Des. Codes Cryptogr. (2009) 50:243–252
DOI 10.1007/s10623-008-9228-0

Maximal values of generalized algebraic immunity

Keqin Feng · Qunying Liao · Jing Yang

Received: 29 February 2008 / Revised: 13 June 2008 / Accepted: 15 July 2008 /
Published online: 15 August 2008

Abstract The notion of algebraic immunity of Boolean functions has been generalized in several ways to vector-valued functions and/or over arbitrary finite fields and reasonable upper bounds for such generalized algebraic immunities has been proved in Armknecht and Krause (Proceedings of ICALP 2006, LNCS, vol. 4052, pp 180–191, 2006), Ars and Faugere (Algebraic immunity of functions over finite fields, INRIA, No report 5532, 2005) and Batten (Canteaut, Viswanathan (eds.) Progress in Cryptology—INDOCRYPT 2004, LNCS, vol. 3348, pp 84–91, 2004). In this paper we show that the upper bounds can be reached as the maximal values of algebraic immunities for most of generalizations by using properties of Reed–Muller codes.

Keywords Algebraic immunity · Reed–Muller codes · Finite field · Cryptography

Mathematics Subject Classifications (2000) 94A60 · 11T71

1 Introduction

In the past few years several successful algebraic attacks on stream ciphers were proposed [1,2,6–8]. As a response to this situation, Meier et al. [8] and Batten [6] introduced the

Communicated by C. Cid.

K. Feng · Q. Liao · J. Yang (✉)
Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China
e-mail: jingyang@math.tsinghua.edu.cn

K. Feng
e-mail: Kfeng@math.tsinghua.edu.cn

Q. Liao
College of Mathematics and Software Science, Sichuan Normal University, Chengdu 610066, China
e-mail: liao_qunying@yahoo.com.cn

notion of algebraic immunity for a Boolean function. Let $\mathbb{B}_m$ be the ring of m-variable Boolean functions $f : \mathbb{F}_2^m \to \mathbb{F}_2$.

Definition 1.1 For a Boolean function $f = f(x_1, \ldots, x_m) \in \mathbb{B}_m$, the algebraic immunity of f is defined by

$$AI_m(f) = \min\{\deg g | 0 \neq g \in \mathbb{B}_m, \quad gf = 0 \text{ or } g(f+1) = 0\}$$

A large $AI_m(f)$ is a necessary (but not sufficient) condition for resisting algebraic attacks. It is proved (see [6] and [4]) that the maximal value of algebraic immunity for m-variable Boolean functions is $\lceil \frac{m}{2} \rceil$ and several Boolean functions with maximal AI have been constructed. The notion of algebraic immunity has been generalized in several ways to vector-valued functions and/or over arbitrary finite fields in [3,4,6], and the reasonable upper bounds of all generalized algebraic immunities have been presented. In this paper we will show that these upper bounds can be reached so that we can determine the maximal values of algebraic immunities for most of generalized cases. For doing this, our main tool is the (generalized) Reed–Muller codes over $\mathbb{F}_q$. In Sect. 2 we introduce basic properties on RM codes we will use in this paper. Then in the next three sections (3, 4 and 5) we introduce three generalizations of algebraic immunity (Definition 1.1) and their upper bounds given in [3,4,6], and prove that these upper bounds can be reached.

2 Reed–Muller codes over $\mathbb{F}_q$

In this section we introduce basic properties of Reed–Muller codes over arbitrary finite fields $\mathbb{F}_q$ which we need in this paper. For systematic theory on RM codes we refer, for example, to Assmus and Key's book [5], Chap. 5.

Let $m \geq 1$ and $\mathbb{F}_q$ be the finite field with q elements ($q = p^l, l \geq 1$ and p is a prime number). Let $\mathbb{B}_{m,q}$ be the ring of all function $f : \mathbb{F}_q^m \to \mathbb{F}_q$. We know that $\mathbb{B}_{m,q} = \mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$ which means that each function $f \in \mathbb{B}_{m,q}$ can be expressed uniquely as polynomial

$$f = f(x_1, \ldots, x_m) = \sum_{a=(a_1,\ldots,a_m)\in Z_q^m} c(a)X^a \quad (c(a) \in \mathbb{F}_q) \tag{2.1}$$

where $Z_q = \{0, 1, \ldots, q-1\}$ and $X^a = x_1^{a_1}, \ldots, x_m^{a_m}$.

