International Journal of Pure and Applied Mathematics
Volume 119 No. 15 2018, 3233-3238
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Results on Dihedral Symmetric Boolean Functions

K.Rajeev, M.Sethumadhavan, K.V.Lakshmy,
Amrita School of Engineering, Amrita Vishwa
Vidyapeetham, Coimbatore, India
k rajeev@cb.amrita.edu, m sethu@cb.amrita.edu, kv
lakshmy@cb.amrita.edu

***Abstract*—Cryptographic applications require Boolean functions for introducing nonlinearity in the cryptosystem. A Boolean function is said to be dihedral symmetric Boolean function if it is invariant under the action of permutations of dihedral group of members to its input variables. In this paper we enumerate the homogeneous dihedral symmetric Boolean functions. The minimal and maximal distances from a given Boolean function to the set of all dihedral symmetric Boolean functions are found. We prove that the set of all dihedral symmetric Boolean functions are metrically regular.**

***Index Terms*—Boolean Functions, Dihedral Symmetric Boolean Functions, Metrically regular sets, Burnside's lemma, Group action**

I. Introduction

Boolean functions plays a major role in the area of symmetric key cryptography and coding theory, a thorough overview of which can be found in [1, 3]. Let $GF(2)$ be the finite field of two element and $GF(2)^n$ be the n-dimensional vector space over $GF(2)$. Let B_n denote the set of all n-variable Boolean functions. Functions which are invariant under the action of dihedral group are dihedral symmetric Boolean functions [7].

Constructing Boolean functions with odd number of variables having maximum possible nonlinearity is an open problem in Cryptology, coding theory and combinatorics. Boolean functions on even number of input variables n, attaining the maximum nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$ are called the bent functions. Kavut et al. and Sumanta Sarkar et al. found 9-variable Boolean functions of nonlinearity greater than the bent concatenation bound in the class of dihedral symmetric Boolean functions [5, 7, 9] These classes of functions are abundant with cryptographically significant functions. In 2007 Sumanta Sarkar et al.[9] computed the size of a few classes of dihedral symmetric functions and made a detailed analysis of the properties of the Walsh transform of these functions. Detailed analysis of the rotation symmetric function is available in literature, but very little study has been done in the area of our consideration. This paper analyse some properties of dihedral symmetric Boolean functions.

II. Preliminaries

Definition 1. (Dihedral Groups)
A group G generated by two elements g and h which satisfies the following two conditions

1) $g^n = h^2 = e$, *where e is the identity element and* $n \geq 3$
2) $hg = g^{-1}h$

is said to be the dihedral group of degree n.

The $2n$ permutations of D_n are

$$\{e, g, g^2, ..., g^{n-1}, h, gh, g^2h, ..., g^{n-1}h\}.$$

which can be generated by

1) rotating the n-gon with respect to the line passing vertically through the centre of n-gon at an angle of $\frac{2\pi}{n}$.
2) reflection of n-gon about a line passing through a vertex and the centre.

D_n is a subgroup of symmetric group S_n and it contains the cyclic group C_n as a subgroup[4] .

Example: Dihedral group of order 3.

$D_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

and is generated by two elements $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Definition 2. (Action of D_n on $GF(2)^n$)
From the definition of dihedral groups the elements of D_n are

$$\{g_n^1, g_2^2, ..., g_n^n, h_n g_n^1, h_n g_n^2, ..., h_n g_n^n\}$$

where g_n and h_n are permutations obtained by rotating the n-gon by an angle of $\frac{2\pi}{n}$ and by taking reflection of n-gon with element "1" fixed. Let $x = (x_0, x_1, ..., x_{n-1}) \in GF(2)^n$, then the action of D_n on $GF(2)^n$ is defined as $\rho.x = (x_{\rho(0)}, x_{\rho(2)}, ..., x_{\rho(n-1)})$ where $\rho \in D_n$.

