Chapter 4

Rotation Symmetric Functions

4.1 Introduction

A variety of criteria for choosing Boolean functions for cryptographic applications have been identified. It is very difficult to construct or find out Boolean functions that satisfies the optimality of all the properties. The tradeoffs among these criteria have received a lot of attention in Boolean function literature for a long time. It is difficult to search appropriate functions from the whole set of Boolean functions as the search space is huge. Thus a natural idea is to decrease the search space by considering certain subclasses. Functions which are invariant under the action of the cyclic group are called rotation symmetric (RotS) functions. This class of functions are extremely rich in terms of cryptographically significant functions. Rotation symmetric Boolean functions were first introduced by Pieprzyk and Qu in 1999 [5]. They used rotation symmetric functions as the components in the rounds of hashing algorithms. Maitra and Stănică [4] presented various counting results for rotation symmetric Boolean functions. In 2008 Yuan Li [13] generalized the concept of rotation symmetric functions from $\mathbb{F}_2$ to $\mathbb{F}_p$ and obtained many enumeration results of rotation symmetric functions over $\mathbb{F}_p$ including the number of homogeneous rotation symmetric functions of degree upto 3 over $\mathbb{F}_p$. But enumeration of the homogeneous rotation symmetric functions with degree

more than 3 was left as an open problem for many years. We solve this problem using Polya's enumeration theorem and give an explicit formula for the number of homogeneous rotation symmetric functions over the finite field $\mathbb{F}_{p^m}$. This result simplifies the proof and the nonexplicit counting formula for the homogeneous rotation symmetric functions over the field $\mathbb{F}_p$ given by Shaojing Fu et al. [15].

4.2 Rotation Symmetric Boolean Functions

Definition 4.1. *(Cyclic rotation)* Let $x_i \in F_2$, for any $1 \leq i \leq n$ and $0 \leq k \leq n-1$ we define

$$\rho_n^k(x_i) = \begin{cases} x_{i+k} & \text{if } i+k \leq n \\ x_{i+k-n} & \text{if } i+k > n \end{cases}$$

Let $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$. Then we can extend the definition of ρ_n^k on tuples as

$$\rho_n^k(x) = (\rho_n^k(x_1), \rho_n^k(x_2), ..., \rho_n^k(x_n))$$

Definition 4.2. *(Rotation symmetric function)* A Boolean function $f(x_1, x_2, ..., x_n)$ is called rotation symmetric (RotS) if for each input $(x_1, x_2, ..., x_n) \in \mathbb{F}_2^n$ and any $0 \leq k \leq n-1$, $f(\rho_n^k(x_1, x_2, ..., x_n)) = f(x_1, x_2, ..., x_n)$.

Note that there are 2^n different input values corresponding to an n-variable Boolean function. From the definition 4.2, it is clear that rotation symmetric Boolean function f possesses the same value corresponding to each of the subsets generated from the rotational symmetry.

Example 4.1. *For $n = 4$ one gets the following partitions of $\mathbb{F}_2^4$.*

$\{(0,0,0,0)\}$

$\{(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0\}$

$\{(0,0,1,1),(0,1,1,0),(1,0,0,1),(1,1,0,0)\}$

$\{(0,1,0,1),(1,0,1,0)\}$

$\{(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\}$

$\{(1,1,1,1)\}$

Since there are 6 different subsets which partition the 16 input patterns, any 4-variable RotS Boolean function can have a specific value corresponding to each subset. Thus there are $2^6 = 64$ RotS Boolean functions on 4 variables.

Let $G_n(x_1, x_2, ..., x_n) = \{\rho_n^k(x_1, x_2, ..., x_n),\ \text{for}\ 0 \leq k \leq n-1\}$ be the orbit of $(x_1, x_2, ..., x_n)$ under the action of ρ_n^k for $0 \leq k \leq n-1$. It is clear that $G_n(x_1, x_2, ..., x_n)$ generates a partition in the set $\mathbb{F}_2^n$. Let g_n be the number of orbits generated then it is clear that there are 2^{g_n} number of n-variable rotation symmetric Boolean functions.

An orbit is completely determined by its representative element $\Lambda_{n,i}$ which is lexicographically the first element in the orbit [55]. The weight of the orbit is defined as the weight of the representative element. These representative elements are again arranged lexicographically as $\Lambda_{n,0}, \Lambda_{n,1}, ..., \Lambda_{n,g_n-1}$. Note that for any n, $\Lambda_{n,0} = (0, 0, ..., 0), \Lambda_{n,1} = (0, 0, ..., 1)$ and $\Lambda_{n,g_n-1} = (1, 1, ..., 1)$. Thus an n- variable RotS Boolean function f can be represented by the g_n length string $f(\Lambda_{n,0}), f(\Lambda_{n,1}), ..., f(\Lambda_{n,g_n-1})$ which we call the rotation symmetric truth table (RSTT) of f.