Let $n = q^m$ and $\mathbb{F}_q^m = \{v_0 = (0, \ldots, 0), v_1, \ldots, v_{n-1}\}$. For $0 \leq \nu \leq m(q-1)$, the ν-th Reed–Muller code over $\mathbb{F}_q$ is defined by

$$RM(\nu, m; q) = \{c_f = (f(v_0), f(v_1), \ldots, f(v_{n-1})) \in \mathbb{F}_q^n | f \in \mathbb{B}_{m,q}, \deg f \leq \nu\}$$

This is a linear code over $\mathbb{F}_q$. Let α be a primitive element of $\mathbb{F}_{q^m}$ so that $\mathbb{F}_{q^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-2}\} (\alpha^{n-1} = 1)$. With a fixed basis $\{e_1, \ldots, e_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ (for example, we can choose $\{e_1, \ldots, e_m\} = \{1, \alpha, \ldots, \alpha^{m-1}\}$), $\mathbb{F}_{q^m}$ can be viewed as a vector space $\mathbb{F}_q^m$ by

$$\varphi : \mathbb{F}_{q^m} \xrightarrow{\sim} \mathbb{F}_q^m, \beta = \beta_1 e_1 + \cdots + \beta_m e_m (\beta_i \in \mathbb{F}_q) \mapsto (\beta_1, \ldots, \beta_m)$$

By the mapping φ, each element $\beta \in \mathbb{F}_{q^m}$ can be considered as the vector $\varphi(\beta) = (\beta_1, \ldots, \beta_m)$ in $\mathbb{F}_q^m$ so that we can set

$$\mathbb{F}_q^m = \{0, v_1, \ldots, v_{n-1}\} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-2}\} \tag{2.2}$$

Namely, we take $v_0 = 0$ and $v_i = \alpha^{i-1}$ for $1 \le i \le n-1$. With this ordering (2.2) of the elements of $\mathbb{F}_q^m$, we define the punctured v-th Reed–Muller codes over $\mathbb{F}_q$ for $0 \le \nu < m(q-1)$ as

$$RM^*(\nu, m; q) = \{c_f^* = (f(1), f(\alpha), \ldots, f(\alpha^{n-1}) | f \in \mathbb{B}_{m,q}, \deg f \le \nu\}$$

$RM^*(\nu, m; q)$ is a cyclic code over $\mathbb{F}_q$.

A linear code C in $\mathbb{F}_q^N$ is called cyclic if $c = (c_0, c_1, \ldots, c_{N-1}) \in C$ implies $(c_1, c_2, \ldots, c_{N-1}, c_0) \in C$. If we identify each codeword $c = (c_0, c_1, \ldots, c_{N-1})$ by the polynomial $c(x) = c_0 + c_1 x + \ldots + c_{N-1}x^{N-1}$ in the quotient ring $R = \mathbb{F}_q[x]/(x^N - 1)$, then a cyclic code C can be identified as a principle ideal $C =< g(x) >$ of R where $g(x)$ is a monic polynomial in $\mathbb{F}_q[x]$, $g(x) \mid x^N - 1$. We call $g(x)$ as the generating polynomial of the cyclic code C. And the dimension of C over $\mathbb{F}_q$ is $N - \deg g(x)$. The basis parameters of $RM(\nu, m; q)$ and $RM^*(\nu, m; q)$ are

Lemma 2.1 ([5], Chap. 5) *Let $0 \le \nu < m(q-1)$, then*

(1) *$RM(\nu, m; q)$ is a linear code over $\mathbb{F}_q$ with code length $n = q^m$, dimension $k(\nu, m; q)$ and minimal distance d where*

$$\begin{aligned} k(\nu, m; q) &= \dim_{\mathbb{F}_q} RM(\nu, m; q) \\ &= \sharp\{X^a = x_1^{a_1} \cdots x_m^{a_m} | 0 \le a_1, \ldots, a_m \le q-1, a_1 + \cdots + a_m \le \nu\} \\ &= \sum_{i=0}^{\nu} \sum_{\lambda=0}^{m} (-1)^\lambda \binom{m}{\lambda} \binom{i + m - 1 - \lambda q}{i - \lambda q} \\ &= \text{the coefficient } a_\nu \text{ in the power series } \frac{(1-t^q)^m}{(1-t)^{m+1}} = \sum_{i=0}^{\infty} a_i t^i \end{aligned}$$

and

$$d = (q-s)q^{m-r-1} \quad \left(r = \left[\frac{\nu}{q-1}\right],\ s = \nu - r(q-1)\right) \tag{2.3}$$

(2) *$RM^*(\nu, m; q)$ is a cyclic code over $\mathbb{F}_q$ with code length $n-1$, dimension $k(\nu, m; q)$ and minimal distance $d-1$ where d is defined by (2.3). The generating polynomial of $RM^*(\nu, m; q)$ is*

$$g(x) = \prod_{\substack{1 \le u \le n-2 \\ 1 \le w_q(u) \le m(q-1)-1-\nu}} (x - \alpha^u) \quad \in \mathbb{F}_q[x] \tag{2.4}$$

where $w_q(u) = u_0 + \cdots + u_{m-1}$ for q-adic expansion of $u = u_0 + u_1 q + \cdots + u_{m-1}q^{m-1}$ ($u_i \in \{0, 1, \ldots, q-1\}$).

