Research Article

Elizabeth M. Reid*

Using Inclusion / Exclusion to find Bent and Balanced Monomial Rotation Symmetric Functions

<https://doi.org/10.1515/jmc-2020-0021>

Received May 20, 2020; accepted Dec 10, 2020

Abstract: There are many cryptographic applications of Boolean functions. Recently, research has been done on monomial rotation symmetric (MRS) functions which have useful cryptographic properties. In this paper we use the inclusion/exclusion principle to construct formulas for the weights of two subclasses of MRS functions: degree d short MRS functions and d -functions. From these results we classify bent and balanced functions of these forms.

Keywords: Boolean function, rotation symmetric, Hamming weight, cryptography, cryptology

2010 Mathematics Subject Classification: 94C10 94A60 06E30

1 Introduction

A Boolean function f in n variables is a mapping from the n -dimensional vector space $\mathbb{V}_n$ over $\mathbb{F}_2$ to $\mathbb{F}_2$. For $i \in \{1, 2, \dots, n\}$, the cyclic permutation ρ^i is defined as $\rho^i(x_1, x_2, \dots, x_n) = (x_{1+i}, x_{2+i}, \dots, x_i)$. We say f is rotation symmetric if $f(\rho(x_1, \dots, x_n)) = f(x_1, \dots, x_n)$. Similarly, f is k -rotation symmetric if $f(\rho^k(x_1, \dots, x_n)) = f(x_1, \dots, x_n)$, but $f(\rho^l(x_1, \dots, x_n)) \neq f(x_1, \dots, x_n)$ for any $l \in \{1, 2, \dots, k-1\}$. Cryptographic applications of rotation symmetric functions can be found in [2]. In this paper we consider monomial rotation symmetric (MRS) functions: rotation symmetric functions that are constructed by summing the powers of ρ on a single monomial. Extending this idea further, a k -MRS function is constructed by summing the powers of ρ^k on a single monomial. For example, $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$ is a MRS function in 3 variables with generating monomial x_1x_2 , while $g(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_2x_3 + x_3x_4x_5 + x_5x_6x_1$ is a 2-MRS function in 6 variables with generating monomial $x_1x_2x_3$. Recent work on 2-MRS functions can be found in [4]. There has been a focus on these types of functions because their structure allows for less storage space and faster computation. We say that the degree of a monomial is the number of variables in the monomial. The degree of a function f is the maximum degree of any monomial of f . If every monomial of f is the same degree then f is homogeneous and if the degree of f is 1 we say f is affine. Additionally, f is defined to be linear if it is both homogeneous and affine.

Let $v_0 = (0, 0, \dots, 0)$, $v_1 = (0, 0, \dots, 1)$, $\dots$, $v_{2^n-1} = (1, 1, \dots, 1)$ be the 2^n vectors in $\mathbb{V}_n$ listed in lexicographical order. Then the truth table of f is defined as the 2^n -tuple given by $(f(v_0), f(v_1), \dots, f(v_{2^n-1}))$. For example, the truth table for $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$ is $(0, 0, 0, 1, 0, 1, 1, 1)$. The weight of f , denoted by $\text{wt}(f)$, is the number of 1's in the truth table for f . The distance between two functions f and g , denoted by $d(f, g)$, is defined as $d(f, g) = \text{wt}(f \oplus g)$. The nonlinearity of a function f , denoted by $NL(f)$, is the minimum distance between f and any affine function.

