IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2024, No. 3, pp. 298–301. DOI:10.46586/tosc.v2024.i3.298-301

Addendum to Classification of All t-Resilient Boolean Functions with $t+4$ Variables

Classification of Quadratic and Cubic t-Resilient Boolean Functions with $t+5$ Variables

Shahram Rasoolzadeh

Ruhr University Bochum, Bochum, Germany
firstname.lastname@rub.de

Abstract. In ToSC 2023(3), Rasoolzadeh presented an algorithm for classifying $(n-m)$-resilient Boolean functions with n variables, up to extended variable-permutation equivalence, for a small given positive integer m and any positive integer n with $n \geq m$. By applying this algorithm along with several speed-up techniques, he classified n-variable $(n-4)$-resilient Boolean functions up to equivalence for any $n \geq 4$. However, for $m = 5$, due to the large number of representative functions, he was unable to classify n-variable $(n-5)$-resilient Boolean functions for $n > 6$.
In this work, we apply this algorithm together with a technique to restrict the ANF degree to classify quadratic and cubic $(n-5)$-resilient Boolean functions with n variables, up to the same equivalence. We show that there are only 131 quadratic representative functions for any $n \geq 8$. Additionally, we show that there are 359 078 cubic representative functions for any $n \geq 14$.

Keywords: correlation immunity · resilient functions · Boolean functions

1 Restricting the ANF Degree of Resilient Functions

According to Theorem 1 in [Sie84], for any $m > 1$, the ANF degree of any $(n-m)$-resilient Boolean function with n variables is at most $m-1$. This implies that any function in $\mathcal{R}^*_{n,n-5}$, the set of all $(n-5)$-resilient representatives with n variables, can have an ANF degree of at most 4. While it is easy to find affine functions, identifying those with higher degrees is not trivial. In this work, we introduce techniques that help us find all quadratic and cubic functions in $\mathcal{R}^*_{n,n-5}$. We will use $\mathcal{R}_{n,t,d}$ to denote the functions in $\mathcal{R}_{n,t}$ with an ANF degree of d, and $\mathcal{R}_{n,t,\leq d}$ to denote those with an ANF degree of at most d.

Lemma 1. *Let $f \in \mathcal{B}_{n+1}$, and let $f_0 \in \mathcal{B}_n$ and $f_1 \in \mathcal{B}_n$ be the two functions derived from f using the following equation:*

$$f(x, x_n) = (x_n \oplus 1) \cdot f_0(x) \oplus x_n \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_n \in \mathbb{F}_2 .$$

The ANF degree of f is at most d if and only if:

- *the ANF degree of both f_0 and f_1 is at most d, and*
- *f_0 and f_1 share the same monomials of degree d.*

Proof. Based on the assumption of the lemma, we have

$$f(x, x_n) = (x_n \oplus 1) \cdot f_0(x) \oplus x_n \cdot f_1(x) = x_n \cdot \big(f_0(x) \oplus f_1(x)\big) \oplus f_0(x) .$$

Received: 2024-06-01 Accepted: 2024-08-01 Published: 2024-09-06

This implies that the ANF degree of both f_0 and f_1 is at most d, and that the monomials of degree d appear equally in the ANF representation of both f_0 and f_1.

Conversely, if both f_0 and f_1 have an ANF degree of at most d and share the same monomials of degree d, then f has an algebraic degree at most d. □

By applying the first condition of Lemma 1 in Siegenthaler's construction, it is sufficient to use only the representative pairs (up to extended bit-permutation equivalence) in $\mathcal{R}^*_{n,t,\leq d}$ to find the functions in $\mathcal{R}^*_{n+1,t+1,\leq d}$. We use the same techniques 1 and 2 from [Ras23] to form the sets $\mathcal{R}^\dagger_{n,t,\leq d}$ and $\mathcal{R}^\ddagger_{n,t,\leq d}$. For simplicity, we will refer to degree check points as those points u with $\mathrm{hw}(u) = d$ for which we need to verify the presence of the same monomials in the f_0 and f_1 functions in the second condition of Lemma 1.

