On Dihedral Group Invariant Boolean Functions (Extended Abstract)

Subhamoy Maitra [1] Sumanta Sarkar [1]
Deepak Kumar Dalai [2]

[1] Applied Statistics Unit
Indian Statistical Institute, Kolkata.

[2] Project CODES
INRIA, Rocquencourt, France.

Workshop on Boolean Functions : Cryptography and Applications, 2007

Outline

1. Motivation
   - The Basic Problem That We Studied
   - Motivation for the Work
   - Definitions and Background

2. Our Results/Contribution
   - Walsh Transform of DSBFs
   - Investigation of the matrix $\mathcal{M}$

Outline

1. **Motivation**
   - The Basic Problem That We Studied
   - Motivation for the Work
   - Definitions and Background
2. **Our Results/Contribution**
   - Walsh Transform of DSBFs
   - Investigation of the matrix $\mathcal{M}$

Outline

The Problems We Studied

- We studied a new class of Boolean functions which are invariant under the action of Dihedral group (DSBFS).
- We studied some theoretical and experimental results in this direction.
- Efficient search for good nonlinear function in this class.
- Most interestingly, we found many 9-variable Boolean functions having nonlinearity 241 belong to this class.

The Problems We Studied

- We studied a new class of Boolean functions which are invariant under the action of Dihedral group (DSBFS).
- We studied some theoretical and experimental results in this direction.
- Efficient search for good nonlinear function in this class.
- Most interestingly, we found many 9-variable Boolean functions having nonlinearity 241 belong to this class.

The Problems We Studied

- We studied a new class of Boolean functions which are invariant under the action of Dihedral group (DSBFS).
- We studied some theoretical and experimental results in this direction.
- Efficient search for good nonlinear function in this class.
- Most interestingly, we found many 9-variable Boolean functions having nonlinearity 241 belong to this class.

The Problems We Studied

- We studied a new class of Boolean functions which are invariant under the action of Dihedral group (DSBFS).
- We studied some theoretical and experimental results in this direction.
- Efficient search for good nonlinear function in this class.
- Most interestingly, we found many 9-variable Boolean functions having nonlinearity 241 belong to this class.

Outline

1. Motivation
   - The Basic Problem That We Studied
   - Motivation for the Work
   - Definitions and Background
2. Our Results/Contribution
   - Walsh Transform of DSBFs
   - Investigation of the matrix $\mathcal{M}$

Motivation

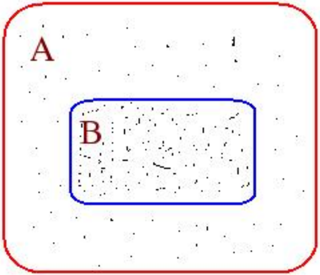
- Let A be a set of Boolean functions.
- A contains some functions having good cryptographic properties.
- $B \subset A$ contains good functions with more density.

Searching good functions in B is easier than searching in A.

Studing the functions in the set B could be better idea than studing in the set A.

Motivation

- Let A be a set of Boolean functions.
- A contains some functions having good cryptographic properties.
- $B \subset A$ contains good functions with more density.



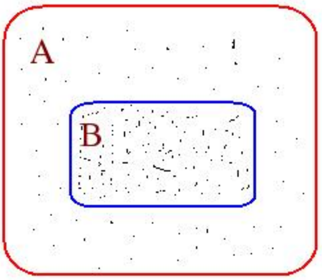
. : Good Function

Searching good functions in B is easier than searching in A.

Studing the functions in the set B could be better idea than studing in the set A.

Motivation

- Let A be a set of Boolean functions.
- A contains some functions having good cryptographic properties.
- $B \subset A$ contains good functions with more density.



. : Good Function

Searching good functions in B is easier than searching in A.

Studing the functions in the set B could be better idea than studing in the set A.

Motivation

- Number of n-variable Boolean functions: 2^{2^n}.
- Not feasible to search exhaustively for a good function when $n \geq 7$.
- Lots of attempts to search in a subclasses like class of Symmetric fuctions and Rotational Symmetric functions.
- Class sizes are 2^{n+1} and 2^{c_n} respectively, where $c_n = \frac{1}{n}\sum_{k|n}\phi(k)2^{n/k}$.
- One may be tempted to take advantange of their small size.
- Symmetric class is not exciting in terms of possession of good functions.
- Rotational symmetric class contains many good functions; but infiseable to search if $n > 9$.
- **Motivation:** to study some other classes inbetween these two classes.

Motivation

- Number of n-variable Boolean functions: 2^{2^n}.
- Not feasible to search exhaustively for a good function when $n \geq 7$.
- Lots of attempts to search in a subclasses like class of Symmetric fuctions and Rotational Symmetric functions.
- Class sizes are 2^{n+1} and 2^{c_n} respectively, where $c_n = \frac{1}{n}\sum_{k|n} \phi(k) 2^{n/k}$.
- One may be tempted to take advantange of their small size.
- Symmetric class is not exciting in terms of possession of good functions.
- Rotational symmetric class contains many good functions; but infiseable to search if $n > 9$.
- **Motivation:** to study some other classes inbetween these two classes.

Motivation

- Number of n-variable Boolean functions: 2^{2^n}.
- Not feasible to search exhaustively for a good function when $n \geq 7$.
- Lots of attempts to search in a subclasses like class of Symmetric fuctions and Rotational Symmetric functions.
- Class sizes are 2^{n+1} and 2^{c_n} respectively, where $c_n = \frac{1}{n} \sum_{k|n} \phi(k) 2^{n/k}$.
- One may be tempted to take advantange of their small size.
- Symmetric class is not exciting in terms of possession of good functions.
- Rotational symmetric class contains many good functions; but infiseable to search if $n > 9$.
- **Motivation:** to study some other classes inbetween these two classes.

