Non-Linearity and Affine Equivalence of Permutations

P R Mishra* Indivar Gupta†
N R Pillai ‡
SAG, DRDO, Mtcalfe House Complex, Delhi-110054, INDIA

November 30, 2014

Abstract

In this paper we consider permutations on n symbols as bijections on $\mathbb{Z}/n\mathbb{Z}$. Treating permutations this way facilitates us with additional structures such as group, ring defined in the set $\mathbb{Z}/n\mathbb{Z}$. We explore some of the properties of permutations arising out of this treatment. We propose two properties viz. affine equivalence and non-linearity for permutations on the lines similar to there description given in the case of functions. We also establish some results which are quite similar to those given for Boolean functions. We also define *Mode Transform* of a permutation and investigate its relationship with non-linearity.

We propose an efficient algorithm using Mode transform for computing non-linearity of a permutation and show that it is $O(n^2)$, as compared to $O(n^3)$ of the direct approach. At the end we discuss these properties in the context of cryptography.

keywords: Permutation Boolean Function Non-Linearity Affine Equivalence Cryptography.

1 Introduction

In this paper we consider permutations on n symbols as bijections on the ring of integers modulo n i.e., $\mathbb{Z}/n\mathbb{Z}$. By viewing a permutation on n symbols as a member of symmetric group S_n only, we miss out on some properties which deal with relations between elements being permuted. Treating them as bijections on $\mathbb{Z}/n\mathbb{Z}$ enables us to explore some interesting properties of permutations and relations between permutations. We introduce a metric structure on the set of permutations and extend the notion of non-linearity and affine equivalence given for Boolean functions[4, 10, 14] to permutations.

*prasanna.r.mishra@gmail.com
†indivar_gupta@yahoo.com,indivargupta@sag.drdo.in
‡rpillai@sag.drddo.in

We adopt the idea of Hamming distance to establish a metric structure in the set of permutations. The same is proposed in Section 2. We term the evaluation function of affine permutation polynomial defined on $\mathbb{Z}/n\mathbb{Z}$ as affine permutations. We also define an equivalence relation viz., *Affine Equivalence* on the set of permutations based on composition of a permutation with an affine permutation. In Section 3 we study affine equivalence of permutations in detail and derive many counting formulae for them.

In Section 4 we define non-linearity of a permutation as the distance of it from the set of all affine permutations. Using this notion of non-linearity, we obtain some relations which are quite similar to the relations for non-linearity of Boolean functions.

In Section 5 we define *Mode Transform* and establish its connection with non-linearity. The naive computation of non-linearity of a permutation has cubic time complexity. We present an algorithm for efficient computation of non-linearity of a permutation using Mode transform. Finally, we prove that, using our algorithm the non-linearity of a permutation can be computed in quadratic time.

Non-linearity and Affine Equivalence of Boolean functions have cryptographic significance. In Section 6, we try to explore the cryptographic relevance of non-linearity and affine equivalence for Permutations. We try to mathematically frame and generalize the existing thumb rules for selection of permutations for cryptographic applications in terms of these properties.

2 Metric Structure of S_n

We consider set of permutations over $\mathbb{Z}/n\mathbb{Z}$. We choose the elements of symmetric group S_n to be the bijections of $\mathbb{Z}/n\mathbb{Z}$. Our aim is to introduce metric structure in S_n. We translate the idea of Hamming metric to the set of permutations on $\mathbb{Z}/n\mathbb{Z}$. For $f_1, f_2 \in S_n$ we define metric d_H as, $d_H(f_1, f_2) = n - \sum_{i=0}^{n-1} \delta(f_1(i) - f_2(i))$. δ being the Dirac delta function defined as,

$$\delta(n) = \begin{cases} 1 \text{ if } n = 0 \\ 0 \text{ otherwise} \end{cases}$$

It can be proved that this distance satisfies all the axioms of a metric i.e.,

$$d_H(f_1, f_2) \geq 0 \tag{1}$$
$$d_H(f_1, f_2) = 0 \text{ iff } f_1 = f_2 \tag{2}$$
$$d_H(f_1, f_2) = d_H(f_2, f_1) \tag{3}$$
$$d_H(f_1, f_2) \leq d_H(f_1, f_3) + d_H(f_3, f_2) \tag{4}$$

In this case we observe an additional property we state in form of proposition.

Proposition 2.1. *For any* $f \in S_n$ $d_H(f_1, f_2) = d_H(ff_1, ff_2) = d_H(f_1 f, f_2 f)$

Proof.

$$\begin{aligned} d_H(f_1 f, f_2 f) &= n - \sum_{i=0}^{n-1} \delta(f_1 f(i) - f_2 f(i)) \\ &= n - \sum_{i=0}^{n-1} \delta(f_1(f(i)) - f_2(f(i))) \end{aligned}$$

Let $f(i) = j$. Then we can write,

$$d_H(f_1 f, f_2 f) = n - \sum_{f^{-1}(j)=0}^{n-1} \delta(f_1(j) - f_2(j))$$

As $f \in S_n, \{j : f^{-1}(j) = i, i \in \mathbb{Z}/n\mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$, we have:

$$d_H(f_1 f, f_2 f) = n - \sum_{j=0}^{n-1} \delta(f_1(j) - f_2(j)) = d_H(f_1, f_2)$$