Clearly one can extend the definition of ρ_n^k to monomials of the form $(x_{i_1}x_{i_2}....x_{i_d})$ as $\rho_n^k(x_{i_1}x_{i_2}....x_{i_d}) = \rho_n^k(x_{i_1})\rho_n^k(x_{i_2})...\rho_n^k(x_{i_d})$. Similarly, let

$$G_n(x_{i_1}x_{i_2}...x_{i_d}) = \{\rho_n^k(x_{i_1}x_{i_2}...x_{i_d}), \quad for \ \ 0 \leq k \leq n-1\}$$

be the orbit of $x_{i_1}x_{i_2}...x_{i_d}$. We select the representative element of $G_n(x_{i_1}x_{i_2}...x_{i_d})$ as the lexicographically first element, for example the representative element of $\{x_1x_2x_3, x_2x_3x_4, x_3x_4x_1, x_4x_1x_2\}$ is $x_1x_2x_3$. Note that the term x_1 will always exist in the lexicographically first element if we consider a non constant rotation symmetric Boolean function.

From the definition of rotation symmetric Boolean functions, we can see that a RotS function $f(x_1, x_2, ..., x_n)$ can be written as $a_0 + a_1x_1 + \sum a_{1j}x_1x_j + ... + a_{12...n}x_1x_2...x_n$, where the coefficients $a_0, a_1, a_{1j}, ..., a_{12...n} \in \mathbb{F}_2$, and the existence of a representative term $x_1x_{i_2}...x_{i_d}$ implies the existence of all the terms from

$G_n(x_1x_{i_2}...x_{i_d})$ in the ANF. This representation of f is called the short algebraic normal form (SANF) of f. A Boolean function is said to be homogeneous if its algebraic normal form contains terms of same degree only.

Example 4.2. *As an example 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* $x_1 + x_1x_2x_3$.

Definition 4.3. (MRS Boolean Functions) A RotS Boolean function is said to be monomial rotation symmetric (MRS) if it is generated by applying powers of the cyclic permutation ρ_n to a single monomial.

Homogeneous bent functions have been extensively studied in literature [3, 55, 56, 57]. Using a computer search, Stănică et al.[4] found the exact number of 4, 6 and 8 variable RotS bent functions as 8, 48 and 15104 respectively.

Filiol and Fontaine [58] discussed a set of idempotent Boolean functions in an experimental setting. The set of idempotent Boolean functions can be identified with the class of RotS Boolean functions under the proper choice of the basis. It is interesting to note that the famous Patterson-Wiedemann functions [11] are in fact rotation symmetric.

4.3 Enumeration of Rotation Symmetric Boolean Functions

Let g_n be the number of orbits generated under the action of cyclic rotations. Then it is clear that there are 2^{g_n} number of n-variable rotation symmetric Boolean functions. Maitra and Stănică [4] calculated the value of g_n using Burnside's lemma as

$$g_n = \frac{1}{n}\sum_{d|n}\phi(d)2^{\frac{n}{d}}$$

where ϕ is the Euler's phi function. They introduced the concepts like long cycle and short cycles to enumerate the homogeneous RotS Boolean functions. It is

clear that $|G_n(x_1x_{i_2}...x_{i_d})| \leq n$. The elements of $G_n(x_1x_{i_2}...x_{i_d})$ is said to form a long cycle if $|G_n(x_1x_{i_2}...x_{i_d})| = n$. On the other hand, if $|G_n(x_0x_{i_2}...x_{i_d})| < n$, we call it a short cycle, which is of length strictly less than n. Let h_n be the number of long cycles. Clearly $h_n < g_n$. They provided a formula for h_n as

$$h_n = \begin{cases} 2 & if \quad n = 1 \\ \frac{1}{n}\sum_{d|n}\phi(d)2^{\frac{n}{d}} \sum_{i=1}^{a-1} \frac{2^{p^i} - 2^{p^{i-1}}}{p^i} - 2 & if \quad n = p^a \\ \frac{1}{n}\sum_{d|n}\phi(d)2^{\frac{n}{d}} \sum_{i=1}^{w_n}\sum_{j=1}^{a_i} \frac{2^{p_i^j} - 2^{p_i^{j-1}}}{p_i^j} - 2 & if \quad n = p_1^{a_1}p_2^{a_2}...p_{w_n}^{a_{w_n}} \end{cases}$$

We have already noted that for RotS Boolean functions, if the term $x_{i_1}x_{i_2}...x_{i_d}$ is present, then all the distinct terms of the form $\{\rho_n^k(x_{i_1}x_{i_2}...x_{i_d})\ 0 \leq k \leq n-1\}$ are also present. Hence, for RotS functions, it is clear that some monomials of the same degree either appear or do not appear at the same time. Now we concentrate on monomials of the same degree.

