TIME-DIVISION MULTIPLEXING SCRAMBLERS: SELECTING PERMUTATIONS AND TESTING THE SYSTEM

A. Ecker
Hahn-Meitner-Institut für Kernforschung Berlin GmbH
Glienicker Str. 100, D-1000 Berlin 39, Germany

Abstract

Selecting permutations for speech scrambling with t.d.m. means to define a suitable weight-function or metric on S_n (the full symmetric group). This can be done in a lot of different ways. We study some of that weight-functions and point out which one should be preferred. An algorithm is given to generate permutations with a prescribed weight. Some hints are given how to compute approximately the distribution function of some weight-functions. Finally rank correlation methods are recommended for testing a t.d.m.-system.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 399-415, 1985.

1. Introduction

We are mainly concerned with some open questions from [2] (see also Chap. 9 of the book [1]). Selecting permutations for speech scrambling with t.d.m. means to define a suitable weight-function or metric on S_n (the full symmetric group). This can be done in a lot of different ways (see [12] p.84). In speech scrambling Houghtons shift factor

$$m_1(\delta) = \sum_{i=1}^{n} |\delta(i) - i| \qquad (\delta \in S_n, n \geq 1)$$

may be taken as a weight function. We tried to use the generalized weight-functions m_2, m_3,... etc.

$$m_k(\delta) = \sum_{i=1}^{n} |\delta(i) - i|^k \qquad (k \geq 1)$$

They are of independent interest from a combinatorial, number-theoretical and probabilistic point of view (see [5, 6], [10]). A thorough study reveals that m_2 should be preferred. An algorithm is given to generate permutations with a prescribed weight. The distribution functions of m_k approach a normal distribution (mean and variance for k = 1,2 are known) for large n. This approximation is good, even if n is small ($n \geq 5$). To compute the distribution function by combinatorial methods seems to be extremely difficult, only a small number of values are known exactly. m_2 is related to the problem of representing an integer number as a sum of squares.

Compared with other crypto-systems speech scramblers have the capability for testing. The approach taken in [2] for testing a t.d.m.-system is unsatisfactory because no statistical methods are used. We recommend rank correlation methods (see [10]) and

that means for example to use Spearman's ρ based on m_2.

It should be noticed that we used the book [2] in its original form as a report (Arbeitsberichte des Instituts f. Mathematische Maschinen u. Datenverarbeitung (Informatik). Bd. 14,9; Erlangen, März 1982). All citations, page numbers etc. are given with respect to that original version of [2].

2. Weights on groups

Let G denote a (multiplicative written) finite group with unit element id and N the natural numbers (zero included).

A mapping

$$p: \quad G \to N$$

will be called a weight-function on G, if

(1) $p(a) = 0 \iff a = id \quad (a \in G)$.

(2) $p(a) = p(a^{-1})$ for all $a \in G$.

(3) $p(a \cdot b) \quad p(a) + p(b)$ for all $a,b \in G$.

By means of $d_p(a,b) = p(a \cdot b^{-1})$ we can associate a metric on G to each weight-function on G. This metric has the property: $d_p(a,b) = d_p(a \cdot c, b \cdot c)$ for any $c \in G$; such a metric is called right-invariant. Conversely if there is a right-invariant metric d on G, a weight-function $p_d(a) = d(a, id)$ on G is associated to d. We are only interested in $G = S_n$, where S_n is to be understood as the full symmetric group on $\{1,2,\ldots, n\}$. There are many ways to define a metric on S_n (see for example [4]). Five common examples are given below, where $\|a\|_p$ is written instead of p(a) to emphasize the relationship to some well-known norm-functions.

Examples $\quad \sigma, \pi \in S_n \quad (n \geq 1)$

a.
$$\|\sigma\|_k = \sum_{i=1}^{n} |\sigma(i) - i|^k \qquad (k = 1,2,\ldots)$$
$$d_k(\sigma, \pi) = \sum_{i=1}^{n} |\sigma(i) - \pi(i)|^k$$

b. $\|\sigma\|_I$ = number of inversions in σ (if $k<l$ and $\sigma(k)>\sigma(l)$ we call this an inversion of σ).

$d_I(\sigma,\pi)$ = the minimum number of pairwise adjacent transpositions needed to bring $\{\sigma^{-1}(1),\ldots,\sigma^{-1}(n)\}$ into the order $\{\pi^{-1}(1),\ldots,\{\pi^{-1}(n)\}$. Here σ^{-1} and π^{-1} are the permutations inverse to σ and π.

c.

