

Linear characteristics of functions over Galois rings

Kamlovskii O.V.

Academy of Cryptography of Russian Federation, Moscow

Let $R = GR(q^l, p^l)$ denote the Galois ring of characteristic p^l with q^l elements, where p is a prime number and $q = p^t$.

Some properties of ring R :

1)

$$GR(q^l, p^l) \cong \mathbb{Z}_{p^l}[x]/f(x),$$

where $\bar{f}(x)$ (image of $f(x)$ under the mod $-p$ reduction map) is irreducible polynomial over the ring $\mathbb{Z}_p$, $\deg f(x) = t$;

2) when $t = 1$ $GR(q^l, p^l)$ is equal to $\mathbb{Z}_{p^l}$, and when $l = 1$ $GR(q^l, p^l)$ is equal to $GF(q)$;

3) $\Gamma(R) = \{x \in R : x^q = x\}$ is a cyclic subgroup of R^* (group of units in the ring R).

Galois rings share with Galois fields almost all their properties.

Additive characters of the Galois rings

The p -adic expansion of element $x \in R$ is given by

$$x = x_0 + px_1 + \dots + p^{l-1}x_{l-1},$$

where $x_0, x_1, \dots, x_{l-1} \in \Gamma(R)$.

The Frobenius automorphism $\varphi : R \rightarrow R$ is defined for such x as

$$\varphi(x) = x_0^p + px_1^p + \dots + p^{l-1}x_{l-1}^p,$$

and the trace Tr from R down to $\mathbb{Z}_{p^l}$

$$\text{Tr}(x) = x + \varphi(x) + \dots + \varphi^{t-1}(x).$$

Every additive character of R has the form

$$\chi_c(x) = \exp \left\{ 2\pi i \frac{\text{Tr}(cx)}{p^l} \right\},$$

where $c \in R$.

Fourier coefficients of a function

Let L_n denote the set of maps $g : R^n \rightarrow \mathbb{C}$.

For arbitrary $g_1, g_2 \in L_n$ let $S : L_n \times L_n \rightarrow \mathbb{C}$ denote

$$S(g_1, g_2) = \frac{1}{|R|^n} \sum_{\vec{x} \in R^n} \psi_1(\vec{x}) \overline{\psi_2(\vec{x})}.$$

Then (L_n, S) is a Euclidean space.

For $\vec{a} = (a_1, \dots, a_n) \in R^n$ consider a map $\chi_{\vec{a}} : R^n \rightarrow \mathbb{C}$, such that

$$\chi_{\vec{a}}(x_1, \dots, x_n) = \chi_{a_1}(x_1) \cdots \chi_{a_n}(x_n).$$

The function system $\chi_{\vec{a}}$, where $\vec{a} \in R^n$, forms an orthonormal basis of (L_n, S) .

For every map $g \in L_n$ there exist unique complex numbers $\nu_g(\vec{a})$, such that

$$g(x_1, \dots, x_n) = \sum_{\vec{a} \in R^n} \nu_g(\vec{a}) \chi_{\vec{a}}(x_1, \dots, x_n).$$

Linear characteristics of a function

The function $f : R^n \rightarrow R$ induces $|R| - 1$ maps $f \cdot \chi_c : R^n \rightarrow \mathbb{C}$, where $c \in R$, $c \neq 0$.

Definition

The linear characteristic of a function $f : R^n \rightarrow R$ is defined as

$$\delta(f) = \max_{c \in R \setminus \{0\}} \max_{\vec{a} \in R^n} |\nu_{f \cdot \chi_c}(\vec{a})|.$$

(Remizov A.B., 1986; Pott A., 2004 in the case of functions in abelian groups)

Definition

The incomplete linear characteristic of a function $f : R^n \rightarrow R$ is defined as

$$\delta(f)^* = \max_{c \in R^*} \max_{\vec{a} \in R^n} |\nu_{f \cdot \chi_c}(\vec{a})|.$$

The Parseval's relation has the form

$$\sum_{\vec{a} \in R^n} |\nu_{f \cdot \chi_c}(\vec{a})|^2 = 1. \quad (1)$$

Proposition

Let f be any function from R^n to R , where $R = GR(q^l, p^l)$. Then we have

$$1 \geq \delta(f) \geq \delta(f)^* \geq q^{-\frac{ln}{2}}.$$

The statement follows from equality (1).