First consider the set $\{G_n(x_1, x_2, ..., x_n)/wt(x_1, x_2..., x_n) = w\}$. Note that this partitions the set of all n bit binary strings of weight w. Let $g_{n,w}$ be the number of such partitions and $h_{n,w}$ be the number of distinct sets $G_n(x_1, x_2..., x_n)$, where $wt(x_1, x_2..., x_n) = w$ and $|Gn(x_1, x_2, ..., x_n)| = n$, that is, the number of long cycles of weight w. Maitra and Stănică [4] calculated the value of $g_{n,w}$ as

$$g_{n,w} = \begin{cases} 1 \quad if \quad w = 0, n \\ \frac{1}{n}\binom{n}{w} \quad if \quad gcd(n, w) = 1 \\ \frac{1}{n}\left(\binom{n}{w} - \sum_{\substack{k|gcd(n,w) \\ 1 \leq k < gcd(n,w)}} \frac{n}{k} h_{\frac{n}{k},\frac{w}{k}}\right) + \sum_{\substack{k|gcd(n,w) \\ 1 \leq k < gcd(n,w)}} h_{\frac{n}{k},\frac{w}{k}} \quad otherwise \end{cases}$$

by solving the recurrence relation

$$h_{n,w} = \frac{1}{n}\left(\binom{n}{w} - \sum_{\substack{k|gcd(n,w) \\ 1\leq k<gcd(n,w)}} \frac{n}{k} h_{\frac{n}{k},\frac{w}{k}}\right)$$

Note that $g_{n,w}$ denotes the number of distinct cycles of weight w. This means that the degree w monomials can be divided in $g_{n,w}$ different cycles. Hence we can derive the following results easily as given in [4] as

- Number of degree w homogeneous Rots Boolean functions $= 2^{g_{n,w}}$
- The number of degree w functions $= (2^{g_{n,w}} - 1)2^{\sum_{i=0}^{w-1} g_{n,i}}$
- The number of functions with degree at most $w = 2^{\sum_{i=0}^{w-1} g_{n,i}}$

However, it was shown by Q. Li et al. in [59] that the more general formula for h_n is sometimes incorrect; for example, computation shows that $h_{12} = 355$, but the formula gives $h_{12} = 344$.

Using Polya's enumeration theorem we can find the explicit formula for $g_{n,w}$.

Let X be the set of all monomials in n-variables and G be the group of cyclic permutations on n elements. Then the cycle index polynomial of G is

$$Z_G(x_1, x_2, ..., x_n) = \frac{1}{n}\sum_{d|n} \phi(d) x_d^{\frac{n}{d}}$$

Consider the set of colors as the finite field $\mathbb{F}_2$. Let us define the weight for each colors as $w(0) = 1,\ w(1) = y$. Then by Polya's theorem, pattern index of nonequivalent colorings of X under G is given by

$$I = Z_G\left(1+y, 1+y^2, ..., 1+y^n\right) = \frac{1}{n}\sum_{d|n} \phi(d)\left(1+y^d\right)^{\frac{n}{d}}.$$

and the coefficient of y^w in the expansion of I gives $g_{n,w}$, the number of orbits of degree w monomials.

$$g_{n,w} = \frac{1}{n}\sum_{d|r}\phi(d)\binom{\frac{n}{d}}{\frac{w}{d}} \quad where\ r = gcd(n,w)$$

4.4 Rotation Symmetric Functions over Finite Fields

In 2008, Yuan Li [13] generalized the concept of rotation symmetric functions from $\mathbb{F}_2$ to $\mathbb{F}_p$ and obtained many counting results about rotation symmetric functions over finite field $\mathbb{F}_p$ by generalizing the results of Boolean functions. They also simplified some known formulas in Boolean case. They calculated the number of long cycles as

$$h_n = \begin{cases} p & if \quad n = 1 \\ \dfrac{p^{q^\alpha} - p^{q^{\alpha-1}}}{n} & if \quad n = q^a \\ \dfrac{1}{n}\displaystyle\sum_{d|n}\mu(d)p^{\frac{n}{d}} & if \quad n = q_1^{a_1}q_2^{a_2}...q_r^{a_r} \end{cases}$$

Note that this simplifies the result for h_{q^α} [4]

$$h_{q^\alpha} = \frac{1}{n}\sum_{d|n}\phi(d)2^{\frac{n}{d}} \sum_{i=1}^{a-1}\frac{2^{q^i} - 2^{q^{i-1}}}{q^i} - 2 \quad to \quad \frac{2^{q^\alpha} - 2^{q^{\alpha-1}}}{n}$$

Li enumerated homogeneous RotS functions with degree 2 as $p^{\lfloor \frac{n}{2} \rfloor + 1} - 1$ and degree 3 as $p^{m(3)-1}$ where $m(3) = n\left\lfloor \frac{n-1}{3} \right\rfloor - \frac{3(\lfloor \frac{n-1}{3} \rfloor)(\lfloor \frac{n-1}{3} \rfloor + 1)}{2} + n$, plus one if and only if $n \equiv 0 (mod\ 3)$. Later, Fu et al. [14] gave a lower bound on the number of homogeneous rotation symmetric functions and a formula to count homogeneous RotS functions when the greatest common divisor of the number of input variables and the algebraic degree of the function is a prime power, which partially solved

the open problem in [13]. Still it remained as an open problem to count the homogeneous rotation symmetric functions with degree more than 3.

