SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

March 2018, Vol. 61 038101:1–038101:3
doi: 10.1007/s11432-017-9123-2

Construction of rotation symmetric bent functions with maximum algebraic degree

Wenying ZHANG[1*] & Guoyong HAN[1,2]

[1]*School of Information Science and Engineering, Shandong Normal University, Jinan* 250014*, China;*
[2]*School of Management Engineering, Shandong Jianzhu University, Jinan* 250101*, China*

Received 22 May 2017/Accepted 2 June 2017/Published online 16 August 2017

Citation Zhang W Y, Han G Y. Construction of rotation symmetric bent functions with maximum algebraic degree. Sci China Inf Sci, 2018, 61(3): 038101, doi: 10.1007/s11432-017-9123-2

Boolean functions that are invariant under the action of cyclic rotation on the inputs are called rotation symmetric functions [1]. Aside from their simple algebraic descriptions, rotation symmetric functions have implementation advantages in either hardware or software employing the bit-slicing technique, since they produce a shallow circuit with high parallelism, and hence high clock frequencies, without expending too many resources [2]. They have been widely applied in the design of symmetric ciphers. For example, both the S-box of block cipher AES and the round functions of hash functions MD4, MD5 and HAVAL are rotation symmetric functions. Moreover the round function in stream cipher Grain is the modification of a rotation symmetric bent function. The quadratic Boolean function $f_o(x) = x_1x_{m+1}+x_2x_{m+2}+\cdots+x_mx_{2m}$ is the first class of rotation symmetric bent functions [3].

Throughout this article, for $n = 2m$ we study the n-variable rotation symmetric bent functions. In the public literature, the main method of constructing new rotation symmetric bent functions is to modify $f_o(x)$ [4–6]. Up to now, only few constructions of rotation symmetric bent functions are known. In [7], Gao et al. proved that the cubic rotation symmetric function $f_t(x_0,\ldots,x_{2m-1}) = \sum_{i=1}^{2m-1}(x_ix_{t+i}x_{m+i} + x_ix_{t+i}) + \sum_{i=0}^{m-1} x_ix_{m+i}$ is bent if and only if $\frac{m}{gcd(m,t)}$ is odd, where $1 \leqslant t \leqslant m-1$ and the subscript of x is modulo $2m$. This is the first theoretical construction of rotation symmetric bent functions with algebraic degree larger than 2. Later on, $2m$-variable rotation symmetric bent functions with algebraic degree 4, where $2m$ is not divisible by 4, were constructed from two known semi-bent rotation symmetric functions in m variables with complementary Walsh supports [8].

Our result. We present a new construction of $2m = 6k, 8k, 14k$-variable rotation symmetric bent functions by modifying $f_o(x)$. We restrict the flipped vectors to be related with some affine subspaces of $GF(2)^m$, hence the constructed functions are from the Miorana-McFarland bent Boolean functions. More significantly, the proposed $2m$-variable rotation symmetric bent functions can reach the maximum algebraic degree m, and our construction method can be generalized to construct many other rotation symmetric bent functions.

An n-variable Boolean function $f(x_1,\ldots,x_n)$ is a mapping from $GF(2)^n$ to $GF(2)$, which can be represented in a unique way as an n-variable polynomial whose degree relative to each variable is at most 1, called its algebraic normal form (ANF):

$$a_0+\sum_{i=1}^{n} a_ix_i+\sum_{1\leqslant i<j\leqslant n} a_{ij}x_ix_j+\cdots+a_{1\cdots n}x_1\cdots x_n.$$

* Corresponding author (email: wenyingzh@sohu.com)
The authors declare that they have no conflict of interest.