*Corresponding Author: Elizabeth M. Reid: Marist College, Mathematics Department, Poughkeepsie, NY 12601, United States of America; University at Buffalo, Mathematics Department, Buffalo, NY 14260, United States of America; Email: elizabeth.reid@marist.edu

A function of n variables is called *balanced* if its weight is exactly 2^{n-1} . Since the weight is exactly 2^{n-1} , balanced functions are resistant to correlation attacks. Intuitively, a function f is called *bent* if it is as nonlinear as possible, making bent functions resistant to linear cryptanalysis. Due to their structure, balanced and bent functions have applications in cryptography and coding theory. Some of these applications can be found in [2]. For a MRS function f we say that it is *short* if f has fewer than n monomials. Note that for a rotation symmetric function of degree greater than 1, if each variable appears exactly once then the function is short. Let $d|n$ and $k = \frac{n}{d}$. We say f is a d -function if $f(x_1, \dots, x_n) = x_1 x_2 \dots x_d + x_{d+1} x_{d+2} \dots x_{2d} + \dots + x_{(k-1)d+1} \dots x_n$. Note that if f is a d -function then $\deg(f) = d$ and f is a d -MRS function. In this paper we consider short monomial rotation symmetric functions and d -functions. We develop formulas for the weight of such functions and use these results to find bent and balanced functions of these forms.

2 Bent and Balanced short MRS functions

In this section we construct a formula for the weight of short MRS functions and determine which are bent or balanced. The following lemmas are well known results and are included here for reference.

Lemma 1. Let f be a Boolean function. f is bent if and only if the nonlinearity of f is $2^{n-1} - 2^{\frac{n}{2}-1}$. Also if f is bent, then $\text{wt}(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.

Remark 2. Lemma 3 and Lemma 4 are Theorem 4 and Lemma 5 in [3].

Lemma 3. Every Boolean function f of degree 2 is affinely equivalent to one of the following three types: If f is balanced, it is equivalent to

$$x_1 x_2 + x_3 x_4 + \dots + x_{2k-1} x_{2k} + x_{2k+1}$$

for some $k \leq \frac{n-1}{2}$.

If f is not balanced, it is equivalent to

$$x_1 x_2 + x_3 x_4 + \dots + x_{2k-1} x_{2k} + b$$

for some $k \leq \frac{n}{2}$ and $b \in GF(2)$. If $\text{wt}(f) < 2^{n-1}$ then $b = 0$. If $\text{wt}(f) > 2^{n-1}$ then $b = 1$.

Lemma 4. Let

$$h(x) = \sum_{i=1}^k x_{2i-1} x_{2i} + \sum_{i=2k+1}^n a_i x_i$$

be an n -variable function for $k \leq \frac{n}{2}$. Then

$$NL(h) = 2^{n-1} - 2^{n-k-1}.$$

If all the linear terms vanish then its weight is the same as the nonlinearity; otherwise it is balanced.

Remark 5. The following theorem is well known. A proof can be found in [2].

Theorem 6. Let n be an even integer and $m = \frac{n}{2}$. Then

$$f_0(x_1, \dots, x_n) = \sum_{i=1}^m x_i x_{m+i}$$

is a rotation symmetric bent function.

Lemma 7. Let $g_1, \dots, g_k$ be arbitrary Boolean functions in n variables. Then

$$\begin{aligned} \text{wt} \left(\sum_{i=1}^k g_i \right) &= \sum_{i=1}^k \text{wt}(g_i) - 2 \sum_{i(1), i(2)} \text{wt}(g_{i(1)} g_{i(2)}) + \dots \\ &\quad + (-2)^{r-1} \sum_{i(1), \dots, i(r)} \text{wt}(g_{i(1)} \dots g_{i(r)}) + \dots \\ &\quad + (-2)^{k-1} \text{wt}(g_1 \dots g_k), \end{aligned}$$

where we use the notation

$$\sum_{i(1), \dots, i(r)} \text{wt}(g_{i(1)} \dots g_{i(r)})$$

to denote summing over the weights of all possible products consisting of r Boolean functions from $g_1, \dots, g_k$.