For second part observe that

$$\begin{aligned} & \delta(f_1(i) - f_2(i)) = 1 \\ \Leftrightarrow \quad & f_1(i) = f_2(i) \\ \Leftrightarrow \quad & f(f_1(i)) = f(f_2(i)) \qquad \text{As } f \in S_n \\ \Leftrightarrow \quad & \delta(ff_1(i) - ff_2(i)) = 1 \end{aligned}$$

Which leads us to conclude

$$\delta(f_1(i) - f_2(i)) = \delta(ff_1(i) - ff_2(i)) \tag{5}$$

Summing both sides of eq.(5) over i from 0 to $n-1$ we get the desired result. □

3 Affinely Equivalent Permutations

We define shift permutation $\tau_b,\ b \in \mathbb{Z}/n\mathbb{Z}$ as,

$$\tau_b(x) = x + b$$

Further, we define scaling permutation $\sigma_a,\ a \in (\mathbb{Z}/n\mathbb{Z})^*$ as,

$$\sigma_a(x) = ax$$

Here we adopt the convention that the operations '+' and '×' are the addition and multiplication modulo n when applied on elements of $\mathbb{Z}/n\mathbb{Z}$. Hereafter, we will continue to follow this convention throughout the paper.

It is easy to verify that both $\tau_b,\ b \in \mathbb{Z}/n\mathbb{Z}$ and $\sigma_a,\ a \in (\mathbb{Z}/n\mathbb{Z})^*$ are permutations. The obvious properties of σ and τ functions are given in the following proposition.

Proposition 3.1. *For $b \in \mathbb{Z}/n\mathbb{Z}$ and $\sigma_a,\ a \in (\mathbb{Z}/n\mathbb{Z})^*$*

1. $\tau_0 = I$
2. $\sigma_1 = I$
3. $\tau_b^{-1} = \tau_{-b}$
4. $\sigma_a^{-1} = \sigma_{a^{-1}}$
5. $\tau_a\tau_b = \tau_{a+b}$
6. $\sigma_a\sigma_b = \sigma_{ab}$

The sets of all shifts and scalings (denoted by $\mathcal{T}$ and $\mathcal{S}$) are actually the subgroups of S_n. As S_n is a group, we have $\sigma_a\tau_b \in S_n$ and $\tau_b\sigma_a \in S_n$. We observe that $\tau_b\sigma_a(x) = ax + b, x \in \mathbb{Z}/n\mathbb{Z}$. We, therefore, term $\tau_b\sigma_a$ as an affine permutation. We denote the set of all affine permutations as $\mathcal{A}$ i.e.,

$$\mathcal{A} = \{\tau_b\sigma_a | a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\}$$

It is easy to observe that $\mathcal{A}$ is also a subgroup of S_n.

Proposition 3.2. $o(\mathcal{A}) = n\phi(n)$

Proof. It is easy to show that $\tau_{b_1}\sigma_{a_1} = \tau_{b_2}\sigma_{a_2} \implies a_1 = a_2$ and $b_1 = b_2$. Therefore,

$$o(\mathcal{A}) = o(\mathbb{Z}/n\mathbb{Z}) \cdot o(\mathbb{Z}/n\mathbb{Z})^* = n\phi(n).$$

□

Proposition 3.3. *Given $a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}\ \exists\ c, d \in \mathbb{Z}/n\mathbb{Z}$ such that*

$$\sigma_a\tau_b = \tau_c\sigma_a$$

and

$$\tau_b\sigma_a = \sigma_a\tau_d.$$

Proof. As $a \in (\mathbb{Z}/n\mathbb{Z})^*$ we can get its multiplicative inverse. Let $c = ab$ and $d = a^{-1}b$. Then for $x \in \mathbb{Z}_n$ we have

$$\begin{aligned} \sigma_a\tau_b(x) &= \sigma_a(x + b) \\ &= ax + ab \\ &= ax + c \\ &= \tau_c\sigma_a(x) \end{aligned}$$

$$\Rightarrow \sigma_a \tau_b = \tau_c \sigma_a$$

Again,

$$\begin{aligned} \tau_b \sigma_a(x) &= \tau_b(ax) \\ &= ax + b \\ &= ax + ad \qquad \text{As } d = a^{-1}b \\ &= \sigma_a(x + d) \\ &= \sigma_a \tau_d(x) \end{aligned}$$

$$\Rightarrow \tau_b \sigma_a = \sigma_a \tau_d$$

□

Proposition 3.4. $\mathcal{A} = \{\sigma_a \tau_b | a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\}$

Proof. Let $\mathcal{B} = \{\sigma_a \tau_b | a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\}$. Using Proposition 3.3 we can prove $\mathcal{B} \subseteq \mathcal{A}$ and $\mathcal{A} \subseteq \mathcal{B}$. □

Corollary 3.1.

$$\mathcal{TS} = \mathcal{ST} = \mathcal{A}$$

Proof. It easily follows from the definition of $\mathcal{A}$ and Proposition 3.4. □

Definition 3.1 (Affinely Equivalent Permutations)**.** *$f, g \in S_n$ are said to be affinely equivalent if $\exists\ a, u \in (\mathbb{Z}/n\mathbb{Z})^*, b, v \in \mathbb{Z}/n\mathbb{Z}$ such that*

$$g = \tau_b \sigma_a f \tau_v \sigma_u$$

It is to be noted that a, b, u, v are not uniquely determined. For example, consider S_4. For a given f there may be 64 distinct quadruples (a, b, u, v) but $o(S_4) = 24$. Clearly, there can not be 64 distinct g's corresponding to 64 distinct quadruples. More precisely, consider $f = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 2 \end{pmatrix}$. We see that two quadruples, $(1, 0, 1, 0)$ and $(1, 2, 3, 3)$ both give the same function i.e., f and $\tau_2 f \tau_3 \sigma_3$ are the same.