Let $\mathcal{B}_n$ denote the set of n-variable Boolean functions. The support of $f \in \mathcal{B}_n$ is defined as $\mathrm{supp}(f) = \{(x_1, \ldots, x_n) : f(x_1, \ldots, x_n) = 1\}$. For a vector $x = (x_1, \ldots, x_n) \in GF(2)^n$, and an integer $l \geqslant 0$, we define the left l-cyclic shift operator ρ_n^l as l-cyclic rotation on x:

$$\rho_n^l(x) = (\rho^l(x_1), \rho^l(x_2), \ldots, \rho^l(x_n)),$$

where $\rho^l(x_i) = x_{i+l}$, if $i + l \leqslant n$ and $\rho^l(x_i) = x_{i+l-n}$, if $i + l > n$. The orbit generated by $x = (x_1, x_2, \ldots, x_n) \in GF(2)^n$ is defined as $C_n(x) = \{x, \rho(x), \ldots, \rho^{n-1}(x)\}$. In other words, each orbit consists of all cyclic shifts of one vector in $GF(2)^n$.

Definition 1 ([9])**.** For $f \in \mathcal{B}_n$, if $f(\rho_n^l(x)) = f(x)$ holds for all $x = (x_1, \ldots, x_n) \in GF(2)^n$ and $1 \leqslant l < n$, then f is called a rotation symmetric Boolean function (RotS).

For instance, if $n = 4$ and $x_1x_2x_3$ is present in the ANF of a rotation symmetric function $f(x)$, then the terms $x_2x_3x_4, x_3x_4x_1, x_4x_1x_2$ must also be present in the ANF of $f(x)$.

We extend the definition of ρ and orbit to monomials by $\rho^k(x_{i_1} \cdots x_{i_l}) = \rho^k(x_{i_1}) \cdots \rho^k(x_{i_l})$, and $G_n(x_{i_1} \cdots x_{i_l}) = \{\rho^k(x_{i_1} \cdots x_{i_l}) : \text{for } 1 \leqslant k \leqslant n\}$.

A RotS function $f(x_1, \ldots, x_n)$ can be written as

$$a_0 + a_1x_1 + \sum_{1<j\leqslant n} a_{1j}x_1x_j + \cdots + a_{1\cdots n}x_1 \cdots x_n,$$

where the coefficients $a_0, a_1, a_{1j}, \ldots, a_{1\cdots n} \in GF(2)$, and the existence of a representative term $x_{i_1}x_{i_2} \cdots x_{i_l}$ implies the existence of all the terms from $G_n(x_{i_1}x_{i_2} \cdots x_{i_l})$ in the ANF. This representation of $f(x)$ is called the short algebraic normal form (SANF) [9]. As an example, let us consider the ANF of a 4-variable RotS Boolean function $x_1 + x_2 + x_3 + x_4 + x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2$. Its SANF is $x_1 + x_1x_2x_3$.

The Walsh spectrum of $f(x)$ is the following real-valued function over $GF(2)^n$:

$$W_f(w) = \sum_{x\in GF(2)^n} (-1)^{f(x)+w\cdot x},$$

where $w = (w_1, \ldots, w_n)$ and $w \cdot x = w_1x_1 + \cdots + w_nx_n$. Let $n = 2m$ be even, $f(x) \in \mathcal{B}_n$ is called bent if its Walsh spectrum satisfies: $|W_f(w)| = 2^m$ for all $w \in GF(2)^{2m}$.

Let $s, t, u, v, w, x, y, z, \delta, \Delta$ be the binary vectors, and $A, B, \Omega, \Gamma, \Lambda, \Upsilon, \Phi$ be the sets of binary vectors.

Theorem 1. Let $t = (t_1, t_2, \ldots, t_{4k})$, $\delta = (0011 \cdots 0011) \in GF(2)^{4k}$. Denote the solutions of $t_1 + t_2 + \cdots + t_{4k} = 0$ by A, let $B = GF(2)^{4k} \setminus A$, $S_1 = \{(t, t + \delta) \mid t \in A\}$, $S_2 = \{(t, t + 0110 \cdots 0110) \mid t \in A\}$, $S_3 = \{(t, t+1100 \cdots 1100) \mid t \in A\}$, $S_4 = \{(t, t + 1001 \cdots 1001) \mid t \in B\}$. Let $\Omega = S_1 \cup S_2 \cup S_3 \cup S_4$. Then

$$f(x, y) = \begin{cases} f_o(x, y) + 1, & (x, y) \in \Omega; \\ f_o(x, y), & (x, y) \in GF(2)^{8k} \setminus \Omega \end{cases}$$

is a rotation symmetric bent function.

