SIAM J. ALG. DISC. METH.
Vol. 8, No. 3, July 1987

004

PERMUTATIONS WITH RESTRICTED DISPLACEMENT*

HENRY BEKER† AND CHRIS MITCHELL‡

Abstract. The permanent of an n by n (0, 1) circulant matrix is known to be equal to the number of permutations on n objects satisfying certain positional restrictions. The size of this number is of major importance for the design of certain analogue speech scramblers, as well as being a generalisation of certain "classical" enumeration problems. In this paper a new method is given for evaluating this permanent, which gives as corollaries many of the previously known results. The analogue speech scrambling scheme is also used to motivate a second enumeration problem, about which little seems to be known.

Key words. speech security, cryptography, permanents, analogue speech scramblers, derangements, menages

AMS(MOS) subject classifications. 05A15, 15A15, 94A60

1. Introduction. In this paper we consider a permutation enumeration problem that is of interest for two main reasons. First, it is a classical combinatorial problem, the study of certain cases of which goes back to the last century. Second, it is of considerable practical significance in the field of cryptography, in particular to the designers of time element speech scramblers.

The set of permutations that concern us here we call $A(n, k)$, where $1 \leqq k \leqq n$, and $A(n, k)$ contains permutations of $\{1, 2, \cdots, n\}$. More formally, we define

$$A(n,k) = \{\pi \in S_n : \overline{i\pi} \in \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-1}\} \text{ for every } i\}$$

where the $\bar{}$ indicates the equivalence class modulo n.

In a combinatorial context, $|A(n, k)|$ has been studied under many guises; in particular note that evaluating $|A(n, k)|$ for $k = n - 1$ is the "problème des rencontres," and for $k = n - 2$ is the "problème des ménages." In addition, $|A(n, k)|$ is equal to the permanent of a certain (0, 1) n by n matrix. For a study of results in this context the reader is referred to Minc's unique book [11].

$|A(n, k)|$ is also of considerable practical significance because it is equal to the number of different "scrambling patterns" that can be used in a certain type of time element scrambling speech encryption device. For a more general introduction to this type of application see [1]–[4] and [12].

In this paper we consider a new approach to the evaluation of $|A(n, k)|$ which gives a direct method of computing it as the sum of the traces of the nth powers of $[(k-1)/2]$ matrices containing only zeros and ones. This new approach gives as immediate corollaries both the recurrence relations of Metropolis, Stein and Stein [9], and a number of previously well-known results.

Although the computational method requires a prohibitively large amount of computer storage for practical use in computing $|A(n, k)|$ for values of k much in excess of 12, it enables the computation of $|A(n, k)|$ for values of n and k not previously accessible. In particular, since the running time of the computation method is polynomial in n for fixed k, values of $|A(n, k)|$ can be directly computed for relatively large values of n given that k is sufficiently small. It is not surprising that computing $|A(n, k)|$ seems a difficult problem, since Valiant ([17] and [18]) has shown that evaluating the permanent of a (0, 1) matrix is a #P-complete problem (see also Garey and Johnson [5]).

* Received by the editors September 3, 1985; accepted for publication (in revised form) September 11, 1986.

† Racal-Guardata Ltd., Fleet, Hampshire GU13 8BU, England.

‡ Hewlett-Packard Ltd., Stoke Gifford, Bristol BS12 6QZ, England.

2. The combinatorial problem. Throughout this paper we will write $a(n, k)$ for the cardinality of the set $A(n, k)$, i.e.,

$$a(n,k) = |\{\pi \in S_n : \overline{i\pi} \in \{\overline{i}, \overline{i+1}, \cdots, \overline{i+k-1}\} \text{ for every } i\}|.$$

As in [11], $a(n, k)$ can also be defined as the permanent of the n by n matrix $Q(n, k)$, where

$$Q(n,k) = \sum_{i=0}^{k-1} P^i$$

and where P denotes the n by n permutation matrix with a one in positions $(1, 2)$, $(2, 3)$, $\cdots$, $(n-1, n)$, $(n, 1)$.

Explicit formulae for $a(n, k)$ have only been derived for values of k either near 0 or near n. We first consider the known results for which k is close to n.

Clearly $A(n, n) = S_n$, and hence $a(n, n) = n!$. As noted above, evaluating $a(n, n-1)$ is the well-known "problème des rencontres," and $a(n, n-1)$ is equal to the number of elements of S_n having no fixed point. The number $a(n, n-1)$ is often written as D_n (the "derangements number"), and is discussed in many combinatorial texts, see for example [7, pp. 541–542]. Similarly, evaluating $a(n, n-2)$ is also a well-known problem, commonly called the "problème des ménages." The solution for both these problems goes back to the last century; according to [6], a formula for $a(n, n-2)$ was obtained by Cayley and Muir in 1878.

The evaluation of $a(n, n-3)$ was first considered in [14], which contains no explicit formula but does give an asymptotic result. Yamamoto [20] considered the same problem, but it was Moser [13], who first produced an explicit formula for $a(n, n-3)$, which is, however, rather complex. Whitehead [19] has more recently considered the problem of evaluating $a(n, n-4)$.

In summary we have the following.

Result 2.1. (i) $a(n, n) = n!$, $n \geqq 1$.

(ii) $a(n, n-1) = n! \sum_{i=0}^{n} (-1)^i/i!$, $n \geqq 2$.

(iii) $a(n, n-2) = \sum_{i=0}^{n} (-1)^i . 2n . \binom{2n-i}{i} . (n-i)!/(2n-i)$, $n \geqq 3$ (Touchard (see [6] and [15])).

For Moser's formula for $a(n, n-3)$ the interested reader is referred to [13].

Second, we consider results for small k. The cases $k = 1$ and 2 are trivial, and simple recurrence relations for $k = 3$ and 4 have been derived by Minc (see [10] or [11]). In addition, Metropolis, Stein and Stein [9] give recursion formulae for $a(n, k)$ for $k \leqq 9$.

In summary we have the following.

Result 2.2. (i) $a(n, 1) = 1$, $n \geqq 1$.

(ii) $a(n, 2) = 2$, $n \geqq 2$.

(iii) $a(n, 3) = a(n-1, 3) + a(n-2, 3) - 2$, $n \geqq 5$, $a(3, 3) = 6$ and $a(4, 3) = 9$.

(iv) $a(n, 4) = a(n-1, 4) + a(n-2, 4) + a(n-3, 4) - 4$, $n \geqq 7$, $a(4, 4) = 24$, $a(5, 4) = 44$ and $a(6, 4) = 80$.

The recursion formulae of [9] for $5 \leqq k \leqq 9$ are much more complex.

3. Time element speech scramblers. The practical application of permutations in $A(n, k)$ is in a certain kind of speech scrambler called a *time element scrambler*. There are a variety of types of time element scrambler systems, but they all employ the same general principle. The technique relies on the scrambler "recording" segments of speech, and then transmitting these segments in a different order.

More specifically, in a conventional so-called *hopping window* time element scrambler, the analogue speech signal is first divided into equal time periods called *frames*. Each frame is then further subdivided into a fixed number n of small equal time periods

called *segments*, where the length of a segment would typically be of the order of 25–50 milliseconds. The scrambling is then achieved by transmitting the segments within a frame in a permuted order. At the receiver the inverse permutation is used to recover the original speech.

A typical system for $n = 8$ is illustrated in Fig. 1 below. For a more detailed discussion of the design considerations for such a device, such as the choices for n, the segment length and the selection of permutations to use in the scrambler, the reader is referred to [3]. The important thing to note here is that the system delay for such a device will be $2nT$ seconds, given that T is the segment length.

Thus, if T is, say, 50 milliseconds, and if $n = 8$, then the system delay will be 0.8 seconds, which is large enough to be noticeable. For larger n and T this delay will become unacceptably long, and yet, if $n = 8$, the total number of available permutations is only $8! = 40320$. So a problem can arise over choosing n sufficiently large to give a wide enough choice of enciphering permutations, and choosing n small enough to make the system delay acceptably short.