Motivation

- Number of n-variable Boolean functions: 2^{2^n}.
- Not feasible to search exhaustively for a good function when $n \geq 7$.
- Lots of attempts to search in a subclasses like class of Symmetric fuctions and Rotational Symmetric functions.
- Class sizes are 2^{n+1} and 2^{c_n} respectively, where $c_n = \frac{1}{n}\sum_{k|n}\phi(k)2^{n/k}$.
- One may be tempted to take advantange of their small size.
- Symmetric class is not exciting in terms of possession of good functions.
- Rotational symmetric class contains many good functions; but infiseable to search if $n > 9$.
- **Motivation:** to study some other classes inbetween these two classes.

Motivation

- Number of n-variable Boolean functions: 2^{2^n}.
- Not feasible to search exhaustively for a good function when $n \geq 7$.
- Lots of attempts to search in a subclasses like class of Symmetric fuctions and Rotational Symmetric functions.
- Class sizes are 2^{n+1} and 2^{c_n} respectively, where $c_n = \frac{1}{n} \sum_{k|n} \phi(k) 2^{n/k}$.
- One may be tempted to take advantange of their small size.
- Symmetric class is not exciting in terms of possession of good functions.
- Rotational symmetric class contains many good functions; but infiseable to search if $n > 9$.
- **Motivation:** to study some other classes inbetween these two classes.

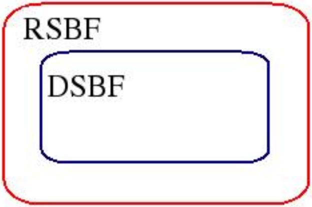
Motivation

- Number of n-variable Boolean functions: 2^{2^n}.
- Not feasible to search exhaustively for a good function when $n \geq 7$.
- Lots of attempts to search in a subclasses like class of Symmetric fuctions and Rotational Symmetric functions.
- Class sizes are 2^{n+1} and 2^{c_n} respectively, where $c_n = \frac{1}{n} \sum_{k|n} \phi(k) 2^{n/k}$.
- One may be tempted to take advantange of their small size.
- Symmetric class is not exciting in terms of possession of good functions.
- Rotational symmetric class contains many good functions; but infiseable to search if $n > 9$.
- **Motivation:** to study some other classes inbetween these two classes.

Motivation

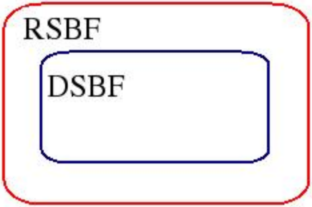
- Literature says that the class of Rotational Symmetric Boolean functions (RSBFs) contains many cryptographically good functions.
- The class of Dihedral Symmetric Boolean functions (DSBFs) is a subclass of RSBFs.
- Is the density of good functions is high in the class of DSBFs ?

Motivation



- Literature says that the class of Rotational Symmetric Boolean functions (RSBFs) contains many cryptographically good functions.
- The class of Dihedral Symmetric Boolean functions (DSBFs) is a subclass of RSBFs.
- Is the density of good functions is high in the class of DSBFs ?

Motivation



- Literature says that the class of Rotational Symmetric Boolean functions (RSBFs) contains many cryptographically good functions.
- The class of Dihedral Symmetric Boolean functions (DSBFs) is a subclass of RSBFs.
- Is the density of good functions is high in the class of DSBFs ?

Outline

Boolean functions

- An n-variable Boolean function can be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$.
- $\mathcal{B}_n$: the set of all Boolean functions of n variables.
- **Truth Table (TT)**: A Boolean function $f \in B_n$ can be represented by a binary string of length 2^n.
  $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.
- **Walsh Transform of f at $a \in F_2^n$:**

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x.a}$$

- Nonlinearity of f: $2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} W_f(a)$.

Boolean functions

- An n-variable Boolean function can be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$.
- $\mathcal{B}_n$: the set of all Boolean functions of n variables.
- **Truth Table (TT)**: A Boolean function $f \in B_n$ can be represented by a binary string of length 2^n.
  $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.
- **Walsh Transform of f at $a \in F_2^n$:**

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x.a}$$

- Nonlinearity of f: $2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} W_f(a)$.

Boolean functions

- An n-variable Boolean function can be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$.
- $\mathcal{B}_n$: the set of all Boolean functions of n variables.
- **Truth Table (TT)**: A Boolean function $f \in B_n$ can be represented by a binary string of length 2^n.
  $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.
- **Walsh Transform of f at $a \in F_2^n$:**

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x.a}$$

- Nonlinearity of f: $2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} W_f(a)$.

Boolean functions

- An n-variable Boolean function can be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$.
- $\mathcal{B}_n$: the set of all Boolean functions of n variables.
- **Truth Table (TT)**: A Boolean function $f \in B_n$ can be represented by a binary string of length 2^n.
  $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.
- **Walsh Transform of f at $a \in F_2^n$:**

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x.a}$$

- Nonlinearity of f: $2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} W_f(a)$.

Boolean functions

Nonlinearity of f: $2^{n-1} - \frac{1}{2}\max_{a \in F_2^n} W_f(a)$.

- n even: Max nonlinearity = $2^{n-1} - 2^{\frac{n}{2}-1}$.
  Function achieving this bound is called *bent* function.

- n odd: Max nonlinearity is unknown.
  $2^{n-1} - 2^{\frac{n-1}{2}} < nl(f) \leq 2^{n-1} - \lceil 2^{\frac{n}{2}-1} \rceil$.