Theorem 2. Let A, B, δ be defined as in Theorem 1. Let $T_1 = \{(x, x + \delta) \mid x \in B\}, T_2 = \{(x, x + 0110 \cdots 0110) \mid x \in B\}, T_3 = \{(x, x + 1100 \cdots 1100) \mid x \in B\}, T_4 = \{(x, x + 1001 \cdots 1001) \mid x \in A\}$. Let $\Upsilon = T_1 \cup T_2 \cup T_3 \cup T_4$. Define

$$f(x, y) = \begin{cases} f_o(x, y) + 1, & (x, y) \in \Upsilon; \\ f_o(x, y), & (x, y) \in GF(2)^{8k} \setminus \Upsilon. \end{cases}$$

Then $f(x, y)$ is a rotation symmetric bent function.

Example 1. For $k = 1, n = 8$, let $\Lambda = C_8(0000\,0011, 11111100, 01100101, 11010100)$. Substituting the orbits of $(00000011), (11111100)$ for the orbits of $(01100101), (11010100) \in \mathrm{supp}(f_o)$. Define

$$f(x, y) = \begin{cases} f_o(x, y) + 1, & (x, y) \in \Lambda; \\ f_o(x, y), & \text{otherwise.} \end{cases}$$

Then $f(x, y)$ is a rotation symmetric bent function. The SANF for $f(x)$ is $x_1x_2 + x_1x_5 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + x_1x_4x_5 + x_1x_2x_3x_4 + x_1x_3x_4x_6$, where $\delta = 0011, t_1 + t_2 + t_3 + t_4 = 0, t = (t_1, t_2, t_3, t_4) \in \{(0000), (1111), (0110)\}$.

Theorem 3. Let $n = 6k$, $\delta = 001001 \cdots 001, \triangle = 011011 \cdots 011 \in GF(2)^{3k}$ be vectors with period 3, $s = (s_1, \ldots, s_{3k})$, $s_1 + s_4 + \cdots + s_{3i+1} + \cdots + s_{3k-2} = 0, i = 0, 1, \cdots, k - 1$, $t = (t_1, t_2, \ldots, t_{3k}) \in GF(2)^{3k}$, $t_1 + t_2 + \cdots + t_{3k} = 0$. Construct $Z = \{z | z = (s, s + \delta) \in GF(2)^{6k}\}, U = \{u | u = (t, t + \Delta) \in GF(2)^{6k}\}$, and get all vectors of their left rotation. Let $C(Z) = \bigcup_{z\in Z} C_{6k}(z), C(U) = \bigcup_{u\in U} C_{6k}(u), \Gamma = C(Z) \cup C(U)$. Then

$$f(x, y) = \begin{cases} f_o(x, y) + 1, & (x, y) \in \Gamma; \\ f_o(x, y), & \text{otherwise} \end{cases}$$

is a rotation symmetric bent function.

Theorem 4. Let $n = 14k$, $\delta = 0000111 \cdots 0000111, \triangle = 0001111 \cdots 0001111 \in GF(2)^{7k}$ be vectors with period 7, $s = (s_1, s_2, \ldots, s_{7k})$, $s_1 + s_8 + \cdots + s_{7k-6} = 0$, $t = (t_1, t_2, \ldots, t_{7k}) \in GF(2)^{7k}$, $t_1 + t_2 + \cdots + t_{7k} = 0$. Construct $Z = \{z | z = (s, s + \delta) \in GF(2)^{14k}\}, U = \{u | u = (t, t + \Delta) \in GF(2)^{14k}\}$, and get all vectors of their

left rotation. Let $C(Z) = \bigcup_{z\in Z} C_{14k}(z), C(U) = \bigcup_{u\in U} C_{14k}(u), \Phi = C(Z) \cup C(U)$. Define

$$f(x,y) = \begin{cases} f_o(x,y) + 1, & (x,y) \in \Phi; \\ f_o(x,y), & (x,y) \in GF(2)^{14k} \setminus \Phi. \end{cases}$$

Then $f(x,y)$ is a rotation symmetric bent function.

The proofs of the proceeding theorems are skipped to make this article more compact.