In 2012, Shaojing Fu et al. [60] gave an enumeration formula for n-variable homogeneous RotS functions with arbitrary degree. They calculated the number of degree w homogeneous RotS Boolean functions $N_{n,d}$ as follows

$$N_{n,d} = \begin{cases} p^{M(n,d)} - 1 & if \quad gcd(n,d) = 1 \\ p^{M(n,d)} p^{\sum_{k|gcd(n,k),\ k\neq 1} \frac{k-1}{k} T(\frac{n}{k}, \frac{n}{k}, \frac{d}{k})} - 1 & if \quad gcd(n,d) \neq 1 \end{cases}$$

where

$$M(n,d) = \sum_{j=1}^{N_\Omega} \frac{(n-1)!}{m_o^{(j)}! m_1^{(j)}! ... m_{p-1}^{(j)}!}$$

$$T(n,n,d) = \frac{1}{gcd(n,d)} \sum_{m|gcd(n,d)} \mu(m) \frac{gcd(n,d)}{m} M(\frac{n}{m}, \frac{d}{m})$$

and N_Ω is the number of solutions for the system of equations

$$\Omega(d,p,n) = \begin{cases} y_1 + y_2 + ... + y_n = d \\ 0 \leq y_n \leq y_{n-1} \leq ... y_2 \leq y_1 \leq p-1 \\ y_i \in \mathbb{Z} \quad 1 \leq i \leq n \end{cases}$$

The evaluation of $N_{n,d}$ depends on the number of solutions of the system of equations $\Omega(d,p,n)$ which is hard to find in general. We considered the more general case of functions over the arbitrary finite field $\mathbb{F}_{p^m}$ and solved the problem of enumeration of homogeneous rotation symmetric functions using Polya's enumeration theorem.

Let $\mathbb{F}_{p^m}$ be the finite field of p^m elements and $\mathbb{F}_{p^m}^n$ be the vector space of dimension n over $\mathbb{F}_{p^m}$. We can generalize the concept of rotation symmetric functions from $\mathbb{F}_2$ to $\mathbb{F}_{p^m}$. An n-variable function $f : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}$ can be considered as a multivariate

polynomial over $\mathbb{F}_{p^m}$ with its ANF

$$f(x_1, x_2, ..., x_n) = \sum_{\substack{k_i=0 \\ i=1,2,...n}}^{p^m-1} a_{k_1,k_2,...,k_n} x_1^{k_1} x_2^{k_2} ... x_n^{k_n},\ a_{k_1,k_2,...,k_n} \in \mathbb{F}_{p^m}.$$

The sum $k_1 + k_2 + ... + k_n$ is defined as the degree of the term with nonzero coefficient. The greatest degree of all terms of f is called the algebraic degree of f. A function is said to be homogeneous if all monomials in the ANF of the function are of same degree. If the ANF of a rotation symmetric function has a term $a x_{i_1}^{k_1} x_{i_2}^{k_2} ... x_{i_d}^{k_d},\ a \in \mathbb{F}_{p^m},\ k_1 + k_2 + ... + k_d = w$, then it has all the terms of the following set

$$\left\{ a x_{i_1+j}^{k_1} x_{i_2+j}^{k_2} ... x_{i_d+j}^{k_d} = a x_{l_1}^{t_1} x_{l_2}^{t_2} ... x_{l_d}^{t_d} / j = 0, 1, ..., n-1, l_1 < l_2 < ... < l_d \right\}$$

where $i_r + j$ is treated as $i_r + j - n$ if $i_r + j > n$. The *minimal term* in this set is the term with the smallest vector $(l_1, l_2, ..., l_d)$. Let $g_{n,w}$ be the number of *minimal monomials* of degree w. We can calculate $g_{n,w}$ over $\mathbb{F}_{p^m}$ using Polya's enumeration theorem.

Theorem 4.4. *The number of minimal monomials of degree $w \geq 1$, over $\mathbb{F}_{p^m}$ is*

$$g_{n,w} = \frac{1}{n} \sum_{\substack{N=(k_0,k_1,...,k_{p^m-1}) \\ : \sum_{i=0}^{p^m-1} k_i = n,\ \sum_{i=1}^{p^m-1} i k_i = w}} \sum_{d|r} \phi(d) \frac{(\frac{n}{d})!}{\prod_{j=0}^{p^m-1} \left(\frac{k_j}{d}\right)!},\ r = gcd(k_0, k_1, ..., k_{p^m-1}, w)$$

Proof. Let X be the set of all monomials in n-variables and G be the group of cyclic permutations on n elements. Then the cycle index polynomial of G is $Z_G(t_1, t_2, ..., t_n) = \frac{1}{n} \sum_{d|n} \phi(d) t_d^{\frac{n}{d}}$. Consider the set of colors as the finite field $\mathbb{F}_{p^m}$. Let us define the weight for each colors as $w(0, 0, ..., 0) = y_0,\ w(0, 0, ..., 1) = y_1, ..., w(p-1, ..., p-1) = y_{p^m-1}$. Then by Polya's theorem, pattern index of nonequivalent colorings of X under G is given by

$$I = Z_G \left(\sum_{i=0}^{p^m-1} y_i, \sum_{i=0}^{p^m-1} y_i^2, ..., \sum_{i=0}^{p^m-1} y_i^n \right) = \frac{1}{n} \sum_{d|n} \phi(d) \left(\sum_{i=0}^{p^m-1} y_i^d \right)^{\frac{n}{d}}.$$

Then the number of *minimal monomials* of degree w is the sum of coefficients of $y_0^{k_0}y_1^{k_1}y_2^{k_2}...y_{p^m-1}^{k_{p^m-1}}$ with $\sum_{i=0}^{p^m-1} k_i = n$ and $\sum_{i=1}^{p^m-1} ik_i = w$ in the expansion of I.