Permutation Group

- **Permutation group** is a finite group of permutations (bijection mappings) on the elements of a given finite set with composition as group operation.
- Group of all permutations is called *Symmetric group* and denoted as S_n where n is the number of elements.
- Group of all cyclic shift permutations is called *rotation (cyclic) group* and denoted as C_n.
- Group of cyclic shift and reflection permutaions is called *Dihedral group* and denoted as D_n.

Permutation Group

- **Permutation group** is a finite group of permutations (bijection mappings) on the elements of a given finite set with composition as group operation.
- Group of all permutations is called *Symmetric group* and denoted as S_n where n is the number of elements.
- Group of all cyclic shift permutations is called *rotation (cyclic) group* and denoted as C_n.
- Group of cyclic shift and reflection permutaions is called *Dihedral group* and denoted as D_n.

Permutation Group

- **Permutation group** is a finite group of permutations (bijection mappings) on the elements of a given finite set with composition as group operation.
- Group of all permutations is called *Symmetric group* and denoted as S_n where n is the number of elements.
- Group of all cyclic shift permutations is called *rotation (cyclic) group* and denoted as C_n.
- Group of cyclic shift and reflection permutaions is called *Dihedral group* and denoted as D_n.

Permutation Group

- **Permutation group** is a finite group of permutations (bijection mappings) on the elements of a given finite set with composition as group operation.
- Group of all permutations is called *Symmetric group* and denoted as S_n where n is the number of elements.
- Group of all cyclic shift permutations is called *rotation (cyclic) group* and denoted as C_n.
- Group of cyclic shift and reflection permutaions is called *Dihedral group* and denoted as D_n.

Dihedral Group

Dihedral Group of degree $n \geq 3$

Generated by two elements σ, ω such that,

1. $\sigma^n = \omega^2 = e$, where e is the identity element,
2. $\omega\sigma = \sigma^{-1}\omega$.

- We denote Dihedral group of degree n as D_n.
- $D_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \omega, \sigma\omega, \sigma^2\omega, \ldots, \sigma^{n-1}\omega\}$.
- $|D_n| = 2n$.

Dihedral Group

Dihedral Group of degree $n \geq 3$

Generated by two elements σ, ω such that,

1. $\sigma^n = \omega^2 = e$, where e is the identity element,
2. $\omega\sigma = \sigma^{-1}\omega$.

- We denote Dihedral group of degree n as D_n.
- $D_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \omega, \sigma\omega, \sigma^2\omega, \ldots, \sigma^{n-1}\omega\}$.
- $|D_n| = 2n$.

Geometric Realization of Dihedral Group

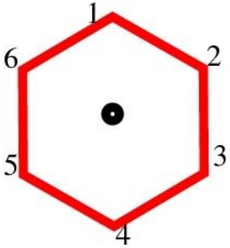
D_n can be realised as a group of permutaions on the vertices of n-gon P_n.

Geometric Realization of Dihedral Group

σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.

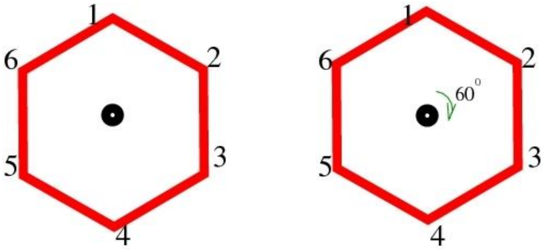
Geometric Realization of Dihedral Group

σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.



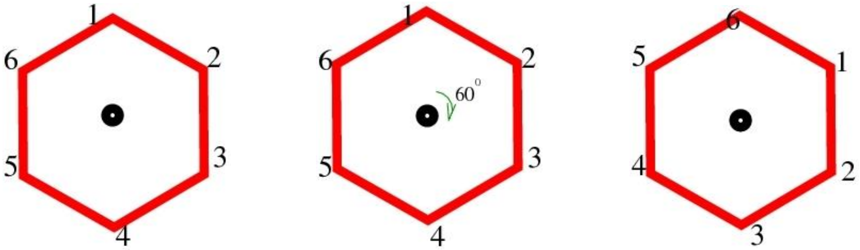
Geometric Realization of Dihedral Group

σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.



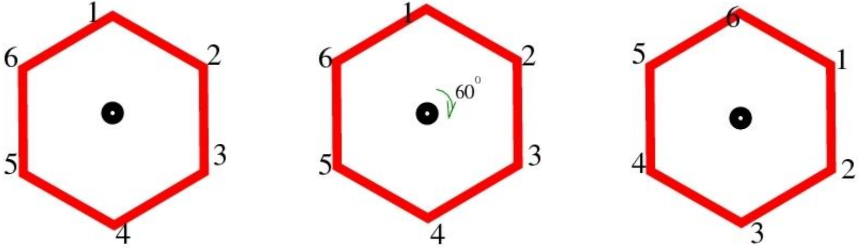
Geometric Realization of Dihedral Group

σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.



Geometric Realization of Dihedral Group

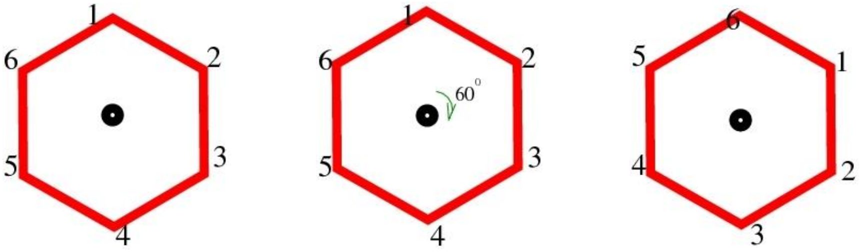
σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.



