Chapter 5

Affine Equivalence of Rotation Symmetric Boolean Functions

The problem of enumerating the types of Boolean functions under the group of variable permutations and complementation was first stated by Jevons in the year 1870s, but not solved in a satisfactory way until the work of Polya in 1940. An affine transformation provides a method of grouping similar Boolean functions into classes. It is meaningful for the following two reasons: first, equivalent functions have similar properties like Hamming weight distribution and same nonlinearity, second, the number of representatives is much less than the number of Boolean functions. Much work have been done on the classification of Boolean functions. The first notable effort to solve an affine equivalence problem was done by Harrison in 1964 [67]. Berlekamp and Welch [68] in 1972 identified and described the complete set of equivalence classes for functions of five inputs using their algebraic normal form. In 1991, Maiorana [69] computed 150357 equivalence classes of six variable Boolean functions. Due to its complexity and size, affine equivalence still remains a tough problem to deal with, especially for a general solution, which addresses for arbitrary number of inputs $n \in \mathbb{N}$.

Besides the pure mathematical perspective, an affine equivalence can be applied to cryptanalysis and cryptographic engineering. For example, differential and

linear cryptanalyses are two major techniques to analyze the S-boxes of block ciphers. If an S-box is vulnerable to differential or linear cryptanalysis, so are the S-boxes realizing affine equivalence functions. This fact simplifies the tasks of cryptanalysts, since they just need to choose and analyze an (easy) representative of an equivalence class. On the other hand, the cryptographic engineers may take advantage of affine equivalent S-boxes of a S-box that is strongly resistant to these attacks, since affine transformations have small delays and preserve much of the cryptographic properties of the original function.

Due to speed and the prospect of being good cryptographic Boolean functions, rotation symmetric Boolean functions have received a lot of attention from cryptographic researchers. There has been consistent effort to investigate the affine equivalence of rotation symmetric Boolean functions. Some recent efforts include [62, 19, 6, 20, 61, 21]. In this chapter, we study the affine equivalence of monomial rotation symmetric (MRS) Boolean functions.

5.1 Affine Equivalence of Boolean Functions

Definition 5.1. (Affine equivalence) Two functions $f, g \in \mathscr{B}_n$ are said to be affinely equivalent if there exist an nonsingular $n \times n$ matrix A over $\mathbb{F}_2$, the vectors $b, c \in \mathbb{F}_2^n$ and $d \in \mathbb{F}_2$ such that $g(x) = f(xA \oplus b) \oplus cx \oplus d$

Example 5.1. *Consider the following five variable Boolean functions,* f, g

$f = x_1x_2 \oplus x_3x_4x_5$ *and* $g = x_3x_4 \oplus x_1x_2x_5 \oplus x_1x_2 \oplus x_1 \oplus 1$

note tat f *and* g *are affine equivalent* $g(x) = f(xA \oplus b) \oplus cx \oplus d$

$$\textit{where } A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \; b = (1,0,0,1,0), \; c = (1,0,1,0,0) \textit{ and } d = 1$$

Some researchers prefer a simplified version of equivalence where $c = 0$ and $d = 0$. A direct verification of affine equivalence of two Boolean functions requires a search over all invertible matrices over $\mathbb{F}_2$ which has computational complexity of $\mathcal{O}(2^{n^2})$. Clearly this is not feasible for $n \geq 7$. The other approach is to consider properties of Boolean functions which are invariant with respect to affine transformations. Algebraic degree and weight distribution of Walsh transformation spectrum and autocorrelation spectrum are most widely used invariants. If two Boolean functions have different algebraic degree or weight distribution of Walsh transformation spectrum or autocorrelation spectrum then these two functions cannot be affine equivalent. The converse is obviously not true. Essentially, a permutation transformation rearranges the order of input, which preserves the Hamming weight of the truth table. Clearly, if f and g are equivalent under affine transformation, then $wt(f) = wt(g)$ and $nl(f) = nl(g)$. However, the sufficiency only holds for quadratic Boolean functions.