Proposition 3.5. *Affine equivalence defines an equivalence relation on S_n.*

Proof. It is easy to show that the relation is reflexive and symmetric and transitive using Proposition 3.4 and subgroup property of $\mathcal{A}$. □

3.1 Counting number of Affinely Equivalent Permutations

Let $f \in S_n$. The equivalence class $\langle f \rangle$ contains permutations affinely equivalent to f. So, $o(\langle f \rangle)$ counts the number of permutations affinely equivalent to f. We try to find bounds for $o(\langle f \rangle)$. Recall the definition of affine equivalence. f and g are affinely equivalent if there exist $a, u \in (\mathbb{Z}/n\mathbb{Z})^*, b, v \in \mathbb{Z}/n\mathbb{Z}$ such that $g = \tau_b \sigma_a f \tau_v \sigma_u$. One obvious observation is stated in form of proposition below.

Proposition 3.6. $o(\langle f \rangle) \leq (n\phi(n))^2$

We try to estimate $o(\langle f \rangle)$ using the partitions formed under an equivalence relation. We define relation $\sim_f$ on $(\mathbb{Z}/n\mathbb{Z})^* \times \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^* \times \mathbb{Z}/n\mathbb{Z}$ as

$$(a_1, b_1, u_1, v_1) \sim_f (a_2, b_2, u_2, v_2) \text{ if } \tau_{b_1} \sigma_{a_1} f \tau_{v_1} \sigma_{u_1} = \tau_{b_2} \sigma_{a_2} f \tau_{v_2} \sigma_{u_2}$$

It is easy to verify that each bijection f on $\mathbb{Z}/n\mathbb{Z}$ defines an equivalence relation $\sim_f$ on $(\mathbb{Z}/n\mathbb{Z})^* \times \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^* \times \mathbb{Z}/n\mathbb{Z}$. We denote the equivalence class of (a, b, u, v) as $\langle (a, b, u, v) \rangle_f$. Observe that $o(\langle f \rangle)$ is the number of equivalence classes under the equivalence relation $\sim_f$. We claim that each of the equivalence classes under $\sim_f$ has the same order. In fact we prove a bit more.

Proposition 3.7. $o(\langle (a, b, u, v) \rangle_f) = o(\langle (1, 0, 1, 0) \rangle_f)$

Proof. We define a map $\Phi : \langle (a, b, u, v) \rangle_f \to \langle (1, 0, 1, 0) \rangle_f$ as

$$\Phi((a_1, b_1, u_1, v_1)) = (a_1^{-1} a, a_1^{-1}(b - b_1), u u_1^{-1}, v - u u_1^{-1} v_1).$$

We have

$$\tau_{a_1^{-1}(b-b_1)} \sigma_{a_1^{-1} a} f \tau_{v - u u_1^{-1} v_1} \sigma_{u u_1^{-1}} = (\tau_{a_1^{-1}(b-b_1)} \sigma_{a_1^{-1}}) \sigma_a f \tau_v (\tau_{-u u_1^{-1} v_1} \sigma_{u u_1^{-1}})$$

Using prop.(3.3) we can write RHS as

$$\begin{aligned} & (\sigma_{a_1^{-1}} \tau_{b-b_1}) \sigma_a f \tau_v (\sigma_{u u_1^{-1}} \tau_{-v_1}) \\ = \; & \sigma_{a_1^{-1}} \tau_{-b_1} \tau_b \sigma_a f \tau_v \sigma_u \sigma_{u_1^{-1}} \tau_{-v_1} \\ = \; & \sigma_{a_1^{-1}} \tau_{-b_1} (\tau_b \sigma_a f \tau_v \sigma_u) \sigma_{u_1^{-1}} \tau_{-v_1} \end{aligned}$$

For $(a_1, b_1, u_1, v_1) \in \langle (a, b, u, v) \rangle_f$ we have $\tau_{b_1} \sigma_{a_1} f \tau_{v_1} \sigma_{u_1} = \tau_b \sigma_a f \tau_v \sigma_u$. Which implies that, $\tau_{a_1^{-1}(b-b_1)} \sigma_{a_1^{-1} a} f \tau_{v - u u_1^{-1} v_1} \sigma_{u u_1^{-1}} = f$. This implies that $\Phi((a_1, b_1, u_1, v_1)) \in \langle (1, 0, 1, 0) \rangle_f$. The map Φ is thus well defined. Now consider,

$$\begin{aligned} & \Phi((a_1, b_1, u_1, v_1)) = \Phi((a_2, b_2, u_2, v_2)) \\ \Rightarrow \; & (a_1^{-1} a, a_1^{-1}(b - b_1), u u_1^{-1}, v - u u_1^{-1} v_1) \\ & = (a_2^{-1} a, a_2^{-1}(b - b_2), u u_2^{-1}, v - u u_2^{-1} v_2) \\ \Rightarrow \; & (a_1, b_1, u_1, v_1) = (a_2, b_2, u_2, v_2) \\ \Rightarrow \; & \Phi \text{ is one-one.} \end{aligned}$$