From Lemma 2.1 we can get the following result which is the main tool in next three sections.

Lemma 2.2 *Suppose that $0 < \nu < m(q-1), k = k(\nu, m; q), s \ge 1$ and $sk \le n = q^m$. Then there exists s disjoint subsets $A_1, \ldots, A_s$ of $\mathbb{F}_q^m$ satisfying the following conditions*

(1) $|A_i| = k (1 \le i \le s)$
(2) *For each nonzero polynomial $f = f(x_1, \ldots, x_m) \in \mathbb{B}_{m,q}$ with $\deg f \le \nu$ and each $i (1 \le i \le s)$, there exists $v \in A_i$ such that $f(v) \ne 0$.*

Proof As before we assume that α is a primitive element of $\mathbb{F}_{q^m}$ and

$$\mathbb{F}_q^m = \mathbb{F}_{q^m} = \{v_0, v_1 = 1, v_2 = \alpha, \ldots, v_{n-1} = \alpha^{n-2}\}(n = q^m)$$

We take

$$\begin{aligned} A_1 &= \{v_0, v_1, \ldots, v_{k-1}\}, \\ A_2 &= \{v_k, v_{k+1}, \ldots, v_{2k-1}\}, \\ &\vdots \\ A_s &= \{v_{(s-1)k}, v_{(s-1)k+1}, \ldots, v_{sk-1}\} \end{aligned} \tag{2.5}$$

From assumption $sk \leq n$ we know that $A_i (1 \leq i \leq s)$ are disjoint subsets of $\mathbb{F}_q^m$ and $|A_i| = k (1 \leq i \leq s)$. Next we confirm the condition (2). Let f be a polynomial in $\mathbb{B}_{m,q}$ with $\deg f \leq \nu$. Then $c_f = (f(v_0), f(v_1), \ldots, f(v_{n-1}))$ is a codeword in $RM(\nu, m; q)$ and $c_f^* = (f(v_1), \ldots, f(v_{n-1})) \in RM^*(\nu, m; q)$. Suppose that there exists $i (1 \leq i \leq s)$ such that $f(v) = 0$ for all $v \in A_i$.

If $i \geq 2$, by definition (2.5) of A_i, we know that there are at least k sequential components of vector c_f^* being zero: $f(v_j) = f(v_{j+1}) = \ldots = f(v_{j+k-1}) = 0$ where $j = (i-1)k$. But $RM^*(\nu, m; q)$ is a cyclic code with dimension $k = k(\nu, m; q)$ by Lemma 2.1 and c_f^* is a codeword in $RM^*(\nu, m; q)$, we know that

$$c^* = (f(v_{i+k}), \ldots, f(v_{n-1}), f(v_1), f(v_2), \ldots, f(v_{i-1}), 0, \ldots, 0) \in RM^*(\nu, m; q)$$

The cyclic code $RM^*(\nu, m; q)$ is considered to be a principle ideal $(g(x))$ of the quotient ring $R = \mathbb{F}_q[x]/(x^{n-1} - 1)$ where $g(x)$ is the generating polynomial of $RM^*(\nu, m; q)$ with $\deg g(x) = n - 1 - k$, and the codeword c^* is considered to be the polynomial

$$\begin{aligned} c^*(x) = f(v_{i+k}) + f(v_{i+k+1})x + \cdots + f(v_{n-1})x^{n-i-k-1} + f(v_1)x^{n-i-k} \\ + \cdots + f(v_{i-1})x^{n-k-2} \in R \end{aligned}$$

Since $g(x)|c^*(x)$ and $n-1-k = \deg g(x) > n-k-2 \geq \deg c^*(x)$, we know that $c^*(x) = 0$ so that $f(v) = 0$ for all $v \in \mathbb{F}_q^m \backslash \{0\}$. From $\nu < m(q-1)$ we know that the minimal distance of $RM(\nu, m; q)$ is at least 2 by (2.3). Therefore $f(0) = 0$ so that $f \equiv 0$.

If $i = 1$, we have $f(v_1) = \cdots = f(v_{k-1}) = 0$ and

$$\begin{aligned} c_f^* &= (0, \ldots, 0, f(v_k), \ldots, f(v_{n-1})) = f(v_k)x^{k-1} + f(v_{k+1})x^k + \ldots + f(v_{n-1})x^{n-2} \\ &= x^{k-1}h(x) \in (g(x)) = RM^*(\nu, m; q) \end{aligned}$$

where $h(x) = f(v_k) + f(v_{k+1})x + \cdots + f(v_{n-1})x^{n-k-1}$ is divisible by $g(x)$. From $\deg g(x) = n-k-1$ we know that $h(x) = ag(x)$ for some $a \in \mathbb{F}_q$. Since $\nu < m(q-1)$, we have $0 = f(v_0) + \cdots + f(v_{n-1}) = f(v_0) + ag(1)$ so that $f(v_0) = -ag(1)$. But $f(v_0) = 0$ by $v_0 \in A_1$, and $g(1) \neq 0$ since 1 is not a root of the polynomial $g(x)$ by (2.4), we know that $a = 0$ so that $f \equiv 0$.