Example 5.2. *$f_1(x) = x_1x_4$ and $f_2(x) = x_1x_2x_3 \oplus x_1x_4$. These two functions both have weight and nonlinearity equal to 4, but they are not affine equivalent since they have different degrees.*

5.2 Affine Equivalence of Quadratic MRS Boolean Functions

The basic theorem on affine equivalence of general quadratic Boolean functions was proved by Dickson [70].

Theorem 5.2. *Suppose f in $\mathscr{B}_n$ has degree 2. If f is balanced, then f is affine equivalent to $x_1x_2 \oplus x_3x_4 \oplus ... \oplus x_{2k-1}x_{2k} \oplus x_{2k+1}$ for some $k \leq \frac{n-1}{2}$. If f is not balanced, it is equivalent to $x_1x_2 \oplus x_3x_4 \oplus ... \oplus x_{2k-1}x_{2k} \oplus b$ for some $k \leq \frac{n}{2}$ and $b \in \mathbb{F}_2$. If $wt(f) < 2^{n-1}$ then $b = 0$. If $wt(f) > 2^{n-1}$ then $b = 1$.*

Given a function f of degree 2, after we find the quadratic form in Theorem 5.2 which is equivalent to f (unfortunately to do this is not trivial), it is easy to compute $wt(f)$ and $nl(f)$. The result is

Lemma 5.3. *Suppose g in $\mathscr{B}_n$ has the form $\sum_{i=1}^{k} x_{2i-1}x_{2i} \oplus \sum_{i=2k+1}^{n} a_i x_i$ be an $n-$variable function for some $k \leq \frac{n}{2}$. Then the nonlinearity is given by $nl(g) = 2^{n-1} - 2^{n-k-1}$. If all the linear term vanish then its weight is same as its nonlinearity , otherwise it is balanced.*

Little is known about the affine equivalence of homogeneous rotation symmetric Boolean functions. The simplest case of quadratic MRS functions which are generated by cyclic permutations of the variables in a single monomial was only settled in 2009 by H. Kim et.al.[61]. Let $f_{n,s} = x_1x_s \oplus x_2x_{s+1} \oplus ... \oplus x_nx_{s-1}$ be the quadratic MRS Boolean function on n variables. Kim noted that these Boolean functions can be uniquely represented using the permutations $\rho_s = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ s & s+1 & \cdots & s-1 \end{smallmatrix}\right)$ where each column $\left(\begin{smallmatrix} i \\ \rho_s(i) \end{smallmatrix}\right)$ of the matrix representation of the permutation ρ_s determines a term $x_ix_{\rho_s(i)}$ of $f_{n,s}$. Since each permutation can be expressed as a product of disjoint cycles. He noted that a characterization of the exact weight and nonlinearity of $f_{n,s}$ using the structe of the cycle decomposition of the associated permutation ρ_s is possible as follows

Theorem 5.4. *Let the permutation ρ_s associated with the $n-$variable Boolean function $f_{n,s}$ has the cycle decomposition as $\rho_s = \tau_1\tau_2...\tau_k$. Then, the number of cycles is $k = gcd(n, s-1)$ and all the cycles ave the same length of $\frac{n}{k}$. More over the weight and nonlinearity of $f_{n,s}$ are characterized as*

$$wt(f_{n,s}) = nl(f_{n,s}) = 2^{n-1} - 2^{\frac{n}{2}+k-1}, \quad if \ \frac{n}{k} \ is \ even,$$

$$wt(f_{n,s}) = 2^{n-1}, \quad nl(f_{n,s}) = 2^{n-1} - 2^{\frac{n+k}{2}-1}, \quad if \ \frac{n}{k} \ is \ odd.$$

Theorem 5.5. *The quadratic MRS functions $f_{n,r}$ and $f_{n,s}$ are affine equivalent if and only if $gcd(n, r-1) = gcd(n, s-1)$.*

5.3 Affine Equivalence of Cubic MRS Boolean Functions

In 2011, Cusick [6] considered the much more complicated cubic MRS Boolean functions and introduced a new concept of patterns to study the affine equivalence of such functions. By means of which the structure of the smallest group G_n whose action on the set of all such cubic MRS functions in n variables gives the affine equivalence classes for these functions under permutation of the variables can be determined. Cusick conjectured that the equivalence classes are the same if all nonsingular affine transformations, not just permutations, are allowed. Later in 2014 he conformed this [71].