$\|\sigma\|_T$ = the minimum number of transpositions required to bring $\{\sigma(1),\ldots,\sigma(n)\}$ into the order $\{1,2,\ldots,n\}$.

$d_T(\sigma,\pi)$ = the minimum number of transpositions required to bring $\{\sigma(1),\ldots,\sigma(n)\}$ into the order $\{\pi(1),\ldots,\pi(n)\}$.

d. $\|\sigma\|_\infty = \max_{i=1,\ldots,n} |\sigma(i)-i|$

$d_\infty(\sigma,\pi) = \max_{i=1,\ldots,n} |\sigma(i)-\pi(i)|$

e. $\|\sigma\|_H = |\{i \mid \sigma(i)\neq i\}|$ (Hamming-Norm)

$d_H(\sigma,\pi) = |\{i \mid \sigma(i)\neq\pi(i)\}|$ (Hamming metric)

We have the following inequalities

$$\|\sigma\|_\infty \leq \|\sigma\|_1 \leq \|\sigma\|_2 \leq \cdots \leq \|\sigma\|_k$$

for all $\sigma \in S_n$.

For a general review of metrics on discrete groups and semigroups see [3].

3. Combinatorics

We start our investigations on weight-functions on the S_n by a combinatorial approach. We are especially interested in $\|\cdot\|_1$ and $\|\cdot\|_2$ and use the notation $m_k(\sigma) = \|\sigma\|_k$ ($\sigma \in S_n$) given by J.L. Davison [5,6]. Let $\varrho \in S_n$ be the reverse permutation $\varrho(i) = n+1-i$ $(1 \leq i \leq n)$. Throughout the paper we will write $\varrho = (n, n-1, \ldots, 1)$ and more general if $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$

is any permutation, then we will write $\delta = (\delta(1), \delta(2), \ldots, \delta(n))$. Multiplication $\delta \cdot \pi$ ($\delta, \pi \in S_n$) of permutations goes from right to left, e.g. if $\delta = (2,3,4,1)$, $\pi = (4,1,3,2)$ then $\delta \cdot \pi = (1,2,4,3)$.

Lemma 3.1 If $\delta \in S_n$, then $m_k(\delta) \leq m_k(\varepsilon)$ and $m_k(\delta)$ is an even integer for any $k \geq 1$.

Lemma 3.2 The maximal values attained by m_1 and m_2 are

$$M_{1,n} = m_1(\varepsilon) = \left\{ \begin{array}{l} \frac{n^2}{2}, \text{ if } n \text{ is an even number} \\ \frac{n^2-1}{2}, \text{ if } n \text{ is an odd number} \end{array} \right\} = [\frac{n^2}{2}]$$

$$M_{2,n} = m_2(\varepsilon) = \frac{1}{3} n(n^2-1)$$

(We use the shorthand notations M_1, M_2).

In table 3.1 we have listed the maximal values for the different weight-functions considered in section 2. Instead of $\|\cdot\|_T$, $\|\cdot\|_I$ ... etc., we use the shorthand notations T, I... and so on. As can be seen from table 3.1 the domain of the functions H, ∞, T is very small related to the number n! of permutations. That means it is impossible to make strong distinctions between different permutations.

weight-function	maximal value
m_2	$\frac{1}{3}n(n^2-1)$
m_1	$[\frac{1}{2}n^2]$
I	$\frac{1}{2} n(n-1)$
H	n
∞	n-1
T	n-1

Tab. 3.1

A useful result due to Cayley states that $T(\delta) = n - C(\delta)$, where $C(\delta)$ is the number of cycles in δ. If a permutation has an inversion at (k,l), $1 \leq k < l \leq n$, that means $\delta(k) > \delta(l)$ then $\delta(k) - \delta(l)$ is called the weight of that inversion.

Lemma 3.3 Let $V(\delta)$ denote the sum of weights taken over all inversions that δ has, then

$$m_2(\delta) = 2V(\delta).$$

Lemma 3.4 If $\tilde{\delta} \in S_{n-2}$ $(n \geq 3)$ we can construct a $\delta \in S_n$ with

$$m_k(\delta) = 2(n-1)^k + m_k(\tilde{\delta}).$$

Theorem 3.1 For $k = 1,2$; $m_k(S_n) \subset [0, M_k] = I_k$ and if $n \geq 4$, let w be an even integer, $w \in I_k$. Then, there exists a $\delta \in S_n$ with $m_k(\delta) = w$.