A Boolean function f is invariant under the action of a group G if $f(\rho.x) = f(x)$, for all $\rho \in G$. Then f assumes the same value in each equivalence classes of $GF(2)^n$ generated by the action of D_n. A subclass of B_n can be found due to this invariance property. Obviously this subclass is smaller than 2^{2^n}, the cardinality of all n-variable Boolean functions. For example rotation-symmetric and symmetric Boolean functions are invariant under the action of cyclic and symmetric group respectively on $GF(2)^n$.

Definition 3. (Dihedral symmetric Boolean function)
Dihedral Symmetric Boolean Function (DSBF) is a function f in n-variables if for every input $(x_0, x_1, ..., x_{n-1}) \in GF(2)^n$ $f(\sigma x) = f(x)$ for any permutation $\sigma \in D_n$.

Dihedral group is a subgroup of the symmetric group and it contains the cyclic group. So the set of DSBFs is a subclass of the set of Rotation Symmetric Boolean functions ($RSBFs$). Hence an exhaustive search in the class of DSBFs is lesser time consuming than in the class of RSBFs. In [9] Sumanta Sarkar et al. reported that Boolean functions in 9-variable having nonlinearity 241 belong to DSBFs.

A. *Polya's Counting Theorem*

Polya's counting theorem and Burnside's lemma are the interesting results in combinatorics related to counting mathematical objects with regard to symmetry [2]. The former theorem uses cycle index of a group for reducing the computational burden whereas the concept of orbits to count mathematical objects is utilized in Burnside's lemma.

The cycle index polynomial (def. see [2] of D_n is given by

$$Z_{D_n}(x_1, x_2, ..., x_n) = \frac{1}{2} Z_{C_n}(x_1, x_2, ..., x_n) + \begin{cases} \frac{1}{2} x_1 x_2^{(n-1)/2}, & \text{if } n \text{ is odd} \\ \frac{1}{4}(x_2^{n/2} + x_1^2 x_2^{(n-2)/2}), & \text{if } n \text{ is even} \end{cases}$$

where $Z_{C_n}(x_1, x_2, ..., x_n) = \frac{1}{n} \sum_{d/n} \phi(d) x_d^{n/d}$ where ϕ is the Euler's Totient function.

Theorem 1. Polya's counting theorem: *For a given set S of weighted elements and G be its permutation group that acts to induce an equivalence relation on the colorings of S using colors c_1,...,c_m then $Z_G\left(\sum_{i=1}^{m} w_{c_i}, \sum_{i=1}^{m} w_{c_i}^2, ..., \sum_{i=1}^{m} w_{c_i}^n\right)$, generates the pattern inventory of distinct colorings by weight w, where n stands for largest cycle length and $Z_G(x_1, x_2, ..., x_n)$, the cycle index polynomial of G.*

III. Enumeration of Dihedral symmetric Boolean functions

A Boolean function f is said to be dihedral symmetric if it is invariant under the action of any of the permutations of the dihedral group. Such function holds the similar value corresponding to all orbits generated from the dihedral symmetry. Let $G_n(x_1, x_2, ..., x_n)$ denote the orbit of $(x_1, x_2, ..., x_n)$ under the action of dihedral symmetric group, then

$$G_n(x_1, x_2, ..., x_n) = \{\sigma(x_1, x_2, ..., x_n) / \ \forall \sigma \in D_n\}.$$

The number of DSBFs is 2^{d_n}, where d_n is number of orbits. Kavut [6] has evaluated the value of d_n as $d_n = \frac{g_n}{2} + l$, where $g_n = \frac{1}{n} \sum_{d/n} \phi(d) 2^{\frac{n}{d}}$ is the number of orbits generated by $(x_1, x_2, ..., x_n)$ under the cyclic group action and $l = \begin{cases} 2^{n-1/2}; & n \text{ odd} \\ \frac{3}{4} 2^{n/2}; & n \text{ even} \end{cases}$.