Lemma 2. *Let $f \in \mathcal{B}_n$ and $g \in \mathcal{B}_n$ such that for constants $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$, it holds $g(x) = f(x \oplus a) \oplus b$ for all $x \in \mathbb{F}_2^n$. Besides, let the ANF representation of f and g be*

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u x^u\,, \qquad \textit{and} \qquad g(x) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda'_u x^u\,.$$

If the ANF degree of f is d, with $d > 0$, then for all $u \in \mathbb{F}_2^n$ with $\mathrm{hw}(u) = d$, we have $\lambda_u = \lambda'_u$.

Proof. By replacing the relation between f and g into the ANF representation, we obtain

$$\bigoplus_{u \in \mathbb{F}_2^n} \lambda'_u x^u = b \oplus \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (x \oplus a)^u\,.$$

On the right-hand side of this equation, monomials of degree d can only appear for $u \in \mathbb{F}_2^n$ with $\mathrm{hw}(u) = d$. In the expansion of $(x \oplus a)^u$ where $\mathrm{hw}(u) = d$, the only monomial of degree d is x^u. This implies that for any u with $\mathrm{hw}(u) = d$, we must have $\lambda_u = \lambda'_u$. □

Lemma 3. *Let $f \in \mathcal{B}_{n+1}$, and let $f_0 \in \mathcal{B}_n$ and $f_1 \in \mathcal{B}_n$ be the two functions derived from f using the following equation:*

$$f(x, x_n) = (x_n \oplus 1) \cdot f_0(x) \oplus x_n \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \textit{ and } x_n \in \mathbb{F}_2\,.$$

If the ANF degree of f is at most d, with $d > 0$, then the number of monomials of degree d in the ANF representation of the functions f_0^* and f_1^* (the representative functions equivalent to f_0 and f_1, respectively) is the same.

Proof. According to Lemma 1, if the ANF degree of f is at most d, then the ANF degrees of both f_0 and f_1 are also at most d, and the monomials of degree d appear equally in their ANF representations. Based on Lemma 2, the addition of input constants a_i and output constants b_i does not affect the appearance of monomials of degree d. Moreover, since permuting the input variables does not change the degree of the monomials, the number of monomials of degree d in the ANF representations of both f_0^* and f_1^* must be the same. □

Based on Lemma 3, for each representative pair remaining after applying technique 2 of the algorithm in [Ras23], we perform two checks to ensure they are the same in both functions: 1. the distribution of magnitudes for the Walsh transform at the linearity check points, and 2. the number of monomials at the degree check points. If both conditions are satisfied, we proceed with iterating over the current representative pair.

Let f_1 be an equivalent function to f_1^*, defined as $f_1(x) = f_1^* \circ P(x \oplus a) \oplus b$, where P is a mapping corresponding to a permutation of n variables, $a \in \mathbb{F}_2^n$, and $b \in \mathbb{F}_2$. According to Lemma 2, f_0^* and f_1 can be combined to form an $(n+1)$-variable function with an ANF degree of at most d if and only if all monomials of degree d in the ANF representations of both f_0^* and $f_1^* \circ P$ are identical.

Note that this condition depends only on the mapping P and is independent of the constants a and b. Thus, for each representative pair (f_0^*, f_1^*) that meets the previous conditions, we first explore all possible choices for the mapping P and check whether, for all degree check points u, the monomial x^u appears the same way in both f_0^* and $f_1^* \circ P$. At this stage, we also verify the condition of matching Walsh coefficients in magnitude at the linearity check points.

Once an appropriate mapping P is found for the representative pair (f_0^*, f_1^*), we proceed as outlined in [Ras23]. Specifically, we determine if there exist values $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$ that satisfy the conditions for the signs of the Walsh transform at the linearity check points. If such values are found, we have successfully constructed an $(n+1)$-variable $(t+1)$-resilient function with an ANF degree of at most d. We then check if this composed function is representative. If it is, we add it to $\mathcal{R}^*_{n+1,t+1,\leq d}$.

2 Results for the Case of $R^*_{n,n-5,2}$ and $R^*_{n,n-5,3}$

We apply the modified algorithm to classify all quadratic and cubic n-variable $(n-5)$-resilient functions up to the extended variable-permutation equivalence.