For some j and k, $1 < j < k$, let

$$f(x) = x_1x_jx_k \oplus x_2x_{j+1}x_{k+1} \oplus ... \oplus x_nx_{j-1}x_{k-1} \tag{5.1}$$

be an MRS Boolean function of degree 3. We shall use the notation $(1, j, k)$ for the function $f(x)$ in 5.1, no matter how the terms on the right-hand side are written. If $(1, j, k)$ is written as in 5.1 (so the first subscripts in the n terms are $1, 2, ..., n$ in order, and the other two subscripts in order each give cyclic permutations of $1, 2, ..., n$, as shown), we say f is written in standard form. Note we do not require $j < k$, so there are two ways to write $f(x)$ in standard form. If we specify the representation of $f(x)$ ($(1, j, k)$ *or* $(1, k, j)$) , then the standard form is unique. We shall use the notation

$$[i, j, k] = x_ix_jx_k \tag{5.2}$$

as shorthand for the monomial on the right-hand side; note that the order of the variables matters, so, for example, the six permutations of i, j, k give 6 different (but equal) representations of form 5.2 for the same monomial $x_ix_jx_k$. In order to study the affine equivalence classes for the functions $(1, j, k)$, we need to be able to identify all of the distinct functions$(1, j, k)$. We define

$D_n = \{(1, j, k) : j < k \leq n$, and every function $(1, j, k)$ is represented by the triple $1, j, k$ with least j, and given that, with least $k\}$

Lemma 5.6. *If* $n \equiv 0(mod\ 3)$, *then* $|D_n| = \frac{(n^2-3n+6)}{6}$ *otherwise,* $|D_n| = \frac{(n^2-3n+2)}{6}$

Cusick defined the notion of pattern for any term $[i, j, k]$. The pattern of $[i, j, k]$ is the integer vector $\big(j - i\ (Mod\ n); k - i\ (Mod\ n); k - j\ (Mod\ n)\big)$. The semicolons distinguish a pattern from a function (i, j, k). Where the "capital mod" notation $a\ (Mod\ n)$ means the unique integer b in $\{1, 2, ..., n\}$ such that $b \equiv a\ (mod\ n)$. Every term $[i, j, k]$ has six patterns$(a; b; c)$, one for each of the orderings of the triple i, j, k.

Lemma 5.7. *Each function* $(1, j, k)$ *in standard form has a unique pattern* $\big(j - 1\ (Mod\ n); k - 1\ (Mod\ n);\ k - j\ (Mod\ n)\big)$, *which is the same for all of the* n *terms* $[u, v, w]$ *in the standard form of the function.*

Lemma 5.8. *A permutation* μ *preserves rotation symmetry for cubic MRS functions in* $n > 4$ *variables if and only if* $\mu(i) = (i - 1)(\mu(2) - 1) + 1\ (Mod\ n),\ 1 \leq i \leq n$.

Let $\sigma_{\tau,n} = \sigma_\tau$ denote the permutation defined by $\sigma_\tau(i) = (i - 1)\tau + 1\ (Mod\ n)$ for $i = 1, 2, ..., n$, where we assume $gcd(\tau, n) = gcd(\sigma_\tau(2) - 1, n) = 1$. Then we have $gcd(\sigma_\tau(j) - 1, n) = gcd((j - 1)\tau, n) = 1$ if and only if $gcd(j - 1, n) = 1$. Since $\sigma_\tau\sigma_\delta = \sigma_\delta\sigma_\tau$ for any δ with $gcd(\delta, n) = 1$, we see that G_n defined by $G_n = \{\sigma_{\tau,n} : gcd(\tau, n) = 1\}$ is a group with the group operation of permutation composition.