Remarks The proof of theorem 3.1 goes through even if $k \geq 3$, see Davison [6], Theorem 1. p. 72. It should be noted that Davisons proof together with some corollaries are only true if $k \geq 3$. As can be seen from the proof of theorem 3.1 the value M_2 is attained by m_2 only if $\delta = \xi$ and this remains true for $k \geq 3$ and M_k. What concerns m_1 it can be seen by examples that it is possible to have $m_1(\delta) = M_1$ and $\delta \neq \xi$. In the case $k \geq 3$ we have $M_k - 4 \notin m_k(S_n)$ for $n \geq 3$ and that means not all even values in $[0, M_k]$ will be attained by m_k. Let $k=3$ and $n \geq 10$ then all even numbers in $[0, M_3 - 112]$ are in the range of m_3. There exists indeed always numbers α_k, n_k for all $k \geq 1$ that have the properties: m_k attains on S_n all even numbers in $[0, M - \alpha_k]$ for $n \geq n_k$. An optimal selection for $k=1,2$ will be $n_1 = 2$, $\alpha_1 = 0$ and $n_2 = 4$, $\alpha_2 = 0$. In case $k > 3$ there are no nontrivial values of n_k, α_k known (see Davison [6] 3.p.74).

Definition 3.1 Let r be a real number, $r \geq 0$.

$$S(\|\cdot\|_a, n, r) = \{\delta \mid \delta \in S_n, \ \|\delta\|_a = r\} \quad (a = 1,2,\ldots,I,T,\infty,H)$$

$$B(\|\cdot\|_a, n, r) = \{\delta \mid \delta \in S_n, \ \|\delta\|_a \leq r\}$$

$|S(\cdot,\cdot,\cdot)|$ or $|B(\cdot,\cdot,\cdot)|$ denotes the number of elements in that sets.

Theorem 3.2 We have

$$|S(m_1, n, M_1)| = \begin{cases} \left(\frac{n}{2}!\right)^2 & \text{if } n \text{ is an even number.} \\ n \cdot \left(\frac{n-1}{2}!\right)^2 & \text{if } n \text{ is an odd number.} \end{cases}$$

Theorem 3.3 We have for $\delta \in S_n (n \geq 2)$,

$$m_2(\delta) + m_2(\delta \cdot \varsigma) = M_{2,n}$$

and $$m_2(\varsigma \cdot \delta) = m_2(\delta \cdot \varsigma).$$

Corollary 3.3.1 Let $n \geq 4$, and let w be an even integer, $w \in [0, \frac{1}{3}n(n^2-1)]$. Then, there exists a $\delta \in S_n$ with $m_2(\delta) = w$.

Lemma 3.5 Let $n \geq 5$, then $n(n^2-1)/6 \leq (n-1)((n-1)^2-1)/3$ and equality holds if and only if $n=5$.

Lemma 3.6 Let $n \geq 5$ and w an integer number $w \in [\frac{1}{6}n(n^2-1), \frac{1}{3}n(n^2-1))$. Then, either $\bar{w} = \frac{1}{3}n(n^2-1) - w \leq \frac{1}{3} \cdot 4 \cdot (4^2-1)$ or there exists a least integer number $\bar{n}$, $5 \leq \bar{n} < n$ and $\bar{w} \in (\frac{1}{6}\bar{n}(\bar{n}^2-1), \frac{1}{3}\bar{n}(\bar{n}^2-1))$.

Lemma 3.7 Let $n \geq 5$ and w an even integer with $\frac{1}{6}n(n^2-1) \leq w < \frac{1}{3}n(n^2-1)$. Then exists a permutation $\bar{\delta} \in S_{\bar{n}}$ with $\bar{n} < n$ and $\| \tilde{\delta} \cdot \varsigma \|_2 = w$, where $\tilde{\delta}$ is an extension of $\bar{\delta}$ from $S_{\bar{n}}$ to S_n.

$\tilde{\delta}$ is defined by $\tilde{\delta}(i) = i$ for $i = \bar{n}+1, \ldots, n$.