Further, given any $(A, B, U, V) \in \langle(1, 0, 1, 0)\rangle_f$, we claim that (A, B, U, V) is the image of $(aA^{-1}, b - aA^{-1}B, U^{-1}u, U^{-1}(v - V))$ under Φ. We have

$$\begin{aligned} & \tau_{b-aA^{-1}B}\sigma_{aA^{-1}}f\tau_{U^{-1}(v-V)}\sigma_{U^{-1}u} \\ = \; & \tau_b(\tau_{-aA^{-1}B}\sigma_{aA^{-1}})f(\tau_{U^{-1}(v-V)}\sigma_{U^{-1}})\sigma_u \\ = \; & \tau_b(\sigma_{aA^{-1}}\tau_{-B})f(\sigma_{U^{-1}}\tau_{v-V})\sigma_u \text{ \{Using prop.(3.3)\}} \\ = \; & \tau_b\sigma_a(\sigma_{A^{-1}}\tau_{-B}f\sigma_{U^{-1}}\tau_{-V})\tau_v\sigma_u \end{aligned} \tag{6}$$

As $(A, B, U, V) \in \langle(1, 0, 1, 0)\rangle_f$, we have $\tau_B\sigma_A f\tau_V\sigma_U = f$. Using this in eq.(6) we get,

$$\tau_{b-a^{-1}AB}\sigma_{aA^{-1}}f\tau_{U^{-1}(v-V)}\sigma_{U^{-1}u} = \tau_b\sigma_a f\tau_v\sigma_u$$

which shows that $(aA^{-1}, b - aA^{-1}B, U^{-1}u, U^{-1}(v - V)) \in \langle(a, b, u, v)\rangle_f$.

$$\begin{aligned} & \Phi((aA^{-1}, b - aA^{-1}B, U^{-1}u, U^{-1}(v - V))) \\ = \; & ((aA^{-1})^{-1}a, (aA^{-1})^{-1}(b - (b - a^{-1}AB)), \\ & u(U^{-1}u)^{-1}, v - u(U^{-1}u)^{-1}(U^{-1}(v - V))) \\ = \; & (A, B, U, V) \end{aligned}$$

This shows that Φ is onto. The proposition is thus proved. □

Clearly, $\sum o(\langle(a, b, c, d)\rangle_f) = (n\phi(n))^2$ where the sum runs over the distinct equivalence classes. From the above proposition

$$o(\langle f\rangle)o(\langle(1, 0, 1, 0)\rangle_f) = (n\phi(n))^2$$

We now state the corollary:

Corollary 3.2. $o(\langle f\rangle) = (n\phi(n))^2/o(\langle(1, 0, 1, 0)\rangle_f)$

The problem of finding $o(\langle f\rangle)$ is reduced to finding of $o(\langle(1, 0, 1, 0)\rangle_f)$. We first attempt it for the case when f is affine.

Proposition 3.8. *$o(\langle(1, 0, 1, 0)\rangle_f) = n\phi(n)$ if f is affine.*

Proof. f is affine then f can be written as $f = \tau_\beta\sigma_\alpha$.

$$\begin{aligned} & (a, b, u, v) \in \langle(1, 0, 1, 0)\rangle_f \\ \Rightarrow \; & \tau_b\sigma_a\tau_\beta\sigma_\alpha\tau_v\sigma_u = \tau_\beta\sigma_\alpha \\ \Rightarrow \; & \tau_b\tau_{a\beta}\sigma_a\sigma_\alpha\tau_v\sigma_u = \tau_\beta\sigma_\alpha \\ \Rightarrow \; & \tau_{b+a\beta}\sigma_{a\alpha}\tau_v\sigma_u = \tau_\beta\sigma_\alpha \\ \Rightarrow \; & \tau_{b+a\beta}\tau_{a\alpha v}\sigma_{a\alpha}\sigma_u = \tau_\beta\sigma_\alpha \\ \Rightarrow \; & \tau_{b+a\beta+a\alpha v}\sigma_{a\alpha u} = \tau_\beta\sigma_\alpha \\ \Rightarrow \; & b + a\beta + a\alpha v = \beta \text{ and } a\alpha u = \alpha \\ \Rightarrow \; & b = \beta - a\beta - a\alpha v \text{ and } a = u^{-1} \\ \Rightarrow \; & b = \beta - u^{-1}\beta - u^{-1}\alpha v \text{ and } a = u^{-1} \end{aligned} \tag{7}$$

The system of equations has only two independent variables viz., u and v. Clearly, this system has at most $n\phi(n)$ solutions. Now, we show that all the solutions given by (7) are distinct. For any two solutions (a_1, b_1) and (a_2, b_2) of (7) we have,

$$\begin{aligned} & (a_1, b_1) = (a_2, b_2) \\ \Rightarrow \quad & u_1^{-1} = u_2^{-1} \text{ and } \beta - u_1^{-1}\beta - u_1^{-1}\alpha v_1 = \beta - u_2^{-1}\beta - u_2^{-1}\alpha v_2 \\ \Rightarrow \quad & u_1 = u_2 \text{ and } -u_1^{-1}\beta - u_1^{-1}\alpha v_1 = -u_2^{-1}\beta - u_2^{-1}\alpha v_2 \\ \Rightarrow \quad & u_1 = u_2 \text{ and } v_1 = v_2 \end{aligned}$$

