On some properties of symmetric Boolean functions

Marion Videau

On some properties of symmetric Boolean functions

Marion Videau
INRIA projet CODES,
BP 105, 78153 Le Chesnay cedex, FRANCE
e-mail: marion.videau@inria.fr

Abstract — **We exhibit the link between the periodicity of the value vectors symmetric Boolean functions and their degrees. We also deduce new results concerning balancedness, resiliency and propagation criteria of symmetric Boolean functions.**

I. Preliminaries

Let $\mathcal{S}_n$ be the set of all symmetric Boolean function in n variables, i.e. of all the Boolean functions in n variables whose output only depends on the weight of the input vector. Any $f \in \mathcal{S}_n$ is related to a function $v_f : \{0,\dots,n\} \to \mathbf{F}_2$ such that $\forall x \in \mathbf{F}_2^n, f(x) = v_f(wt(x))$. The algebraic normal form of f is

$$f(x_1,\dots,x_n) = \bigoplus_{i=0}^{n} \lambda_f(i) \bigoplus_{u,wt(u)=i} \left(\prod_{j=1}^{n} x_j^{u_j}\right) \quad \lambda_f(i) \in \mathbf{F}_2^n.$$

We will refer to $v(f) = (v_f(0),\dots,v_f(n))$ as the *simplified value vector* of f and $\lambda(f) = (\lambda_f(0),\dots,\lambda_f(n))$ as the *simplified ANF vector* of f.

Proposition 1 *For all $i \in \{0,\dots,n\}$,*

$$v_f(i) = \bigoplus_{k \preceq i} \lambda_f(k) \quad \text{and} \quad \lambda_f(i) = \bigoplus_{k \preceq i} v_f(k),$$

where $k \preceq i$ if and only if $\forall j,\ k_j \le i_j$ in their 2-adic representations.

II. Periodicity of the simplified value vector

We say that a n-bit vector a is *periodic with period T* if it is composed of the the first n bits of the sequence $(a_0,\dots,a_{T-1})$ repeated infinitely. Some periodic patterns may occur in the simplified value vectors of symmetric functions, for instance, it was shown in [1] that the patterns for quadratic symmetric functions are (0011) and all its circular shifts.

Proposition 2 *Let $f \in \mathcal{S}_n$. Then $v(f)$ is periodic with period 2^t if and only if $\deg(f) \le 2^t - 1$. Moreover, $(v_0,\dots,v_{2^t-1})$ is the simplified value vector of the function of $\mathcal{S}_{(2^t-1)}$ with $(\lambda_0,\dots,\lambda_{2^t-1})$ as simplified ANF vector.*

For instance, the previous proposition enables to compute the weights of all symmetric functions of degree 3 and to deduce that they cannot be balanced.

III. Resiliency

A Boolean function is *t-resilient* if it remains balanced when t variables are fixed [4]. There is no general bound on the resiliency of symmetric functions, but in [2] a computer search up to 128 variables has lead to the conjecture that they are at most 2-resilient. Thanks to the periodicity property, we deduce that if $f \in \mathcal{S}_n$ with $\deg f \neq 1$, is $(2^\ell - 1)$-resilient with $\ell = \lfloor \log_2 \deg f \rfloor + 1$, then for any $t \ge 0$ there exists a function of degree $\deg f$ in $\mathcal{S}_{n+t}$ which is $(2^\ell - 1 + t)$-resilient. Using that if $(n+1)$ is a prime, all balanced functions of $\mathcal{S}_n$ have degree 1, [2, Th. 2.6], we come to a contradiction which leads to a bound on the resiliency related to the degree. Then using Siegenthaler's inequality, we get a bound only lying on n.

Theorem 1 *Let $f \in \mathcal{S}_n$, $\deg f \neq 1$, $\ell = \lfloor \log_2(\deg f) \rfloor + 1$, $\alpha = \lceil \log_2 n \rceil$.*
If f is t-resilient, then $t < 2^\ell - 1$ and $t \le 2^{\alpha-1} - 2$.

IV. Propagation characteristics

For any $a \in \mathbf{F}_2^n$, the *derivative of $f \in \mathcal{B}_n$ with respect to a* is the function $D_a f \in \mathcal{B}_n$ defined by $D_a f(x) = f(x \oplus a) \oplus f(x)$. f satisfies the *propagation criterion of degree k*, $(PC(k))$ if $D_a f$ is balanced for all $a \in \mathbf{F}_2^n \setminus \{0\}$ such that $wt(a) \le k$ [3].

Let $a \in \mathbf{F}_2^n \setminus \{0, \mathbf{1}\}$ and consider $x \mapsto D_a f(x \oplus b)$, $x \in \text{span}\{e_i, i \notin \text{supp}(a)\}$, $b \in \text{span}\{e_i, i \in \text{supp}(a)\}$, where e_i is the i-th vector of the canonical basis of $\mathbf{F}_2^n$.

Proposition 3 *Let $f \in \mathcal{S}_n$. Then $D_a f(\cdot \oplus b) \in \mathcal{S}_{n-wt(a)}$, only depends on $wt(b)$ and $D_{\mathbf{1}} f \in \mathcal{S}_n$. The coefficients of their ANF are:*

$$\lambda_{D_a f(\cdot \oplus b)}(i) = \bigoplus_{j \preceq wt(a)-wt(b)} \lambda_f(i+j) \oplus \bigoplus_{j \preceq wt(b)} \lambda_f(i+j)$$

$$\lambda_{D_{\mathbf{1}} f}(i) = \bigoplus_{k \neq 0, k \preceq n-i} \lambda_{i+k}, \quad i \in \{0,\dots,n-1\}$$

Let $f \in \mathcal{S}_n$ and $d = \deg(f)$. The case $wt(a) = 2$ leads to the corollary: for all $a \in \mathbf{F}_2^n \setminus \{0, \mathbf{1}\}$, $\deg(D_a f) = d - 1$. Moreover we can deduce:

Theorem 2 *$f \in \mathcal{S}_n$ satisfies $PC(2)$ if and only if $\deg f = 2$. Then f satisfies $PC(n)$ if n is even and $PC(n-1)$ if n is odd.*

The case $a = \mathbf{1}$ leads to

- $\deg(D_{\mathbf{1}} f) = d - 1$ if and only if $n - d$ is even;
- if $n - d$ is odd, then either $\deg(D_{\mathbf{1}} f) = d - 2$ or $\deg(D_{\mathbf{1}} f) \le d - 4$.

References

[1] S.Maitra and P. Sarkar. Maximum nonlinearity of symmetric Boolean functions on odd number of variables. *IEEE Trans. Inform. Theory*, IT-48(9):2626–2630, 2002.

[2] J. von zur Gathen and J.R. Roche. Polynomials with two values. *Combinatorica*, 17(3):345–362, 1997.

[3] B. Preneel, W. Leekwijck, L. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *EUROCRYPT'90*, LNCS 437, pp. 155–165. Springer-Verlag, 1991.

[4] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory*, IT-30(5):776–780, 1984.