Permutation form: $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$

Geometric Realization of Dihedral Group

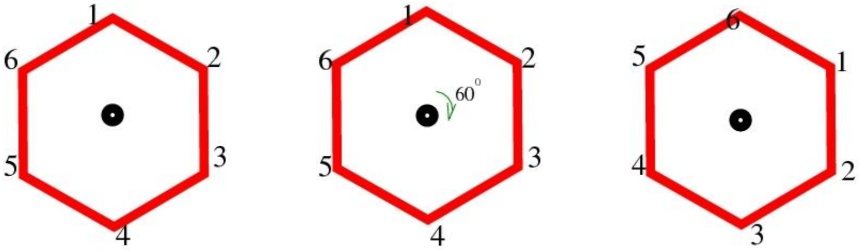
σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.



$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}, \sigma^i = \begin{pmatrix} 1 & 2 & \dots & n \\ i+1 & i+2 & \dots & i \end{pmatrix}.$$

Geometric Realization of Dihedral Group

σ is the clockwise rotation of P_n with respect to the line passing vertically through the center of P_n at an angle $\frac{2\pi}{n}$.



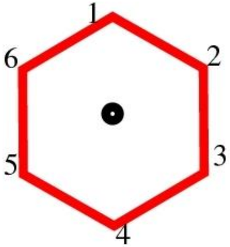
$\sigma^n = e$.

Geometric Realization of Dihedral Group

ω is the reflection (or, rotation of P_n by π) about a line passing through a vertex and the center of P_n.

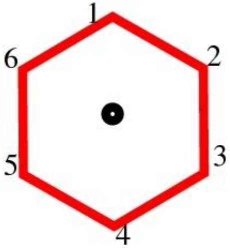
Geometric Realization of Dihedral Group

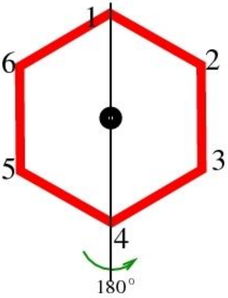
ω is the reflection (or, rotation of P_n by π) about a line passing through a vertex and the center of P_n.



Geometric Realization of Dihedral Group

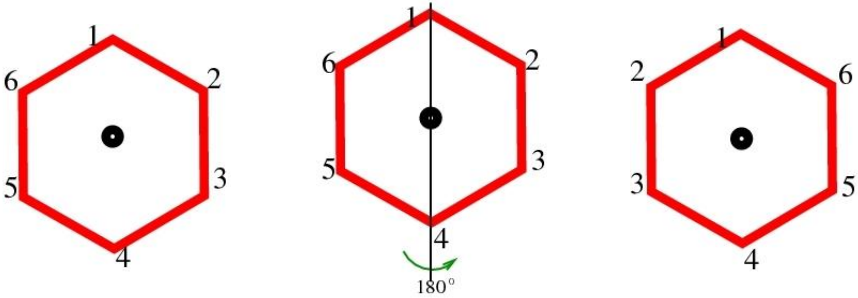
ω is the reflection (or, rotation of P_n by π) about a line passing through a vertex and the center of P_n.





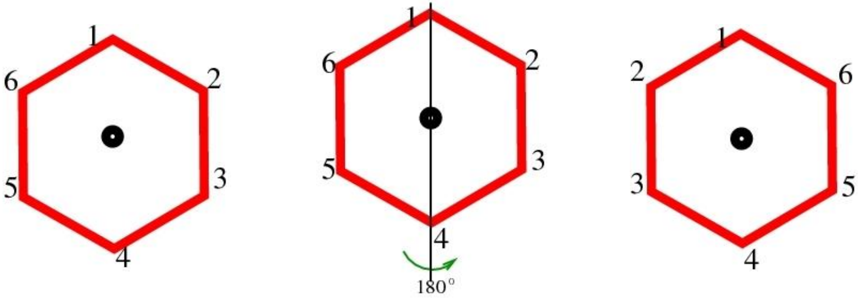
Geometric Realization of Dihedral Group

ω is the reflection (or, rotation of P_n by π) about a line passing through a vertex and the center of P_n.



Geometric Realization of Dihedral Group

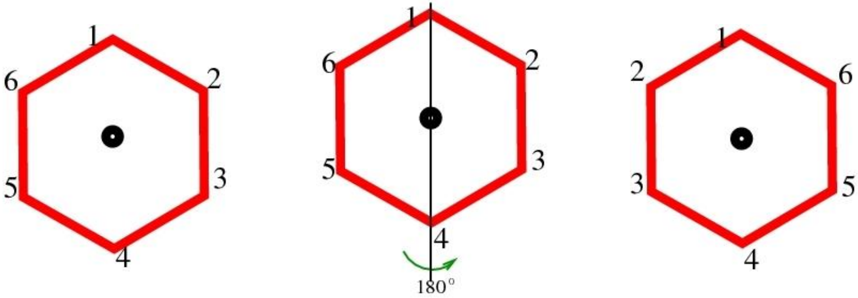
ω is the reflection (or, rotation of P_n by π) about a line passing through a vertex and the center of P_n.



Permutation form: $\omega = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$

Geometric Realization of Dihedral Group

ω is the reflection (or, rotation of P_n by π) about a line passing through a vertex and the center of P_n.



$\omega^2 = e$.

Group Action

Definition (Group action)

The group action of a group G on a set X is a mapping $\psi : G \times X \to X$ denoted as $g \cdot x$, which satisfies the following two actions.

1. $(gh) \cdot x = g \cdot (h \cdot x)$, for all $g, h \in G$ and for all $x \in X$.
2. $e \cdot x = x$, for every $x \in X$, e is the identity element of G.

Group action of a group G on a set X forms equivalence classes under the equivalent relation $x \sim y$ iff $g.x = y$ for $x, y \in X$ and $g \in G$.

Group Action

Definition (Group action)

The group action of a group G on a set X is a mapping $\psi : G \times X \to X$ denoted as $g \cdot x$, which satisfies the following two actions.