The idea of *sliding window* time element scramblers is to reduce the inherent time delay of the system, whilst at the same time increasing the number of possible scrambling patterns that can be used. There are a number of different types of sliding window systems, and for a description of some of these see [13] and [12]; we consider here one particular type, which we call *overlapping frame* sliding window time element scrambling, chosen for its ease of implementation.

As in a straightforward time element scrambler, the speech is again divided into frames of n segments, where each segment is T seconds long. However, we restrict ourselves to using a special subset of permutations from S_n, and we use these permutations in a slightly different way.

We first choose an integer k less than n. As we shall see, the choice of k directly affects the total system delay, which is equal to $(k + 1)T$ seconds. Thus if $k = 16$ and $T = 30$ milliseconds then the system delay would be 0.51 seconds. Note also that the system delay is independent of the choice of n.

Having fixed k, we then restrict our choice for scrambling permutations from S_n to those permutations π satisfying:

$$\overline{i\pi} \in \{\overline{i-1}, \overline{i-2}, \cdots, \overline{i-k}\} \quad \text{for each } i\ (1 \leqq i \leqq n)$$

where $\bar{i}$ denotes the residue class of i modulo n. The idea is that at time t the segment spoken at time s is transmitted, where $\bar{s} = \overline{t\pi}$ and $1 \leqq t - s \leqq k$; this is possible because π satisfies the above property.

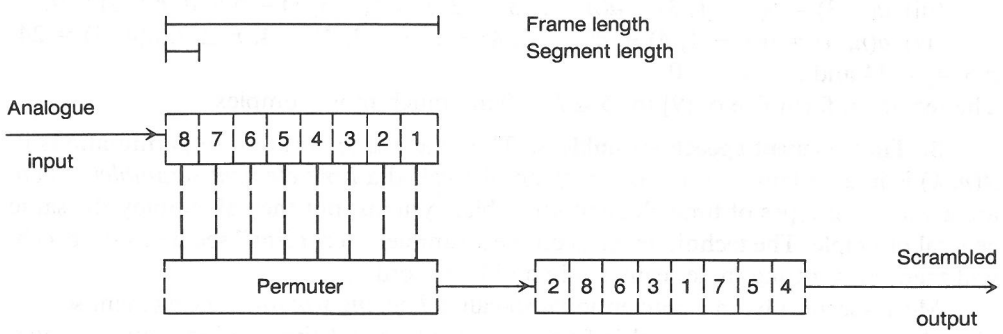

FIG. 1. *Hopping window time element scrambling.*

In Fig. 2, the use of such a permutation is illustrated for a system having $n = 8$, $k = 3$ and

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 8 & 3 & 2 & 5 & 4 & 7 \end{pmatrix}.$$

In the figure we have used different letters to distinguish between frames, so that A1, A2, $\cdots$, A8 are used to denote the eight segments of the first frame, B1, B2, $\cdots$, B8 denote the segments of the second frame, and so on.

Because of the condition imposed on the permutation, we know that each segment will be transmitted at most $3T$ seconds after it has been spoken, and hence the receiver can output the recovered descrambled speech signal $4T$ seconds after it has been input to the transmitting device. In general, each segment will be transmitted within kT seconds and thus the total system delay will be $(k+1)T$ seconds. This assumes that each segment must spend at least T seconds in both the transmitting and receiving devices.

As we have stated above, the only permutations that are usable in this type of sliding window time element scrambler are those permutations $\pi \in S_n$ satisfying:

$$\overline{i\pi} \in \{\overline{i-1}, \overline{i-2}, \cdots, \overline{i-k}\} \quad \text{for every } i.$$

In this paper we are concerned with the problem of enumerating these permutations, which is obviously a problem of considerable practical cryptographic significance.

As in § 1 above, we thus define:

$$A^*(n,k) = \{\pi \in S_n : \overline{i\pi} \in \{\overline{i-1}, \overline{i-2}, \cdots, \overline{i-k}\} \text{ for every } i\}$$

and we are interested in $a(n, k) = |A^*(n, k)|$.

For the purposes of the theory which follows it is easier to consider the set:

$$A(n,k) = \{\pi \in S_n : \overline{i\pi} \in \{\overline{i}, \overline{i+1}, \cdots, \overline{i+k-1}\} \text{ for every } i\}$$

and it is clear that $a(n, k) = |A(n, k)|$.

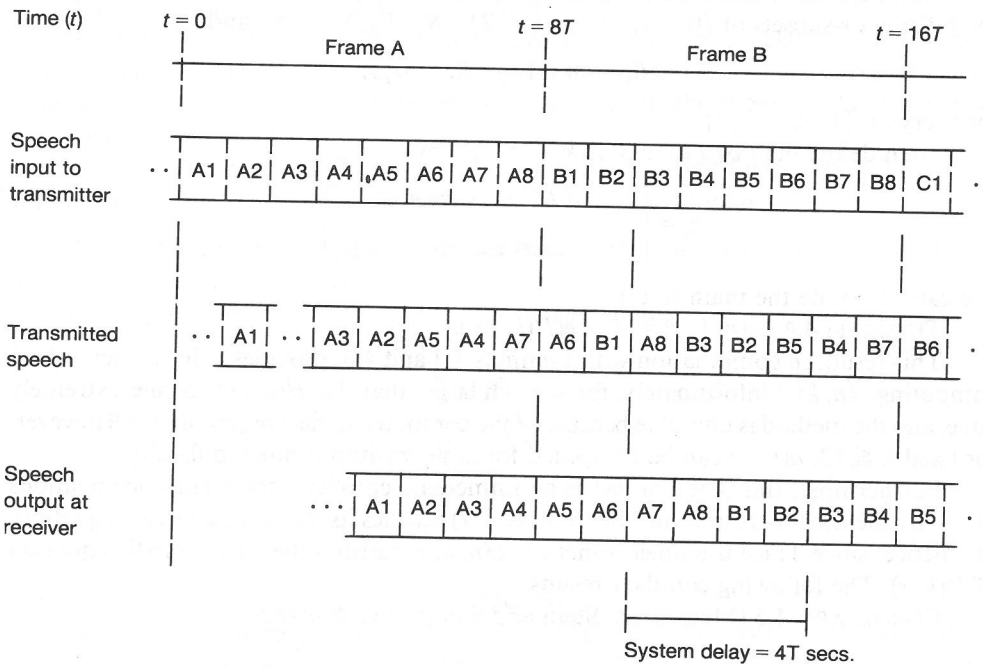

FIG. 2. *Overlapping frame sliding window time element scrambling.*

4. The main result and some corollaries. In this section we state the main results of this paper without proof; the proofs of all the results given here can be found in the next section.

Before stating the main theorem we first need a little notation. If $\pi \in S_n$ and $i \in \{1, 2, \cdots, n\}$, then define

$$X_k(\pi, i) = \{j\pi, \bar{j} \in \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-2}\} : \bar{j}\pi \in \{\bar{j}, \overline{j+1}, \cdots, \overline{i+k-2}\}\}.$$

Clearly by definition, $0 \leqq |X_k(\pi, i)| \leqq k-1$.

We now state the following result, which is of fundamental importance.

LEMMA 4.1. *If $\pi \in A(n, k)$, then there exists an integer r, $r \in \{0, 1, \cdots, k-1\}$, such that*

$$|X_k(\pi, i)| = r \quad \textit{for every } i \in \{1, 2, \cdots, n\}.$$

Because of this result, we make the following definition:

$$A(n, k, r) = \{\pi \in A(n, k) : |X_k(\pi, i)| = r \text{ for every } i\}, \qquad 0 \leqq r \leqq k-1.$$

By Lemma 4.1 it is clear that $A(n, k)$ is equal to the disjoint union of the $A(n, k, r)$'s for r satisfying $0 \leqq r \leqq k-1$, and hence, if we let $a(n, k, r) = |A(n, k, r)|$, then we have the following lemma.

LEMMA 4.2.

$$a(n, k) = \sum_{r=0}^{k-1} a(n, k, r).$$

In fact, in order to compute $a(n, k)$ using this lemma it is only necessary to compute $a(n, k, r)$ for r satisfying $1 \leqq r \leqq [(k-1)/2]$, since we also have the following.