This completes the proof of Lemma 2.2. □

3 Generalized algebraic immunity (1): from $\mathbb{F}_2$ to $\mathbb{F}_q$

Let $\mathbb{B}_{m,q}$ be the ring of all functions $f : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q$. Batten [6] presented the following generalization of algebraic immunity. Each function of $f \in \mathbb{B}_{m,q}$ can be expressed uniquely as a polynomial in formula (2.1).

Definition 3.1 For $f = f(x_1, \ldots, x_m) \in \mathbb{B}_{m,q}$, the algebraic immunity of f is defined by

$$AI_m(f) = \min\{\deg g \mid 0 \neq g \in \mathbb{B}_{m,q}, \quad gf = 0 \text{ or } g(f^{q-1} - 1) = 0\}$$

It is easy to see that this definition is a generalization of the Definition 1.1 with $q = 2$.

Lemma 3.2 *For each* $0 \neq f \in \mathbb{B}_{m,q}$, $AI_m(f) \leq \lceil \frac{(q-1)m}{2} \rceil$ *where, for real number* α, $\lceil \alpha \rceil$ *is the smallest integer* n *such that* $n \geq \alpha$.

Proof See [6]. □

Now we prove that the upper bound can be reached for any $m \geq 1$ and prime power q.

Theorem 3.3 *For each* $m \geq 1$ *and finite field* $\mathbb{F}_q$, *there exists* $f \in \mathbb{B}_{m,q}$ *such that* $AI_m(f) = \lceil \frac{(q-1)m}{2} \rceil$.

Proof Let $\nu = \lceil \frac{(q-1)m}{2} \rceil - 1$ and consider the Reed–Muller code $RM(\nu, m; q)$. Let $n = q^m$ and α be a primitive element of $\mathbb{F}_{q^m}$. As before we identify a vector $v = (v_0, \ldots, v_{m-1}) \in \mathbb{F}_{q^m}$ with $v_0 + v_1\alpha + \cdots + v_{m-1}\alpha^{m-1} \in \mathbb{F}_{q^m}$.

From $\nu = \lceil \frac{(q-1)m}{2} \rceil - 1 < \frac{(q-1)m}{2}$ we know that

$$k = k(\nu, m; q) (= \dim RM(\nu, m; q)) = \sharp\{x_1^{a_1} \cdots x_m^{a_m} | 0 \leq a_i \leq q - 1 (1 \leq i \leq m)\} \leq \frac{q^m}{2}$$

By Lemma 2.2, we have two disjoint subsets A_1 and A_2 of $\mathbb{F}_{q^m}$ such that $|A_1| = |A_2| = k$ and any $g \in \mathbb{B}_{m,q}$ with $\deg g \leq \nu$ satisfying $g(\beta) = 0$ for all $\beta \in A_1$ or $g(\gamma) = 0$ for all $\gamma \in A_2$ is necessarily equal to zero. Now we consider $f \in \mathbb{B}_{m,q}$ defined by

$$f(\beta) = \begin{cases} 0, & \text{for } \beta \in A_1 \\ b^*, & \text{for } \beta \in A_2 \\ b, & \text{otherwise} \end{cases} \tag{3.1}$$

where b^* can be any non-zero element of $\mathbb{F}_q$ and b can be arbitrary element of $\mathbb{F}_q$. We claim that $AI_m(f) = \lceil \frac{(q-1)m}{2} \rceil = \nu + 1$.

Suppose that $g \in \mathbb{B}_{m,q}$, $\deg g \leq \nu$. If $gf = 0$ and then $g(\beta) = 0$ for each $\beta \in A_2$ by (3.1). Therefore $g = 0$.

Similarly, if $g(f^{q-1} - 1) = 0$, then $f^{q-1}(\beta) - 1 = -1$ and $g(\beta) = 0$ for each $\beta \in A_1$. Therefore we also have $g = 0$. Thus $AI_m(f) \geq \nu + 1$ and by Lemma 3.2 we have $AI_m(f) = \lceil \frac{(q-1)m}{2} \rceil$. □

By action of $GL(m, \mathbb{F}_q)$ as $\mathbb{F}_q$-linear transformations on $\{x_1, \ldots, x_m\}$, we can get more functions $f \in \mathbb{B}_{m,q}$ with algebraic immunity $AI_m(f) = \lceil \frac{(q-1)m}{2} \rceil$.