1. $(gh) \cdot x = g \cdot (h \cdot x)$, for all $g, h \in G$ and for all $x \in X$.
2. $e \cdot x = x$, for every $x \in X$, e is the identity element of G.

Group action of a group G on a set X forms equivalence classes under the equivalent relation $x \sim y$ iff $g.x = y$ for $x, y \in X$ and $g \in G$.

Group Action

H is a subgroup of G and G, H act on a set X then

no. of equivalent classes by $G \leq$ no.of equivalent classes by H.

$C_n \subseteq D_n \subseteq S_n$ act on the set F_2^n.

no. of equivalent classes by $S_n \leq$ no.of equivalent classes by $D_n \leq$ no.of equivalent classes by C_n.

Group Action

H is a subgroup of G and G, H act on a set X then

no. of equivalent classes by $G \leq$ no.of equivalent classes by H.

$C_n \subseteq D_n \subseteq S_n$ act on the set F_2^n.

no. of equivalent classes by $S_n \leq$ no.of equivalent classes by $D_n \leq$ no.of equivalent classes by C_n.

Boolean function Invariant under Group Action

Definition

Let G acts on X.
A Boolean function f is said to be invariant under the action of G if $f(g \cdot x) = f(x)$, for all $g \in G$ and for all $x \in X$.
That is, $f(x)$ is same for all x in each class.

- Boolean functions invariant under the action of S_n is called Symmetric Boolean function and denoted as $S(S_n)$.
- Boolean functions invariant under the action of C_n is called Rotational Symmetric Boolean function(RSBF) and denoted as $S(C_n)$.
- Boolean functions invariant under the action of D_n is called Dihedral Symmetric Boolean function(DSBF) and denoted as $S(D_n)$.

Boolean function Invariant under Group Action

Definition

Let G acts on X.
A Boolean function f is said to be invariant under the action of G if $f(g \cdot x) = f(x)$, for all $g \in G$ and for all $x \in X$.
That is, $f(x)$ is same for all x in each class.

- Boolean functions invariant under the action of S_n is called Symmetric Boolean function and denoted as $S(S_n)$.
- Boolean functions invariant under the action of C_n is called Rotational Symmetric Boolean function(RSBF) and denoted as $S(C_n)$.
- Boolean functions invariant under the action of D_n is called Dihedral Symmetric Boolean function(DSBF) and denoted as $S(D_n)$.

Boolean function Invariant under Group Action

Definition

Let G acts on X.
A Boolean function f is said to be invariant under the action of G if $f(g \cdot x) = f(x)$, for all $g \in G$ and for all $x \in X$.
That is, $f(x)$ is same for all x in each class.

- Boolean functions invariant under the action of S_n is called Symmetric Boolean function and denoted as $S(S_n)$.
- Boolean functions invariant under the action of C_n is called Rotational Symmetric Boolean function(RSBF) and denoted as $S(C_n)$.
- Boolean functions invariant under the action of D_n is called Dihedral Symmetric Boolean function(DSBF) and denoted as $S(D_n)$.

Boolean function Invariant under Group Action

Definition

Let G acts on X.
A Boolean function f is said to be invariant under the action of G if $f(g \cdot x) = f(x)$, for all $g \in G$ and for all $x \in X$.
That is, $f(x)$ is same for all x in each class.

- Boolean functions invariant under the action of S_n is called Symmetric Boolean function and denoted as $S(S_n)$.
- Boolean functions invariant under the action of C_n is called Rotational Symmetric Boolean function(RSBF) and denoted as $S(C_n)$.
- Boolean functions invariant under the action of D_n is called Dihedral Symmetric Boolean function(DSBF) and denoted as $S(D_n)$.

Boolean function Invariant under Group Action

- # of equiv. classes by S_n $(s_n) = n + 1$. $|S(S_n)| = 2^{n+1}$.
- # of equiv. classes by C_n $(c_n) = \frac{1}{n}\sum_{k|n}\phi(k)2^{n/k}$. $|S(C_n)| = 2^{c_n}$.
- # of equiv. classes by D_n $(d_n) = \frac{c_n}{2} + l$,
  $l = \begin{cases} \frac{3}{4}2^{\frac{n}{2}} \text{ if n is even} \\ 2^{\frac{n-1}{2}} \text{ if n is odd} \end{cases}$.
  $|S(D_n)| = 2^{d_n}$.

Hierarchy of the subclasses of B_n =>

Boolean function Invariant under Group Action

- # of equiv. classes by S_n $(s_n) = n + 1$. $|S(S_n)| = 2^{n+1}$.
- # of equiv. classes by C_n $(c_n) = \frac{1}{n}\sum_{k|n}\phi(k)2^{n/k}$. $|S(C_n)| = 2^{c_n}$.
- # of equiv. classes by D_n $(d_n) = \frac{c_n}{2} + l$,
  $$l = \begin{cases} \frac{3}{4}2^{\frac{n}{2}} \text{ if n is even} \\ 2^{\frac{n-1}{2}} \text{ if n is odd} \end{cases}.$$
  $|S(D_n)| = 2^{d_n}$.

Hierarchy of the subclasses of B_n =>

Boolean function Invariant under Group Action

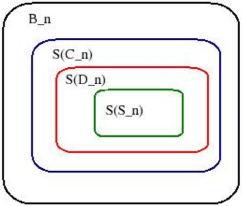
- # of equiv. classes by S_n $(s_n) = n + 1$. $|S(S_n)| = 2^{n+1}$.
- # of equiv. classes by C_n $(c_n) = \frac{1}{n}\sum_{k|n}\phi(k)2^{n/k}$. $|S(C_n)| = 2^{c_n}$.
- # of equiv. classes by D_n $(d_n) = \frac{c_n}{2} + l$,
$$l = \begin{cases} \frac{3}{4}2^{\frac{n}{2}} \text{ if n is even} \\ 2^{\frac{n-1}{2}} \text{ if n is odd} \end{cases}.$$
$|S(D_n)| = 2^{d_n}$.