This gives us a constructive method for finding for any given even number w, $0 \leq w \leq \frac{1}{3}n(n^2-1)$ a permutation $\delta \in S_n$ with $\| \delta \|_2 = w$. We have thus proved any given integer w may be (constructive!) represented as a sum of squares (see Davison [5] Th.1.).

Example $\delta \in S_8$, $\| \delta \|_2 = 128$ we are looking for such a permutation.

(1) $w = 128$, $\frac{1}{6} \cdot 8 \cdot 3 = 84 < 128 < 168 = \frac{1}{3} \cdot 8 \cdot 35$, $n = 8$

(2) $\bar{w} = 40$, $\frac{1}{6} \cdot 6 \cdot 35 = 35 < 40 < 70 = \frac{1}{3} \cdot 6 \cdot 35$, $\bar{n} = 6$

(3) $\bar{\bar{w}} = 30$, $\frac{1}{6} \cdot 5 \cdot 24 = 20 < 30 < 40 = \frac{1}{3} \cdot 5 \cdot 24$, $\bar{\bar{n}} = 5$

(4) $\bar{\bar{\delta}} = (3,5,2,4,1) \in S_5$, $\| \bar{\bar{\delta}} \|_2 = 30$

(5) $\tilde{\bar{\delta}} = (3,5,2,4,1,6) \in S_6$, $\| \tilde{\bar{\delta}} \|_2 = 30$

$\bar{\delta} = (3,5,2,4,1,6) \cdot \underbrace{(6,5,4,3,2,1)}_{\varsigma} = (6,1,4,2,5,3)$

$\| \bar{\delta} \|_2 = 40$

(6) $\tilde{\delta} = (6,1,4,2,5,3,7,8) \in S_8$, $\| \tilde{\delta} \|_2 = 40$

$\delta = (8,7,3,5,2,4,1,6) = \tilde{\delta} \cdot \varsigma$

$\| \delta \|_2 = 128 = 7^2+5^2+0^2+1^2+3^2+2^2+6^2+2^2$

It is possible to generate immediately a second permutation of m_2-weight 128. We note that by theorem 3.3 it is admissible to multiply by ϱ from the left side in steps (5) and (6) above. This gives:

$$\sigma_2 = (5,7,4,6,3,8,2,1)$$
$$128 = 4^2+5^2+1^2+2^2+2^2+2^2+5^2+7^2$$

Taking into consideration all possible combinations of left and right multiplication by ϱ gives four permutations at all.

$$\sigma_3 = (8,7,1,6,3,5,2,4)$$
$$128 = 7^2+5^2+2^2+2^2+2^2+1^2+5^2+4^2$$
$$\sigma_4 = (3,8,5,7,4,6,2,1)$$
$$128 = 2^2+6^2+2^2+3^2+1^2+0^2+5^2+7^2$$

In Figure 3.1 another approach for generating permutations of m_2-weight 128 is seen. We will not go into the details of an algorithm that generates a lot of different permutations. Our description is only an informal one a more formal treatment will be given elsewhere.

There are important relations between the various weight-functions which generally take the form of inequalities.

Theorem 3.4 Let $\sigma \in S_n$, then

(U1) $2I(\sigma) \leq m_2(\sigma) \leq 2(n-1)\cdot I(\sigma)$

(U2) $m_2(\sigma)/n-1 \leq m_1(\sigma) \leq \text{Min}\{m_2(\sigma), (n\cdot m_2(\sigma))^{\frac{1}{2}}\}$

(U3) $m_2(\sigma) \geq \text{Max}\{4/3I(\sigma)\cdot(1+I(\sigma)/n), 2I(\sigma)\}$
(Durbin-Stuart inequality)

(U4) $I(\sigma) + T(\sigma) \leq m_1(\sigma) \leq 2I(\sigma)$
(Diaconis-Graham inequality)

The Diaconis-Graham inequality suggests that the difference between I and m_1 is not very great. The results in Table 3.1 suggest that H,∞ and T are unsuitable for use, having a very small range. There remains only m_2 that has the largest range and indeed as Lemma 3.3 shows is of a kind essentially different from I and m_1.