Note that when $d > 1$ the expansion of I contributes a term $y_0^{k_0}y_1^{k_1}y_2^{k_2}...y_{p^m-1}^{k_{p^m-1}}$ with $\sum_{i=1}^{p^m-1} k_i = n$ if and only if $r = gcd(k_0, k_1, ..., k_{p^m-1}, w)$ is greater than one and when $d = 1$ the term $y_0^{k_0}y_1^{k_1}y_2^{k_2}...y_{p^m-1}^{k_{p^m-1}}$ with $\sum_{i=1}^{p^m-1} k_i = n$ occurs exactly once in the expansion of I with the multinomial coefficient $\frac{(n)!}{\prod_{j=0}^{p^m-1}(k_j)!}$. Hence by summing over all divisors of r we can deduce the sum of coefficients of $y_0^{k_0}y_1^{k_1}y_2^{k_2}...y_{p^m-1}^{k_{p^m-1}}$ with $\sum_{i=1}^{p^m-1} k_i = n$ and $\sum_{i=1}^{p^m-1} ik_i = w$ in the expansion of I as

$$g_{n,w} = \frac{1}{n} \sum_{N=(k_0,k_1,...,k_{p^m-1}) : \sum_{i=0}^{p^m-1} k_i = n \sum_{i=1}^{p^m-1} ik_i = w} \sum_{d|r} \phi(d) \frac{(\frac{n}{d})!}{\prod_{j=o}^{p^m-1}\left(\frac{k_j}{d}\right)!},\ r = gcd(k_0, k_1, ..., k_{p^m-1}, w)$$

□

Corollary 4.5. The number of n-variable homogeneous rotation symmetric functions over $\mathbb{F}_{p^m}$ of degree $w \geq 1$ is $(p^m)^{g_{n,w}} - 1$.

Remark 4.6. This result simplifies not just the proof, but also the counting formula given in Fu et al.[60]. Theorem 11 in [60] involves the nonexplicit number N_Ω but here the formula is more explicit.

-

4.5 Weight and Nonlinearity of Homogeneous Rotation Symmetric Boolean Functions

Knowledge of Hamming weight of Boolean functions is important to decide whether the functions are useful in cryptography. In 2002, Cusick and Stănică [7] studied the nonlinearity and the weight of the rotation symmetric Boolean functions. They gave exact results for the nonlinearity and weight of quadratic RotS Boolean functions with the help of the semi-bent functions and gave the generating function for the weight of the cubic RotS Boolean function. Based on the numerical examples and observations they conjectured that the Hamming weight of the cubic MRS RotS Boolean functions generated by $x_1x_2x_3$ is same as its nonlinearity. In 2009, Kim et al.[61] improved parts of the results obtained by Cusick and Stănică and derived a closed formula for the weights of quadratic functions in terms of the number of variables n. Later Maxwell et al.[62] provided an algorithm for finding a homogeneous recursion for the truth table of any cubic MRS Boolean functions. In 2011, Zhang et al. [63] proved the conjecture, given by Cusick and Stănică. Yang et al. [64] studied the case of quartic rotation symmetric Boolean functions generated by $x_1x_2x_3x_4$ and proved that the nonlinearity of these functions is the same as its weight. Later in 2012 Cusick and Dan Padgett [65] presented a method for recursively computing the weights of certain kinds of rotation symmetric Boolean functions with arbitrary degree and obtained some detailed information on relationships between the weights of some of these cubic functions as n increases. It is natural to ask: Is the nonlinearity of rotation symmetric Boolean functions of degree d (≥ 3) generated by $x_1x_2....x_d$ equal to its weight? We have noted that the Hamming weight of homogeneous RotS Boolean functions of degree $d \geq 4$ is same as its nonlinearity. We have calculated the weight of homogeneous RotS Boolean functions of degree greater than $\frac{n}{2}$.

Consider the n variable homogenous rotation symmetric Boolean function f of degree d ($\lfloor \frac{n}{2} \rfloor \leq d \leq n-1$) with SANF

$$f(x_1, x_2, ...x_n) = x_1x_2...x_d + x_2x_3...x_{d+1} + ... + x_nx_1...x_{d-1}, \left\lfloor \frac{n}{2} \right\rfloor \leq d \leq n-1$$

The function takes the value one only when the odd number of terms in its ANF is evaluated to one. This will happen only when there are odd number of d consecutive ones in the input $(x_1, x_2, ..., x_n)$ of the function f. The possible values of $(x_1, x_2, ..., x_n)$ are all possible rotations of the following vectors.