Hence the theorem. □

Corollary 3.3. *$o(\langle f \rangle) = n\phi(n)$ when f is affine.*

Proof. The proof directly follows from corollary 3.2 and prop.(3.8). □

Corollary 3.4. *Any two affine functions on $\mathbb{Z}/n\mathbb{Z}$ are affinely equivalent. Also, an affine function and a non-affine function can never be affinely equivalent.*

Proof. The proof is obvious. □

Theorem 3.1. *For any permutation f, $o(\langle f \rangle) = kn\phi(n)$, for some $k \in \mathbb{N}$.*

Proof. Consider the special type of cosets $\tau_b \sigma_a f \mathcal{A}$ of S_n. We notice that

$$\langle f \rangle = \bigcup_{a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}} \tau_b \sigma_a f \mathcal{A}.$$

As $o(\mathcal{A}) = n\phi(n)$, it is clear from the property of cosets that $o(\langle f \rangle)$ is a multiple of $n\phi(n)$. □

If we combine the theorem with corollary (3.2) we get the following corollary:

Corollary 3.5. *For a permutation f, $o(\langle 1, 0, 1, 0 \rangle_f)$ is a divisor of $n\phi(n)$.*

Note: We have given order of $\langle f \rangle$ when f is affine. Based on our calculations and experiments, we believe what we state in the form of a conjecture.
Conjecture: For any $f \in S_n$, $o(\langle f \rangle) = n\phi(n) \implies f$ is affine.

4 Non-linearity of Permutations

Definition 4.1 (Non-Linearity)**.** *Non-Linearity of a permutation $f \in S_n$, denoted by $NL(f)$ is defined as the distance of f from the set $\mathcal{A}$.*

In other words, non-linearity of $f \in S_n$ is the minimum of distances of f from affine permutations.

$$NL(f) = \min\{d_H(f, \tau_b\sigma_a) \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\}$$

Remarks: In view of corollary(3.1) the order of τ and σ in definition (3.1) and (4.1) may be interchanged. Yet another obvious remark, we state in form of proposition.

Proposition 4.1. *The number of permutations in S_n having non-zero non-linearity is given by $n! - n\phi(n)$.*

Corollary 4.1. *For $n < 4$, S_n contains all affine permutations.*

Proof. We observe that the quantity $n! - n\phi(n)$ vanishes for $n = 1, 2, 3$. Hence, no permutation in S_n has non-zero non-linearity when $n = 1, 2, 3$ i.e., all permutations in S_n are affine. □

Proposition 4.2. *Affinely equivalent permutations have the same non - linearity.*

Proof. Let $f \in S_n$. Then an affinely equivalent permutation g can be written as, $g = \tau_b\sigma_a f \tau_v \sigma_u$ where $a, u \in (\mathbb{Z}/n\mathbb{Z})^*, b, v \in \mathbb{Z}/n\mathbb{Z}$
Now,

$$\begin{aligned} NL(g) &= \min\{d_H(g, \tau_m\sigma_l) \mid l \in (\mathbb{Z}/n\mathbb{Z})^*, m \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \min\{d_H(\tau_b\sigma_a f \tau_v\sigma_u, \tau_m\sigma_l) \mid l \in (\mathbb{Z}/n\mathbb{Z})^*, m \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \min\{d_H(f, \sigma_a^{-1}\tau_b^{-1}\tau_m\sigma_l\sigma_u^{-1}\tau_v^{-1}) \mid l \in (\mathbb{Z}/n\mathbb{Z})^*, m \in \mathbb{Z}/n\mathbb{Z}\} \end{aligned}$$

Using prop.(3.1) and prop.(3.3) and absorbing the constant quantities in l and m we get

$$NL(g) = \min\{d_H(f, \tau_m\sigma_l) \mid l \in (\mathbb{Z}/n\mathbb{Z})^*, m \in \mathbb{Z}/n\mathbb{Z}\} = NL(f)$$

□

Proposition 4.3.

$$NL(f) = n - \max_{a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}} \{\#\ \textit{fixed points of}\ \tau_b\sigma_a f\}$$

Proof. We have,

$$\begin{aligned} NL(f) &= \min\{d_H(f, \sigma_a\tau_b) \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \min\{d_H(\tau_b^{-1}\sigma_a^{-1}f, I) \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \min\{d_H(\tau_b\sigma_a f, I) \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \min\{n - \#\text{ fixed points of } \tau_b\sigma_a f \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, \\ &\quad b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= n - \max\{\#\text{ fixed points of } \tau_b\sigma_a f \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, \\ &\quad b \in \mathbb{Z}/n\mathbb{Z}\} \end{aligned}$$

□

The important consequence of this proposition is that we can easily tell the upper bound on non-linearity just by observing the function f.

Corollary 4.2. *If $\tau_s\sigma_r f$ has k fixed points for some $r \in (\mathbb{Z}/n\mathbb{Z})^*, s \in \mathbb{Z}/n\mathbb{Z}$ then*

$$NL(f) \leq n - k$$

In particular, if f has k fixed points then $NL(f) \leq n - k$.