4 Generalized algebraic immunity (2): vector-valued

Let $m \geq n \geq 1$ and $\mathbb{B}_{m,n}$ be the ring of all functions

$$f = (f_1, \ldots, f_n) : \mathbb{F}_2^m \to \mathbb{F}_2^n$$

where $f_i \in \mathbb{B}_m (1 \leq i \leq n)$. For a subset S of $\mathbb{F}_2^m$, the annihilating ideal of S is defined by

$$N(S) = \{g \in \mathbb{B}_m : g|_S = 0\}$$

where $g|_S$ is the restriction of g on S. Namely, $g|_S = 0$ means that $g(v) = 0$ for all $v \in S$. Let

$$AI(S) = \min\{\deg g | 0 \neq g \in N(S)\} = \min\{\deg g | 0 \neq g \in \mathbb{B}_m, g|_S = 0\}$$

Armknecht and Krause [3] presented the following definition of generalized algebraic immunity to deal with S-boxes in block ciphers.

Definition 4.1 For $0 \neq f = (f_1, \ldots, f_n) \in \mathbb{B}_{m,n}$, the algebraic immunity of f is defined by

$$\begin{aligned} AI(f) &= \min\{AI(f^{-1}(a)) : a \in \mathbb{F}_2^n\} \\ &= \min\{\deg g : 0 \neq g \in \mathbb{B}_m \text{ and } \exists a \in \mathbb{F}_2^n \text{ such that } g|_{f^{-1}(a)} = 0\} \end{aligned}$$

where for $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$, $f^{-1}(a)$ is defined by

$$f^{-1}(a) = \{v \in \mathbb{F}_2^m : f_i(v) = a_i (1 \leq i \leq n)\}$$

It is easy to see that Definition 4.1 is a generalization of Definition 1.1($n = 1$). Let d be the smallest integer such that $\sum_{i=0}^{d} \binom{m}{i} > 2^{m-n}$. An upper bound of $AI(f)$ has been presented in [3].

Lemma 4.2 ([3]) *Assume that $m \geq n \geq 1$. For $0 \neq f \in \mathbb{B}_{m,n}$ we have $AI(f) \leq d$.*

Now we prove that the upper bound d can be reached.

Theorem 4.3 *Assume that $m \geq n \geq 1$. There exists $f \in \mathbb{B}_{m,n}$ such that $AI(f) = d$ where d is the smallest integer satisfying $\sum_{i=0}^{d} \binom{m}{i} > 2^{m-n}$.*

Proof From the definition of d we know that $\sum_{i=0}^{d-1} \binom{m}{i} \leq 2^{m-n}$. By Lemma 2.1(1) we konw that $\sum_{i=0}^{d-1} \binom{m}{i}$ is the dimension $k = k(d-1, m; 2)$ of the binary Reed–Muller code $RM(d-1, m; 2)$. By Lemma 2.2 we have 2^n disjoint subsets $S_j (0 \leq j \leq 2^n - 1)$ of $\mathbb{F}_2^m$ satisfying $|S_j| = \sum_{i=0}^{d-1} \binom{m}{i}$ $(0 \leq j \leq 2^n - 1)$ and for each $0 \neq g \in \mathbb{B}_m$, $\deg g \leq d-1$, and each $j (0 \leq j \leq 2^n - 1)$ there exists $v \in S_j$ such that $g(v) \neq 0$.

Now we define $f_\lambda \in \mathbb{B}_m (0 \leq \lambda \leq n-1)$ by

$$f_\lambda(v) = \begin{cases} 1, & \text{if } v \in S_j \text{ and } j_\lambda = 1 (0 \leq j \leq 2^n - 1) \\ 0, & \text{if } v \in S_j \text{ and } j_\lambda = 0 (0 \leq j \leq 2^n - 1) \\ c, & \text{if } v \notin S_0 \bigcup S_1 \bigcup \ldots \bigcup S_{2^n-1} \end{cases}$$

where j_λ is the coefficient in the 2-adic expansion $j = j_0 + j_1 2 + \cdots + j_{n-1} 2^{n-1}$, and c can be any element of $\mathbb{F}_2$.

