ON COUNTING CERTAIN PERMUTATIONS USED FOR SPEECH SCRAMBLING

B. Jayaramakrishnan[1], Rajesh Vijayaraghavan[2] and V. Ravichandran[3]

[1]School of Management, Circuit House Area (East),
Jamshedpur 831 001. Jharkhand, India
[2]Department of Computer Science, Courant Institute of Mathematical Sciences
New York University, New York, NY-10012, USA
[3]School of Mathematical Sciences, Universiti Sains Malaysia,
11800 USM Pulau Pinang, Malaysia

*Corresponding author: vravi@cs.usm.my

Abstract: *The shift factor of a permutation is the average of the displacement of elements. In this paper, we count the number of permutations having maximum shift factor in which adjacent elements not appearing together.*

Keywords: speech scrambling, key generation, permutations, derangements, shift factor, residual intelligibility

1. INTRODUCTION

In a scrambling system, the signal is encrypted by rearranging the input (plain text) data using permutations. When the signal is divided into portions or sub-bands, the method directs the rearrangement or jumbling the order of these portions or sub-bands. This rearrangement is enabled by a key and the inverse of this key would decrypt back the original data. The scrambling works with permutation as the key element for encryption and its inverse permutation as the key for decryption. However, not all of these permutations generated result in a scrambled signal with acceptably low Residual Intelligibility (RI). The prime requirement of any encryption algorithm is that the RI should be minimized, i.e. after permutation one should not be in a position to decipher any details from the permuted data. The problem of key selection is therefore an important issue in the design of a scrambling system.

The following are examples of permutations that can minimize RI:

- **C1** (Derangements) permutations whose elements are displaced from their original position.
- **C2** Permutations whose elements do not retain their relative adjacency with respect to the original permutation. Thus if the permutation is given by Eq. (1) below, then p_i and p_{i+1} should not be adjacent, that is, $p_i + 1 \neq p_{i+1}$.
- **C3** Permutations with maximum *shift factor*. The shift factor of a permutation is defined below.

A rearrangement p_1, p_2, ..., p_n of 1, 2, 3,..., n is called a permutation of degree n. This permutation can be written as

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix} \tag{1}$$

and for the sake of simplicity we write this permutation as $p_1, p_2, ..., p_n$. For a permutation p of degree n, given by Eq. (1), the *shift factor* is defined by

$$\alpha_p = \frac{1}{n} \sum_{i=1}^{n} \; | i - p_i |.$$

The order of displacement (OD) of a permutation p, given by Eq. (1), is defined by

$$OD(p) = \min_{i=1,\dots,n} | i - p_i |.$$

Thus the minimum distance between an element's original position and its displaced position is the OD. Derangement is a permutation where no element retains its old position after being subjected to permutation or in other words it is a permutation for which $i \neq p_i$. Thus a derangement is a permutation with an OD of at least one.

By using computer programs, Mahadeva Prasanna et al. [1] counted the number of permutations satisfying various combinations of the above conditions C1–C3. Ravichandran et al. [2] developed recurrence relations for counting the permutations except for the two cases: permutations satisfying (i) both C1 and C2, and (ii) both C2 and C3.

Our main result in this paper is a recurrence relation for the number of permutations satisfying both C2 and C3. Since the proof of our main result depends on the description of the permutations having maximum shift factor, we first review this and also provide a summary of the already known results.

2. PERMUTATION WITH THE MAXIMUM SHIFT FACTOR

High shift factor is essential for ensuring minimum or zero RI, since the permutations with high shift factor displaces the elements much farther. If the shift factor is taken to be the maximum possible value, we can describe all the permutations with the maximum shift factor.

The following theorem gives the value for the maximum shift factor among all permutations of degree *n*.

Theorem 1. *The maximum shift factor among all permutations of degree n is given by*

$$\alpha_{max} = \begin{cases} \dfrac{n}{2} & (n\ even) \\ \dfrac{n}{2}-\dfrac{1}{2n} & (n\ odd) \end{cases}$$

The maximum shift factor is attained for the permutations described in the Subsections 2.1 and 2.2.

Essentially, the proof of Theorem 1 depends on the following result which can be verified by a direct computation:

Lemma 1. *Let p and p' be permutations given by*

$$p = \begin{pmatrix} 1 & \dots & a & \dots & c & \dots & n \\ p_1 & \dots & b & \dots & d & \dots & p_n \end{pmatrix} \tag{2}$$

and

$$p' = \begin{pmatrix} 1 & \dots & a & \dots & c & \dots & n \\ p_1 & \dots & d & \dots & b & \dots & p_n \end{pmatrix} \tag{3}$$

and α_p, $\alpha_{p'}$ *be the shift factors of p, p' respectively. If max* {*a,b*} < min {*c,d*}, *then* $\alpha_p < \alpha_{p'}$.