If $n - d$ is even then

$(\underbrace{111...1}_{d}\ 0\mathbf{0...00}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...00}0)$	...	$(\underbrace{111...1}_{n-4}\ 0\mathbf{00}0)$	$(\underbrace{111...1}_{n-2}\ 0\mathbf{0})$
$(\underbrace{111...1}_{d}\ 0\mathbf{0...01}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...01}0)$	...	$(\underbrace{111...1}_{n-4}\ 0\mathbf{01}0)$	
$(\underbrace{111...1}_{d}\ 0\mathbf{0...10}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...10}0)$	...	$(\underbrace{111...1}_{n-4}\ 0\mathbf{10}0)$	
$(\underbrace{111...1}_{d}\ 0\mathbf{0...11}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...11}0)$	...	$(\underbrace{111...1}_{n-4}\ 0\mathbf{11}0)$	
...	...	...		
...	...	...		
$(\underbrace{111...1}_{d}\ 0\mathbf{1...11}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{1...11}0)$			
Total 2^{n-d-2}	Total 2^{n-d-4}		Total 2^2	Total 2^0

Hence f will take the value one at

$$n(2^0 + 2^2 + 2^4 + ... + 2^{n-d-4} + 2^{n-d-2}) = n\frac{2^{n-d} - 1}{3}$$

If $n - d$ is odd then

$(\underbrace{111...1}_{d}\ 0\mathbf{0...00}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...00}0)$	...	$(\underbrace{111...1}_{n-5}\ 0\mathbf{000}0)$	$(\underbrace{111...1}_{n-3}\ 0\mathbf{0}0)$	$(\underbrace{111...1}_{n-1}\ 0)$
$(\underbrace{111...1}_{d}\ 0\mathbf{0...01}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...01}0)$	...	$(\underbrace{111...1}_{n-5}\ 0\mathbf{001}0)$	$(\underbrace{111...1}_{n-3}\ 0\mathbf{1}0)$	
$(\underbrace{111...1}_{d}\ 0\mathbf{0...10}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...10}0)$	...	$(\underbrace{111...1}_{n-5}\ 0\mathbf{010}0)$		
$(\underbrace{111...1}_{d}\ 0\mathbf{0...11}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{0...11}0)$	...	$(\underbrace{111...1}_{n-5}\ 0\mathbf{011}0)$		
...	...	...	...		
...	...	...	...		
$(\underbrace{111...1}_{d}\ 0\mathbf{1...11}0)$	$(\underbrace{111...1}_{d+2}\ 0\mathbf{1...11}0)$	...	$(\underbrace{111...1}_{n-5}\ 0\mathbf{111}0)$		
Total 2^{n-d-2}	Total 2^{n-d-4}		Total 2^3	Total 2^1	Total 2^0

Hence f will take the value one at

$$n(1 + 2^1 + 2^3 + ... + 2^{n-d-2}) = n\frac{2^{n-d} - 1}{3}$$

if n is odd, f will take the value one at $(\underbrace{111...1}_{n})$

Hence the weight of f is given by

$$wt(f) = \begin{cases} \frac{n(2^{n-d}-1)}{3} & \text{if } n \text{ is even} \\ 1 + \frac{n(2^{n-d}-1)}{3} & \text{if } n \text{ is odd} \end{cases} \quad \left\lfloor \frac{n}{2} \right\rfloor \leq d \leq n-1$$

4.6 Enumeration of Balanced Rotation Symmetric Boolean Functions

A Boolean function is said to be balanced if it takes equal number of zeros and ones for all of its inputs. So in order to get balanced rotation symmetric Boolean functions, we need to partition $\mathbb{F}_2^n$ into two groups each of size 2^{n-1}. Let N_n be the number of balanced n-variable rotation symmetric Boolean functions and let h_n denote the number of orbits with maximal length n. In 2004, Stănică, Maitra and Clark [3, Th. 1] calculated the value of N_n when $n = p$, where p is an odd prime as

$$N_p = 2 \begin{pmatrix} \frac{2^p - 2}{p} \\ \frac{2^{p-1} - 1}{p} \end{pmatrix}$$

Later Stănică and Maitra [4, Th. 8 (ii)] gave a lower bound of N_n when $n = p^r$ as

$$N_{p^r} \geq 2 \prod_{i=1}^{r} \begin{pmatrix} h_{p^i} \\ \frac{h_{p^i}}{2} \end{pmatrix}$$

where

$$h_{p^i} = \begin{cases} \frac{2^{p^i}-2^{p^{i-1}}}{p^i}, & 1 \le i \le r-1 \\ p^{-r}\left(2^{p^a} + \sum_{j=1}^{r} \phi(p^j) 2^{p^{r-j}}\right) - \sum_{j=1}^{r-1} h_{p^i} - 2, & i = r \end{cases}$$