Hierarchy of the subclasses of B_n =>

Boolean function Invariant under Group Action

- # of equiv. classes by S_n $(s_n) = n + 1$. $|S(S_n)| = 2^{n+1}$.
- # of equiv. classes by C_n $(c_n) = \frac{1}{n}\sum_{k|n}\phi(k)2^{n/k}$. $|S(C_n)| = 2^{c_n}$.
- # of equiv. classes by D_n $(d_n) = \frac{c_n}{2} + l$, $l = \begin{cases} \frac{3}{4}2^{\frac{n}{2}} \text{ if n is even} \\ 2^{\frac{n-1}{2}} \text{ if n is odd} \end{cases}$. $|S(D_n)| = 2^{d_n}$.

Hierarchy of the subclasses of B_n =>



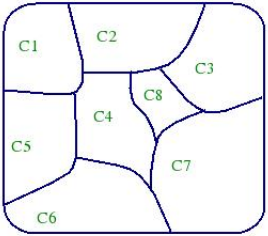
Comparision of sizes of $S(C_n)$ and $S(D_n)$

n	3	4	5	6	7	8	9	10	11	12	13	14
c_n	4	6	8	14	20	36	60	108	188	352	632	1182
d_n	4	6	8	13	18	30	46	78	126	224	380	687

Table: Comparison between c_n and d_n

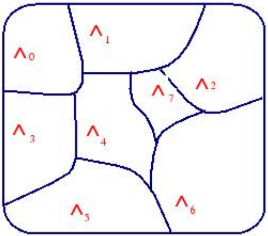
Representation of DSBFs

- There are d_n many equivalence classes in F_2^n.
- Each class can be represented by an element of that class.
- Let assign the lexicographically least element of each class to be leader of the class.
- Rename the leaders as $\Lambda_0, \Lambda_1, \dots \Lambda_{d_n - 1}$.



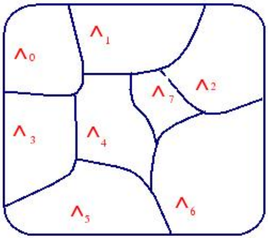
Representation of DSBFs

- There are d_n many equivalence classes in F_2^n.
- Each class can be represented by an element of that class.
- Let assign the lexicographically least element of each class to be leader of the class.
- Rename the leaders as $\Lambda_0, \Lambda_1, \ldots \Lambda_{d_n-1}$.



Representation of DSBFs

- There are d_n many equivalence classes in F_2^n.
- Each class can be represented by an element of that class.
- Let assign the lexicographically least element of each class to be leader of the class.
- Rename the leaders as $\Lambda_0, \Lambda_1, \ldots \Lambda_{d_n - 1}$.



A DSBF can be represented by a d_n bit string $[f(\Lambda_0), f(\Lambda_1), \ldots, f(\Lambda_{d_n-1})]$.

Outline

Walsh Transform of DSBFs

- $W_f(w) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot w}$.
- If f is a *DSBF*, then

$$W_f(w) = \sum_{i=0}^{d_n - 1} (-1)^{f(\Lambda_i)} \sum_{x \in cls(\Lambda_i)} (-1)^{x \cdot w}.$$

Let w, z are in same class and f be a *DSBF*, then $W_f(w) = W_f(z)$.

- Walsh spectra of a DSBF can be described by d_n many values.

Walsh Transform of DSBFs

- $W_f(w) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot w}$.
- If f is a *DSBF*, then

$$W_f(w) = \sum_{i=0}^{d_n - 1} (-1)^{f(\Lambda_i)} \sum_{x \in cls(\Lambda_i)} (-1)^{x \cdot w}.$$

Let w, z are in same class and f be a *DSBF*, then $W_f(w) = W_f(z)$.

- Walsh spectra of a DSBF can be described by d_n many values.

Walsh Transform of DSBFs

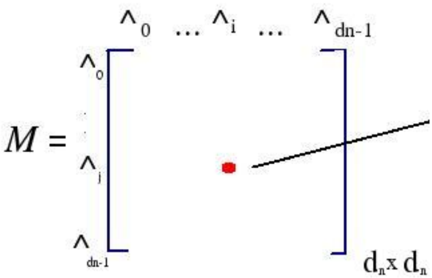
- $W_f(w) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot w}$.
- If f is a *DSBF*, then

$$W_f(w) = \sum_{i=0}^{d_n - 1} (-1)^{f(\Lambda_i)} \sum_{x \in cls(\Lambda_i)} (-1)^{x \cdot w}.$$

Let w, z are in same class and f be a *DSBF*, then $W_f(w) = W_f(z)$.

- Walsh spectra of a DSBF can be described by d_n many values.

Computing Walsh spectra of DSBFs



$$\sum_{x \in cls(\Lambda_i)} (-1)^{x \cdot \Lambda_{n,j}}$$

Walsh spectra of f can be determined by a matrix product as

$$[(-1)^{f(\Lambda_0)}, (-1)^{f(\Lambda_1)}, \ldots, (-1)^{f(\Lambda_{d_n-1})}]\ \mathcal{M}.$$

Computing cryptographic numericals of DSBFs

Let f be an n-variable DSBF.

