin{aligned} \sum_{j=0}^6 a_j x^j &= (1+x^2)(1+x)(A_0 + A_1 x + A_2 x^2 + A_3 x^3) \quad ((0,0,0,0) \neq (A_0, A_1, A_2, A_3) \in \mathbb{F}_2^4) \\ &= (1+x^2)(B_0 + B_1 x + B_2 x^2 + B_3 x^3 + B_4 x^4) \\ &\quad ((0,0,0,0,0) \neq (B_0, B_1, B_2, B_3, B_4) \in \mathbb{F}_2^5, B_0 + B_1 + B_2 + B_3 + B_4 = 0) \\ &= (1+x^2)(B_0 + B_2 x^2 + B_4 x^4) + (1+x^2)(B_1 x + B_3 x^3). \end{aligned}$$

若 $(B_1, B_3) \neq (0,0)$, 则 $w_H(B_1, B_1 + B_3, B_3) = 2$ 并且 $(a_1, a_3), (a_3, a_5)$ 以及 (a_1, a_5) 中至少有一个为 $(1,1)$. 否则 $(B_0, B_2, B_4) \neq (0,0,0), B_0 + B_2 + B_4 = 0$, 此时 $w_H(B_0, B_2, B_4) = 2$. 即引理 A.2 当 $n = 3$ 时成立.

现在假设 $k \geq 4$ 并且引理 A.2 对于所有的 $n, 2 \leq n \leq k-1$ 均成立. 现在我们来证明引理 A.2 当 $n = k$ 时仍然成立.

设 $f(x) \in \mathbb{F}_2[x], 0 \leq \deg f \leq k$, 则 $f(x) = f_0(x^2) + x f_1(x^2)$ 并且 $(f_1, f_2) \neq (0,0)$.

(I) 若 $k = 2m (\geq 4)$, 则 $\deg f_0 \leq m, \deg f_1 \leq m-1$, 并且

$$\sum_{j=0}^{4m} a_j x^j = (1+x)^{2m} f(x) = (1+x^2)^m f_0(x^2) + x(1+x^2)^m f_1(x^2).$$

于是

$$\sum_{i=0}^{2m} a_{2i} y^i = (1+y)^m f_0(y), \quad \sum_{i=0}^{2m-1} a_{2i+1} y^i = (1+y)^m f_1(y).$$

由归纳假设可知, 存在 $l \geq 1, \lambda \geq m - 2^l$ 使得 $f_0(y) \neq 0$ 时 $a_{2\lambda} = a_{2(\lambda+2^l)} = 1$, 或者 $\lambda \geq m - 1 - 2^l$ 而 $f_1(y) \neq 0$ 时 $a_{2\lambda+1} = a_{2(\lambda+2^l)+1} = 1$.

(II) 若 $k = 2m + 1$ (≥ 5), 则 $\deg f_0 \leq m, \deg f_1 \leq m$, 并且

$$\begin{aligned} \sum_{j=0}^{4m+2} a_j x^j &= (1+x)^{2m+1} f(x) \\ &= (1+x^2)^m (f_0(x^2) + f_1(x^2)) + (1+x^2)^{m+1} f_1(x^2) + x(1+x^2)^m (f_0(x^2) + f_1(x^2)). \end{aligned}$$

因此

$$\sum_{i=0}^{2m} a_{2i+1} y^i = (1+y)^m (f_0(y) + f_1(y)), \quad \sum_{i=0}^{2m+1} a_{2i} y^i = (1+y)^m (f_0(y) + f_1(y)) + (1+y)^{m+1} f_1(y).$$

若 $f_0 + f_1 \neq 0$, 则由归纳假设知存在 $l \geq 1, \lambda + 2^l \geq m$ 使得 $a_{2\lambda+1} = a_{2(\lambda+2^l)+1} = 1$. 否则 $f_0 + f_1 = 0, (f_0, f_1) \neq (0, 0), f_1(y) \neq 0$. 从而 $\sum_{i=0}^{2m+1} a_{2i} y^i = (1+y)^{m+1} f_1(y)$. 再由归纳假设知存在 $l \geq 1, \lambda + 2^l \geq m + 1$, 使得 $a_{2\lambda} = a_{2(\lambda+2^l)} = 1$. 这就完成了引理 A.2 的证明. $\square$

现在我们考虑 $\mathbb{F}_2$ 上的无限级矩阵:

$$M = (a_{ij})_{i,j \geq 0} \quad \left(a_{ij} = \binom{j}{i} \in \mathbb{F}_2 \right)$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots \\ & 1 & 0 & 1 & & 1 & 0 & 1 & & 1 & 0 & 1 & \cdots \\ & & 1 & 1 & & 1 & 1 & & & 1 & 1 & \cdots \\ & & & 1 & & & 1 & & & & 1 & \cdots \\ & & & & 1 & 1 & 1 & 1 & & & & \cdots \\ & & & & & 1 & 0 & 1 & & & & \cdots \\ & & & & & & 1 & 1 & & & & \cdots \\ & & & & & & & 1 & & & & \cdots \\ & & & & & & & & 1 & 1 & 1 & 1 & \cdots \\ & & & & & & & & & 1 & 0 & 1 & \cdots \\ & & & & & & & & & & 1 & 1 & \cdots \\ & & & & & & & & & & & 1 & \cdots \\ & & & & & & & & & & & & \cdots \end{pmatrix},$$