We claim that for $f = (f_0, \ldots, f_{n-1}) \in \mathbb{B}_{m,n}$, we have $AI(f) = d$. In fact, for each $b = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_2^n$, and $a \in S_0 \bigcup S_1 \bigcup \ldots \bigcup S_{2^n-1}$,

$$\begin{aligned} a \in f^{-1}(b) &\iff f_\lambda(a) = b_\lambda (0 \leq \lambda \leq n-1) \\ &\iff \text{for each } \lambda (0 \leq \lambda \leq n-1), a \in \bigcup \{S_j | 0 \leq j \leq 2^n - 1, j_\lambda = b_\lambda\} \\ &\iff a \in S_j \text{ where } j = b_0 + b_1 2 + \cdots + b_{n-1} 2^{n-1} \end{aligned}$$

Therefore $f^{-1}(b) \supseteq S_j$ for $j = b_0 + b_1 2 + \cdots + b_{n-1}2^{n-1}$. Suppose that $g \in \mathbb{B}_m$ and $\deg g \leq d-1$. If $g|_{f^{-1}(b)} = 0$ for some $b = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_2^n$, then $g|_{S_j} = 0$ for $j = b_0 + b_1 2 + \cdots + b_{n-1}2^{n-1}$ so that $g \equiv 0$. Thus $AI(f) \geq d$ and then $AI(f) = d$ by Lemma 4.2. This completes the proof of Theorem 4.3. □

There is another kind of algebraic immunity of $f \in \mathbb{B}_{m,n}$ defined in [3]. The subset

$$gr(f) = \{(x, f(x)) \in \mathbb{F}_2^{m+n} \mid x \in \mathbb{F}_2^m\}$$

of $\mathbb{F}_2^{m+n}$ is called the graph of f. The algebraic immunity of $gr(f)$ is defined by

$$AI(gr(f)) = \min\{\deg G \mid 0 \neq G = G(x, y) \in \mathbb{B}_{m+n}, G|_{gr(f)} = 0\}$$

It is proved in [3] that $AI(f) \leq AI(gr(f)) \leq AI(f)+n$ for each $f \in \mathbb{B}_{m,n}$, and $AI(gr(f)) \leq D_{m,n}$ where $D_{m,n}$ is the smallest integer such that $\sum_{i=0}^{D} \binom{m+n}{i} > 2^m$. For $n = 1$, the maximal value $AI(gr(f)) = D_{m,1}(=\lceil \frac{n+1}{2} \rceil)$ can be reached by some $f \in \mathbb{B}_{m,1} = \mathbb{B}_m$. It is conjectured in [3] that the upper bound $D_{m,n}$ can also be reached for general case $m \geq n \geq 2$. A necessary and sufficient condition for $\max\{AI(gr(f)) : f \in \mathbb{B}_{m,n}\} = D_{m,n}$ has been made in [3] with matroid language. Using the matroid criterion and by computation, the conjecture has been verified to be true for $2 \leq n \leq m \leq 14$ and $(m, n) = (15, 2)$ in [3]. But it seems that the conjecture has not been solved completely.

5 Generalized algebraic immunity (3): $\mathbb{F}_q$ and vector-valued

Let $m \geq n \geq 1$ and q be a prime power. Ars and Faugere [4] present the following definition of algebraic immunity for a function $f = (f_1, \ldots, f_n) : \mathbb{F}_q^m \to \mathbb{F}_q^n (f_i = f_i(X) = f_i(x_1, \ldots, x_m) \in \mathbb{B}_{m,q})$. They consider the ring

$$R = \mathbb{F}_q[x_1, \ldots, x_m; z_1, \ldots, z_n]/(x_i^q - x_i, z_j^q - z_j \mid 1 \leq i \leq m, 1 \leq j \leq n)$$

and the ideal

$$I =< z_1 - f_1(X), \ldots, z_n - f_n(X) >$$

of R generated by $z_i - f_i(X) (1 \leq i \leq n)$.

Definition 5.1 ([4]) The algebraic immunity $AI_S(f)$ of $f \in \mathbb{B}_{m,n,q}$ is defined by

$$AI_S(f) = \min\{\deg_X P \mid 0 \neq P = P(X, Z) \in I\}$$

where $\deg_X P$ is the degree of $P = P(X, Z) = P(x_1, \ldots, x_m; z_1, \ldots, z_n)$ viewed as a polynomial in $x_1, \ldots, x_m$.

Lemma 5.2 (1) *If $n = 1$ and $q = 2$, then for $f \in \mathbb{B}_m$, $AI_S(f)$ is the same as $AI_m(f)$ defined by the Definition 1.1.*

(2) ([4]) *Let $\frac{(1-t^q)^m}{(1-t)^{m+1}} = \sum_{i \geq 0} c_i t^i \in \mathbb{Z}[[t]]$ and $d = d(m, n; q)$ be the smallest integer such that $c_d > q^{m-n}$, then $AI_S(f) \leq d$.*

Proof (1) Let $f \in \mathbb{B}_m, d' = AI_m(f)$ and $d = AI_S(f)$. Let $g \in \mathbb{B}_m, \deg g = d'$ such that $fg = 0$ or $g(f + 1) = 0$. Remark that $I =< z + f >$ so that $(z + f)g \in I$. And

$$(z + f)g = \begin{cases} zg, & \text{if } fg = 0 \\ zg + g, & \text{if } (f + 1)g = 0 \end{cases}$$

