On a new classification of the Boolean functions

Sergey N. Fëdorov

Information Security Institute
of
Lomonosov University, Moscow

CTCrypt '18

Some notation

Boolean functions in n variables: $\mathcal{F}_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$

Inner product of $u, v \in V_n = \mathbb{F}_2^n$: $\langle u, v\rangle = \bigoplus_{i=1}^{n} u_i v_i$

Weight: $\mathrm{wt}(u) = \sum_{i=1}^{n} u_i, \quad \mathrm{wt}(f) = \sum_{u \in V_n} f(u)$

Support: $\operatorname{supp}\varphi = \{u \in V_n \mid \varphi(u) \neq 0\}$

Walsh–Hadamard spectrum: $W_f(u) = \sum_{v \in V_n} (-1)^{f(v) \oplus \langle u,v\rangle}$

Autocorrelation function: $\Delta_f(u) = \sum_{v \in V_n} (-1)^{f(v) \oplus f(u \oplus v)}$

Δ-equivalence

Global Avalanche Characteristics are two numerical parameters of *autocorrelation function* [Zhang X. M., Zheng Y., 1995].
Some other approaches implicitly use this function as well.

In a forthcoming paper of O. A. Logachev, V. V. Yashchenko, and S. F., it is proposed to treat autocorrelation function, on its own, for classifying Boolean functions.

Definition

Two Boolean functions f and g are Δ-*equivalent*, $f \overset{\Delta}{\sim} g$,

if their autocorrelation functions are identical, $\Delta_f = \Delta_g$.

Proposition

$$f \overset{\Delta}{\sim} g \iff |W_f| = |W_g|$$

Example

Consider the plateaued functions of order $2r$
$\left\{ f \in \mathcal{F}_n \mid \forall u \in V_n,\ W_f(u) \in \{0, \pm 2^{n-r}\} \right\}$

The plateaued functions f with fixed $\operatorname{supp} W_f$
form one Δ-equivalence class.

In particular,

- there is a Δ-equivalence class consisting of all bent functions;
- there are 2^n two-element classes $\{f,\ f \oplus 1\}$ for each linear f.

Cardinality κ of a $2r$-order plateaued function class satisfies
$2 \leqslant \kappa \leqslant C_{2^{2r}}^{2^{r-1}(2^r+1)}$.

Cryptographic properties / classes of Boolean functions

- Affine ($\mathcal{A}_n$)
- Algebraic degenerate,
  $\{f \mid \exists k < n, \exists g \in \mathcal{F}_k, \exists D \in \mathbb{F}_2^{k\times n} \colon \forall u \in V_n,\ f(u) = g(Du)\}$
- Balanced
- Plateaued of order $2r$, $\{f \mid \forall u \in V_n,\ W_f(u) \in \{0, \pm 2^{n-r}\}\}$
- Maximal nonlinear, or bent when n is even
- Correlation immune
  - CI_a: w. r. t. a vector a ($f(u) \oplus \langle a, u\rangle$ is balanced)
  - $\mathrm{CI}(k)$: of order k
    $(\forall i_j, \forall a_j \in \mathbb{F}_2,\ \Pr[f(u) = 1] = \Pr[f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}(u) = 1])$
- k-Resilient (i. e., balanced and $\mathrm{CI}(k)$)

Criteria

- Strict avalanche criterion (SAC)
  $(\forall a\colon \mathrm{wt}(a) = 1,\ \Pr[f(u \oplus a) \neq f(u)] = \frac{1}{2})$
- Propagation criterion (PC)
  - PC_a: w. r. t. a vector a $(\Pr[f(u \oplus a) \neq f(u)] = \frac{1}{2})$
  - $\mathrm{PC}(k)$: of degree k (PC_a for all a with $1 \leqslant \mathrm{wt}(a) \leqslant k$)