Proof. As f has k fixed points, we have

$$\max\{\#\text{ fixed points of } \tau_b\sigma_a f \mid a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\} \geq k$$

Therefore,

$$NL(f) \leq n - k$$

□

5 Algorithm for Computing Non-linearity

5.1 The Exhaustive Search Algorithm

The exhaustive search algorithm computes distance of a given permutation from every affine permutation and returns the minimum distance. For the

Algorithm 1 Naive algorithm for non-linearity of a permutation

```
1:  function NaiveNL(f,n)
2:      NL ← n
3:      Compute φ(n) numbers a_i such that gcd(a_i, n) = 1
4:      for i ← 1 ... φ(n) do
5:          for j ← 0 ... n − 1 do
6:              dist ← d(f, τ_j σ_{a_i})
7:              if NL > dist then
8:                  NL ← dist
9:              end if
10:         end for
11:     end for
12:     return NL
13: end function
```

time complexity of line 3, recall that the gcd computation of two numbers $\leq n$ takes $O(\log n)$ steps. So, the time complexity for finding a_is can be at most $O(n\log(n))$. Moreover, if we fix the size of permutation n then this step can be a part of pre-computation. So, now we consider the other parts of the algorithm. The two *For* loops require $n\phi(n)$ distance calculations. Each distance computation takes n comparisons which means $n^2\phi(n)$ comparisons

in all. The selection of the minimum from the $n\phi(n)$ distance values requires $n\phi(n)$ comparisons. So, the total number of operations needed for this computation is $n^2\phi(n) + n\phi(n)$. As $\phi(n) \sim O(n)$, the algorithm is therefore $O(n^3)$.

5.2 Improvements over Exhaustive algorithm

We define a Mode transform for permutations which in some sense is analogous to the Walsh transform [1, 11] for Boolean functions.

Definition 5.1 (Mode Transform)**.** *Let f be a permutation on $\mathbb{Z}/n\mathbb{Z}$. The mode transform of f is a function $M_f : (\mathbb{Z}/n\mathbb{Z})^* \to \{1, 2, \ldots, n\}$ defined as,*

$$M_f(\omega) = \max_{b \in \mathbb{Z}/n\mathbb{Z}} \#\{x | f(x) - \omega x = b\}$$

It is easy to observe that for a given $x_0 \in \mathbb{Z}/n\mathbb{Z}, \exists b \in \mathbb{Z}/n\mathbb{Z}$ such that $x_0 \in \{x | f(x) - \omega x = b\}$. This can be seen by taking $b = f(x_0) - \omega x_0$. This shows that $M_f(\omega) \geq 1$. Also, as the number of choices for x is limited to n, we have $M_f(\omega) \leq n$. Hence, M_f is well defined.

Proposition 5.1. *The non-linearity of a permutation f on $\mathbb{Z}/n\mathbb{Z}, n > 2$ is given by*

$$NL(f) = n - \max_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*} M_f(\omega)$$

Proof. We have

$$\begin{aligned}
NL(f) &= \min\{d_H(f, \tau_b\sigma_\omega) \mid \omega \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}\} \\
&= \min_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}} \#\{x | f(x) \neq \tau_b\sigma_\omega(x)\} \\
&= n - \max_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}} \#\{x | f(x) = \tau_b\sigma_\omega(x)\} \\
&= n - \max_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z}} \#\{x | f(x) - \omega x = b\} \\
&= n - \max_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*} \Big[\max_{b \in \mathbb{Z}/n\mathbb{Z}} \#\{x | f(x) - \omega x = b\} \Big] \\
&= n - \max_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*} M_f(\omega)
\end{aligned}$$

□

This formula helps in calculating non-linearity in $O(n^2)$ time. This can be easily seen as $M_f(\omega)$ can be calculated in $3n$ steps. We maintain frequency counters which count the number of times a particular value of b occurs when for a fixed ω, variable x is allowed to vary over all possible choices. We need n steps for assigning frequency counters to zero, n steps for computing $f(x) - \omega x$ for $x = 0 \ldots n-1$ and incrementing the frequency

counter corresponding to the value of $f(x)-\omega x$. The last n steps are needed for finding the maximum frequency which will be $M_f(\omega)$.

We can calculate $\max_\omega M_f(\omega)$ in $O(n\phi(n))$ steps which is $O(n^2)$ and thus non-linearity can be computed in $O(n^2)$ steps.
Now, we present further modification in the non-linearity formula for the case $n > 2$. We show that the maximum can actually be found from a subset of $(\mathbb{Z}/n\mathbb{Z})^*$.

Theorem 5.1. *The non-linearity of a permutation f on $\mathbb{Z}/n\mathbb{Z}, n > 2$ is given by*

$$NL(f) = n - \max\left\{\max_{\omega\in T} M_f(\omega), \max_{\omega\in T} M_f(-\omega)\right\}$$

where

$$T = \left\{x|(x,n) = 1, 1 \le x \le \left\lfloor \frac{n}{2} \right\rfloor\right\} \bigcap (\mathbb{Z}/n\mathbb{Z})^*$$

and

$$o(T) = \phi(n)/2$$

Proof. We have

$$(\mathbb{Z}/n\mathbb{Z})^* = T \cup T'$$

where,

$$T' = \left\{x|(x,n) = 1, \left\lfloor \frac{n}{2} \right\rfloor + 1 \le x \le n\right\} \bigcap (\mathbb{Z}/n\mathbb{Z})^*$$

We claim that $x \in T \iff n - x \in T'$. We see that

$$(x,n) = 1 \iff (x-n,n) = 1 \iff (n-x,n) = 1$$

There may be two cases on n:
Case 1: n is even. Then $n = 2k$ for some $k \in \mathbb{N}, k > 1$.
We have $\left\lfloor \frac{n}{2} \right\rfloor = k$. Also, $(k,n) = (k,2k) = k > 1 \implies k \notin T$

$$\begin{aligned} x \in T &\Rightarrow 1 \le x < k \\ &\Rightarrow -k < -x \le -1 \\ &\Rightarrow n-k < n-x \le n-1 \\ &\Rightarrow k < n-x \le n \\ &\Rightarrow k+1 \le n-x \le n \\ &\Rightarrow n-x \in T' \end{aligned} \tag{8}$$