Theorem 5.9. *The group* G_n *acts on the set* $C_n = \{$*cubic MRS functions* $f(x)$ *in* n *variables*$\}$ *as* $\sigma_{\tau,n}(f(x)) = \sigma_{\tau,n}((1, j, k))$ *where* $f(x)$ *has the unique standard form* $(1, j, k)$ *in* D_n. *The orbits for this group action are exactly the affine equivalence classes for* C_n *under permutations which preserve rotation symmetry.*

Let E_n be the number of equivalence classes of cubic MRS functions in n variables. When n is a prime Cusick calculated the value of E_n as $E_n = \frac{\lfloor p \rfloor}{6} + 1$. If $n = 3^k$ for $k \geq 1$ then $E_{3^k} = 3^{k-1}$

5.4 Affine Equivalence of Quartic MRS Boolean Functions

In 2014 Cusick and Younhwan Cheon [20] extended the notioin of patterns to the quartic case and enumerated the number of affine equivalence classes for quartic MRS Boolean functions as

$$E_p = \begin{cases} \frac{p^2-2p+25}{24} & \text{if } p \equiv 1(mod\ 12) \\ \frac{p^2-2p+9}{24} & \text{if } p \equiv 5(mod\ 12) \\ \frac{p^2-2p+13}{24} & \text{if } p \equiv 7(mod\ 12) \\ \frac{p^2-2p-3}{24} & \text{if } p \equiv 11(mod\ 12) \end{cases}$$

Stănică [21] used the theory of circulant matrices to study the affine equivalence of MRS Boolean functions. An $n \times n$ matrix C, denoted by $C(c_1, c_2, ..., c_n)$, is circulant if all its rows are successive circular rotations of the first row, that is,

$$C = \begin{bmatrix} c_1 & c_2 & ... & c_n \\ c_n & c_1 & ... & c_{n-1} \\ ... & ... & ... & ... \\ c_2 & c_3 & ... & c_1 \end{bmatrix}$$

Let C_n be the set of circulant matrices and let $A_1 = C(a_1, a_2, ..., a_n)$, $A_2 = C(b_1, b_2, ..., b_n) \in C_n$. Define the relation '$\approx$' on C_n as follows $A_1 \approx A_2$ if and only if $(a_1, a_2, ..., a_n) = \rho_n^k(b_1, b_2, ..., b_n)$ for some $0 \leq k \leq n-1$. We can easily see that '$\approx$' defines an equivalence relation on the set of circulant matrices C_n. Let $A = \langle C(a_1, a_2, ..., a_n) \rangle$ denote the equivalence class of the circulant matrix A.

Let $x_1 x_{j_2} ... x_{j_d}$ be the SANF of the MRS Boolean function f on n variables then we can associate f with a unique circulant matrix equivalence class A_f as

$$A_f =< C(1, 0, ...1, 0, ..1, .) >$$

where the bit '1' appear in positions given by the indices in the SANF of f. Then Stănică has noted that two MRS Boolean functions f, g in n variables is affine equivalent if and only if their corresponding circulant matrices A_f and A_g are $P-Q$ equivalent. In 2007 Wiedemann et al.[72] proved that

Theorem 5.10. *Let A, B be two $n \times n$ 0/1 circulants of weight at most 5 with first rows support indices $\Delta(A)$ and $\Delta(B)$ respectively , where n is odd. Then the following are equivalent:*

1. *There exits $u, v \in \mathbb{Z}_n$ such that $gcd(u, v) = 1$ and $\Delta(A) = u\Delta(B) + v$*
2. *A, B are $P-Q$ equivalent*
3. *There is an $n \times n$ permutation matrix P such that $AA^T = PBB^TP^{-1}$*
4. *The matrices AA^T, BB^T are similar.*