The value of d_n can also be derived using Polya's counting theorem by assigning weight =1 to the elements in $GF(2)$. Table 1 shows the values of d_n up to $n = 10$. The following theorem provides a general formula for number of orbits with weight w under the action of dihedral groups and thereby we

TABLE I
COUNT OF DIHEDRAL SYMMETRIC BOOLEAN FUNCTION OF n VARIABLES

n	1	2	3	4	5	6	7	8	9	10
d_n	2^2	2^3	2^4	2^6	2^8	2^{13}	2^{18}	2^{30}	2^{46}	2^{78}

get a partition of the n-bit binary strings of weight w. Let $d_{n,w}$ means the count of partitions of weight w. The value of $d_{n,w}$ can be efficiently calculated using Polya's enumeration theorem [8].

Theorem 2. *The number of orbits $G_n(x_1, x_2, ..., x_n)$, such that $wt(x_1, x_2, ..., x_n) = w$ under the action of the dihedral group of n members is given by $d_{n,w}$ =*

$$\frac{1}{2n}\sum_{d/r}\phi(d)\binom{\frac{n}{d}}{\frac{w}{d}} + \begin{cases} \frac{1}{2}\binom{\frac{n-1}{2}}{\lfloor\frac{w}{2}\rfloor}; & n \text{ odd} \\ \frac{1}{2}\binom{\frac{n}{2} - w \bmod 2}{\lfloor\frac{w}{2}\rfloor}; & n \text{ even} \end{cases}$$

where $r = gcd(n, w)$

Proof. Let X and D_n be all monomials in n-variables and dihedral group of permutations on n-elements. Then $Z_{D_n}(x_1, x_2, ..., x_n) =$

$$\frac{1}{2n}\sum_{d/n}\phi(d)x_d^{n/d} + \begin{cases} \frac{1}{2}x_1x_2^{n-1/2}; & n \text{ odd} \\ \frac{1}{4}(x_2^{n/2} + x_1^2x_2^{n-2/2}); & n \text{ even} \end{cases}$$

Consider the set of colors as the finite field $GF(2)$. Let us define the weight for each colors as $w(0) = 0$ and $w(1) = y$. Then by Polya's theorem, pattern index of nonequivalent colorings of X under G is given by

$$I = Z_{D_n}(1+y, 1+y^2, ..., 1+y^n) = \frac{1}{2n}\sum_{d/n}\phi(d)(1+y^d)^{n/d} + \begin{cases} \frac{1}{2}(1+y)(1+y^2)^{n-1/2}; & n \text{ odd} \\ \frac{1}{4}((1+y^2)^{n/2} + \\ (1+y)^2(1+y^2)^{n-2/2}); & n \text{ even} \end{cases}.$$

Then count of orbits of weight w is exactly the coefficient of y^w in the expansion of I. Expanding the RHS of above expression by using binomial expansion and collecting the coefficients of y^w will give the required result. Table II shows the values of $d_{n,w}$ for $n = 3, 4, 5$. □

TABLE II
NUMBER OF ORBITS OF WEIGHT w

n \ w	0	1	2	3	4	5
3	1	1	1	1		
4	1	1	2	1	1	
5	1	1	2	2	1	1

Corollary 1. *The count of n-variable homogeneous dihedral symmetric Boolean functions of degree $w \geq 1$ is $2^{d_{n,w}} - 1$.*

IV. METRIC REGULARITY OF DIHEDRAL SYMMETRIC BOOLEAN FUNCTIONS

Definition 4. *Let $X \subseteq GF(2)^n$ be an arbitrary set and let $y \in GF(2)^n$ be an arbitrary vector. The distance from y to X is defined as $dist(y, X) = \min_{x\in X} dist(y, x)$. The maximal distance from the set X is denoted as dist(X) and is given by dist(X)= $\max_{z\in GF(2)^n} dist(z, X)$*