In Theorems 1–4 we constructed several rotation symmetric bent functions by flipping some vectors in $\mathrm{supp}(f_o)$. In the design of cryptographic transformations such as block ciphers, hash functions and stream ciphers, the algebraic degrees play important roles. A Boolean function may provide low security by high order differential attack if it has low algebraic degree. So the algebraic degree of a Boolean function in a cipher system should be as high as possible. Since the algebraic degree of any bent function on $GF(2)^{2m}$ is upper bounded by m, the bent function with algebraic degree of m is an excellent option. Now we consider the algebraic degrees of functions constructed in the foregoing theorems. We will show that the ANF has the term $x_{m+1}\cdots x_{2m}$, so the algebraic degree is m, which is the maximum for a bent function.

Lemma 1. If the truth table of $b(x) \in \mathcal{B}_n$ includes odd number of vectors from which $i_1, i_2, \ldots, i_s$ positions are zeros, then the ANF of $b(x)$ has $\prod_{i=1}^{n} x_i / x_{i_1} x_{i_2} \cdots x_{i_s}$ as one of its monomial term.

Theorem 5. Let $f(x)$ be $2m$-variable Boolean function defined as in Theorems 1–4, then $x_{m+1}\cdots x_{2m}$ must be present in the ANF of $f(x)$, that is the algebraic degree of $f(x)$ is m.

It should be pointed out that, a close scrutiny shows that the construction does not apply to the condition when $n = 2m, m \pmod 4 = 1$.

In this article, concrete constructions for a large number of rotation symmetric bent functions with maximum algebraic degree are given. We can see that for even number $n, n = 6k, 7k, 8k$, the rotation symmetric bent functions can be given. This is a large proportion of even natural number. Therefore, in terms of practical applications, our constructions provide a sufficient source of such functions. Our method is based on that we can flip the vectors with the difference of the first halves and the second halves which are periodical such as $\delta = 0011\cdots0011, 011\cdots011$ in $f_o(x)$. And the first halves of the flipped vectors form an affine subspace of $GF(2)^{\frac{n}{2}}$. The number of such functions can be enumerated by counting the number of δ, we skip it to make this article more compact. It must be pointed out that the functions constructed in [4] only by using the subspace of $GF(2)^{\frac{n}{2}}$, in this article, we use affine subspace of $GF(2)^{\frac{n}{2}}$. It is well known that the amount of affine subspace is much larger than that of subspace, so we can construct more bent functions than that in [4].

From the cryptography designer's perspective, this approach is very intuitive and practical. The method is flexible, simple to use, and easy to be extended to the construction of rotation symmetric bent functions with larger number of variables. For example, when $n = 42$, we can use either Theorem 3 for multiple of 6 or Theorem 4 for multiple of 7 to construct rotation symmetric bent functions.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61272434, 61672330, 61602887).

References

1 Kavut S, Maitra S, Yücel M D. Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans Inf Theory, 2007, 53: 1743–1751
2 Rijmen V, Barreto P S L M, Filho D L G. Rotation symmetry in algebraically generated cryptographic substitution tables. Inf Process Lett, 2008, 106: 246–250
3 Rothaus O S. On bent functions. J Comb Theory, 1976, 20: 300–305
4 Su S H, Tang X H. On the systematic constructions of rotation symmetric bent functions with any possible algebraic degrees. Cryptology ePrint Archive, Report 2015/451, 2015. https://eprint.iacr.org/2015/451
5 Su S H, Tang X H. Systematic constructions of rotation symmetric bent functions, 2-rotation symmetric bent functions, and bent idempotent functions. IEEE Trans Inf Theory, 2017, 63: 4658–4667
6 Carlet C, Gao G P, Liu W F. Results on constructions of rotation symmetric bent and semi-bent functions. In: Sequences and Their Applications-SETA 2014. Berlin: Springer, 2014. 21–33
7 Gao G P, Zhang X Y, Liu W F, et al. Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Trans Inf Theory, 2012, 58: 4908–4913
8 Carlet C, Gao G P, Liu W F. A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. J Comb Theory, 2014, 127: 161–175
9 Cusick T W, Stănică P. Cryptographic Boolean Functions and Applications. Oxford: Elsevier, 2017. 124–125