Stănică used this result and the idea of patterns to find the equivalence class of MRS Boolean functions of degree 4 when n is a prime power (p^l, $l \geq 2$) and calculated the value of E_{p^l} as

$$E_{p^l} = \begin{cases} \frac{p^{2l+2}+p^{2l+1}+p^{2l}-3p^{l+2}-6p^{l+1}-3p^l+p^2(27l+2)+5p-27l+2}{24(p^2-1)} & \text{if } p \equiv 1 (mod\ 12) \\ \frac{p^{2l+2}+p^{2l+1}+p^{2l}-3p^{l+2}-6p^{l+1}-3p^l+p^2(11l+2)+5p-11l+2}{24(p^2-1)} & \text{if } p \equiv 5 (mod\ 12) \\ \frac{p^{2l+2}+p^{2l+1}+p^{2l}-3p^{l+2}-6p^{l+1}-3p^l+p^2(15l+2)+5p-15l+2}{24(p^2-1)} & \text{if } p \equiv 7 (mod\ 12) \\ \frac{p^{2l+2}+p^{2l+1}+p^{2l}-3p^{l+2}-6p^{l+1}-3p^l-p^2(l-2)+5p+l+2}{24(p^2-1)} & \text{if } p \equiv 11 (mod\ 12) \end{cases}$$

5.5 Affine Equivalence of MRS Functions of Degree d

Recently Cusick and Stănică [22] derived an asymptotic formula for the number of affine equivalence classes for degree d-MRS Boolean functions where the number of variables p is prime as

$$E_{p,d} = \frac{1}{d!}p^{d-2} + \frac{1}{d!}\frac{d^2-d-2}{2}p^{d-3} + \mathcal{O}(p^{d-4}) \quad \text{if } d \geq 5$$

Still the enumeration of affine equivalence of MRS Boolean functions of degree d for arbitrary number of variables is unanswered. We solve this problem of enumeration of affine equivalence of MRS Boolean functions using Pólya's theory. We define a permutation group, the action of which on the set of monomials of n-variables gives the affine equivalence of MRS Boolean functions.

Definition 5.11. (Permutation preserving rotation symmetry) A permutation σ on n variables is said to preserves rotation symmetry if for any given rotation symmetric Boolean function f of n- variables the function $\sigma(f)$ is also rotation symmetric.

Lemma 5.12. *Let μ be a permutation on n letters. Then μ preserves rotation symmetry if and only if for any $a, b \in \{1, 2, ..., n\}$ the circular distance between a and b is same as $\mu(a)$ and $\mu(b)$ that is $(a - b)\ (mod\ n) = (\mu(a) - \mu(b))\ (mod\ n)$.*

Let $g_{\tau j}$ be a permutation on n letters defined by

$$g_{\tau j}(i) = (i + j - 1)\tau + 1(Mod\ n)$$

Note that $g_{\tau j}$ preserves rotation symmetry by Lemma 5.12 because

$$\begin{aligned}(g_{\tau j}(a) - g_{\tau j}(b))(Mod\ n) &= ((a + j - 1)\tau + 1) - ((b + j - 1)\tau + 1)(Mod\ n) \\ &= (a - b)\tau(Mod\ n) \\ &= (a - b)(Mod\ n) \quad since\ gcd(\tau, n) = 1.\end{aligned}$$

Let $G = \{g_{\tau j} : gcd(\tau, n) = 1 \ \ \& \ \ 1 \leq j \leq n\}$. Then G forms a group under the operation of permutation composition. Let X be the set of all monomials in n variables.

Define the action of G on X as follows:

$$g_{\tau j}(x_{i_1}x_{i_2}....x_{i_k}) = x_{g_{\tau j}(i_1)}x_{g_{\tau j}(i_2)}....x_{g_{\tau j}(i_k)}$$

The orbits for this group action are the affine equivalence classes for set of MRS Boolean functions under permutations which preserve rotation symmetry.

Let E_n be the total number of orbits generated and $E_{n,w}$ be the number of orbits of weight w. Then E_n will give the number of affine equivalent MRS Boolean functions and $E_{n,w}$ will give the number of affine equivalent MRS Boolean functions of degree w. The value of E_n and $E_{n,w}$ can be calculated using the Pólya's enumeration theorem as

$$E_n = Z_G(2, 2, ..., 2) \quad \text{and}$$

$$E_{n,w} = \frac{1}{w!}\Big[D^w(Z_G(1+x, 1+x^2, ..., 1+x^n))\Big]_{x=0}$$

where $Z_G(y_1, y_2, ..., y_n)$ is the cycle index polynomial of the group G and D denotes the formal derivative.