LEMMA 4.3. (i) $a(n, k, r) = a(n, k, k-1-r)$, $0 \leqq r \leqq k-1 \leqq n-1$.

(ii) $a(n, k, 0) = a(n, k, k-1) = 1$, $0 \leqq k-1 \leqq n-1$.

Now suppose k and r are integers satisfying $0 \leqq r \leqq k-1$, and let $t = \binom{k-1}{r}$. Label the t distinct r-subsets of $\{0, -1, \cdots, -k+2\} : R_1, R_2, \cdots, R_t$, and let

$$R_i^* = \{j+1 : j \in R_i - \{0\}\},$$

for every $i \in \{1, 2, \cdots, t\}$.

Then define the t by t matrix $H(k, r) = (h_{ij})$ by

$$h_{ij} = \begin{bmatrix} 1 & \text{if } R_i^* \text{ is a subset of } R_j \\ 0 & \text{otherwise} \end{bmatrix}.$$

We can now state the main result.

THEOREM 4.4. $a(n, k, r) = \text{Trace}(H(k, r)^n)$.

This result, in combination with Lemmas 4.2 and 4.3, provides a direct method for computing $a(n, k)$. Unfortunately, for k much larger than 12, $H(k, r)$ becomes extremely large, and the method is unusable because of the computer storage requirements. However, for fixed $k \leqq 12$, $a(n, k)$ can be computed for large n without much difficulty.

Furthermore, this theorem has as an immediate corollary, the recurrence relations of [9]. By the Cayley–Hamilton Theorem, $H(k, r)$ satisfies its own characteristic equation, and hence, since Trace is a linear function, $a(n, k, r)$ satisfies the characteristic equation of $H(k, r)$. The following corollary results.

COROLLARY 4.5 (Metropolis, Stein and Stein). *Suppose that*

$$\det(H(k, r) - xI) = \sum_{i=0}^{t} c_i x^i.$$

Then

$$\sum_{i=0}^{t} c_i a(n+i,k,r)=0.$$

Moreover, since the Trace of a matrix is equal to the sum of its eigenvalues, we immediately have the following corollary.

COROLLARY 4.6. *Suppose* $q_1, q_2, \cdots, q_t$ *are the eigenvalues of* $H(k, r)$. *Then*

(i) $a(n, k, r) = \sum_{i=1}^{t} q_i^n$.

(ii) *If* $s \in \{1, 2, \cdots, t\}$ *satisfies* $|q_s| > |q_i|$ *for every* $i \in \{1, 2, \cdots, t\} - \{s\}$, *then* $a(n, k, r)/(q_s)^n$ *tends to* 1 *as* n *tends to infinity.*

Note that (ii) above has as an immediate corollary a conjecture of [9], namely that $a(n + 1, k, r)/a(n, k, r)$ tends to q_s as n tends to infinity; [9, Table IV] lists the maximal eigenvalues of $H(k, r)$ for $k = 4, 5, 6, 7, 8, 9$ and all r satisfying $1 \leqq r \leqq [(k - 1)/2]$. Corollary 4.6 (ii) also implies that, for a fixed k, $a(n, k)$ is asymptotic to $(q_{\max})^n$, where $q_{\max}$ is the maximum value from the set of eigenvalues for all the matrices $H(k, r)$, $0 \leqq r \leqq [(k - 1)/2]$.

Although $a(n, k, r)$ has meaning only if $n \geqq k$, $H(k, r)^n$ exists for every $n \geqq 1$. We can thus define $a(n, k, r)$ to be Trace $(H(k, r)^n)$ for every n satisfying $1 \leqq n \leqq k - 1$. These values of $a(n, k, r)$ will clearly satisfy Corollary 4.5, and so they can be used as initial values for the recurrence relation.

The case $r = 1$ is an especially tractable one, and we give below a complete solution for this case. The first of the results is given in [9], but the second seems to be previously unknown.

Result 4.7. (Metropolis, Stein and Stein).

$$a(n+k-1,k,1)=\sum_{i=0}^{k-2} a(n+i,k,1), \qquad n\geqq 1.$$

THEOREM 4.8. *If* $1 \leqq n \leqq k - 1$ *then* $a(n, k, 1) = 2^n - 1$.

Note that Result 4.7 and Theorem 4.8 provide a recurrence relation and sufficient initial conditions to easily compute $a(n, k, 1)$ for any reasonable values of n and k. Also note that in combination with Lemmas 4.2 and 4.3, the above two results have as an immediate corollary Result 2.2.

We have thus seen that Theorem 4.4 is the basis of straightforward proofs of all the results known previously on the computation of $a(n, k)$ for "small" k.

5. Proof of the main results. In this section we prove the results given in § 4 above. We first consider Lemmas 4.1–4.3.

Proof of Lemma 4.1. Choose $\pi \in A(n, k)$, and suppose $i, j \in \{1, 2, \cdots, n\}$ satisfy $\bar{j} = \overline{i+1}$ (where, as always, the bars denote residue classes modulo n). By inspection:

$$X_k(\pi,i)-X_k(\pi,j)=\begin{cases}\{i\pi\} & \text{if } \overline{i\pi}\in\{\bar{i},\overline{i+1},\cdots,\overline{i+k-2}\},\\ \phi & \text{if } \overline{i\pi}=\overline{i+k-1},\end{cases}$$

and

$$X_k(\pi,j)-X_k(\pi,i)=\begin{cases}\{i+k-1\} & \text{if } \overline{i+k-1}\in\{\overline{(i+1)\pi},\cdots,\overline{(i+k-1)\pi}\},\\ \phi & \text{if } \overline{i\pi}=\overline{i+k-1}.\end{cases}$$

Hence $|X_k(\pi, i)| = |X_k(\pi, j)|$ and the result follows. □

Lemma 4.2 is immediate from the definition, and we also have the following proof.

Proof of Lemma 4.3. (i) Define the mapping ϕ_k from S_n into S_n by:

$$\phi_k(\pi) \text{ maps } i \text{ to } (n+1)-s\pi, \text{ where } s\in\{1,2,\cdots,n\} \text{ and } \bar{s}=\overline{-i-k+2}.$$

Then we claim that ϕ_k is a one-to-one mapping from $A(n, k, r)$ into $A(n, k, k-1-r)$. This will establish the result.

It is not difficult to see that ϕ_k permutes the elements of S_n, so we need only show that ϕ_k maps $A(n, k, r)$ into $A(n, k, k-1-r)$ to complete the proof of (i).

Choose $\pi \in A(n, k, r)$ and define $\pi^* = \phi_k(\pi)$. By definition, if $i \in \{1, 2, \cdots, n\}$ then $\overline{i\pi^*} = \overline{1 - s(i)\pi}$, where $s(i) \in \{1, 2, \cdots, n\}$ and $\overline{s(i)} = \overline{-i-k+2}$. Now since $\pi \in A(n, k)$, we know that

$$\overline{s(i)\pi} \in \{\overline{-i-k+2}, \overline{-i-k+3}, \cdots, \overline{-i+1}\},$$

and hence

$$\overline{i\pi^*} \in \{\overline{i+k-1}, \overline{i+k-2}, \cdots, \bar{i}\},$$

and so $\pi^* \in A(n, k)$. Now, by definition,

$$X_k(\pi^*, n-k+2) = \{j\pi^*, \overline{s(j)} \in \{\bar{n}, \overline{n-1}, \cdots, \overline{n-k+2}\} : \overline{s(j)\pi} \in \{\overline{s(j)+k-1}, \overline{s(j)+k-2}, \cdots, \bar{1}\}\}$$

and since $\pi \in A(n, k, r)$, $|X_k(\pi, n-k+2)| = r$, i.e.,

$$|\{j\pi, \bar{j} \in \{\overline{n-k+2}, \overline{n-k+3}, \cdots, \bar{n}\} : \overline{j\pi} \in \{\bar{j}, \overline{j+1}, \cdots, \bar{n}\}\}| = r,$$

and hence $|X_k(\pi^*, n-k+2)| = k-1-r$, and (i) follows.