Consider the special case when $R = GF(2) = \{0, e\}$:

$$\delta(f)^* = \delta(f) = \max_{\vec{a} \in R^n} |\nu_{f \cdot \chi_e}(\vec{a})| = \frac{1}{2^n} \max_{\vec{a} \in R^n} |W_f(\vec{a})|,$$

where $W_f(\vec{a})$ is the Walsh coefficient defined by the equation

$$W_f(\vec{a}) = \sum_{x_1, \dots, x_n \in R} (-1)^{f(\vec{x}) \oplus a_1 x_1 \oplus \dots \oplus a_n x_n}.$$

Nonlinearity $nl(f)$ of a function $f : R^n \rightarrow R$ is to use the minimum Hamming distance between f and all affine Boolean functions.

With this approach

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\vec{a} \in R^n} |W_f(\vec{a})| = 2^{n-1} - 2^{n-1} \delta(f) = 2^{n-1} - 2^{n-1} \delta(f)^*.$$

Cross-correlation coefficients

Let $f(\vec{x})$ and $g(\vec{x})$ be any functions from R^n to R , $\vec{x} = (x_1, \dots, x_n)$.

Definition

Cross-correlation coefficient between the functions f and g is given for $a \in R$ by the rule

$$C_a(f, g) = \sum_{x_1, \dots, x_n \in R} \chi_a(f(\vec{x}) - g(\vec{x})).$$

A function $f : R^n \rightarrow R$ is balance if the size $f^{-1}(z)$ is the same for every $z \in R$.

Proposition (Weil criterion)

Equality $C_a(f, g) = 0$ is true for all $a \in R \setminus \{0\}$ if and only if the function $f - g$ is balance.

Linear characteristics and cross-correlation coefficients

Let $A_n(R)$ be the set of all functions $g(\vec{x})$ defined by:

$$g(\vec{x}) = a_0 + a_1x_1 + \dots + a_nx_n,$$

where $a_0, a_1, \dots, a_n \in R$.

Proposition

We have

$$\delta(f) \geq \frac{1}{q^{ln}} \max_{a \in R \setminus \{0\}} \max_{g \in A_n(R)} |C_a(f, g)|;$$

$$\delta(f)^* = \frac{1}{q^{ln}} \max_{a \in R^*} \max_{g \in A_n(R)} |C_a(f, g)|;$$

and in case $R = GF(q)$

$$\delta(f) = \delta(f)^* = \frac{1}{q^{ln}} \max_{a \in R^*} \max_{g \in A_n(R)} |C_a(f, g)|.$$

(Bugrov A.D. in the case of Galois fields, 2015)

Linear characteristic and coefficients of the statistical structure

We consider the probabilities

$$P(f(\vec{x}) = g(\vec{x}))$$

where $g(\vec{x}) \in A_n(R)$ and the vector $\vec{x}$ is chosen randomly and equally likely from the set R^n .

An ordered set of such probabilities is called statistical structure of the function f .

Ambrosimov A.S. (1985) proved that in the case of $R = GF(q)$ and $R = \mathbb{Z}_k$ the function f is uniquely restored according to the statistical structure.

Proposition

For every function $g \in A_n(R)$ we have

$$\left| P(f(\vec{x}) = g(\vec{x})) - \frac{1}{q^l} \right| \leq \frac{q^l - 1}{q^l} \delta(f).$$

For the functions $f, g : R^n \rightarrow R$ proximity is determined by the rule

$$\delta(f, g) = \frac{q^l}{q^l - 1} \sum_{b \in R} \left(P(f(\vec{x}) - g(\vec{x}) = b) - \frac{1}{q^l} \right)^2,$$

where the vector $\vec{x}$ is chosen randomly and equally likely from the set R^n .

This function is similar to the consent function from the works of Kusmin A.S., Markov V.T., Nechaev A.A., Shishkin V.A., Shishkov A.B. (2006, 2007, 2008).