In 2010 ShaoJing Fu, et al. [17] proved that the problem of enumeration of balanced rotation symmetric Boolean functions is equivalent to solving a system of equations and enumerating the solutions. As a result they gave an enumeration formula for N_n when $n = p^r$, a prime power as

$$N_{p^r} = \sum_{j=1}^{T} \prod_{i=1}^{r} \begin{pmatrix} h_{p^i} \\ z_i^j \end{pmatrix}$$

where

$$\left\{(z_1^{(1)}, z_2^{(1)}, ..., z_r^{(1)}), (z_1^{(2)}, z_2^{(2)}, ..., z_r^{(2)}), ..., (z_1^{(T)}, z_2^{(T)}, ..., z_r^{(T)})\right\}$$

is the set of solutions of the system of equations

$$\theta : \begin{cases} \sum_{i=0}^{r} z_i p^i = 2^{p^{r-1}} \\ z_i \in Z, 0 \le z_i \le h_{p^i}, 0 \le i \le r \end{cases}$$

For large values of r, solving the system of equations is highly complex and hence a tighter lower bound for N_{p^r} was given in [17] as

$$N_{p^r} \ge 4 \sum_{j=2}^{r-1} \left(\sum_{l=1}^{\left\lfloor \frac{h_{p^j}}{2p} \right\rfloor} \begin{pmatrix} h_{p^j} \\ \frac{h_{p^j}}{2} - lp \end{pmatrix} \begin{pmatrix} h_{p^{j+1}} \\ \frac{h_{p^{j+1}}}{2} + l \end{pmatrix} \prod_{\substack{i=1 \\ i \ne j \pm 1}}^{r} \begin{pmatrix} h_{p^i} \\ \frac{h_{p^i}}{2} \end{pmatrix} \right) + 2 \prod_{i=1}^{r} \begin{pmatrix} h_{p^i} \\ \frac{h_{p^i}}{2} \end{pmatrix}$$

Consider the n-variable balanced rotation symmetric Boolean functions where n is a product of two primes.

Theorem 4.7. *Let $n = pq$ be a product of two primes then the number of n-variable balanced rotation symmetric Boolean functions is given by:*
Case 1: $p = 2$, q is an odd prime

$$N_n = 4 \sum_{\substack{r=0 \\ r\equiv 1 (mod 2)}}^{\frac{d_{n,q}}{2}} \binom{d_{n,q}}{\frac{d_{n,q}+2r}{2}} \binom{d_{n,n}}{\frac{d_{n,n}-r}{2}}$$

Case 2: p and q are odd primes

$$N_n = 4 \sum_{\substack{r=0 \\ r\equiv 0 (mod 2)}}^{\left\lfloor \frac{d_{n,q}}{p} \right\rfloor} \sum_{\substack{s=0 \\ s\equiv 0 (mod 2)}}^{\left\lfloor \frac{d_{n,p}}{q} \right\rfloor} \binom{d_{n,p}}{\frac{d_{n,p}+sq}{2}} \binom{d_{n,q}}{\frac{d_{n,q}+rp}{2}} \left[\binom{d_{n,n}}{\frac{d_{n,n}+r+s}{2}} + \binom{d_{n,n}}{\frac{d_{n,n}+r-s}{2}} \right]$$

where $d_{n,l} = \frac{1}{l} \sum_{k/l} \mu\left(\frac{l}{k}\right) 2^{gcd(n,k)}$ denote the number of orbits of length l.

Proof. In order to count N_n we divide the 2^n elements of $\mathbb{F}_2^n$ into two groups A_n and B_n of equal size 2^{n-1}. Since the function that we are considering is rotation symmetric, the vectors in the same orbit must be in the same group. We know that the length of the orbit should be a divisor of n. Since $n = pq$, the only possible lengths of the orbits are $1, p, q$ and n. Using Lemma 1 of [66] we can calculate the number of orbits of length l as $d_{n,l} = \frac{1}{l} \sum_{k/l} \mu\left(\frac{l}{k}\right) 2^{gcd(n,k)}$.

Case 1: $p = 2$, q is an odd prime

We have

$$d_{n,1} = 2,\ d_{n,2} = 1,\ d_{n,q} = \frac{2^q - 2}{q} \text{ and } d_{n,n} = \frac{2^n - 2^q - 2}{2q}$$

Note that $d_{n,q}$ is always even and $d_{n,n}$ is always odd. Hence the only possible ways to group the elements into two groups of equal size are (4-tuples give the number of orbits of each size)

$$\left\{ \left(2, 0, \frac{d_{n,q}+2r}{2}, \frac{d_{n,n}-r}{2}\right), \left(2, 0, \frac{d_{n,q}-2r}{2}, \frac{d_{n,n}+r}{2}\right), \right.$$
$$\left. \left(0, 1, \frac{d_{n,q}+2r}{2}, \frac{d_{n,n}-r}{2}\right), \left(0, 1, \frac{d_{n,q}-2r}{2}, \frac{d_{n,n}+r}{2}\right) \right\}$$

where $0 \leq r \leq \frac{d_{n,q}}{2}$, r being odd. So the number of balanced rotation symmetric Boolean functions on n variables is given by