其中矩阵 M 的第 i 行由下列幂级数所生成:

$$\begin{aligned} a_i(x) &= \sum_{j=0}^{\infty} a_{ij} x^j = \sum_{j=0}^{\infty} \binom{j}{i} x^j = x^i \sum_{j=0}^{\infty} \binom{j+i}{i} x^j = x^i \sum_{j=0}^{\infty} \binom{-(i+1)}{j} x^j \\ &= x^i / (1+x)^{i+1} \in \mathbb{F}_2[[x]]. \end{aligned}$$

对任意的 $k \geq 1$, 记 A_k 为幂级数环 $\mathbb{F}_2[[x]]$ 中如下定义子集合:

$$A_k = \left\{ \sum_{j=0}^{\infty} b_j x^j \in \mathbb{F}_2[[x]] \mid t \geq k, b_t = \sum_{j < t} b_j \right\},$$

其中 $\preceq$ 为本文第 1 节中定义的 $\{0, 1, 2, \dots\}$ 上的偏序. 由于每个幂级数 $\sum_{j=0}^{\infty} b_j x^j$ 均由前面的 k 个系数 $b_0, \dots, b_{k-1}$ 所唯一决定, 因此 A_k 为 $\mathbb{F}_2[[x]]$ 的一个 k 维 $\mathbb{F}_2$ 子空间.

引理 A.3 (1) 设 $k \geq 1$, 则 $\{a_i(x) = x^i/(1+x)^{i+1} \mid 0 \leq i \leq k-1\}$ 为 $\mathbb{F}_2$ 上向量空间 A_k 的一组基底.

(2) 若 $k \leq 2^l$ ($l \geq 1$), 则 A_k 中的每个幂级数 $\sum_{j=0}^{\infty} b_j x^j$ 都有周期 2^l . 即对任意的 $j \geq 0, b_j = b_{j+2^l}$.

证明 (1) 对每个 $k \geq 1$, 设 k 的 2-adic 展开式为 $k = 2^{\lambda_1} + 2^{\lambda_2} + \dots + 2^{\lambda_t}$ ($0 \leq \lambda_1 < \lambda_2 < \dots < \lambda_t$), 则

$$\begin{aligned} \sum_{j \preceq k} (1+y)^j &= 1 + \sum_{a=1}^t (1+y)^{2^{\lambda_a}} + \sum_{1 \leq a < b \leq t} (1+y)^{2^{\lambda_a} + 2^{\lambda_b}} + \dots + (1+y)^k \\ &= (1 + (1+y^{2^{\lambda_1}})) \cdots (1 + (1+y^{2^{\lambda_t}})) = y^k. \end{aligned}$$

于是对每个 $i, 0 \leq i \leq k-1$, 我们有 $\sum_{j \preceq k} \binom{j}{i} = 0$, 从而

$$\binom{k}{i} = \sum_{j \prec k} \binom{j}{i} \in \mathbb{F}_2 \quad (\text{对所有的 } i, k, 0 \leq i \leq k-1).$$

由此可知

$$a_i = x^i/(1+x)^{i+1} = \sum_{j=0}^{\infty} \binom{j}{i} x^j \quad (0 \leq i \leq k-1)$$

属于 A_k . 易知 $\{a_i(x) \mid 0 \leq i \leq k-1\}$ 是 $\mathbb{F}_2$ 线性无关的, 从而构成 $\mathbb{F}_2$ 向量子空间 A_k 的一组基底.

(2) 注意到 $i \leq k-1 \leq 2^l, \binom{j+2^l}{i} = \binom{j}{i}$. 于是由 Lucas 定理知 A_k 中每个元素

$$a_i(x) = \sum_{j=0}^{\infty} \binom{j}{i} x^j \quad (0 \leq i \leq k-1)$$

均有周期 2^l . 从而 A_k 中每个幂级数均有周期 2^l .

定理 A.1 的证明 设 $m \geq 3, 1 \leq b \leq 2^{m-2} - 1, h \in SB_{2^m-2b}$ 并且 $0 \leq \deg h \leq 2^{m-1} - b - 1$. 若

$$\lambda_h = (\lambda_h(0), \dots, \lambda_h(2^{m-1} - b - 1), 0, \dots, 0) \in \mathbb{F}_2^{2^m-2b}, \quad (\lambda_h(0), \dots, \lambda_h(2^{m-1} - b - 1)) \neq (0, \dots, 0),$$

则对每个 $i \geq 2^{m-1} - b$, 由式 (1.3) 可知 $0 = \lambda_h(i) = \sum_{j \preceq i} v_h(j)$. 于是

$$v_h(i) = \sum_{j \prec i} v_h(j) \quad (i \geq 2^{m-1} - b). \quad (\text{A1})$$