(ii) If $\pi \in A(n, k, 0)$, then it is straightforward to show that $\overline{i\pi} = \overline{i+k-1}$ for every i, and hence $|A(n, k, 0)| = 1$. The result follows from (i). □

In order to establish Theorem 4.4, it is necessary to prove a number of preliminary results. We first make some definitions.

If $0 \leqq r \leqq k-1$ and $k \geqq 2$, then define $\mathbf{E}(k, r)$ to be the class of all $(k-1)$-subsets E of $\{-k+2, -k+3, \cdots, k-1\}$ satisfying the property that E contains precisely r elements of $\{-k+2, -k+3, \cdots, 0\}$.

If $E \in \mathbf{E}(k, r)$ then define $U_k(E)$ to be the set:

$$\{(c_1, c_2, \cdots, c_{k-1}) : \{c_1, c_2, \cdots, c_{k-1}\} = E, c_i \in \{i-k+1, i-k+2, \cdots, i\}\}.$$

In addition let $u_k(E) = |U_k(E)|$.

Lastly, for any set of integers $E = \{e_1, e_2, \cdots, e_s\}$, say, let $\bar{E} = \{\overline{e_1}, \overline{e_2}, \cdots, \overline{e_s}\}$, where, as always, we are working modulo n.

As an immediate result we have the following lemma.

LEMMA 5.1.

$$|\mathbf{E}(k, r)| = \binom{k-1}{r}^2, \qquad 0 \leqq r \leqq k-1, \quad k \geqq 2.$$

We may now state the following important result, which justifies the definition of $U_k(E)$.

LEMMA 5.2. *Suppose* $0 \leqq r \leqq k-1$ *and* $2 \leqq k \leqq n$. *Then* $(c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$ *for some* $E = \{c_1, c_2, \cdots, c_{k-1}\}$ *satisfying* $E \in \mathbf{E}(k, r)$ *and* $|\bar{E}| = k-1$, *if and only if there exists* $\pi \in A(n, k, r)$ *satisfying*:

$$j\pi = \begin{cases} c_i & \text{if } j\pi < j \\ c_i + n & \text{if } j\pi \geqq j \end{cases} \quad \text{where } j = n-k+1+i, \quad i \in \{1, 2, \cdots, k-1\}.$$

Proof. First suppose $\pi \in A(n, k, r)$, and let $(c_1, c_2, \cdots, c_{k-1})$ be as in the statement of the lemma. Then if $E = \{c_1, c_2, \cdots, c_{k-1}\}$, we must show the following:

(i) $|\bar{E}| = k-1$,

(ii) $E \in \mathbf{E}(k, r)$,

(iii) $(c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$.

Item (i) follows since $\overline{c_i} = \overline{(n-k+1+i)\pi}$ for every $i \in \{1, 2, \cdots, k-1\}$ and $\overline{c_i} = \overline{c_j}$ if and only if $i = j$ (since $\pi \in S_n$).

Next, since $\pi \in A(n, k)$, we know that

$$\overline{(n-k+1+i)\pi} \in \{\overline{n-k+1+i}, \overline{n-k+2+i}, \cdots, \overline{n+i}\}.$$

Hence if $(n-k+1+i)\pi \geqq (n-k+1+i)$, then

$$(n-k+1+i)\pi \in \{n-k+1+i, n-k+2+i, \cdots, n\},$$

i.e.,

$$c_i = (n-k+1+i)\pi - n \in \{-k+1+i, -k+2+i, \cdots, 0\}.$$

Similarly, if $(n-k+1+i)\pi < (n-k+1+i)$, then

$$c_i = (n-k+1+i)\pi \in \{1, 2, \cdots, i\}.$$

We have thus shown that $E \in \mathbf{E}(k, s)$, where

$$s = |\{j \in \{n-k+2, n-k+3, \cdots, n\} : j\pi \geqq j\}|,$$

and moreover that $c_i \in \{i-k+1, i-k+2, \cdots, i\}$ for every i, and so we have shown (iii).

Now $\pi \in A(n, k, r)$, and hence $|X_k(\pi, n-k+2)| = r$, i.e.,

$$|\{j\pi, j \in \{n-k+2, n-k+3, \cdots, n\} : \overline{j\pi} \in \{\overline{j}, \overline{j+1}, \cdots, \overline{n}\}\}| = r.$$

But $\overline{j\pi} \in \{\overline{j}, \overline{j+1}, \cdots, \overline{n}\}$ iff $j\pi \in \{j, j+1, \cdots, n\}$ iff $j\pi \geqq j$. Hence $s = r$ and (ii) follows.

Now suppose $(c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$, where $\{c_1, c_2, \cdots, c_{k-1}\} = E$, and $E \in \mathbf{E}(k, r)$ has the property: $|\bar{E}| = k-1$.

If $D = \{\bar{1}, \bar{2}, \cdots, \bar{n}\} - \bar{E}$, then $|D| = n-k+1$. Hence let $\{d_1, d_2, \cdots, d_{n-k+1}\}$ be the set satisfying the following three properties:

(i) $D = \{\overline{d_1}, \overline{d_2}, \cdots, \overline{d_{n-k+1}}\}$,

(ii) $d_i \in \{1, 2, \cdots, n\}$ for every $i \in \{1, 2, \cdots, n-k+1\}$, and

(iii) $d_i < d_{i+1}$ for every $i \in \{1, 2, \cdots, n-k\}$.

Note that by (ii) and (iii) it is immediate that

$$i \leqq d_i \leqq i+k-1 \quad \text{for every } i \in \{1, 2, \cdots, n-k+1\}. \tag{1}$$

Define $\pi \in S_n$ as follows. Let:

$$j\pi = \begin{cases} d_j & \text{if } 1 \leqq j \leqq n-k+1, \\ c_i & \text{if } n-k+2 \leqq j \leqq n \text{ and } c_i > 0 \quad \text{where } i = j-n+k-1, \\ c_i+n & \text{if } n-k+2 \leqq j \leqq n \text{ and } c_i \leqq 0 \quad \text{where } i = j-n+k-1. \end{cases}$$

It is clear that π is well defined, since, by definition,

$$\{\overline{c_1}, \overline{c_2}, \cdots, \overline{c_{k-1}}, \overline{d_1}, \overline{d_2}, \cdots, \overline{d_{n-k+1}}\} = \{\bar{1}, \bar{2}, \cdots, \bar{n}\}.$$

Again by definition, $d_i \in \{1, 2, \cdots, n\}$ for every i. Finally if $c_i > 0$, then

$$c_i \in \{1, 2, \cdots, k-1\},$$

and if $c_i \leqq 0$, then $c_i \in \{-k+2, -k+3, \cdots, 0\}$, and hence

$$c_i + n \in \{n-k+2, n-k+3, \cdots, n\}.$$

Now suppose $j = n-k+1+i$, $i \in \{1, 2, \cdots, k-1\}$. Then

$$j\pi = \begin{cases} c_i & \text{if } c_i > 0 \\ c_i+n & \text{if } c_i \leqq 0 \end{cases} \quad \text{and } c_i \in \{i-k+1, i-k+2, \cdots, i\} \text{ for all } i.$$

Hence if $j\pi = c_i$ then $c_i > 0$, and so $c_i \in \{1, 2, \cdots, i\}$, i.e., $j\pi \leqq i$. Now

$$j = n-k+1+i > i,$$

i.e., $j\pi < j$. Similarly, if $j\pi = c_i + n$, then we have $c_i \leqq 0$, and so

$$c_i \in \{i-k+1, i-k+2, \cdots, 0\},$$

i.e., $j\pi \geqq n - k + 1 + i = j$. Hence

$$j\pi = \begin{cases} c_i & \text{if } j\pi < j, \\ c_i + n & \text{if } j\pi \geqq j. \end{cases}$$

We now only need show that $\pi \in A(n, k, r)$. By (1), $j \leqq d_j \leqq j + k - 1$ and hence $\overline{j\pi} \in \{\bar{j}, \overline{j+1}, \cdots, \overline{j+k-1}\}$ for every $j \in \{1, 2, \cdots, n - k + 1\}$. Also, if $n - k + 2 \leqq j \leqq n$, then $\overline{j\pi} = \overline{c_i} \in \{\overline{i-k+1}, \overline{i-k+2}, \cdots, \bar{i}\}$, where $j = n - k + 1 + i$. This implies that $\overline{j\pi} \in \{\bar{j}, \overline{j+1}, \cdots \overline{j+k-1}\}$ for every $j \in \{n - k + 2, n - k + 3, \cdots, n\}$, and so $\pi \in A(n, k)$.