Therefore $\deg_X(z+f)g = d'$ so that $AI_S(f) \le d' = AI_m(f)$. On the other hand, let $g, h, g', h' \in \mathbb{B}_m$, $\max(\deg g', \deg h') = d$ and $(z+f)(gz+h) = g'z + h'$ which means that

$$fh = h' \text{ and } (f+1)g + h = g'$$

Then $fg' = fh = h'$, $f(g'+h') = 0$ and $\deg(g'+h') \le d$. If $g'+h' \neq 0$, from $f(g'+h') = 0$ we get $AI_m(f) \le d = AI_S(f)$. If $g'+h' = 0$, then from $fg' = h'$ we get $(f+1)g' = 0$ and $d = \max(\deg g', \deg h') = \deg g'$ since $g' = h'$. Therefore we also get $AI_m(f) \le d = AI_S(f)$.

(2) $A = R/I$ is a vector space over $\mathbb{F}_q$ with dimension q^m since $\{x_1^{a_1} \cdots x_m^{a_m} | 0 \le a_i \le q-1 (1 \le i \le m)\}$ is a basis of A. Consider the set

$$S = \{X^a Z^b = x_1^{a_1} \cdots x_m^{a_m} z_1^{b_1} \cdots z_n^{b_n} \mid 0 \le a_i, b_j \le q-1, a_1 + \ldots + a_m (= \deg_X(X^a Z^b)) \le d\}$$

It is easy to see that $|S| = q^n c_d$. By assumption $q^n c_d > q^m = \dim A$ we know that there exists $0 \neq g(X, Z) \in R, \deg_X g \le d$ such that $g(X, Z) = 0 \in A$. Namely, $g(X, Z) \in I$ which means that $AI_S(f) \le d$. □

Now we show that the upper bound of $AI_S(f)$ given in Lemma 5.2(2) can be reached.

Theorem 5.3 *For each prime power q and $1 \le n \le m$, let $d = d(m, n; q)$ be the integer defined in Lemma 5.2. Then there exists $f \in \mathbb{B}_{m,n,q}$ such that $AI_S(f) = d$.*

Proof By the definition of d we have $c_{d-1} \le q^{m-n}$. Since c_{d-1} is just the same as the dimension $k(d-1, m; q)$ of the Reed–Muller code $RM(d-1, m; q)$, from Lemma 2.2 we have q^n disjoint subsets $S_b (b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n)$ of $\mathbb{F}_q^m$ as a partition of $\mathbb{F}_q^m$, such that $|S_b| = q^{m-n} (b \in \mathbb{F}_q^n)$, and for each $b \in \mathbb{F}_q^n$ and $0 \neq g(X) \in \mathbb{B}_{m,q}$ with $\deg g(X) \le d-1$, there exists $v \in S_b$ such that $g(v) \neq 0$. Now we define $f_i \in \mathbb{B}_{m,q} (1 \le i \le n)$ by, for each $X \in \mathbb{F}_q^m$,

$$f_i(X) = b_i \text{ if } X \in S_b \text{ and } b = (b_1, \ldots, b_n) \tag{5.1}$$

We claim that for $f = (f_1, \ldots, f_n) : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^n$, we have $AI_S(f) = d$.

Suppose that

$$\sum_{i=1}^{n} (z_i - f_i(X)) H_i(X, Z) = G(X, Z) \in I \tag{5.2}$$

where $H_i(X, Z) \in \mathbb{F}_q[x_1, \ldots, x_m; z_1, \ldots, z_n] (1 \le i \le n)$ and $\deg_X G(X, Z) \le d-1$, we need to prove $G(X, Z) \equiv 0$. For doing this, we consider the following polynomials $\{M^{(b)}(Z) | b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n\}$ defined by

$$M^{(b)}(Z) = (1 - (z_1 - b_1)^{q-1}) \cdots (1 - (z_n - b_n)^{q-1}) = \begin{cases} 1, & \text{if } (z_1, \ldots, z_n) = b \\ 0, & \text{otherwise} \end{cases}$$

Then each polynomial $H_i(X, Z)$ can be expressed uniquely as

$$H_i(X, Z) = \sum_{b \in \mathbb{F}_q^n} M^{(b)}(Z) h_i^{(b)}(X)$$

where

$$h_i^{(b)}(X) = H_i(X, b) (1 \le i \le n, b \in \mathbb{F}_q^n)$$

Similarly we have

$$G(X, Z) = \sum_{b\in\mathbb{F}_q^n} M^{(b)}(Z)g^{(b)}(X)$$

and assumption $\deg_X G(X, Z) \le d-1$ is the same as $\deg g_i^{(b)}(X) \le d-1$ for all $b \in \mathbb{F}_q^n$. We need to prove $g_i^{(b)}(X) \equiv 0$ for all $b \in \mathbb{F}_q^n$.