Proof. This follows from induction on k , the number of Boolean functions, with the base case that for two Boolean functions g_1 and g_2 , $\text{wt}(g_1 + g_2) = \text{wt}(g_1) + \text{wt}(g_2) - 2\text{wt}(g_1 g_2)$. $\square$

Theorem 8. Let $\mathbf{x} = (x_1, \dots, x_n)$ and

$$f(\mathbf{x}) = \sum_{i=1}^k x_i x_{i+k} \dots x_{i+(d-1)k}$$

where $d = \deg(f)$ and $k = \frac{n}{d}$. Then

$$\text{wt}(f(\mathbf{x})) = \sum_{i=1}^k (-2)^{i-1} \binom{k}{i} 2^{n-id}.$$

Proof. Define $A_i(\mathbf{x}) = x_i x_{i+k} \dots x_{i+(d-1)k}$ for $1 \leq i \leq k$. Then

$$f(\mathbf{x}) = \sum_{i=1}^k A_i.$$

By Lemma 7,

$$\begin{aligned} \text{wt}(f) &= \text{wt} \left(\sum_{i=1}^k A_i \right) \\ &= \sum_{i=1}^k \text{wt}(A_i) - 2 \sum_{i(1), i(2)} \text{wt}(A_{i(1)} A_{i(2)}) + \dots \\ &\quad + (-2)^{r-1} \sum_{i(1), \dots, i(r)} \text{wt}(A_{i(1)} \dots A_{i(r)}) + \dots \\ &\quad + (-2)^{k-1} \text{wt}(A_{i(1)} \dots A_{i(k)}), \end{aligned}$$

where

$$\sum_{i(1), \dots, i(r)} \text{wt}(A_{i(1)} \dots A_{i(r)})$$

is defined as in Lemma 7.

Since each A_i has a disjoint set of variables, $\text{wt}(A_{i(1)} \dots A_{i(r)}) = 2^{n-rd}$. Note that $\sum_{i(1), \dots, i(r)} 1 = \binom{k}{r}$. Thus

$$\sum_{i(1), \dots, i(r)} \text{wt}(A_{i(1)} \dots A_{i(r)}) = \binom{k}{r} 2^{n-rd}.$$

Therefore

$$\text{wt}(f(\mathbf{x})) = \sum_{i=1}^k (-2)^{i-1} \binom{k}{i} 2^{n-id}.$$

□

Example 9. Consider $f(\mathbf{x}) = f(x_1, \dots, x_6) = x_1x_4 + x_2x_5 + x_3x_6$. So $n = 6$, $d = 2$, and $k = 3$. By our formula above,

$$\text{wt}(f(\mathbf{x})) = \sum_{i=1}^3 (-2)^{i-1} \binom{3}{i} 2^{6-2i} = 28.$$

Let $A_1(\mathbf{x}) = x_1x_4$, $A_2(\mathbf{x}) = x_2x_5$, and $A_3(\mathbf{x}) = x_3x_6$. Note that when $i = 1$ in our formula above, we have $\binom{3}{1} 2^4 = 48$. This represents the number of $\mathbf{x}$ so that $A_\alpha(\mathbf{x}) = 1$ for $1 \leq \alpha \leq 3$.

$$\begin{aligned} \{\mathbf{x} : A_1(\mathbf{x}) = 1\} = \{ & (100100), (100101), (100110), (100111), (101100), (101101), \\ & (101110), (101111), (110100), (110101), (110110), (110111), \\ & (111100), (111101), (111110), (111111)\} \rightarrow 16 \end{aligned}$$

$$\begin{aligned} \{\mathbf{x} : A_2(\mathbf{x}) = 1\} = \{ & (010010), (010011), (010110), (010111), (011010), (011011), \\ & (011110), (011111), (110010), (110011), (110110), (110111), \\ & (111010), (111011), (111110), (111111)\} \rightarrow 16 \end{aligned}$$

$$\begin{aligned} \{\mathbf{x} : A_3(\mathbf{x}) = 1\} = \{ & (001001), (001011), (001101), (001111), (011001), (011011), \\ & (011101), (011111), (101001), (101011), (101101), (101111), \\ & (111001), (111011), (111101), (111111)\} \rightarrow 16 \end{aligned}$$