Quadratic Functions: We start by using the affine or quadratic functions in $\mathcal{B}_4^*$ to find all the functions in $\mathcal{R}^*_{5,0,\leq 2}$. Then, we repeat for another 4 steps until we reach the step of finding the functions in $\mathcal{R}^*_{9,4,\leq 2}$. The algorithm stops by reaching $\mathcal{R}^\dagger_{9,4,\leq 2} = \emptyset$.

The number of quadratic representative functions in each $\mathcal{R}^*_{n,n-5,2}$ with $5 \leq n \leq 8$ is summarized in Table 1. We recall that $\mathcal{R}^*_{n,t,2}$ and $\mathcal{R}^\dagger_{n,t,2}$ denote the set of all and not-type-1 extension quadratic n-variable t-resilient representatives, respectively.

An interesting observation is that within the functions in $\mathcal{R}^\dagger_{n,n-5,2}$, for $n=5$ increasing to $n=8$, there are 2, 4, 2, and 1 functions, respectively, which can be written as the direct sum of two functions: one from $\mathcal{R}^\dagger_{n',n'-3,2}$ and the one from $\mathcal{R}^\dagger_{n'',n''-3,2}$ with $n'+n''=n$. Moreover, within the functions in $\mathcal{R}^\dagger_{n,n-5,2}$, for $n=5$ increasing to $n=7$, there are 7, 5, and 2 functions, respectively, which are type-0 extension of a function from $\mathcal{R}^\dagger_{n-1,n-5,2}$.

Cubic Functions: We start by using the functions in $\mathcal{B}_4^*$ with algebraic degree at most 3, find all the functions in $\mathcal{R}^*_{5,0,\leq 3}$.

We repeat the algorithm for another 10 steps until the step of finding the functions in $\mathcal{R}^*_{15,10,\leq 3}$ with an outcome of $\mathcal{R}^\dagger_{15,10,\leq 3} = \emptyset$.

The number of cubic representative functions in each $\mathcal{R}^*_{n,n-5,3}$ with $5 \leq n \leq 15$ is summarized in Table 2.

All the results of this work are publicly available at the following link:

https://gitlab.science.ru.nl/shahramr/ResilientFunctions.git

References

[Ras23] Shahram Rasoolzadeh. Classification of all t-resilient boolean functions with t + 4 variables. *IACR Trans. Symmetric Cryptol.*, 2023(3):213–226, 2023.

[Sie84] Thomas Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inf. Theory*, 30(5):776–780, 1984.

Table 1: Number of quadratic $(n-5)$-resilient n-variable representatives. The half bottom part of the table shows the number of functions for each possible Walsh transform spectrum.

n	5	6	7	8
$\lvert\mathcal{R}^*_{n,n-5,2}\rvert$	60	102	124	131
$\lvert\mathcal{R}^\dagger_{n,n-5,2}\rvert$	37	42	22	7
4 times 2^{n-1}	18	17	9	3
16 times 2^{n-2}	19	25	13	4

Table 2: Number of cubic $(n-5)$-resilient n-variable representatives. The half bottom part of the table shows the number of functions for each possible Walsh transform spectrum; by (x, y, z) we mean x times appearance of 2^{n-2}, y times 2^{n-1} and z times $3 \cdot 2^{n-2}$ in absolute values of the Walsh transform.

n	5	6	7	8	9	10	11	12	13	14
$\lvert\mathcal{R}^*_{n,n-5,3}\rvert$	3 570	61 402	210 194	315 799	349 717	356 981	358 233	359 333	359 693	359 723
$\lvert\mathcal{R}^\dagger_{n,n-5,3}\rvert$	3 466	57 832	148 792	105 605	33 918	7 264	1 252	188	21	2
(16, 0, 0)			133 561	98 464	32 407	7 101	1 246	188	21	2
(12, 1, 0)	1 793	10 055	14 028	6 592	1 375	142	5	–	–	–
(8, 2, 0)	529	1 247	1 182	546	136	21	1	–	–	–
(7, 0, 1)	57	56	21	3	–	–	–	–	–	–