Proposition (Penzyakov R.V., 2024)

For all functions $f, g : R^n \rightarrow R$ over the ring $R = GR(q^l, p^l)$

$$\delta(f, g) = \frac{1}{(q^l - 1)q^{2ln}} \sum_{a \in R \setminus \{0\}} |C_a(f, g)|^2.$$

Proximity function of Solodovnikov V.I. and linear characteristics

Proposition

For all function $f : R^n \rightarrow R$ over the ring $R = GR(q^l, p^l)$

$$\frac{1}{q^l - 1} (\delta(f)^*)^2 \leq \max_{g \in A_n(R)} \delta(f, g) \leq \delta(f)^2.$$

Bent functions (the first approach)

The function $f : R^n \rightarrow R$ is called bent function if

$$|\nu_{f \cdot \chi_c}(\vec{a})| = q^{-\frac{nl}{2}}$$

for all $c \in R \setminus \{0\}$ and $\vec{a} \in R^n$.

(Ambrosimov A.S., 1994, for the case of Galois fields;

Solodovnikov V.I., 2002, for the case of abelian groups;

Carle C., Ding C., 2004, the functions with perfect nonlinearity)

Proposition

Let $R = GR(q^l, p^l)$ be Galois ring. The function $f : R^n \rightarrow R$ is bent function if and only if $\delta(f) = q^{-\frac{nl}{2}}$. If the function f is bent, then $\delta(f)^* = q^{-\frac{nl}{2}}$.

Are there bent functions over rings (the first approach)?

This question is open problem.

Theorem (Shishkov A.B., 2015)

Let $R = \mathbb{Z}_{p^l}$ be residue ring modulo p^l where p is a prime number. If $f : R \rightarrow R$ is a bent function, then

$$l = \begin{cases} 2, & \text{if } p = 2; \\ 1, 2, & \text{if } p \geq 3. \end{cases}$$

There are no examples of bent functions in the case $l = 2$.

Bent functions (the second approach)

The function $f : R^n \rightarrow R$ is called generalized bent function if

$$|\nu_{f \cdot \chi_e}(\vec{a})| = q^{-\frac{nl}{2}}$$

for all $\vec{a} \in R^n$, where e is the unit of the ring R .

(Kumar P.V., Sholtz R.A., Welch L.R., 1985, for the case of residue ring)

Example (Panpurin A.A., 2025)

Let $R = GF(4) = \{0, 1, \alpha, \alpha + 1\}$ be finite field, where α is the root of the polynomial $x^2 + x + 1$. Let $f : R^2 \rightarrow R$ be the function defined by:

$$f(x_1, x_2) = \alpha(x_1x_2 + x_1^2x_2^2).$$

Then the spectral coefficients have the form

$$|\nu_{f \cdot \chi_c}(\vec{a})| = \begin{cases} \frac{1}{4}, & \text{if } c \in \{1, \alpha\}, \vec{a} \in R^2; \\ 1, & \text{if } c = \alpha + 1, \vec{a} = (0, 0); \\ 0, & \text{if } c = \alpha + 1, \vec{a} \neq (0, 0). \end{cases}$$

Let $R = GR(q^l, p^l)$ be Galois ring, $n = 2k$ and π is a mapping from R^k to R^k with coordinate functions $\pi_1, \dots, \pi_k$ such that

$$\pi(\vec{x}) = (\pi_1(\vec{x}), \dots, \pi_k(\vec{x})) \text{ for all } \vec{x} \in R^k.$$

For any function $h : R^k \rightarrow R$ and all $\vec{x}, \vec{y} \in R^k$ we defined the function $f : R^n \rightarrow R$

$$f(\vec{x}, \vec{y}) = \langle \pi(\vec{x}), \vec{y} \rangle + h(\vec{x}) = \pi_1(\vec{x})y_1 + \dots + \pi_k(\vec{x})y_k + h(\vec{x}). \quad (2)$$

Proposition

For any permutation π on R^k the equality $\delta(f)^* = q^{-\frac{nl}{2}}$ will be true.