Finally, by definition,

$$X_k(\pi, n-k+2) = \{j\pi, j \in \{n-k+2, n-k+3, \cdots, n\} : \overline{j\pi} \in \{\bar{j}, \overline{j+1}, \cdots, \bar{n}\}\}$$

$$= \{j\pi, j \in \{n-k+2, n-k+3, \cdots, n\} : j\pi \geqq j\}.$$

Hence, by the above arguments,

$$|X_k(\pi, n-k+2)| = |\{c_i \in E : c_i \leqq 0\}| = r, \text{ since } E \in \mathbf{E}(k, r).$$

The result follows. □

The above result gives us a means of classifying the "endings" of permutations in $A(n, k, r)$, where the ending of a permutation π is the $(k - 1)$-tuple $((n - k + 2)\pi, (n - k + 3)\pi, \cdots, n\pi)$. The next result gives us a way of enumerating the number of "starts" for each possible ending.

LEMMA 5.3. *Suppose* $0 \leqq r \leqq k - 1$, $2 \leqq k \leqq n$, *and let* $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1})$ *and* $\mathbf{d} = (d_1, d_2, \cdots, d_{k-1})$ *be elements of* $U_k(E)$ *for some* $E \in \mathbf{E}(k, r)$. *If* $P(\mathbf{c})$ *is the set of permutations* $\pi \in A(n, k, r)$ *satisfying*

$$j\pi = \begin{cases} c_i & \text{if } j\pi < j, \\ c_i + n & \text{if } j\pi \geqq j, \end{cases} \quad j = n-k+1+i, \quad i \in \{1, 2, \cdots, k-1\},$$

and $P(\mathbf{d})$ *is the set of permutations* $\pi^* \in A(n, k, r)$ *satisfying*

$$j\pi^* = \begin{cases} d_i & \text{if } j\pi^* < j, \\ d_i + n & \text{if } j\pi^* \geqq j, \end{cases} \quad j = n-k+1+i, \quad i \in \{1, 2, \cdots, k-1\},$$

then $|P(\mathbf{c})| = |P(\mathbf{d})|$.

Proof. We define ϕ which maps $P(\mathbf{c})$ into $P(\mathbf{d})$ by:

$$i\phi(\pi) = \begin{cases} i\pi & \text{if } 1 \leqq i \leqq n-k+1 \\ i\pi^* & \text{if } n-k+2 \leqq i \leqq n \end{cases} \quad \text{where } \pi^* \text{ is any element of } P(\mathbf{d}).$$

We now show why ϕ is well defined. First suppose π^* and $\pi^{*\prime}$ are two elements of $P(\mathbf{d})$, and then, by definition, $i\pi^* = i\pi^{*\prime}$ for every $i \in \{n - k + 2, n - k + 3, \cdots, n\}$. Second, $\phi(\pi) \in S_n$, since if $\pi \in A(n, k, r)$ satisfies

$$j\pi = \begin{cases} c_i & \text{if } j\pi < j, \\ c_i + n & \text{if } j\pi \geqq j, \end{cases} \quad j = n-k+1+i, \quad i \in \{1, 2, \cdots, k-1\},$$

$\pi^* \in A(n, k, r)$ satisfies

$$j\pi^* = \begin{cases} d_i & \text{if } j\pi < j, \\ d_i + n & \text{if } j\pi \geqq j, \end{cases} \qquad j = n-k+1+i, \quad i \in \{1, 2, \cdots, k-1\}$$

and $(c_1, c_2, \cdots, c_{k-1})$, $(d_1, d_2, \cdots, d_{k-1}) \in U_k(E)$, then it is clear that

$$\{j\pi : n-k+2 \leqq j \leqq n\} = \{j\pi^* : n-k+2 \leqq j \leqq n\}.$$

Third, it is straightforward to see that $\phi(\pi)$ is an element of $A(n, k)$ since $\pi, \pi^* \in A(n, k)$. Fourth, since $X_k(\phi(\pi), n-k+2) = X_k(\pi^*, n-k+2)$, and since $\pi^* \in A(n, k, r)$, it is clear that $\phi(\pi) \in A(n, k, r)$. Finally, by definition it is clear that $\phi(\pi) \in P(\mathbf{d})$. We have thus shown that ϕ is well defined.

To conclude the proof we show that ϕ is one to one. Suppose that $\phi(\pi) = \phi(\pi')$, where $\pi, \pi' \in A(n, k, r)$ and where $\pi, \pi' \in P(\mathbf{c})$. Then $i\pi = i\pi'$ for every i satisfying $1 \leqq i \leqq n-k+1$. But since $\pi, \pi' \in P(\mathbf{c})$ we know that $i\pi = i\pi'$ for every

$$i \in \{n-k+2, n-k+3, \cdots, n\}.$$

Hence, $\pi = \pi'$ and the result follows. □

Because of Lemma 5.3 we can make the following definition, the relevance of which is apparent in the next result. If $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$, and $P(\mathbf{c})$ is as in the statement of Lemma 5.3, then let $v_{n,k}(E) = |P(\mathbf{c})|$. $v_{n,k}(E)$ is well defined precisely because of Lemma 5.3. We can now state the following important result.

THEOREM 5.4. *If* $0 \leqq r \leqq k-1$ *and* $2 \leqq k \leqq n$, *then*

$$a(n, k, r) = \sum_{E \in \mathbb{E}(k,r)} u_k(E) v_{n,k}(E).$$

Proof. By definition,

$$a(n, k, r) = |A(n, k, r)|$$

$$= \sum_{*} \left(\sum_{\mathbf{c} \in U_k(E)} |P(\mathbf{c})| \right) \quad \text{(by Lemma 5.2)}$$

$$\left(\text{where } \sum_{*} \text{ denotes the sum over all } E \in \mathbb{E}(k, r) \text{ satisfying } |\bar{E}| = k-1 \right)$$

$$= \sum_{*} u_k(E) v_{n,k}(E) \quad \text{(by Lemma 5.3)}$$

$$= \sum_{E \in \mathbb{E}(k,r)} u_k(E) v_{n,k}(E)$$

since if $|\bar{E}| < k-1$, then it is clear that $v_{n,k}(E) = 0$. □

We have thus transformed the problem of evaluating $a(n, k, r)$ into the problem of evaluating $v_{n,k}(E)$ and $u_k(E)$ for every $E \in \mathbb{E}(k, r)$. In the next two results we show how these values may be computed.

THEOREM 5.5. *Suppose* $0 \leqq r \leqq k-1$ *and* $2 \leqq k \leqq n$, *and let* $E \in \mathbb{E}(k, r)$. *Then*

(i) *If* $n = k$ *then*

$$v_{n,k}(E) = \begin{cases} 1 & \text{if } |\bar{E}| = k-1, \\ 0 & \text{if } |\bar{E}| < k-1; \end{cases}$$

(ii) $v_{n+1,k}(E) = \sum_* v_{n,k}(F)$, *where* $\sum_*$ *represents the sum over all* $F \in \mathbb{E}(k, r)$ *which contain the set* E^* *which is defined to be the union of* $\{i : i \in E, i > 0\}$ *and* $\{i + 1 : i \in E, i < 0\}$.

Proof. First note that $U_k(E)$ is nonempty for any $E \in \mathbb{E}(k, r)$, since an element of $U_k(E)$ can always be produced by assemblying the elements of E in ascending order.