$$\begin{aligned} N_n = & \sum_{\substack{r=0 \\ r\equiv 1(mod 2)}}^{\frac{d_{n,q}}{2}} \binom{2}{2}\binom{1}{0}\binom{d_{n,q}}{\frac{d_{n,q}+2r}{2}}\binom{d_{n,n}}{\frac{d_{n,n}-r}{2}} \\ & + \binom{2}{2}\binom{1}{0}\binom{d_{n,q}}{\frac{d_{n,q}-2r}{2}}\binom{d_{n,n}}{\frac{d_{n,n}+r}{2}} \\ & + \binom{2}{0}\binom{1}{1}\binom{d_{n,q}}{\frac{d_{n,q}+2r}{2}}\binom{d_{n,n}}{\frac{d_{n,n}-r}{2}} \\ & + \binom{2}{0}\binom{1}{1}\binom{d_{n,q}}{\frac{d_{n,q}-2r}{2}}\binom{d_{n,n}}{\frac{d_{n,n}+r}{2}} \end{aligned}$$

i.e;

$$N_n = 4 \sum_{\substack{r=0 \\ r\equiv 1(mod 2)}}^{\frac{d_{n,q}}{2}} \binom{d_{n,q}}{\frac{d_{n,q}+2r}{2}}\binom{d_{n,n}}{\frac{d_{n,n}-r}{2}}$$

Case 2: p and q are odd primes

We have

$$d_{n,1} = 2,\ d_{n,p} = \frac{2^p-2}{p},\ d_{n,q} = \frac{2^q-2}{q}\ and\ d_{n,n} = \frac{2^n-2^p-2^q+2}{n}$$

Note that $d_{n,l}$ is even for $l = 1, p, q, n$. Hence the only possible ways to group the elements into two groups of equal size are

$$\begin{aligned} \Big\{ & \left(1, \frac{d_{n,p}+sq}{2}, \frac{d_{n,q}+rp}{2}, \frac{d_{n,n}-r-s}{2}\right), \left(1, \frac{d_{n,p}-sq}{2}, \frac{d_{n,q}-rp}{2}, \frac{d_{n,n}+r+s}{2}\right), \\ & \left(1, \frac{d_{n,p}+sq}{2}, \frac{d_{n,q}-rp}{2}, \frac{d_{n,n}+r-s}{2}\right), \left(1, \frac{d_{n,p}-sq}{2}, \frac{d_{n,q}+rp}{2}, \frac{d_{n,n}-r+s}{2}\right) \Big\} \end{aligned}$$

where $0 \leq r \leq \left\lfloor \frac{d_{n,q}}{p} \right\rfloor$, $0 \leq s \leq \left\lfloor \frac{d_{n,p}}{q} \right\rfloor$, r, s even.

So the number of balanced rotation symmetric Boolean functions on n variables

is given by

$$\begin{aligned} N_n =& 4 \sum_{\substack{r=0 \\ r\equiv 0(mod 2)}}^{\left\lfloor \frac{d_{n,q}}{p} \right\rfloor} \sum_{\substack{s=0 \\ s\equiv 0(mod 2)}}^{\left\lfloor \frac{d_{n,p}}{q} \right\rfloor} \binom{2}{1} \binom{d_{n,p}}{\frac{d_{n,p}+sq}{2}} \binom{d_{n,q}}{\frac{d_{n,q}+rp}{2}} \binom{d_{n,n}}{\frac{d_{n,n}-r-s}{2}} \\ &+ \binom{2}{1} \binom{d_{n,p}}{\frac{d_{n,p}-sq}{2}} \binom{d_{n,q}}{\frac{d_{n,q}-rp}{2}} \binom{d_{n,n}}{\frac{d_{n,n}+r+s}{2}} \\ &+ \binom{2}{1} \binom{d_{n,p}}{\frac{d_{n,p}+sq}{2}} \binom{d_{n,q}}{\frac{d_{n,q}+rp}{2}} \binom{d_{n,n}}{\frac{d_{n,n}+r-s}{2}} \\ &+ \binom{2}{1} \binom{d_{n,p}}{\frac{d_{n,p}-sq}{2}} \binom{d_{n,q}}{\frac{d_{n,q}-rp}{2}} \binom{d_{n,n}}{\frac{d_{n,n}-r+s}{2}} \end{aligned}$$

i.e;

$$N_n = 4 \sum_{\substack{r=0 \\ r\equiv 0(mod 2)}}^{\left\lfloor \frac{d_{n,q}}{p} \right\rfloor} \sum_{\substack{s=0 \\ s\equiv 0(mod 2)}}^{\left\lfloor \frac{d_{n,p}}{q} \right\rfloor} \binom{d_{n,p}}{\frac{d_{n,p}+sq}{2}} \binom{d_{n,q}}{\frac{d_{n,q}+rp}{2}} \left[\binom{d_{n,n}}{\frac{d_{n,n}+r+s}{2}} + \binom{d_{n,n}}{\frac{d_{n,n}+r-s}{2}} \right]$$

□