Note that in the sets of $\mathbf{x}$ above we have many duplicates. We also have included $\mathbf{x}$ from both $\{\mathbf{x} : A_\alpha(\mathbf{x}) = 1\}$ and $\{\mathbf{x} : A_\beta(\mathbf{x}) = 1\}$ so that $A_\alpha(\mathbf{x}) = 1$ and $A_\beta(\mathbf{x}) = 1$, where $1 \leq \alpha, \beta \leq 3$ and $\alpha \neq \beta$. To correct for overcounting, we remove two times the number of $\mathbf{x}$ where $A_\alpha(\mathbf{x}) = 1$ and $A_\beta(\mathbf{x}) = 1$. Note that when $i = 2$ from our formula above we have $-2 \binom{3}{2} 2^2 = -24$. This represents that we are removing two times the number of $\mathbf{x}$ so that $A_\alpha(\mathbf{x}) = 1$ and $A_\beta(\mathbf{x}) = 1$, where $1 \leq \alpha, \beta \leq 3$ and $\alpha \neq \beta$.

$$\begin{aligned} \{\mathbf{x} : A_1(\mathbf{x}) = 1 \text{ and } A_2(\mathbf{x}) = 1\} = \{ & (110110), (110111), (111110), (111111)\} \\ & \rightarrow 4 \end{aligned}$$

$$\begin{aligned} \{\mathbf{x} : A_1(\mathbf{x}) = 1 \text{ and } A_3(\mathbf{x}) = 1\} = \{ & (101101), (101111), (111101), (111111)\} \\ & \rightarrow 4 \end{aligned}$$

$$\begin{aligned} \{\mathbf{x} : A_2(\mathbf{x}) = 1 \text{ and } A_3(\mathbf{x}) = 1\} = \{ & (011011), (011111), (111011), (111111)\} \\ & \rightarrow 4 \end{aligned}$$

So far we have counted $\mathbf{x}$ so that $A_\alpha(\mathbf{x}) = 1$, where $1 \leq \alpha \leq 3$, and removed $\mathbf{x}$ so that $A_\alpha(\mathbf{x}) = 1$ and $A_\beta(\mathbf{x}) = 1$, where $1 \leq \alpha, \beta \leq 3$ and $\alpha \neq \beta$. However we still need to make sure that we have $\mathbf{x}$ so that $A_1(\mathbf{x}) = 1$, $A_2(\mathbf{x}) = 1$, and $A_3(\mathbf{x}) = 1$. Note that $\{\mathbf{x} : A_1(\mathbf{x}) = 1, A_2(\mathbf{x}) = 1, \text{ and } A_3(\mathbf{x}) = 1\} = \{(111111)\}$. From our first step, we counted $\mathbf{x} = (111111)$ for each $\{\mathbf{x} : A_\alpha(\mathbf{x}) = 1\}$, giving us 3. From our second step, we subtracted twice $\mathbf{x} = (111111)$ for each $\{\mathbf{x} : A_\alpha(\mathbf{x}) = 1 \text{ and } A_\beta(\mathbf{x}) = 1\}$, giving us $-2(3) = -6$. Thus so far we have counted $3 - 6 = -3$ of $\mathbf{x} = (111111)$.

Note that when $i = 3$ from our formula above we have $(-2)^2 \binom{3}{3} 2^0 = 4$. This represents that we are adding four times the sum of the number of $\mathbf{x}$ so that $A_1(\mathbf{x}) = 1$, $A_2(\mathbf{x}) = 1$ and $A_3(\mathbf{x}) = 1$. Hence we are adding back 4 more (111111) . Therefore we have counted $3 - 6 + 4 = 1$ of $\mathbf{x} = (111111)$, as desired.

Therefore the $48 - 24 + 4 = 28$ from our formula above is the number of $\mathbf{x}$ so that $f(\mathbf{x}) = 1$. Thus $\text{wt}(f(\mathbf{x})) = 28$.

Remark 10.

$$f(\mathbf{x}) = \sum_{i=1}^k x_i x_{i+k} \cdots x_{i+(d-1)k}$$

where $d = \deg(f)$ and $k = \frac{n}{d}$ is a short function.