$\delta\sim = (\delta(1), \delta(2), \cdots, \delta(n), n+1)$

$\delta+ = (1, \delta(1)+1, \delta(2)+1, \cdots, \delta(n)+1)$

$(\delta \in S_n)$

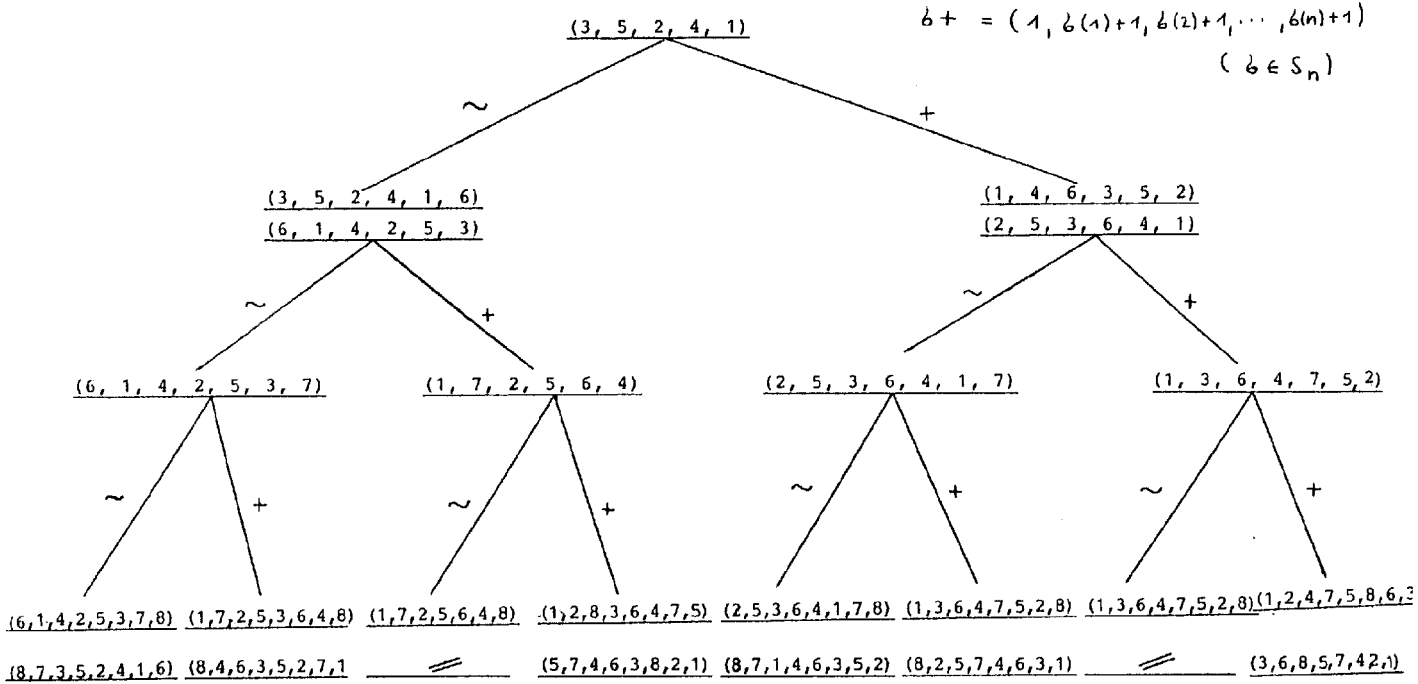

Fig. 3.1

Definition 3.2 Let $\|\cdot\|_a$ ($a = 1,2,\ldots,I,T,\infty,H$) be a weight-function on S_n ($n\geq 1$). Then, the map

$$f_{a,n} : [0,M] \to [0,n!]$$

where $M = \mathrm{Max}\{\ \|\sigma\|_a \mid \sigma \in S_n\}$ and

$$f_{a,n}(r) = \left| S\ (\ \|\cdot\|_a, n, r) \right|,\ r \in [0,M]$$

is called the distribution-function of $\|\cdot\|_a$.

From theorems 3.1, 3.2 we know $f_{1,n}(M_1)$, $f_{2,n}(M_2) = 1$ and $f_{i,n}(0) = 1$, $f_{i,n}(r) = 0$ if r is an even integer ($i = 1,2$). The distribution-function $f_{2,n}$ is symmetric about $\frac{1}{6}n(n^2-1)$.