Further,

$$\begin{aligned} n-x \in T' &\Rightarrow k+1 \le n-x < 2k \ \{\text{As } 2k \notin T'\} \\ &\Rightarrow -2k < x-n \le -k-1 \\ &\Rightarrow n-2k < x \le n-k-1 \\ &\Rightarrow 0 < x \le k-1 \\ &\Rightarrow x \in T \end{aligned} \tag{9}$$

From eq.(8) and eq.(9) the claim is proved for even n.
Case 2: n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{N}, k > 1$.
We have $\left\lfloor \frac{n}{2} \right\rfloor = k$.

$$\begin{aligned} x \in T &\Rightarrow 1 \leq x \leq k \\ &\Rightarrow -k \leq -x \leq -1 \\ &\Rightarrow n - k \leq n - x \leq n - 1 \\ &\Rightarrow k + 1 \leq n - x \leq n - 1 \\ &\Rightarrow n - x \in T' \end{aligned} \tag{10}$$

Further,

$$\begin{aligned} n - x \in T' &\Rightarrow k + 1 \leq n - x \leq 2k \ \{\text{As } 2k + 1 \notin T'\} \\ &\Rightarrow -2k \leq x - n \leq -k - 1 \\ &\Rightarrow n - 2k \leq x \leq n - k - 1 \\ &\Rightarrow 1 \leq x \leq k \\ &\Rightarrow x \in T \end{aligned} \tag{11}$$

Eq.(10) and eq.(11) prove the claim for odd n.
Now, from theorem (5.1) we have

$$\begin{aligned} NL(f) &= n - \max_{\omega \in (\mathbb{Z}/n\mathbb{Z})^*} M_f(\omega) \\ &= n - \max \left\{ \max_{\omega \in T} M_f(\omega), \max_{\omega \in T'} M_f(\omega) \right\} \\ &= n - \max \left\{ \max_{\omega \in T} M_f(\omega), \max_{\omega \in T} M_f(n - \omega) \right\} \\ &= n - \max \left\{ \max_{\omega \in T} M_f(\omega), \max_{\omega \in T} M_f(-\omega) \right\} \end{aligned}$$

Also, from the bijection $x \to n - x$ it is clear that $o(T) = o(T') = \phi(n)/2$ □

Proposition 5.2. *Let f be a permutation on $\mathbb{Z}/n\mathbb{Z}$ and $\omega \in (\mathbb{Z}/n\mathbb{Z})^*$. Define recurrence relation*

$$t_i = t_{i-1} + \Delta_i - \omega \text{ with } t_0 = f(0)$$

where $\Delta_i = f(i) - f(i-1), i = 1, 2, \ldots, n-1$. Then $t_i = f(i) - \omega i$.

Proof. For $i = 0$ we have $t_0 = f(0) = f(0) - 0\omega$. So the proposition is true for $i = 0$.
We consider $i > 0$

Summing the recurrence relation over 1 to r we get

$$\begin{aligned} & \sum_{r=1}^{i} t_i = \sum_{r=1}^{i} t_{i-1} + \sum_{r=1}^{i} \Delta_i + \sum_{r=1}^{i} \omega \\ \Rightarrow \quad & \sum_{r=1}^{i} t_i - \sum_{r=1}^{i} t_{i-1} = \sum_{r=1}^{i} f(i) - \sum_{r=1}^{i} f(i-1) - i\omega \\ \Rightarrow \quad & t_i = f(i) - i\omega \end{aligned}$$

□

We now give the modified algorithm. The correctness of the algorithm is implied by the above results.

Algorithm 2 Algorithm for non-linearity of a permutation using Mode Transformation

function NL_MOD(f, n)
  $max := 0$
  Compute $T = \{a_1, a_2, \ldots, a_{\phi(n)/2}\}$, where $\gcd(a_i, n) = 1$ and $a_i \leq \lfloor \frac{n}{2} \rfloor$ where $i = 1, 2, \ldots, \phi(n)/2$
  Compute differences $\Delta_i = f(i) - f(i-1), i = 1, 2, \ldots, n-1$.
  for $i := 1$ to $\phi(n)/2$ **do**
    mode:=0
    $fr_0^+ := 0, fr_1^+ := 0, \ldots, fr_{n-1}^+ := 0$
    $fr_0^- := 0, fr_1^- := 0, \ldots, fr_{n-1}^- := 0$
    $t^+ := f(0), t^- := f(0)$
    $fr_{f(0)}^+ := 1, fr_{f(0)}^- := 1$
    for $j = 1$ to $n-1$ **do**
      $t^+ := (t^+ + \Delta_j + a_i) \pmod n, t^- := (t^- + \Delta_j - a_i) \pmod n$
      $fr_{t^+}^+ := fr_{t^+}^+ + 1, fr_{t^-}^- := fr_{t^-}^- + 1$
    end for
    for $j := 0$ to $n-1$ **do**
      if $mode < fr_j^+$ **then** $mode := fr_j^+$
      end if
      if $mode < fr_j^-$ **then** $mode := fr_j^-$
      end if
    end for
    if $max < mode$ **then** $max := mode$
    end if
  end forreturn $(n - max)$
end function

The initialization and calculation steps roughly take $3n$ additions and assignment operations. The maximum value of mode transform is calculated

over $\mathbb{Z}/n\mathbb{Z}$ which requires $\phi(n)$ calculations of mode transform. Therefore the time complexity of this algorithm is $\approx 3n\phi(n)$. As, $\phi(n) = O(n)$, the algorithm is $O(n^2)$. Moreover, the computation of numbers relatively prime to n is also reduced to $\phi(n)/2$ as compared to earlier $\phi(n)$. We also observe that the algorithm has two chains of similar computations. Therefore, the time may further be reduced using 2-core parallel implementation of the algorithm.