In the case of even degree permutations, for any permutation other than those given in Subsection 2.1, we have elements satisfying the conditions of the Lemma. Therefore, the new permutation obtained using the Lemma will have higher shift factor. This can be seen directly as follows. If the permutation is not the one in Subsection 2.1, then one of the element $a = p_i$, $1 \le i, p_i \le m$ will be moved to the element $b = p_j$ where $1 \le j, p_j \le m$. Correspondingly, one of the elements $c = p_k$, $m+1 \le k, p_k \le 2m$ will be moved to the element $d = p_l$ where $m+1 \le l, p_l \le 2m$. Now max {*a,b*} < *m* and min {*c,d*} < *m*+1 and hence max {*a,b*} < min {*c,d*}. Therefore, the permutation obtained by interchanging the numbers *b* and *d* will have higher shift factor. This proves that the permutations given in Subsection 2.1 are the permutations with maximum shift factor. See Ravichandran et al. [2] for the complete proof.

2.1 Permutations of Even Degree Having Maximum Shift Factor

Let *n* be an even integer, say, *n* = 2*m*, *m* + 1. In this case, the following permutations have shift factor *n*/2:

$$p = \begin{pmatrix} 1 & 2 & \dots & m & m+1 & \dots & 2m \\ p_1 & p_2 & \cdots & p_m & p_{m+1} & \cdots & p_{2m} \end{pmatrix} \tag{4}$$

where p_1, p_2, ..., p_m is a permutation of *m* + 1, *m* + 2, ..., 2*m* and p_{m+1}, p_{m+2}, ..., p_{2m} is a permutation of 1, 2, ..., *m*. It should be noted that

$$p_i \ge i \quad \text{for} \quad i \le m \quad \text{and} \quad p_i \le i \quad \text{for} \quad i \ge m+1.$$

Also

$$\sum_{i=1}^{m} p_i = \sum_{i=1}^{m} (m+i) \quad \text{and} \quad \sum_{i=1}^{m} p_{m+i} = \sum_{i=1}^{m} i.$$

The shift factor α is given by $m = \frac{n}{2}$ (see Ravichandran et al. [2].)

2.2 Permutations of Odd Degree Having Maximum Shift Factor

Let n be an odd integer, say, $n = 2m + 1$, $m + 1$. In this case, permutations in the following classes have the shift factor $(n/2) - (1/2n)$.

This maximum is attained for the permutations described in the following three classes:

Class I consists of permutations of the form

$$\begin{pmatrix} 1 & 2 & \ldots & m & m+1 & m+2 & \ldots & 2m+1 \\ p_1 & p_2 & \cdots & p_m & m+1 & p_{m+2} & \cdots & p_{2m+1} \end{pmatrix} \tag{5}$$

where p_1, p_2, ..., p_m is a permutation of $m + 2$, $m + 3$, ..., $2m + 1$ and p_{m+2}, p_{m+3}, ..., p_{2m+1} is a permutation of 1, 2, ..., m.

Class II consists of permutations of the form

$$\begin{pmatrix} 1 & 2 & \ldots & m & m+1 & m+2 & \ldots & 2m+1 \\ p_1 & p_2 & \cdots & p_m & p_{m+1} & p_{m+2} & \cdots & p_{2m+1} \end{pmatrix} \tag{6}$$

where p_1, p_2, ..., p_{m+1} is a permutation of $m + 1$, $m + 2$, ..., $2m + 1$ and p_{m+2}, p_{m+3}, ..., p_{2m+1} is a permutation of 1, 2, ..., m.

Class III consists of permutations of the form (6) where p_1, p_2, ..., p_m is a permutation of $m + 2$, $m + 3$, ..., $2m + 1$ and p_{m+1}, p_{m+2}, ..., p_{2m+1} is a permutation of 1, 2, ..., $m + 1$.

The permutations in class I are those permutations in class II and III which fix $m+1$.

The following theorems give the number of permutations satisfying the conditions C1, C2, C3 respectively.

Theorem 2. *The number of derangement, or permutations with all the elements displaced from their original positions, is*

$$d_n = n!\sum_{r=0}^{n} \frac{(-1)^n}{r!} = \sum_{r=0}^{n} (-1)^n \binom{n}{r}(n-r)!$$

Theorem 3. *Let* t_n *denotes the number of permutations of degree n satisfying C2. Then*

$$t_n = \frac{(n+1)!}{n}\left[\frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^{n+1}}{(n+1)!}\right].$$

The above theorems can be found in Vilenkin [3]. Also the following recurrence relation is satisfied:

$$t_n = (n-1)t_{n-1} + (n-2)t_{n-2}, (n \ge 4)$$
$$t_2 = 1,\ t_3 = 3.$$

(See Ravichandran et al. [2].)