Lemma 3.8 $f_{2,n}(r) = f_{2,n}(M_{2,n}-r)$, $r \in [0,M_2]$ an integer number.

$$f_{2,n}(r) \geq n-3 \text{ for } n\geq 4 \text{ and } r\neq 0,M_2.$$

In Table 3.2 we have computed some values of $f_{2,n}(n\geq 4)$.

r	$f_{2,n}(r)$	r
0	1	M_2
2	$n-1$	M_2-2
4	$3+\frac{1}{2}n(n-5)$	M_2-4
6	$\frac{1}{6}n(n^2+59)-2n^2-14$	M_2-6

Tab. 3.2

To compute the distribution-functions of m_1 and m_2 by combinatorial methods until now nobody succeeded.

4. Statistics

An example from Kendall [10] p.3 will clarify the discussion. Consider a number of boys (or girls) ranked according to their ability in mathematics and in musics:

Boy	A	B	C	D	E	F	G	H	I	J
Mathematics (δ)	7	4	3	10	6	2	9	8	1	5
Music (π)	5	7	3	10	1	9	6	2	8	4

We are interested in whether there is any relationship between ability in mathematics and music. In statistics widely used non-parametric measures of associations such as Kendall's τ and Spearman's ϱ lead to natural metrics or weight-functions on S_n. Statisticians most often normalize metrics so that they have the properties of a correlation coefficient. The translation is the following one: if d is a metric on S_n and its maximal value is M, define a rank correlation coefficient by:

$$K(\pi,\delta) = 1 - \frac{2\,d(\pi,\delta)}{M}$$

Most of the metrics that we mentioned in section 2. were known for a long time in statistics as measures of disarray.

$$\tau(\pi,\delta) = 1 - \frac{2\cdot I(\pi\cdot\delta^{-1})}{\frac{1}{2}n(n-1)} \qquad \text{(Kendall, 1938)}$$

$$\varrho(\pi,\delta) = 1 - \frac{6\cdot m_2(\pi\cdot\delta^{-1})}{n^3-n} \qquad \text{(Spearman, 1904)}$$

$$R(\pi,\delta) = 1 - \frac{2\cdot m_1(\pi\,\delta^{-1})}{\left[\frac{1}{2}n^2\right]} \qquad \text{(Spearman's footrule, 190}$$

Most of the combinatorial results given in section 3. are therefore known in statistics, e.g. nearly all results of Davison [5,6].

We look at weight-functions now from the point of view of probability theory. Then S_n is the sample space and a weight-function is a random variable on that sample space. We assign the probability 1/n! to each event (permutation) in S_n. As can be seen from a graphical representation the distribution of the weight-functions corresponds with the normal curve. A limit theorem for $\|\cdot\|_I$ and $\|\cdot\|_T$ was given by Feller [8], p. 256, what concerns $\|\cdot\|_1$, $\|\cdot\|_2$ the limiting normality was proved by Kendall [10] Chap. 5.8, p. 72 by computation of higher moments or one can use Hoeffding's [9] Th. 3, p.560 combinatorial central limit theorem. In Table 4.1 mean and variance of m_1, m_2, I and T are given. Its now very easy to calculate approximately the number of permutations $\delta \in S_n$ with $r_1 \le \|\delta\|_a \le r_2 (a = I, T, m_1, m_2)$. Let

$$x_1 = \frac{r_1 - (E(\|\cdot\|_a)+1)}{(Var(\|\cdot\|_a)^{1/2}} \qquad x_2 = \frac{r_2 - (E(\|\cdot\|_a)-1)}{(Var(\|\cdot\|_a))^{1/2}}$$

then we have approximatively

$$n! \cdot \frac{1}{(2\pi)^{1/2}} \int_{x_1}^{x_2} e^{-\frac{1}{2}x^2} dx \qquad (1)$$

permutations $\delta \in S_n$ with $r_1 \le \|\delta\|_a \le r_2$.

weight-function	mean	variance
m_1	$\frac{1}{3}(n^2-1)$	$\frac{2}{45}n^3 + O(n^2)$
m_2	$\frac{1}{6}n(n^2-1)$	$(\frac{n^3-n}{6})^2 \cdot \frac{1}{n-1}$
T	n-log n	log n
I	$\frac{1}{4}n^2$	$\frac{1}{36}n^3$

Tab. 4.1

In Table 4.1 for T, I only the leading terms of the mean and variance are indicated. The results in Table 4.1 suggest again that m_2 should be preferred. Of the four metrics m_2 has the greatest variability.