现设 $c(x) = \sum_{j=0}^{\infty} c_j x^j$ 为 $A_{2^{m-1}-b}$ 中如下定义的幂级数:

$$(c_0, \dots, c_{2^{m-1}-b-1}) = (v_h(0), \dots, v_h(2^{m-1} - b - 1)) \neq (0, \dots, 0).$$

由 (A1) 可得

$$\sum_{j=0}^{2^m-2b} v_h(j) x^j \equiv c(x) = \sum_{j=0}^{\infty} c_j x^j \pmod{x^{2^m-2b+1}}.$$

注意到 $a_i = x^i/(1+x)^{i+1}$ ($0 \leq i \leq 2^{m-1} - b - 1$) 为 $A_{2^{m-1}-b}$ 的一组基底, 因此

$$\sum_{j=0}^{2^m-2b} v_h(j) x^j \equiv \sum_{i=0}^{2^{m-1}-b-1} b_i \frac{x^i}{(1+x)^{i+1}} \pmod{x^{2^m-2b+1}}, \quad (\text{A2})$$

并且 $(b_0, \dots, b_{2^{m-1}-b-1}) \neq (0, \dots, 0)$.

若存在 $\lambda, 0 \leq \lambda \leq 2^{m-1} - 2b$ 使得 $v_h(\lambda) = 1$. 则由 $2^{m-1} - b < 2^{m-1}$ 知 $\lambda + 2^{m-1} \leq 2^m - 2b$ 以及 $v_h(\lambda + 2^{m-1}) = 1$. 于是 $A_{2^{m-1}-b}$ 中的元素 $\sum b_i x^i / (1+x)^{i+1}$ 有周期 2^{m-1} . 此时取 $t = m-1, i_t = \lambda$ 可知定理 A.1 成立. 否则, 我们有 $(v_h(0), \dots, v_h(2^{m-1}-2b)) = (0, \dots, 0)$. 此时由 (A2) 可知 $(b_0, \dots, b_{2^{m-1}-2b}) = (0, \dots, 0)$. 由 $v_h(j)$ 的周期性, 仍然可得 $v_h(2^{m-1}) = \dots = v_h(2^m - 2b) = 0$. 于是 (A2) 等价于:

$$\sum_{j=2^{m-1}-2b+1}^{2^{m-1}-1} v_h(j) x^j \equiv \sum_{i=2^{m-1}-2b+1}^{2^{m-1}-b-1} b_i x^i / (1+x)^{i+1} \pmod{x^{2^m-2b+1}}.$$

从而

$$\begin{aligned} \sum_{j=0}^{2b-2} v_h(j + 2^{m-1} - 2b + 1) x^j &\equiv \sum_{i=0}^{b-2} d_i \frac{x^i}{(1+x)^{2^{m-1}-2b+i+2}} \pmod{x^{2^{m-1}}} \\ &\equiv (1+x^{2^{m-1}}) \sum_{i=0}^{b-2} d_i \frac{x^i}{(1+x)^{2^{m-1}-2b+i+2}} \pmod{x^{2^{m-1}}} \\ &\equiv \sum_{i=0}^{b-2} d_i x^i (1+x)^{2b-2-i} \pmod{x^{2^{m-1}}}, \end{aligned} \quad (\text{A3})$$

其中 $d_i = b_{i+2^{m-1}-2b+1}, (d_0, \dots, d_{b-2}) \neq (0, \dots, 0)$. 故 $b \geq 2$. 又 $b \leq 2^{m-2} - 1$, 因此式 (A3) 两边多项式的次数 $\leq 2b-2 < 2^{m-1}$. 于是可得等式

$$\begin{aligned} \sum_{j=0}^{2b-2} v_h(j + 2^{m-1} - 2b + 1) x^j &= \sum_{i=0}^{b-2} d_i x^i (1+x)^{2b-2-i} = (1+x)^b \sum_{i=0}^{b-2} d_i x^i (1+x)^{b-2-i} \\ &= (1+x)^b f(x), \end{aligned}$$

其中 $f(x) \neq 0, \deg f \leq b-2$. 但由引理 A.2 知 $l \geq 1, \lambda \geq 0$ 且 $\lambda + 2^l \geq b$, 于是 $v_h(\lambda + 2^{m-1} - 2b + 1) = v_h(\lambda + 2^l + 2^{m-1} - 2b + 1) = 1$. 取 $t = l, i_t = \lambda + 2^l - 2b + 1$, 可得 $i_t + b = \lambda + 2^l - b + 1 \geq 1$, 即定理 A.1 成立. 这就完成了定理 A.1 的证明. $\square$

On 2^m -variable symmetric Boolean functions with maximum algebraic immunity 2^{m-1}

LIAO QunYing, FENG KeQin & LIU Feng

Abstract In this paper we prove a necessary and sufficient condition for a 2^m -variable symmetric Boolean function f having maximum algebraic immunity $AI_{2^m}(f) = 2^{m-1}$. As its consequences, we present a simple recursive procedure to construct all 2^m -variable symmetric Boolean functions f with maximum algebraic immunity for all $m \geq 2$, and prove that the number of such functions is $3 \cdot 2^m$.

Keywords: symmetric Boolean function, algebraic immunity, cryptography

MSC(2000): 11T30, 11T55