(i) Suppose $n = k$. First let $|\bar{E}| < k - 1$, and then, using the notation of Lemma 5.3, suppose that $\pi \in A(n, k, r)$ is an element of $P(\mathbf{c})$ for some $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$. Then, since $|\bar{E}| < k - 1$, there exists a pair c_i, c_j $(i \neq j)$ with $\bar{c}_i = \bar{c}_j$. Hence $\overline{(i+1)\pi} = \overline{(j+1)\pi}$, i.e., $(i + 1)\pi = (j + 1)\pi$, which is a contradiction since π is a permutation. Hence $v_{k,k}(E) = 0$ if $|\bar{E}| < k - 1$.

Now suppose $|\bar{E}| = k - 1$, and choose a $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$. If $\pi \in P(\mathbf{c})$ (π exists by Lemma 5.2) then, by definition, $\{\overline{2\pi}, \overline{3\pi}, \cdots, \overline{k\pi}\} = \bar{E}$, and hence $\{\overline{1\pi}\} = \{\bar{1}, \bar{2}, \cdots, \bar{k}\} - \bar{E}$. So 1π is fixed by the choice of E, and, by definition, $2\pi, 3\pi, \cdots, k\pi$ are also fixed since $\pi \in P(\mathbf{c})$. Thus π is uniquely defined, and so $v_{k,k}(E) = 1$.

(ii) First note that the elements of E are all distinct modulo $n + 1$ if and only if the elements of E^* are all distinct modulo n. Hence we assume that both these statements are true, since otherwise both sides of the equation are zero by (i) above.

First, choose $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$. If $0 \in E$, then let h satisfy $c_h = 0$, and, if $0 \notin E$, then set $h = 0$. Then, by definition, if $\pi \in A(n + 1, k, r)$ satisfies $\pi \in P(\mathbf{c})$ we have

$$(n-k+2+h)\pi = n+1.$$

Next, suppose that $F = \{d_1, d_2, \cdots, d_{k-1}\} \in \mathbb{E}(k, r)$ contains E^*.

Then, if $0 \notin E$ we have $F = E^*$, and we let

$$d_i = \begin{cases} c_i + 1 & \text{if } c_i < 0, \\ c_i & \text{if } c_i > 0, \end{cases} \qquad 1 \leqq i \leqq k-1.$$

Note that if $0 \notin E$ then it is clear that $E^* \in \mathbb{E}(k, r)$.

If $0 \in E$, then we let $d_1, d_2, \cdots, d_{k-1}$ be defined as follows:

d_1 is the element of $\{-k + 2, -k + 3, \cdots, 0\} - E^*$ that is contained in F.

$$d_i = \begin{cases} c_{i-1} + 1 & \text{if } c_{i-1} < 0, \\ c_{i-1} & \text{if } c_{i-1} > 0, \end{cases} \qquad 2 \leqq i \leqq h,$$

$$d_i = \begin{cases} c_i + 1 & \text{if } c_i < 0, \\ c_i & \text{if } c_i > 0, \end{cases} \qquad h+1 \leqq i \leqq k-1.$$

Now let $\mathbf{d}_F = (d_1, d_2, \cdots, d_{k-1})$ and we now show that $\mathbf{d}_F \in U_k(F)$. To do this we need only show that $d_i \in \{i - k + 1, i - k + 2, \cdots, i\}$ for every $i \in \{1, 2, \cdots, k - 1\}$. First, suppose that $i \leqq h$:

If $i = 1$, then $d_1 \in \{-k + 2, -k + 3, \cdots, 0\} - E^*$, i.e.,

$$d_1 \in \{-k+2, -k+3, \cdots, 1\}.$$

If $i > 1$, then we have

$$d_i = \begin{cases} c_{i-1} + 1 & \text{if } c_{i-1} < 0, \\ c_{i-1} & \text{if } c_{i-1} > 0. \end{cases}$$

If $c_{i-1} < 0$ then $d_i = c_{i-1} + 1 \in \{i-k+1, i-k+2, \cdots, i\}$, since $\mathbf{c} \in U_k(E)$.
If $c_{i-1} > 0$ then $d_i = c_{i-1} \in \{1, 2, \cdots, i-1\}$, i.e.,

$$d_i \in \{i-k+2, i-k+3, \cdots, i\},$$

since $\mathbf{c} \in U_k(E)$ and $c_{i-1} > 0$. Second, suppose that $i > h$:
Then we have

$$d_i = \begin{cases} c_i + 1 & \text{if } c_i < 0, \\ c_i & \text{if } c_i > 0. \end{cases}$$

If $c_i < 0$ then $d_i = c_i + 1 \in \{i-k+2, i-k+3, \cdots, 0\}$, since $\mathbf{c} \in U_k(E)$.
If $c_i > 0$ then $d_i = c_i \in \{1, 2, \cdots, i\}$ (since $\mathbf{c} \in U_k(E)$), i.e.,

$$d_i \in \{i-k+1, i-k+2, \cdots, i\}.$$

Hence $\mathbf{d}_F \in U_k(F)$.

Now, using the same notation as before, let $P(\mathbf{c})$ and $P(\mathbf{d}_F)$ be sets of permutations from $A(n+1, k)$ and $A(n, k)$ respectively, defined as in the statement of Lemma 5.3. We will show that

$$|P(\mathbf{c})| = \sum_{*} |P(\mathbf{d}_F)|,$$

where, as in the statement of the theorem, $\sum_*$ represents the sum over all $F \in \mathbf{E}(k, r)$ which contain E^*. This will establish the result. We actually prove this claim by exhibiting a one-to-one correspondence ϕ between $P(\mathbf{c})$ and the union of the sets $P(\mathbf{d}_F)$, which are clearly all disjoint. We define ϕ as follows:

Suppose $\pi \in A(n+1, k, r)$ is contained in $P(\mathbf{c})$, i.e., suppose that

$$j\pi = \begin{cases} c_i & \text{if } j\pi < j, \\ c_i + n + 1 & \text{if } j\pi \geqq j, \end{cases} \qquad j = n-k+2+i, \quad i \in \{1, 2, \cdots, k-1\}.$$

Then define $\pi^* = \phi(\pi)$ by

$$i\pi^* = \begin{cases} i\pi & \text{if } 1 \leqq i \leqq n-k+1+h, \\ (i+1)\pi & \text{if } n-k+2+h \leqq i \leqq n. \end{cases}$$

We now show that π^* is an element of $P(\mathbf{d}_F)$, where $F \in \mathbf{E}(k, r)$ contains E^*, and hence show that ϕ is well defined.

First, note that $\pi^* \in S_n$ since $\pi \in S_{n+1}$ and h is chosen so that $(n-k+2+h)\pi = n+1$.

Second, observe that $\pi^* \in A(n, k)$. We show this as follows:
If $1 \leqq i \leqq n-k+1$ then, since $\pi \in A(n+1, k)$, we have

$$i\pi^* = i\pi \in \{i, i+1, \cdots, i+k-1\}.$$

If $n-k+2 \leqq i \leqq n-k+1+h$ (which only applies if $h > 0$) then, since $\pi \in A(n+1, k)$, $i\pi \in \{i, i+1, \cdots, n, 1, 2, \cdots, i-n+k-2\}$; note that $i\pi \neq n+1$ since $i \neq n-k+2+h$. Hence $\overline{i\pi^*} \in \{\bar{i}, \overline{i+1}, \cdots, \bar{n}, \bar{1}, \bar{2}, \cdots, \overline{i-n+k-2}\}$, i.e., $\overline{i\pi^*} \in \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-2}\}$.

If $n-k+2+h \leqq i \leqq n$ then, since $\pi \in A(n+1, k)$, we have

$$i\pi^* = (i+1)\pi \in \{i+1, i+2, \cdots, n, 1, 2, \cdots, i-n+k-1\};$$

note that $i\pi^* \neq n+1$ since $i+1 \neq n-k+2+h$. Hence

$$\overline{i\pi^*} \in \{\overline{i+1}, \overline{i+2}, \cdots, \overline{i+k-1}\}.$$

Thus $\pi^* \in A(n, k)$.