From the report of Beth et al. [2] we have taken the distribution of m_1 on S_8 and listed in Table 4.2. In Table 4.3 we have calculated that distribution by formula (1) by means of a HP25 pocket-caluclator. In comparison with Table 4.2 it becomes quite clear that for all practical purposes such an approximation is good enough.

m_1-weight	score	m_1-weight	score
0	1	20	5708
2	7	22	5892
4	33	24	5452
6	115	26	4212
8	327	28	2844
10	765	30	1764
12	1523	32	576
14	2553		
16	3696		
18	4852		

Tab. 4.2 Distribution of m_1 on S_8

m_1-weight	approximate score	true score	error in %
22	6551	5892	+ 11
22 - 24	12006	11344	+ 6
22 - 26	15957	15556	+ 2,5
22 - 28	18274	18400	- 0,7
22 - 30	19433	20164	- 3,6
22 - 32	19920	20740	- 4
32	487	576	- 15

Tab. 4.3 Normal approximation to the distribution of m_1 on S_8.

The distribution of m_2 on S_n is known for n = 4-13 from tables given by Kendall [10] (Appendix Table 2, pp. 174-177), if $n \geq 14$ then the normal approximation is good enough.

5. Testing a t.d.m.-system.

We look at an example given by Beth et al. [2], pp. 136, 140. Six different texts together with their intelligibility and the permutation used for scrambling are listed in Table 5.1. This gives the following ranking.

$$\begin{array}{cccccccc} & & & & & \overbrace{\quad\quad\quad} & & \\ 1 & 2 & 3 & 4 & 5 & 1/2 & 5 & 1/2 \\ 1 & 3 & 4 & 5 & & 2 & & 6 \end{array}$$

where equal weights of the last two permutations give rise to ties. We then have

$$\varsigma = 1 - \frac{16}{35} = 0.56$$

where the rank correlation coefficient ς is modified because of the tied ranks (see Kendall [10] Chap. 3). The standard error of ς is $\frac{1}{\sqrt{5}} = 0.45$. Thus the observed value is 0.56/0.45 = 1.24 times the standard error. This is barely significant.

text no.	permutation	intelligibility	m_1-weight
1	(1,2,3,4,8,6,5,7)	1	6
2	(7,1,3,4,5,2,6,8)	3	12
3	(7,2,6,3,4,5,8,1)	4	20
4	(6,4,8,1,2,7,3,5)	5	26
5	(5,6,7,8,1,2,3,4)	2	32
6	(6,5,8,7,2,1,4,3)	6	32

Tab. 5.1

Rank order statistics are thus well-suited for use in testing a t.d.m.-system. What concerns refinements and further possibilities we refer to Kendall [10]. We emphasize that a thorough testing of a t.d.m.-system should improve its security.

References

[1] H. Beker and F. Piper: Ciper Systems. Northwood Books, London(1982).

[2] Th. Beth, P. Heß, K. Wirl: Kryptographie. Teubner, Stuttgart (1983).

[3] G. Cohen and M. Deza: Distances invariantes et L-cliques sur certains demi-groupes finis. Math.Sci.Humaines 67,(1979), 49-69.

[4] G. Cohen and M. Deza: Some metrical problems on S_n. Annuals of discrete math. 8, (1980), 211-216.

[5] J.L. Davison: A result on sums of squares. Cand. Math. Bull. 18(3),(1975), 425-426.

[6] J.L. Davison: Some mappings associated with permutation groups. Canad. Math. Bull. 20(1),(1977), 71-75.

[7] P. Diaconis and R.L. Graham: Spearman's footrule as a measure of disarray. J. Roy. Statist. Soc. Ser.B39-2, (1977), 262-268.

[8] W. Feller: An Introduction to Probability Theory and Its Applications, Vol. 1, Wiley, New York (1968), 3rd edn..

[9] W. Hoeffding: A combinatorial central limit theorem. Ann. Math. Statist. 22, (1951), 558-566.

[10] M.G. Kendall: Rank Correlation Methods. Griffin, London (1970), 4th edn..

[11] M.R. Lagrange: Quelques résultats dans la métrique des permutations. Ann. Sci. Ecole Norm. Sup. 79 (1962a), 199-241.

[12] N.J.A. Sloane: Encryption by Random Rotations. Lecture Notes in Computer Science Vol. 149, Springer Verlag (1983), pp. 71, Cryptography (Proc., Burg Feuerstein 1982, Ed. Th. Beth