Now by the definition of $M^{(b)}(Z)$ the equality (5.2) becomes that

$$\begin{aligned}\sum_{b\in\mathbb{F}_q^n} M^{(b)}(Z)g^{(b)}(X) &= \sum_{i=1}^{n}(z_i - f_i(X)) \sum_{b\in\mathbb{F}_q^n} M^{(b)}(Z)h_i^{(b)}(X)\\ &= \sum_{b\in\mathbb{F}_q^n} M^{(b)}(Z) \sum_{i=1}^{n}(z_i - f_i(X))h_i^{(b)}(X)\\ &= \sum_{b\in\mathbb{F}_q^n} M^{(b)}(Z) \sum_{i=1}^{n}(b_i - f_i(X))h_i^{(b)}(X)\end{aligned}$$

Therefore for each $b \in \mathbb{F}_q^n$,

$$g^{(b)}(X) = \sum_{i=1}^{n}(b_i - f_i(X))h_i^{(b)}(X)$$

which implies that $g^{(b)}(X)|_{f^{-1}(b)} = 0$. But

$$\begin{aligned}f^{-1}(b) &= \{X = (x_1, \ldots, x_m) \in \mathbb{F}_q^m | f_i(X) = b_i (1 \le i \le n)\}\\ &= S_b \quad \text{(by definition (5.1) of } f_i(X))\end{aligned}$$

Thus $g^{(b)}(X)|_{S_b} = 0$ so that $g^{(b)}(X) \equiv 0$ by assumption $\deg g^{(b)}(X) \le d-1$ for all $b \in \mathbb{F}_q^n$. This completes the proof of $AI_S(f) \ge d$ and then $AI_S(f) = d$ by Lemma 5.2. □

Remark Ars and Faugere [4] have defined another algebraic immunity of $f = (f_1, \ldots, f_n) : \mathbb{F}_q^m \to \mathbb{F}_q^n$ by

$$AI_B(f) = \min\{\deg g(X, Z) | 0 \ne g(X, Z) \in I\}$$

where $\deg g$ is the degree of $g(X, Z)$ as a polynomial in $x_1, \ldots, x_m; z_1, \ldots, z_n$. Let $\frac{(1-t^q)^{m+n}}{(1-t)^{m+n+1}} = \sum_{i\ge 0} A_i t^i$ and $D = D(m, n; q)$ be the smallest integer i satisfying $A_i > q^n$. It is shown in [4] by a similar argument in the proof of Lemma 5.2(2) that $AI_B(f) \le D$ for all $f \in \mathbb{B}_{m,n,q}$. We are not sure if the upper bound $D(m, n; q)$ of $f \in \mathbb{B}_{m,n;q}$ is tight.

Acknowledgments We thank two anonymous referees for several suggestions that corrected some imprecisions in an earlier version of this paper. This paper is supported by the National Fundamental Science Research Program 973 of China with No. 2004 CB3180004, grant of NSFC with No. 60433050 and grant of NSFC with No. 60503011.

References

1. Armknecht F.: Improving fast algebraic attacks. In: Roy B., Meier W. (eds.) FSE 2004, LNCS, vol. 3017, pp. 65–82 (2004).

2. Armknecht F., Krause M.: Algebraic attacks on combiners with memory. In: Boneh D. (ed.) Advances in Cryptology—Crypto 2003, LNCS, vol. 2729, pp. 162–176 (2003).
3. Armknecht F., Krause M.: Constructing single- and multi-output Boolean functions with maximal algebraic immunity. In: Proceedings of ICALP 2006, LNCS, vol. 4052, pp. 180–191 (2006).
4. Ars G., Faugere J.-C.: Algebraic immunity of functions over finite fields, INRIA, No report 5532 (2005).
5. Assmus E.F., Key J.D. Jr.: Designs and their Codes. Cambridge University Press (1992).
6. Batten L.M.: Algebraic attacks over $GF(q)$. In: Canteaut A., Viswanathan K. (eds.) Progress in Cryptology—INDOCRYPT 2004, LNCS, vol. 3348, pp. 84–91 (2004).
7. Courtois N.: Fast algebraic attacks over $GF(q)$. In: Boneh D. (ed.) Advances in Cryptology—Crypto 2003, LNCS, vol. 2729, pp. 176–194 (2003).
8. Meier W., Pasalic E., Carlet C.: Algebraic attacks and decomposition of Boolean functions. In: Cachin C., Camenisch J. (eds.) Advances in Cryptology—EUROCRYPT 2004, LNCS, vol. 3207, pp. 474–491 (2004).