Theorem

Assume that $|\pi^{-1}(\vec{c})| \leq t$ for all $\vec{c} \in R^k$, then

$$\delta(f) \leq tq^{-\frac{n}{2}}, \quad \delta(f)^* \leq tq^{-\frac{nl}{2}}.$$

Correlation-immune functions over Galois rings

Let k be natural number and $f : R^n \rightarrow R$. We call the function f is k -th order correlation-immune if for all $a_1, \dots, a_k \in R$, $1 \leq i_1 < \dots < i_k \leq n$ and for all $z \in R$

$$\left| \left(f_{i_1, \dots, i_k}^{a_1, \dots, a_k} \right)^{-1} (z) \right| = \frac{|f^{-1}(z)|}{q^{lk}}. \quad (3)$$

The function f is k -resilient if it k -th order correlation-immune and balanced.

Example

For any permutations $g_1, \dots, g_{n+1}$ on R the function

$$f(x_1, \dots, x_n) = g_{n+1}(g_1(x_1) + \dots + g_n(x_n))$$

is a $(n-1)$ -resilient function on R^n .

Spectral coefficients of correlation-immune functions over Galois rings

Theorem (Camion P., Canteaut A., 1999)

Function f from R^n to R is k -th order correlation-immune if and only if

$$\nu_{f \cdot \chi_c}(\vec{a}) = 0$$

for every $c \in R \setminus \{0\}$ and every $\vec{a} \in R^n$ such that $1 \leq \|\vec{a}\| \leq k$.

Corrolary (Camion P., Canteaut A., 1999)

Function f from R^n to R is k -resilient if and only if

$$\nu_{f \cdot \chi_c}(\vec{a}) = 0$$

for every $c \in R \setminus \{0\}$ and every $\vec{a} \in R^n$ such that $0 \leq \|\vec{a}\| \leq k$.

Let $R = GR(q^l, p^l) = \{r_1, \dots, r_{q^l}\}$ be Galois ring and $f_{r_i} : R^{n-1} \rightarrow R, i = 1, \dots, q^l$.

We consider the function $f : R^n \rightarrow R$

$$f(x_1, x_2, \dots, x_n) = \begin{cases} f_{r_1}(x_2, \dots, x_n), & \text{если } x_1 = r_1; \\ \vdots & \\ f_{r_{q^l}}(x_2, \dots, x_n), & \text{если } x_1 = r_{q^l}. \end{cases} \quad (4)$$

Such Boolean functions from 7 variables were used in the stream encryption algorithms GEA-1 and GEA-2.

Theorem

Let f be the function constructed by the formula (4). Then

- 1) if the functions $f_{r_1}, \dots, f_{r_{q^l}}$ are k -th order correlation-immune and $\nu_{f_{r_1} \cdot \chi_c}(\vec{0}) = \dots = \nu_{f_{r_{q^l}} \cdot \chi_c}(\vec{0})$ for every $c \in R \setminus \{0\}$, then the function f is k -th order correlation-immune;*
- 2) if the functions $f_{r_1}, \dots, f_{r_{q^l}}$ are k -resilient, then the function f is k -resilient;*
- 3) for the linear characteristics we have*

$$\delta(f) \leq \frac{1}{q^l} \left(\delta(f_{r_1}) + \dots + \delta(f_{r_{q^l}}) \right),$$

$$\delta(f)^* \leq \frac{1}{q^l} \left(\delta(f_{r_1})^* + \dots + \delta(f_{r_{q^l}})^* \right).$$

Corrolary

Let f be the function constructed by the formula (4). If $f_{r_1}, \dots, f_{r_{q^l}}$ are the bent functions, then

$$q^{-\frac{nl}{2}} \leq \delta(f) \leq q^{-\frac{(n-1)l}{2}}.$$

Corrolary

Let f be the function constructed according to the rule (4). If $f_{r_1}, \dots, f_{r_{q^l}}$ are the functions from Eliseev-Maiorana-McFarland class, then

$$q^{-\frac{nl}{2}} \leq \delta(f)^* \leq q^{-\frac{(n-1)l}{2}}.$$

Thank you for your attention!