Third, note that $\pi^* \in A(n, k, r)$. This can be demonstrated by considering $X_k(\pi^*, n-k+2)$. By definition,

$$\begin{aligned} X_k(\pi^*, n-k+2) &= \{j\pi^*, j \in \{n-k+2, n-k+3, \cdots, n\} : j\pi^* \in \{j, j+1, \cdots, n\}\} \\ &= \text{the union of } \{j\pi, j \in \{n-k+2, n-k+3, \cdots, \\ &\qquad n-k+1+h\} : j\pi \in \{j, j+1, \cdots, n\}\} \end{aligned}$$

and

$$\{j\pi, j \in \{n-k+3+h, n-k+4+h, \cdots, n+1\} : j\pi \in \{j\pi \in \{j-1, j, \cdots, n\}\}\}.$$

Now since $\pi \in A(n+1, k)$, where $n+1 > n \geqq k$, we know that $j\pi \neq j-1$ for any j, and hence

$$\begin{aligned} X_k(\pi^*, n-k+2) = \{j\pi, j \in \{n-k+2, n-k+3, \cdots, n\}, \\ j \neq n-k+2+h : j\pi \in \{j, j+1, \cdots, n\}\}. \end{aligned}$$

Also note that $(n-k+2+h)\pi = n+1$ and hence $X_k(\pi^*, n-k+2) = X_k(\pi, n-k+2)$ and hence $\pi^* \in A(n, k, r)$.

Fourth, we let

$$F = \begin{cases} E^* & \text{if } h = 0, \\ \text{the union of } E^* \text{ and } \{(n-k+2)\pi - n\} & \text{if } h > 0. \end{cases}$$

Then F contains E^* by definition. We claim that $F \in \mathbf{E}(k, r)$, and, defining $\mathbf{d}_F$ as above, we also claim that $\pi^* \in P(\mathbf{d}_F)$.

We first show that $F \in \mathbf{E}(k, r)$.

If $h = 0$ then $0 \notin E$ and hence $F = E^* \in \mathbf{E}(k, r)$.

If $h > 0$ then $0 \in E$ and hence E^* contains $r-1$ elements of

$$\{-k+2, -k+3, \cdots, 0\}$$

and $k-1-r$ elements of $\{1, 2, \cdots, k-1\}$. Now since

$$\pi \in A(n+1, k), (n-k+2)\pi \in \{n-k+2, n-k+3, \cdots, n+1\},$$

and hence $(n-k+2)\pi - n \in \{-k+2, -k+3, \cdots, 0, 1\}$. Now since $h > 0$, $(n-k+2)\pi \neq n+1$, i.e., $(n-k+2)\pi - n \neq 1$. Hence

$$(n-k+2)\pi - n \in \{-k+2, -k+3, \cdots, 0\},$$

and so to show that $F \in \mathbf{E}(k, r)$ we need only show that $(n-k+2)\pi - n \notin E^*$. But since $\pi \in A(n+1, k)$, $(n-k+2)\pi - (n+1) \notin E$ and the result follows.

To see that $\pi^* \in P(\mathbf{d}_F)$ we need only examine the values of $j\pi^*$, where $j = n-k+1+i$ and $i \in \{1, 2, \cdots, k-1\}$. Choose such a j.

If $i > h$ then

$$\begin{aligned} j\pi^* &= (j+1)\pi \\ &= \begin{cases} c_i & \text{if } j\pi < j \\ c_i + n + 1 & \text{if } j\pi \geqq j \end{cases} \quad \text{since } \pi \in P(\mathbf{c}) \end{aligned}$$

$$= \begin{cases} d_i & \text{if } j\pi < j \\ d_i + n & \text{if } j\pi \geqq j \end{cases} \quad \text{since, given } i > h,$$

$$d_i = \begin{cases} c_i & \text{if } c_i > 0 \\ c_i + 1 & \text{if } c_i < 0 \end{cases} \quad \text{and } c_i < 0 \text{ iff } j\pi \geqq j.$$

If $i \leqq h$ then we have two cases to consider: $i = 1$ and $i > 1$.

If $i = 1$ then

$$j\pi^* = (n-k+2)\pi^* = (n-k+2)\pi \in \{n-k+2, n-k+3, \cdots, n\}, \text{ i.e., } j\pi \geqq j.$$

Now, by the above, $(n-k+2)\pi - n \in F$, $(n-k+2)\pi - n \in \{-k+2, -k+3, \cdots, 0\}$ and $(n-k+2)\pi - n \notin E^*$. Hence $d_1 = (n-k+2)\pi - n$, i.e., $(n-k+2)\pi^* = d_1 + n$ and $(n-k+2)\pi \geqq n-k+2$.

If $2 \leqq i \leqq h$ then

$$j\pi^* = j\pi = \begin{cases} c_{i-1} & \text{if } j\pi < j, \\ c_{i-1} + n + 1 & \text{if } j\pi \geqq j, \end{cases}$$

$$= \begin{cases} d_i & \text{if } j\pi < j, \\ d_i + n & \text{if } j\pi \geqq j, \end{cases}$$

since, given $i \leqq h$,

$$d_i = \begin{cases} c_{i-1} & \text{if } c_{i-1} > 0 \\ c_{i-1} + 1 & \text{if } c_{i-1} < 0 \end{cases} \quad \text{and } c_{i-1} < 0 \text{ iff } j\pi \geqq j.$$

Hence $\pi^* \in P(\mathbf{d}_F)$ and we have shown that ϕ is well defined.

To complete the proof, we need to show that ϕ is one to one and onto.

First, suppose that $\pi_1, \pi_2 \in P(\mathbf{c})$ satisfy $\phi(\pi_1) = \phi(\pi_2)$. Then, by definition of ϕ, $i\pi_1 = i\pi_2$ for every $i \in \{1, 2, \cdots, n+1\}$ except for $i = n-k+2+h$. However, since π_1 and π_2 are permutations, they cannot disagree in exactly one position and hence $\pi_1 = \pi_2$ and thus we have shown that ϕ is one to one.

We now show that ϕ is onto, and hence complete the proof. Suppose that $\pi^* \in A(n, k, r)$ is contained in $P(\mathbf{d}_F)$, where $F \in \mathbf{E}(k, r)$ contains E^*.

Then let $\pi \in S_{n+1}$ satisfy

$$i\pi = \begin{cases} i\pi^* & \text{if } 1 \leqq i \leqq n-k+1+h, \\ n+1 & \text{if } i = n-k+2+h, \\ (i-1)\pi^* & \text{if } n-k+3+h \leqq i \leqq n+1. \end{cases}$$

Note that π is clearly in S_{n+1} since $\pi^* \in S_n$.

It is now straightforward to verify that $\pi \in A(n+1, k, r)$, and moreover that $\pi \in P(\mathbf{c})$ and $\phi(\pi) = \pi^*$. This establishes that ϕ is onto and the result follows. □

THEOREM 5.6. *Suppose* $0 \leqq r \leqq k-1$, $2 \leqq k$ *and* $n = 2k-2$, *and let* $E \in \mathbf{E}(k, r)$. *Then* $u_k(E) = v_{n,k}(F)$, *where* $F \in \mathbf{E}(k, r)$ *is defined by*

$$F = \{i \in \{-k+2, -k+3, \cdots, k-1\} : \bar{i} = \overline{j+k-1},$$
$$j \in \{-k+2, -k+3, \cdots, k-1\} - E\}.$$

Proof. We first show that F as defined in the statement of the theorem is always in $\mathbf{E}(k, r)$. By definition, $F \in \mathbf{E}(k, s)$, where

$$s = |\{i \in F : i \in \{-k+2, -k+3, \cdots, 0\}\}|,$$

and so we need only show that $r = s$.