Vector sets

- $\operatorname{supp} W_f$
- $L_f = \{u \in V_n \mid \forall v \in V_n \quad f(v \oplus u) = f(v) \oplus \varepsilon_u,\ \varepsilon_u \in \mathbb{F}_2\}$ (space of linear structures)
- $\mathrm{PC}_f = \{u \in V_n \mid f \text{ satisfies } \mathrm{PC}_u\}$
- $\mathrm{CI}_f = \{u \in V_n \mid f \text{ is correlation immune w. r. t. } u\}$

Numerical characteristics

- Nonlinearity (distance to $\mathcal{A}_n$):

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in V_n} |W_h(u)|$$

- Curvature: $\mathrm{curv}(f) = \sum_{u \in V_n} |W_f(u)|$

[R. A. de la Cruz Jimenez, O. V. Kamlovskiy, 2016]

[O. A. Logachev, S. N. Fedorov, V. V. Yashchenko, 2018]

- Global avalanche characteristics (GAC):

$$\sigma_f = \sum_{u \in V_n} \Delta_f^2(u) \quad \text{and} \quad \delta_f = \max_{\mathbf{0} \neq u \in V_n} |\Delta_f(u)|$$

- Distance to $\{g \mid L_g \neq \{\mathbf{0}\}\}$: $\mathrm{ls}(f) = 2^{n-2} - \frac{1}{4}\delta_f$
- Distance to algebraic degenerate functions:

$$\mathrm{nd}(f) = 2^{n-2} - \frac{1}{4} \max_{\mathbf{0} \neq u \in V_n} \Delta_f(u) \quad \text{[E. K. Alekseev, 2011]}$$

- Maximal order of correlation immunity: $\mathrm{cor}(f)$

Preserving properties within Δ-equivalence classes

For any $f, g \in \mathcal{F}_n$ being Δ-equivalent to each other, i. e., $f \overset{\Delta}{\sim} g$, the following statements are true:

- f is balanced $\iff$ g is balanced;
- $f(x)$ has inessential $x_i \iff g(x)$ has inessential x_i;
- f satisfies SAC $\iff$ g satisfies SAC;
- f satisfies PC(k) $\iff$ g satisfies PC(k);
- f is CI(k) $\iff$ g is CI(k);
- f is k-resilient $\iff$ g is k-resilient.

- $\operatorname{supp} W_f = \operatorname{supp} W_g$;
- $L_f = L_g$;
- $CI_f = CI_g$;
- $PC_f = PC_g$.

- $\operatorname{nl}(f) = \operatorname{nl}(g)$;
- $\operatorname{curv}(f) = \operatorname{curv}(g)$;
- $(\sigma_f, \delta_f) = (\sigma_g, \delta_g)$;
- $\operatorname{ls}(f) = \operatorname{ls}(g)$;
- $\operatorname{nd}(f) = \operatorname{nd}(g)$;
- $\operatorname{cor}(f) = \operatorname{cor}(g)$.

Some further properties of Δ-equivalence

There are characteristics of Boolean function that are not invariant within Δ-equivalence classes. These are, for example, $\mathrm{wt}(f)$, $\deg(f)$, algebraic immunity $AI(f)$, $nl_r(f)$ $(r > 1)$,...

$$\mathfrak{G}_n = \{(A, a, l) \mid A \in \mathfrak{GL}_n(\mathbb{F}_2),\ a \in V_n,\ l \in \mathcal{A}_n\}$$

$$f^{(A,a,l)}(u) = f(Au \oplus a) \oplus l(u)$$

The classification induced by this group action does not correlate with Δ-equivalence.

The Δ-equivalence classes are blocks of imprimitivity for the group $\mathfrak{G}_n$.

The translation group $\mathfrak{I}_n \subset \mathfrak{G}_n$ acts on $\mathcal{F}_n$ $(f(u) \mapsto f(u \oplus a))$ so that each orbit $f^{\mathfrak{I}_n}$ is a subset of some Δ-equivalence class.