Corollary 11. Let $\mathbf{x} = (x_1, \dots, x_n)$ and

$$f(\mathbf{x}) = \sum_{i=1}^k x_i x_{i+k} \cdots x_{i+(d-1)k}$$

where $d = \deg(f)$ and $k = \frac{n}{d}$. Then

$$f(\mathbf{x}) = x_1 + \cdots + x_n$$

is the only balanced function of this form.

Proof. By Theorem 8 it follows that

$$\text{wt}(f(\mathbf{x})) = \sum_{i=1}^k (-1)^{i-1} 2^{i-1} \binom{k}{i} 2^{n-id} = 2^{n-1} \left(1 - \left(2^{-d} (2^d - 2) \right)^k \right).$$

Setting

$$2^{n-1} \left(1 - \left(2^{-d} (2^d - 2) \right)^k \right) = 2^{n-1}$$

and solving for d , we see that $d = 1$. Hence $k = \frac{n}{d} = \frac{n}{1} = n$ and so the only balanced function of the form above is $f(\mathbf{x}) = x_1 + \cdots + x_n$. $\square$

Corollary 12. Let $\mathbf{x} = (x_1, \dots, x_n)$ and

$$f(\mathbf{x}) = \sum_{i=1}^k x_i x_{i+k} \cdots x_{i+(d-1)k}$$

where $d = \deg(f)$ and $k = \frac{n}{d}$. Then

$$f(\mathbf{x}) = x_1 x_{\frac{n}{2}+1} + \cdots + x_{\frac{n}{2}} x_n$$

is the only bent function of this form.

Proof. By Theorem 8 it follows that

$$\text{wt}(f(\mathbf{x})) = \sum_{i=1}^k (-1)^{i-1} 2^{i-1} \binom{k}{i} 2^{n-id} = 2^{n-1} - 2^{-1} \left(2^d - 2 \right)^{\frac{n}{d}}.$$

By the contrapositive of Lemma 1, if $\text{wt}(f) \neq 2^{n-1} \pm 2^{\frac{n}{2}-1}$ then f is not bent. So we will only consider functions of the form above where $\text{wt}(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Setting

$$2^{n-1} - 2^{-1} \left(2^d - 2 \right)^{\frac{n}{d}} = 2^{n-1} \pm 2^{\frac{n}{2}-1}$$

and solving for d we see that $d = 2$. Hence $k = \frac{n}{d} = \frac{n}{2}$ and so the only function of the form above where $\text{wt}(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ is $f(\mathbf{x}) = x_1 x_{\frac{n}{2}+1} + \cdots + x_{\frac{n}{2}} x_n$. By Theorem 6, $f(\mathbf{x}) = x_1 x_{\frac{n}{2}+1} + \cdots + x_{\frac{n}{2}} x_n$ is bent. $\square$

Lemma 13. Let $\mathbf{x} = (x_1, \dots, x_n)$ and $f(\mathbf{x})$ be a monomial rotation symmetric short function with disjoint variables and $\deg(f) \neq 2$. Then

$$\text{wt}(f(\mathbf{x})) \neq 2^{n-1} \pm 2^{\frac{n}{2}}.$$

Proof. By Corollary 2.5 in [1],

$$\text{wt}(f) = 2^{n-1} - 2^{\frac{n}{d}-1}(2^{d-1} - 1)^{\frac{n}{d}}.$$

Note that

$$2^{n-1} - 2^{\frac{n}{d}-1}(2^{d-1} - 1)^{\frac{n}{d}} = 2^{n-1} \pm 2^{\frac{n}{2}}$$

if and only if $d = 2$. Hence if $\deg(f) \neq 2$ then

$$\text{wt}(f(\mathbf{x})) \neq 2^{n-1} \pm 2^{\frac{n}{2}}.$$

□

Remark 14. Since every bent function has weight $2^{n-1} \pm 2^{\frac{n}{2}-1}$ there are no bent monomial rotation symmetric short functions with disjoint variables of degree $\neq 2$.