Hence it is the knowledge of cycle index polynomial of the group G is enough to derive the number of affine equivalent MRS Boolean functions of degree w.

5.6 Cycle Index Polynomial of the Group G

Now we prove that the cycle index polynomial Z_G of the group $G = \{g_{\tau j} : gcd(\tau, n) = 1 \ \ \& \ \ 1 \leq j \leq n\}$ is same as the cycle index polynomial Z_H of the group H of Wan-Di-wei and Ju-Yong Xu [73]. Wan-Di-wei and Ju-Yong Xu defined the following permutation group to find the number of equivalence classes of subsets of $\mathbb{Z}_n$.

Let n be a positive integer and let $\sigma_{t,s}$ be a permutation on n letters defined by

$$\sigma_{t,s}(i) = it + s(mod\ n).$$

Let H_n=$\{\sigma_{t,s} : gcd(t, n) = 1 \ \ \& \ \ 0 \leq t, s \leq n-1\}$ then H_n forms a group of order $n\phi(n)$ under the operation of permutation composition. Let X be the set of all monomials in n variables. Define the action of H_n on X as as follows:

$$\sigma_{t,s}(x_{i_1}x_{i_2}....x_{i_k}) = x_{\sigma_{t,s}(i_1)}x_{\sigma_{t,s}(i_2)}....x_{\sigma_{t,s}(i_k)}$$

Wan-Di-wei and Ju-Yong Xu have found the cycle index polynomial for this group H_n as follows.

Theorem 5.13. *Let p be an odd prime and $\alpha \geq 1$ then the cycle index of $Z_{H_{p^\alpha}}$ is*

$$Z_{H_{p^\alpha}}(x_1, x_2, ..., x_{p^\alpha}) = \frac{1}{p^{2\alpha-1}(p-1)} \Bigg\{ \sum_{w=1}^{\alpha} p^{2(w-1)}(p-1) x_{p^w}^{p^{\alpha-w}} + \sum_{w=0}^{\alpha-1} \sum_{l|p-1} p^{w+\delta(l)(\alpha-w)} \phi(lp^w) x_1 x_l^{\frac{p^{\alpha-w-1}-1}{l}} \times \Big(\prod_{u=0}^{w} x_{lp^u}\Big)^{\frac{p^{\alpha-w-1}(p-1)}{l}} \Bigg\}$$

where

$$\delta(l) = \begin{cases} 1 & \text{if } l > 1 \\ 0 & \text{if } l = 1 \end{cases}$$

The cycle index of H_{2^α} is

$$Z_{H_{2^\alpha}}(x_1, x_2, ..., x_{2^\alpha}) = \begin{cases} \frac{1}{2}(x_1^2 + x_2) & \text{if } \alpha = 1 \\ \frac{1}{8}(x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4) & \text{if } \alpha = 2 \\ \frac{1}{2^{2\alpha-1}} \Bigg\{ 2^{2\alpha-3} x_{2^\alpha} + \sum_{w=1}^{\alpha-1} (2^{2(w-1)} + \phi(2^{w-1}) 2^{\alpha-1}) x_{2^w}^{2^{\alpha-w}} \\ \quad + \sum_{w=0}^{\alpha-2} \phi(2^w)(2^w x_1^{2^{\alpha-w}} + 2^{\alpha-1} x_1^2 x_2^{2^{\alpha-w-1}-1}) \\ \quad \times \Big(\prod_{u=1}^{w} x_{2^u}\Big)^{2^{\alpha-w-1}} \Bigg\} & \text{if } \alpha \geq 3 \end{cases}$$

It is easy to see that the groups G_n and H_n are isomorphic, but this does not suffice to show that they have the same cycle index polynomials. We prove this in our next theorem.