6 Cryptographic Significance of NL and AE

Permutations are the fundamental ingredients used for embedding diffusion in a cryptosystem and hence are used as building blocks for stream and block ciphers (like RC4, AES [5, 6, 8]). Restricted permutations i.e permutations with minimum assured displacement are used in time domain speech scramblers [2, 3]. Thus generation or selection of random permutations is important for cryptological applications.

Depending upon the application, different properties need to be satisfied by the permutations. Thus it is important to analyze their cryptographic properties. As far as we know not much work has been done in this direction. Some work has been done on use of permutation polynomials for cryptographic applications [7, 9, 12, 13]. When permutations are used as S-Boxes(substitution boxes), or in collections of S-boxes of a cryptosystem, they should necessarily satisfy the following properties:

(a) It should not have many fixed points i.e., for a bijection f over $\mathbb{Z}/n\mathbb{Z}$ and a bound $b \in \mathbb{N}$, $|\{x : f(x) = x, x \in \mathbb{Z}/n\mathbb{Z}\}| \leq b$.

(b) It should not be a cyclic shift of identity permutation i.e., $f(x)$ should not have the form $f(x) = (x + u) \bmod n, u \in \mathbb{Z}/n\mathbb{Z}$.

(c) If a group of permutations is used in a cryptographic design, the permutations should not be cyclic shift of each other i.e., for f_1, f_2 and any $k \in \mathbb{N}$, the relation $f_1(x) = f_2(x + k \bmod n)$ should not hold identically.

We can include some more properties depending on the application in question.

If a set of permutations contains permutations which are cyclic shifts of one-another then knowledge of any one of them will leak information about others which can be exploited in polynomial time to reveal the other permutations. If we check affine equivalence in a given set of permutations, we can effectively avoid these types of cases. We have shown that higher the fixed point bound, lower will be the non-linearity. Since the non-linearity of the identity permutation and of all of its shifts is zero, these permutations are not suitable for cryptographic applications. However, the relevance of these properties in the field of cryptology is not fully explored as yet.

The notion of non-linearity and affine equivalence of permutations captures and generalizes the properties listed above. Permutations with high non-linearity are desirable for cryptographic. If multiple permutations are being used, they should not be affinely equivalent.

7 Conclusion

In this paper we have investigated some properties of permutations over $\mathbb{Z}/n\mathbb{Z}$ which would help in selecting good permutations for cryptographic applications. There is a scope of further exploration of the properties we have studied. In future, we will try to generalize these properties for asymmetric s-boxes.

References

[1] Braeken A. *Cryptographic Properties of Boolean Function and S-Boxes.* PhD thesis, Department Elektrotechniek-ESAT, Katholieke Universiteit Leuven, 2006.

[2] Goldburg B., Dawson E., and Sridharan S. The automated cryptanalysis of analog speech scrambles. *LNCS*, 547, 1991.

[3] Goldburg B., Sridharan S., and Dawson E. Design and cryptanalysis of transform based analog speech scramblers. *IEEE Journal of Seclected Areas in Communications*, 11(5), 1993.

[4] Carlet C. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering.* Cambridge University Press, 2010. See the chapter Boolean Functions for Cryptography and Error Correcting Codes.

[5] Rijmen V. Daemen J. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Springer-Verlag, New York, 2002.

[6] Paul G. and Maitra S. *Rc4 Stream Cipher and Its Variants.* CRC Press, 2011.

[7] Levine J. and Brawley J. V. Some cryptographic applications of permutation polynomials. *Cryptologia*, 1:76–92, 1977.

[8] Menezes A. J., Oorschot P., and Vanstone S. *Handbook of Applied Cryptography.* CRC Press, 1997.

[9] Rivest R. L. Permutation polynomial modulo 2^w. *Journal of Finite Fields and their applications*, 7:287–292, 2001.

[10] O.A. Logachev, A.A. Salnikov, and V. V. Yashchenko. *Boolean Functions in Coding Theory and Cryptography*. American Mathematical Society, 2012.

[11] Forre R. The strict avalanche criterion: Spectral properties of boolean functions and an extended definition. In Goldwasser S., editor, *Crypto 1988*, Lecture Notes in Computer Science, pages 450–468, 1988.

[12] Lidl R. and Niederreiter H. *Encyclopedia of Mathematics and their applications: Finite Fields*, volume 20. Cambridge University Press, 1997.

[13] Lidl R and Mullen G L. When does a permutation polynomial over a finite field permutes the elements of the field. *Amer. Math. Monthly*, 100:71–74, 1993.

[14] Cusik T. W. and Stanica P. *Cryptographic Boolean Functions and Applications*. Academic Press, 1 edition, 2009.