- f is balanced iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ M_{i,0} = 0$.
- Nonlinearity of f is

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\Lambda_j, 0 \leq j < d_n} \left| \sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ M_{i,j} \right|.$$

- f is bent iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ M_{i,j} = \pm 2^{\frac{n}{2}}$ for $0 \leq j \leq d_n - 1$.
- f is m-order Correlation Immune (respectively m-resilient) iff

$$\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ M_{i,j} = 0, \text{ for } 1 \text{ (respectively } 0) \leq wt(\Lambda_j) \leq m.$$

Computing cryptographic numericals of DSBFs

Let f be an n-variable DSBF.

- f is balanced iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ \ M_{i,0} = 0$.
- Nonlinearity of f is

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\Lambda_j, 0 \le j < d_n} \left| \sum_{i=0}^{d_n-1} (-1)^{f(\Lambda_i)} \ \ M_{i,j} \right|.$$

- f is bent iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ \ M_{i,j} = \pm 2^{\frac{n}{2}}$ for $0 \le j \le d_n - 1$.
- f is m-order Correlation Immune (respectively m-resilient) iff

$$\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \ \ M_{i,j} = 0, \ \text{for } 1 \text{ (respectively 0)} \le wt(\Lambda_j) \le m.$$

Computing cryptographic numericals of DSBFs

Let f be an n-variable DSBF.

- f is balanced iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,0} = 0$.
- Nonlinearity of f is

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\Lambda_j, 0 \leq j < d_n} \left| \sum_{i=0}^{d_n-1} (-1)^{f(\Lambda_i)} \; M_{i,j} \right|.$$

- f is bent iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,j} = \pm 2^{\frac{n}{2}}$ for $0 \leq j \leq d_n - 1$.
- f is m-order Correlation Immune (respectively m-resilient) iff

$$\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,j} = 0, \text{ for } 1 \text{ (respectively 0)} \leq wt(\Lambda_j) \leq m.$$

Computing cryptographic numericals of DSBFs

Let f be an n-variable DSBF.

- f is balanced iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,0} = 0$.
- Nonlinearity of f is

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\Lambda_j, 0 \leq j < d_n} \left| \sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,j} \right|.$$

- f is bent iff $\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,j} = \pm 2^{\frac{n}{2}}$ for $0 \leq j \leq d_n - 1$.
- f is m-order Correlation Immune (respectively m-resilient) iff

$$\sum_{i=0}^{d_n-1}(-1)^{f(\Lambda_i)} \; M_{i,j} = 0, \text{ for } 1 \text{ (respectively 0)} \leq wt(\Lambda_j) \leq m.$$

Outline

1. Motivation
   - The Basic Problem That We Studied
   - Motivation for the Work
   - Definitions and Background
2. Our Results/Contribution
   - Walsh Transform of DSBFs
   - Investigation of the matrix $\mathcal{M}$

the matrix $\mathcal{M}$ for odd n

Let n be odd and $x \in F_2^n$.

- $wt(x)$ is odd iff $wt(\overline{x})$ is even.
- $cls(x) \neq cls(\overline{x})$.
- Order the leaders Λ_i as $\Lambda_0, \ldots, \Lambda_{d_n/2-1}$ are having odd weight and $\Lambda_{d_n/2+i} = \overline{\Lambda_i}, 0 \leq i < d_n/2$.

the matrix $\mathcal{M}$ for odd n

Let n be odd and $x \in F_2^n$.

- $wt(x)$ is odd iff $wt(\overline{x})$ is even.
- $cls(x) \neq cls(\overline{x})$.
- Order the leaders Λ_i as $\Lambda_0, \ldots, \Lambda_{d_n/2-1}$ are having odd weight and $\Lambda_{d_n/2+i} = \overline{\Lambda_i}, 0 \leq i < d_n/2$.

the matrix $\mathcal{M}$ for odd n

Let n be odd and $x \in F_2^n$.

- $wt(x)$ is odd iff $wt(\overline{x})$ is even.
- $cls(x) \neq cls(\overline{x})$.
- Order the leaders Λ_i as $\Lambda_0, \ldots, \Lambda_{d_n/2-1}$ are having odd weight and $\Lambda_{d_n/2+i} = \overline{\Lambda_i}, 0 \leq i < d_n/2$.

the matrix $\mathcal{M}$ for odd n

Let n be odd and $x \in F_2^n$.

- $wt(x)$ is odd iff $wt(\overline{x})$ is even.
- $cls(x) \neq cls(\overline{x})$.
- Order the leaders Λ_i as $\Lambda_0, \ldots, \Lambda_{d_n/2-1}$ are having odd weight and $\Lambda_{d_n/2+i} = \overline{\Lambda_i}, 0 \leq i < d_n/2$.

The matrix after reordering:

$$M_n = \begin{array}{c|cc} & \Lambda_0 \cdots \Lambda_{d_n/2-1} & \overline{\Lambda_0} \cdots \overline{\Lambda_{d_n/2-1}} \\ \hline \begin{array}{c} \Lambda_0 \\ \Lambda_{d_n/2-1} \\ \overline{\Lambda_0} \\ \overline{\Lambda_{d_n/2-1}} \end{array} & \multicolumn{2}{c}{\left[\begin{array}{c|c} S_n & S_n \\ \hline S_n & -S_n \end{array}\right]} \end{array}$$

the matrix $\mathcal{M}$ for odd n

The matrix after reordering:

$$M_n = \begin{array}{c} \\ \Lambda_0 \\ \vdots \\ \Lambda_{d_n/2-1} \\ \overline{\Lambda_0} \\ \vdots \\ \overline{\Lambda_{d_n/2-1}} \end{array} \begin{array}{c} \Lambda_0 \cdots \Lambda_{d_n/2-1} \quad \overline{\Lambda_0} \cdots \overline{\Lambda_{d_n/2-1}} \\ \left[\begin{array}{c|c} S_n & S_n \\ \hline S_n & -S_n \end{array}\right] \end{array}$$