Theorem 5.14. *For all integers $n > 1$, the groups G_n and H_n have the same cycle index polynomial.*

Proof. From the definition of the permutations $g_{\tau,j}$ *and* $\sigma_{t,s}$, for any τ with $gcd(\tau, n) = 1$ we have the equality of functions

$$g_{\tau,j} = \sigma_{\tau,\tau(j-1)+1}.$$

For any i, $1 \leq i \leq n$ we have

$$\sigma_{t,s}(i) = (i + st^{-1} + 1 - t^{-1} - 1)t + 1 = g_{t,st^{-1}+1-t^{-1}}(i),$$

hence this isomorphism preserves the cycle structure also. Therefore cycle index polynomial of G is same as cycle index polynomial of H. □

Cycle index polynomial of the direct product of groups

Let G_1, G_2 be permutation groups acting on sets X_1, X_2 respectively. Let $G = G_1 \times G_2$ be the direct product of groups and $X = X_1 \times X_2$ the cartesian product of corresponding sets. For an element $x = (x_1, x_2)$ of X and an element $g = (g_1, g_2)$ of G, we define the action of g on x by

$$\phi(g, x) = (\phi_1(x_1, g_1), \phi_2(x_2, g_2))$$

Let

$$P(f_1, f_2 ... f_l) = \sum_{(j)} c_{(j)} \prod_{p=1}^{l} f_p^{j_p}$$
$$Q(f_1, f_2 ... f_m) = \sum_{(k)} d_{(k)} \prod_{q=1}^{m} f_q^{k_q}$$

Define the combinatorial multiplication of the polynomial defined as

$$P \circledast Q = \sum_{(j)} c_{(j)} \sum_{(k)} d_{(k)} \prod_{p=1}^{l} f_p^{j_p} \circledast \prod_{q=1}^{m} f_q^{k_q}$$

where the $\circledast$ operation on the indeterminates is defined as

$$\prod_{p=1}^{l} f_p^{j_p} \circledast \prod_{q=1}^{m} f_q^{k_q} = \prod_{p=1}^{l} \prod_{q=1}^{m} f_p^{j_p} \circledast f_q^{k_q}$$

and

$$f_p^{j_p} \circledast f_q^{k_q} = f_{lcm(p,q)}^{j_p k_q gcd(p,q)}$$

Lemma 5.15. *Let the cycle index polynomial of the action of the group G_1 on the set X_1 be $Z_{(G_1,X_1)}$ and G_2 on X_2 be $Z_{(G_2,X_2)}$. Then the cycle index of the natural action of permutation group $G_1 \times G_2$ on $X_1 \times X_2$ induced by actions G_1 on X_1 and G_2 on X_2 can be expressed as:*

$$Z_{(G_1 \times G_2, X_1 \times X_2)} = Z_{(G_1,X_1)} \circledast Z_{(G_2,X_2)}$$

Let $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ then there exists integers $a_1, a_2, ...a_r$ such that

$$\sum_{i=1}^{r} a_i \prod_{\substack{j \neq i \\ 1 \leq j \leq r}} p_j^{\alpha_j} = 1$$

for any $t \in \mathbb{Z}_n$ let

$$t_i \equiv t\ a_i \prod_{\substack{j \neq i \\ 1 \leq j \leq r}} p_j^{\alpha_j} (Mod\ p_i^{\alpha_i}) \quad (1 \leq i \leq r)$$

Then the map $\beta(t) = (t_1, t_2, ..., t_r)$ is an isomorphism from

$$\mathbb{Z}_n \quad to \quad \oplus_{i=1}^{s} \mathbb{Z}_{p_i^{\alpha_i}}.$$

It is easy to see that $gcd(t, n) = 1$ if and only if $gcd(t_i, p_i) = 1 \quad (1 \leq i \leq r)$. Then

$$G_n = \oplus_{i=1}^{s} G_{p_i^{\alpha_i}}.$$

Hence, according to Lemma 5.15 we have the cycle index of G_n as

$$Z_{G_n}(x_1, x_2, ..., x_n) = \circledast_{i=1}^{s} Z_{G_{p_i^{\alpha_i}}}.$$

Since Theorem 5.14 shows that the groups G_{p^α} and H_{p^α} for all primes p have the same cycle index polynomial then we can combine the cycle index polynomials of these groups G for all prime powers p^α together in order to obtain the cycle index polynomial of G_n where n is the product of those prime power components.