A. Metric Regularity

The notion of metrically regular subsets of $GF(2)^n$ is introduced by N. Tokareva [12] in 2011 and she proved the metrically regularity of all bent functions . The metrically regular characterization of subclasses of functions is posed as an open problem. In 2016 A.K Oblaukhov [10] gave a general form for the metric complement of linear subspaces. In 2017 Stănică et al. [11] showed degenerate functions, symmetric functions, self-anti-dual-functions, rotation symmetric functions and linear structure functions are metrically regular. Let $X \subseteq GF(2)^n$ and Y be all vectors from $GF(2)^n$ which are at maximal distance from X. Let X' be maximal distance from Y. Then X is metrically regular if $X = X'$ [12]. Trivial examples are given below:

1) X=$\{010, 011\}$ is metrically regular Consider
   $GF(2)^3 = \{000, 001, 010, 010, 011, 100, 101, 110, 111\}$
   $dist(000, X) = 1,\ dist(001, X) = 1,$
   $dist(010, X) = 0,\ dist(011, X) = 0,$
   $dist(100, X) = 2, dist(101, X) = 2,$
   $dist(110, X) = 1,\ \ dist(111, X) = 1.$
   Then $dist(X) = 2$ and $Y = \{100, 101\}$.
   Now, $dist(000, Y) = 1,\ dist(001, Y) = 1,$
   $dist(010, Y) = 2,\ dist(011, Y) = 2,$
   $dist(100, Y) = 1,\ dist(101, Y) = 1,$
   $dist(110, Y) = 1,\ \ dist(111,) = 1.$
   Then $dist(Y) = 2$ and $X' = \{010, 011\}$
   Hence X'= X

2) The set $X = \{00...0, 11...1\} \subset GF(2)^n$ is metrically regular. Here $Y = \{x \in GF(2)^n / wt(x) = \begin{cases} \text{n/2} & ; n\, is\, even \\ \frac{n-1}{2}\, or\, \frac{n+1}{2} & ; n\, is\, odd \end{cases}\}$
Let X={000, 111} Then Y={001, 010, 011, 100, 101, 110}
3) X={010, 111}. d(X)=2 and Y={100} but X'={011} so this is not metrically regular

A subclass of Boolean functions is metrically regular if the collection of all corresponding output vectors are metrically regular [12]. Our analysis consider that the classes of all DSBFs forms an equivalence class of its input variables which is invariant under the group action. For example consider the set of all 4-variable DSBFs, the input variables $GF(2)^4$ could be partitioned as

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

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

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

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

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

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

Stănică et al. proved that the class of functions which forms an equivalence class under respective group actions are metrically regular [11]. And he gave general formulas for maximum distance from class of functions which forms equivalence class like above and number of functions attain the maximum distance. So the same is applicable for dihedral functions.

V. Minimal and Maximal distances from DSBFs

Let f_j denotes the weight function for the Boolean function $f(x)$ with level $||x|| = j$ where $||x|| = wt(x)$. Then

$$f_j = \sum_{x \in GF(2)^n} f(x).I(||x|| = j) \tag{1}$$

where I is the index set.
Distance between an arbitrary Boolean function $f \in B_n$ and a Boolean function g which induces an equivalence classes

$$\{U_j\}_{j=1}^{Q}$$

of its inputs.
Let $f \in B_n$ and $g \in$ DSBFs . Assume that $U_1, U_2, ..., U_Q$ be the orbits of length $k_1, ..., k_Q$ corresponding to g

$$dist(f,g) = ||f+g||$$

$$= \sum_{j=1}^{Q} \Big[\sum_{x \in GF(2)^n} f(x) + g(x) - 2f(x)g(x) \Big] I(x \in U_j)$$

by(1)