Theorem 4. *The number of permutations of degree n with maximum shift factor is*

$$c_n = \begin{cases} \left[\left(\dfrac{n}{2}\right)!\right]^2 & (n\ even) \\ n\left[\left(\dfrac{n-1}{2}\right)!\right]^2 & (n\ odd) \end{cases}$$

The result follows by counting, since the permutations with maximum shift factor are known. For example, when *n* is odd, we need to count the distinct permutations in classes I, II, and III. Since all the permutations in class I belong to both the classes II and III, we subtract the number of permutations in class I from the combined permutation of class II and class III. The proof is explained in detail in Ravichandran et al. [2].

The following result gives the number of permutations satisfying both C1 and C3.

Theorem 5. *The number of derangements with maximum shift factor is*

$$f_n = \begin{cases} \left[\left(\dfrac{n}{2}\right)!\right]^2 & (n\ even) \\ (n-1)\left[\left(\dfrac{n-1}{2}\right)!\right]^2 & (n\ odd) \end{cases}$$

We sketch the proof when n is even. Set $n = 2m$, $m + 1$. The following permutation with $p_1, p_2, ..., p_m$ as a permutation of $m + 1$, $m + 2, ..., 2m$ and $p_{m+1}, p_{m+2}, ..., p_{2m}$ as a permutation of 1, 2,..., m will have the maximum shift factor and also is deranged as seen in

$$\begin{pmatrix} 1 & 2 & ... & m & m+1 & ... & 2m \\ p_{m+1} & p_{m+2} & \cdots & p_{2m} & p_1 & p_1\cdots & p_m \end{pmatrix}$$

Hence the number of derangements with maximum shift factor in this case is

$$(m!)\cdot(m!) = \left[\left(\frac{n}{2}\right)!\right]^2 .$$

Similar proof can be given when n is odd.

The following theorem gives the number of permutations satisfying all three conditions C1, C2 and C3.

Theorem 6. *The number of permutation of degree n with maximum shift factor in which no element is fixed and no adjacent elements are mapped to adjacent elements is* [2].

$$a_n = \begin{cases} \left[t_{\frac{n}{2}}\right]^2 & (n\ even) \\ 2t_{\frac{n-1}{2}}\left[t_{\frac{n+1}{2}} - t_{\frac{n-1}{2}}\right] & (n\ odd) \end{cases}$$

3. NUMBER OF PERMUTATIONS SATISFYING C2 AND C3

In this section, we count the number of permutations having maximum shift factor with adjacent elements not appearing together.

Theorem 7. *The number of permutations with maximum shift factor and adjacent elements not appearing together is*

$$b_n = \begin{cases} \left[t_{\frac{n}{2}}\right]^2 & (n \quad even) \\ t_{\frac{n-1}{2}} \left[2t_{\frac{n+1}{2}} - t_{\frac{n-1}{2}}\right] & (n \quad odd) \end{cases}$$

Proof. Let n be even and set $n = 2m$. Consider the permutation below

$$\begin{pmatrix} 1 & 2 & \dots & m & m+1 & \dots & 2m \\ p_{m+1} & p_{m+2} & \cdots & p_{2m} & p_1 & \cdots & p_m \end{pmatrix}$$

and assume that it has the maximum shift factor and adjacent elements do not appear together. Since it has maximum shift factor, it is clear that $p_1, p_2, \dots, p_m$ is a permutation of 1, 2,..., m and $p_{m+1}, \dots, p_{2m}$ is a permutation of m + 1, ..., 2m. Since adjacent elements does not occur together, the number of possible permutations $p_1, p_2, \dots, p_m$ of 1, 2, ..., m is t_m. Similarly the number of permutations $p_{m+1}, p_{m+2}, \dots, p_{2m}$ is t_m. In this case, the number of permutations having maximum shift factor in which adjacent elements do not appear together is t_m^2 or $[t_{n/2}]^2$.

Now let n be odd and set $n = 2m + 1$. Consider the permutations in the classes I–III given Section 2.2. In class I, the number of permutations with adjacent elements not appearing together is t_m^2. In each of classes II and III, the number of permutations with adjacent elements not appearing together is $t_m t_{m+1}$. Thus when n is odd, the total number of permutations in these three classes with adjacent elements not appearing together is $2t_m t_{m+1} - t_m^2$ or $t_{(n-1)/2}\left[2t_{(n+1)/2} - t_{(n-1)/2}\right]$.

4. REFERENCES

1. Mahadeva Prasanna, S.R., Ashalatha, M.E., Nirmala, S.R. & Haribhat, K.N. (2000). Study of permutations in the context of speech privacy. *Proc. ECCAP 2000*, Allied, India, 99–106.
2. Ravichandran, V., Srinivasan, N., Jayamala, M. & Sivagurunathan, S. (2003). Permutation for speech scrambling. *J. Indian Acad. Math,* 25(1), 95–107.
3. Vilenkin, N. Ya. (1971). *Combinatorics*. Translated from Russian by A. Shenitzer and S. Shenitzer. New York-London: Academic Press.