Then by Pólya's theorem we can calculate the number of affine equivalent n-variable MRS Boolean functions of degree w as

$$E_{n,w} = \frac{1}{w!}\left[D^w(Z_{G_n}(1+x, 1+x^2, ..., 1+x^n))\right]_{x=0}$$

The special groups where n is a prime p have been studied for a long time (see [74] for example). We can give very explicit descriptions of the structure of the groups in this case. Let $GA(p)$ denote the well known *general affine group* $Z_p \rtimes Z_p^*$ for odd primes p. It is clear from their definitions that both G_p and H_p are isomorphic to $GA(p)$. Since

$$\sigma_{1,1}(i) = i + 1 \ (Mod\ p) \tag{5.3}$$

gives a p-cycle and $\sigma_{k,p-1}(i)$ gives a $(p-1)$-cycle for suitably chosen k, we can prove the following lemmas about the group H_p.

Lemma 5.16. *We can represent H_p as the normalizer of the subgroup K of the symmetric group S_p generated by the p-cycle $(12\ldots p)$.*

Proof. Since $|H_p| = p(p-1)$ and H_p contains a subgroup K of order p generated by the p-cycle

$$\mu = (1, 2 \ldots p),$$

the other generator of H_p must be a $(p-1)$-cycle ν which normalizes K. This means

$$\nu K \nu^{-1} = K,$$

which is equivalent to

$$\nu\mu\ \nu^{-1} = \mu^{(p-1)/2}, \tag{5.4}$$

since then

$$\{\nu\mu^k\ \nu^{-1} = (\nu\mu\nu^{-1})^k : 1 \leq k \leq p\} = \{\mu^{k(p-1)/2} : 1 \leq k \leq p\} = K.$$

□

Lemma 5.17. *In the representation* $H_p =< \mu, \nu >$ *in terms of the generators* μ, ν *we can choose*

$$\nu = \sigma_{(p-1)/2,(p+3)/2}. \tag{5.5}$$

Thus ν *is a* $(p-1)$*-cycle with* $\nu(1) = 1$ *and* $\nu(p-1) = 2$.

Proof. From (5.3) and (5.5) we have

$$\nu(\mu^2(i)) = \nu(i+2) = ((p-1)/2)i + ((p+1)/2) \tag{5.6}$$

and (since $\mu^{-1}(i) = i - 1\ (Mod\ p)$)

$$\mu^{-1}(\nu(i)) = \mu^{-1}((p-1)/2)i + ((p+3)/2) = ((p-1)/2)i + ((p+1)/2). \tag{5.7}$$

From (5.6) and (5.7) we obtain $\nu\mu^2 = \mu^{-1}\nu$ which is equivalent to

$$(\nu\mu\nu^{-1})^2 = \nu\mu^2\nu^{-1} = \mu^{-1} = \mu^{p-1} \tag{5.8}$$

and this implies (5.4). □

When $n\ (= p)$ is a prime we have the cycle index polynomial of the group G as

$$Z_G = \frac{1}{p(p-1)}\left[x_1^p + (p-1)x_p + p\sum_{\substack{d|(p-1)\\ d>1}} \phi(d)x_1 x_d^{\frac{(p-1)}{d}}\right] for \quad 1 \le w < p$$

Hence by Pólya's theorem we have the number of equivalence classes of n variables MRS Boolean functions of degree w as

$$E_{p,w} = \frac{1}{p(p-1)}\left[\binom{p}{w} + \sum_{\substack{d|gcd(p-1,w)\\ d>1}} \phi(d)\binom{\frac{p-1}{d}}{\frac{w}{d}} + \sum_{\substack{d|gcd(p-1,w-1)\\ d>1}} \phi(d)\binom{\frac{p-1}{d}}{\frac{w-1}{d}}\right]$$

Let $g_{n,w}$ denote the number of MRS Boolean functions of degree w then we have

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

Substituting this in the above relation we get the recurrence relation on the number of affine equivalent MRS Boolean functions in terms of number of MRS Boolean functions as

$$E_{p,w} = g_{p-1,w} + g_{p-1,w-1} - g_{p,w}.$$