Corollary 15. Let $\mathbf{x} = (x_1, \dots, x_n)$. Then

$$f(\mathbf{x}) = x_1 x_{\frac{n}{2}+1} + \dots + x_{\frac{n}{2}} x_n$$

is the only short bent monomial rotation symmetric function with disjoint variables.

Proof. Corollary 15 follows directly from Corollary 12 and Lemma 13. □

3 Bent and Balanced d -functions

In this section we look at the weights of d -functions and determine whether or not they are bent or balanced.

Remark 16. Note that, up to a permutation of the variables,

$$f(\mathbf{x}) = \sum_{i=1}^k x_i x_{i+k} \dots x_{i+(d-1)k}$$

is equivalent to

$$g(\mathbf{x}) = \sum_{i=1}^k x_{d(i-1)+1} x_{d(i-1)+2} \dots x_{d(i-1)+d},$$

where $d = \deg(f)$ and $k = \frac{n}{d}$, since each monomial in f and g is degree d and every variable appears exactly once in both functions. Therefore the results in this section follow directly from the results in the previous section.

Theorem 17. Let $\mathbf{x} = (x_1, \dots, x_n)$ and

$$g(\mathbf{x}) = \sum_{i=1}^k x_{d(i-1)+1} x_{d(i-1)+2} \dots x_{d(i-1)+d}$$

where $d = \deg(g)$ and $k = \frac{n}{d}$. Then

$$\text{wt}(g(\mathbf{x})) = \sum_{i=1}^k (-2)^{i-1} \binom{k}{i} 2^{n-id}.$$

Corollary 18. Let $\mathbf{x} = (x_1, \dots, x_n)$ and

$$g(\mathbf{x}) = \sum_{i=1}^k x_{d(i-1)+1} x_{d(i-1)+2} \dots x_{d(i-1)+d}$$

where $d = \deg(g)$ and $k = \frac{n}{d}$. Then

$$g(\mathbf{x}) = x_1 + \dots + x_n$$

is the only balanced function of this form.

Corollary 19. Let $\mathbf{x} = (x_1, \dots, x_n)$ and

$$g(\mathbf{x}) = \sum_{i=1}^k x_{d(i-1)+1} x_{d(i-1)+2} \cdots x_{d(i-1)+d}$$

where $d = \deg(g)$ and $k = \frac{n}{d}$. Then

$$g(\mathbf{x}) = x_1 x_2 + x_3 x_4 + \cdots + x_{n-1} x_n$$

is the only bent function of this form.

4 Discussion / Conclusion

In this paper we constructed formulas for the weights of short MRS functions and d -functions by using the inclusion / exclusion principle. We used these results to determine which functions of those forms are bent or balanced. Next, it would be interesting to use the techniques demonstrated in this paper to develop formulas for weights of other rotation symmetric functions to potentially classify additional functions with cryptographic applications.

Acknowledgement: I would like to thank Thomas Cusick for his support and advice throughout this process.

Author's Statement: There are no potential financial, personal, or professional conflicts regarding the publication of this article.

Biography: Elizabeth Reid earned her Ph.D. in Mathematics at the University at Buffalo. She is currently an Assistant Professor of Mathematics in the School of Computer Science and Mathematics at Marist College in Poughkeepsie, NY. Her research interests include Number Theory, Cryptography, and Combinatorics.

References

- [1] T. W. Cusick and D. Padgett, A recursive formula for weights of Boolean rotation symmetric functions, *Discrete Appl. Math.* 160 (2011), 391-397.
- [2] T.W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, 2nd ed., London: Academic Press (2017).
- [3] H. Kim, S-M. Park, and S. G. Hahn, On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2, *Discr. Appl. Math.* 157 (2009), 428-432.
- [4] E. M. Reid and T. W. Cusick, Affine equivalence classes of 2-rotation symmetric cubic Boolean functions, *Int. J. Comput. Math.: Computer Systems Theory* 3:3 (2018), 145-159.