- Computing $\frac{d_n}{2} \times \frac{d_n}{2}$ matrix S_n is suffice to compute $d_n \times d_n$ matrix $\mathcal{M}_\backslash$.
- 4 times advantage to compute the matrix $\mathcal{M}_\backslash$.
- This advantage carries to compute Walsh spectra, nonlinearity, resiliencey etc.

the matrix $\mathcal{M}$ for odd n

The matrix after reordering:

$$M_n = \begin{array}{c|c} & \Lambda_0 \cdots \Lambda_{d_n/2-1} \quad \overline{\Lambda_0} \cdots \overline{\Lambda_{d_n/2-1}} \\ \hline \begin{array}{c} \Lambda_0 \\ \vdots \\ \Lambda_{d_n/2-1} \\ \overline{\Lambda_0} \\ \vdots \\ \overline{\Lambda_{d_n/2-1}} \end{array} & \left[\begin{array}{c|c} S_n & S_n \\ \hline S_n & -S_n \end{array}\right] \end{array}$$

- Computing $\frac{d_n}{2} \times \frac{d_n}{2}$ matrix S_n is suffice to compute $d_n \times d_n$ matrix $\mathcal{M}_\backslash$.
- 4 times advantage to compute the matrix $\mathcal{M}_\backslash$.
- This advantage carries to compute Walsh spectra, nonlinearity, resiliencey etc.

the matrix $\mathcal{M}$ for odd n

The matrix after reordering:

$$M_n = \begin{array}{c} \\ \Lambda_0 \\ \vdots \\ \Lambda_{d_n/2-1} \\ \overline{\Lambda_0} \\ \vdots \\ \overline{\Lambda_{d_n/2-1}} \end{array} \begin{array}{c} \Lambda_0 \cdots \Lambda_{d_n/2-1} \quad \overline{\Lambda_0} \cdots \overline{\Lambda_{d_n/2-1}} \\ \left[\begin{array}{c|c} S_n & S_n \\ \hline S_n & -S_n \end{array}\right] \end{array}$$

- Computing $\frac{d_n}{2} \times \frac{d_n}{2}$ matrix S_n is suffice to compute $d_n \times d_n$ matrix $\mathcal{M}_\backslash$.
- 4 times advantage to compute the matrix $\mathcal{M}_\backslash$.
- This advantage carries to compute Walsh spectra, nonlinearity, resiliencey etc.

Highly nonlinear Boolean functions

- Recently[Indocrypt 2006], shown that there are Boolean functions of odd number variables having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}, n > 7$.
- They showed existence of 9-variable Boolean function of nonlinearity $241 > 2^8 - 2^4 = 240$.
- They found 8×189 many RSBFs having nonlinearity 241 out of 2^{60} functions.
- We found 8×21 DSBFs having nonlinearity 241 out of 2^{46}.
- **Density :** 241-nonlinearity functions are $\frac{2^{14}}{9}$ times more dense in the class of DSBFs than the class of RSBFs.
- Hope it will be happen for higher number of variables too.

Highly nonlinear Boolean functions

- Recently[Indocrypt 2006], shown that there are Boolean functions of odd number variables having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}, n > 7$.
- They showed existence of 9-variable Boolean function of nonlinearity $241 > 2^8 - 2^4 = 240$.
- They found 8×189 many RSBFs having nonlinearity 241 out of 2^{60} functions.
- We found 8×21 DSBFs having nonlinearity 241 out of 2^{46}.
- **Density :** 241-nonlinearity functions are $\frac{2^{14}}{9}$ times more dense in the class of DSBFs than the class of RSBFs.
- Hope it will be happen for higher number of variables too.

Highly nonlinear Boolean functions

- Recently[Indocrypt 2006], shown that there are Boolean functions of odd number variables having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}, n > 7$.
- They showed existence of 9-variable Boolean function of nonlinearity $241 > 2^8 - 2^4 = 240$.
- They found 8×189 many RSBFs having nonlinearity 241 out of 2^{60} functions.
- We found 8×21 DSBFs having nonlinearity 241 out of 2^{46}.
- **Density :** 241-nonlinearity functions are $\frac{2^{14}}{9}$ times more dense in the class of DSBFs than the class of RSBFs.
- Hope it will be happen for higher number of variables too.

Highly nonlinear Boolean functions

- Recently[Indocrypt 2006], shown that there are Boolean functions of odd number variables having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}, n > 7$.
- They showed existence of 9-variable Boolean function of nonlinearity $241 > 2^8 - 2^4 = 240$.
- They found 8×189 many RSBFs having nonlinearity 241 out of 2^{60} functions.
- We found 8×21 DSBFs having nonlinearity 241 out of 2^{46}.
- **Density :** 241-nonlinearity functions are $\frac{2^{14}}{9}$ times more dense in the class of DSBFs than the class of RSBFs.
- Hope it will be happen for higher number of variables too.

Highly nonlinear Boolean functions

- Recently[Indocrypt 2006], shown that there are Boolean functions of odd number variables having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}, n > 7$.
- They showed existence of 9-variable Boolean function of nonlinearity $241 > 2^8 - 2^4 = 240$.
- They found 8×189 many RSBFs having nonlinearity 241 out of 2^{60} functions.
- We found 8×21 DSBFs having nonlinearity 241 out of 2^{46}.
- **Density :** 241-nonlinearity functions are $\frac{2^{14}}{9}$ times more dense in the class of DSBFs than the class of RSBFs.
- Hope it will be happen for higher number of variables too.

Summary

- We introduced a new class Boolean functions inbetween symmetric class and RSBFs.
- We studied some theoretical and experimental results on this class.
- Expectation that high nonlinear functions are more dense in DSBFs than RSBFs.

End

Thanks :)