$$= \sum_{j=1}^{Q} \Big(f_j + g_j k_j - 2 f_j g_j \Big)$$

$$= \sum_{j=1}^{Q} \Big(f_j + g_j (k_j - 2 f_j) \Big) \tag{2}$$

Put $k_j - 2f_j = b_j$ for $j = 1, 2, 3, ..., Q$ Then

$$\begin{aligned} dist(f,g) &= \sum_{j=1}^{Q} \Big(f_j + g_j b_j) \Big) \\ &= \sum_j f_j + \sum_j g_j b_j \\ &= ||f|| + \sum_j g_j b_j \\ &= \sum_j \frac{k_j - b_j}{2} + \sum_j g_j b_j \\ &= \frac{1}{2} \sum_j^{Q} k_j - \frac{1}{2} \sum_j b_j + \sum_j g_j b_j \\ &= \frac{1}{2} 2^n - \frac{1}{2} \sum_j \Big(b_j - 2 g_j b_j) \Big) \\ &= 2^{n-1} - \frac{1}{2} \sum_{j=1}^{Q} \Big(1 - 2 g_j \Big) b_j \\ &= 2^{n-1} - \frac{1}{2} \sum_{j=1}^{Q} (-1)^{g_j} b_j \end{aligned} \tag{3}$$

Then minimal and maximal distances from a an arbitrary Boolean function to the collection of all dihedral symmetric Boolean functions are given by $dist_{min} = 2^{n-1} - \frac{1}{2} \sum_{j=0}^{Q} |b_j|$ and $dist_{max} = 2^{n-1} + \frac{1}{2} \sum_{j=0}^{Q} |b_j|$

VI. Conclusion

We analysed dihedral symmetric Boolean functions and derived a formula which allows the direct computation for the number of homogeneous DSBFs of degree w using Polya's enumeration theorem. We also analysed some metric properties of DSBFs and proved that this class of functions are metrically regular.

REFERENCES

[1] Claude Carlet. Boolean functions for cryptography and error correcting codes. Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 2, 2010.

[2] Thomas W Cusick, KV Lakshmy, and Madathil Sethumadhavan. Affine equivalence of monomial rotation symmetric boolean functions: A polyas theorem approach. Journal of Mathematical Cryptology, 10(3-4):145156, 2016.

[3] Thomas W. Cusick and Pantelimon Stanica. Cryptographic Boolean functions and applications. Academic Press, 2009.

[4] David Steven Dummit and Richard M Foote. Abstract algebra, volume 3. Wiley Hoboken, 2004.

[5] Selcuk Kavut, Subhamoy Maitra, and MD Yucel. Search for Boolean functions with excellent profiles in the rotation symmetric class. Information Theory, IEEE, 53(5):17431751, 2007.

[6] Selcuk Kavut and M Yucel. Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functionsa 9 Variable Boolean Functions with Nonlinearity 242. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 2:18, 2007.

[7] Selcuk Kavut and Melek Diker Yucel. 9-variable boolean functions with nonlinearity 242 in the generalized rotation symmetric class. Information and Computation, 208(4):341350, 2010.

[8] KV Lakshmy, Madathil Sethumadhavan, and ThomasWCusick. Counting rotation symmetric functions using polyas theorem. Discrete Applied Mathematics, 169:162167,2014.

[9] Subhamoy Maitra, Sumanta Sarkar, and Deepak Kumar Dalai. On dihedral group invariant boolean functions. In Proc. of Third International Workshop on Boolean Functions: Cryptography and Applications (BFCA07), May 23, 2007, Paris, France, 2007.

[10] Aleksei Konstantinovich Oblaukhov. Metric complements to subspaces in the boolean cube. Journal of Applied and Industrial Mathematics, 10(3):397403, 2016.

[11] Pantelimon Stanica, Tsutomu Sasao, and Jon T Butler. Distance duality on some classes of boolean functions, 2017.

[12] Natalia Tokareva. Duality between bent functions and affine functions. Discrete Mathematics, 312(3):666670, 2012.