Suppose $i \in \{-k+2, -k+3, \cdots, 0\}$. Then, by definition, $i \in F$ if and only if $\overline{i-k+1} \notin \bar{E}$, since $n = 2k-2$ (note that bars denote residue classes modulo $n = 2k-2$). Hence, again by definition,

$$\begin{aligned} s &= k-1-|\{i \notin F : i \in \{-k+2, -k+3, \cdots, 0\}\}| \\ &= k-1-|\{\bar{i} \in \bar{E} : \bar{i} \in \{\bar{1}, \bar{2}, \cdots, \overline{k-1}\}\}| \\ &= r \quad (\text{since } E \in \mathbf{E}(k, r)) \quad \text{and thus } F \in \mathbf{E}(k, r). \end{aligned}$$

Now choose an element $\mathbf{d} = (d_1, d_2, \cdots, d_{k-1})$ from $U_k(F)$. We must show (using the above notation) that $|U_k(E)| = |P(\mathbf{d})|$, and we will then have completed the proof. To do this we define ϕ which maps $U_k(E)$ into $P(\mathbf{d})$, as follows:

Suppose $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1}) \in U_k(E)$. Then $\pi = \phi(\mathbf{c})$ satisfies

(i)

$$\overline{i\pi} = \begin{cases} \overline{c_i + k - 1} & \text{if } 1 \leqq i \leqq k-1, \\ \bar{d}_{i-k+1} & \text{if } k \leqq i \leqq 2k-2, \end{cases}$$

(ii) $i\pi \in \{1, 2, \cdots, n\}$, $1 \leqq i \leqq 2k-2$.

We must first show that ϕ is well defined, i.e., that $\pi \in P(\mathbf{d})$. We first show that $\pi \in S_n$. By definition, π maps $\{1, 2, \cdots, n\}$ into $\{1, 2, \cdots, n\}$, and hence we need only show that π is one to one. Also, since $\bar{c}_i \neq \bar{c}_j$ and $\bar{d}_i \neq \bar{d}_j$ $(i \neq j)$, we need only show that $\overline{c_i + k - 1} \neq \bar{d}_j$ for any $i, j \in \{1, 2, \cdots, k-1\}$.

Suppose $\overline{c_i + k - 1} = \bar{d}_j$; then, by definition of F, $\bar{d}_j = \overline{s+k-1}$, where $s \in \{-k+2, -k+3, \cdots, k-1\} - E$. Hence $\bar{c}_i = \bar{s}$, where $s \notin E$ and $c_i \in E$. This gives us the required contradiction, and hence $\pi \in S_n$.

We next show that $\pi \in A(n, k)$. If $1 \leqq i \leqq k-1$, then

$$\overline{i\pi} = \overline{c_i + k - 1} \in \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-1}\} \quad (\text{since } \mathbf{c} \in U_k(E)).$$

If $k \leqq i \leqq 2k-2$, then $\overline{i\pi} = \bar{d}_{i-k+1} \in \{\overline{i-2k+2}, \overline{i-2k+3}, \cdots, \overline{i-k+1}\}$ (since $\mathbf{d} \in U_k(F)$) $= \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-1}\}$ (since $n = 2k-2$). Hence $\pi \in A(n, k)$.

Next observe that, by Lemma 5.2, since $F \in \mathbf{E}(k, r)$ and $\mathbf{d} \in U_k(F)$ there exists a $\pi^* \in A(n, k, r)$ satisfying $\overline{i\pi^*} = \overline{i\pi}$ for every $i \in \{k, k+1, \cdots, 2k-2\}$. Hence $X_k(\pi, k) = X_k(\pi^*, k)$, and so $\pi \in A(n, k, r)$. Finally, note that $\pi \in P(\mathbf{d})$ by definition, and so ϕ is well defined.

By definition it is clear that ϕ is one to one, and so to complete the proof we need only show that ϕ is onto. Suppose $\pi \in P(\mathbf{d})$. We must show that if $\mathbf{c} = (c_1, c_2, \cdots, c_{k-1})$ satisfies

(i) $\bar{c}_i = \overline{i\pi - k + 1}$, and

(ii) $c_i \in \{-k+2, -k+3, \cdots, k-1\}$ for every i, then $\mathbf{c} \in U_k(E)$.

Since $\pi \in A(n, k, r)$, $\overline{i\pi} \in \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-1}\}$, and hence $\bar{c}_i = \overline{i\pi - k + 1} \in \{\overline{i-k+1}, \overline{i-k+2}, \cdots, \bar{i}\}$. Thus we need only show that $\{c_1, c_2, \cdots, c_{k-1}\} = E$. By definition, $\pi \in P(\mathbf{d})$, and hence

$$\{\overline{k\pi}, \overline{(k+1)\pi}, \cdots, \overline{(2k-2)\pi}\} = \bar{F} = \{\bar{i} : 1 \leqq i \leqq n, \bar{i} = \overline{j+k-1}, \\ j \in \{-k+2, -k+3, \cdots, k-1\} - E\}.$$

Thus, since $n = 2k - 2$,

$$\{\overline{k\pi + k - 1}, \overline{(k+1)\pi + k - 1}, \cdots, \overline{(2k-2)\pi + k - 1}\} = \{\bar{1}, \bar{2}, \cdots, \bar{n}\} - \bar{E}.$$

Finally, since $\pi \in S_n$, $\{\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_{k-1}\} = \bar{E}$, and since $n = 2k - 2$,

$$\{c_1, c_2, \cdots, c_{k-1}\} = E. \qquad \square$$

Theorems 5.5 and 5.6 now enable us to prove the main result of this paper, namely Theorem 4.4.

Proof of Theorem 4.4. First suppose $0 \leqq r \leqq k - 1$ and $2 \leqq k$. Then, as before we let

$$t = \binom{k-1}{r} = \binom{k-1}{k-1-r}.$$

As in the definition of $H(k, r)$ preceding the statement of Theorem 4.4, label the t distinct r-subsets of $\{-k + 2, -k + 3, \cdots, 0\}$: $(R_1, R_2, \cdots, R_t)$, and let

$$R_i^* = \{j + 1 : j \in R_i - \{0\}\}$$

for every i. Then $H(k, r) = (h_{ij})$ satisfies

$$h_{ij} = \begin{cases} 1 & \text{if } R_i^* \text{ is a subset of } R_j, \\ 0 & \text{otherwise.} \end{cases}$$

We need to show that $a(n, k, r) = \text{Trace } (H(k, r)^n)$ for every $n \geqq k$.

For every $i \in \{1, 2, \cdots, t\}$ define

$$C_i = \{j + k - 1 : j \in \{-k + 2, -k + 3, \cdots, 0\} - R_i\}.$$

Then C_i is a $(k - 1 - r)$-subset of $\{1, 2, \cdots, k - 1\}$ for every i, and $(C_1, C_2, \cdots, C_t)$ forms a labeling of all such subsets. Now let

$$X_{ij} = \{s : s \in R_i \text{ or } s \in C_j\},$$

i.e., X_{ij} is the union of R_i and C_j. Then it is clear that

$$\mathbb{E}(k, r) = \{X_{ij} : 1 \leqq i \leqq t, 1 \leqq j \leqq t\}.$$

Next, for every $n \geqq k$, define the t by t matrix $W(n) = (w(n)_{ij})$ by $w(n)_{ij} = v_{n,k}(X_{ij})$.

We first consider $W(k)$. By Theorem 5.5 (i),

$$w(k)_{ij} = v_{k,k}(X_{ij}) = \begin{cases} 1 & \text{if } \bar{R}_i \text{ and } \bar{C}_j \text{ are disjoint,} \\ 0 & \text{otherwise,} \end{cases}$$

where the bars denote residue classes modulo k.

We now claim that $W(k) = H(k, r)$. This is clear since

$h_{ij} = 1$ iff R_i^* is contained in R_j,
iff $\bar{R}_i^*$ is contained in $\bar{R}_j$ (since R_s is a subset of $\{-k + 2, -k + 3, \cdots, 0\}$ for every s),
iff $\bar{s} \in \bar{R}_i - \{\bar{0}\}$ implies $\overline{s+1} \in \bar{R}_j$ (by definition of R_i^*),
iff $\bar{s} \in \bar{R}_i - \{\bar{0}\}$ implies $\bar{s} \notin \bar{C}_j$ (by definition of C_j, and working modulo k),
iff $\bar{R}_i$ and $\bar{C}_j$ are disjoint (since $\bar{0} \notin \bar{C}_s$ for any s),
iff $w(k)_{ij} = 1$

and hence $W(k) = H(k, r)$.

Second, consider $W(n)$, $n \geqq k$. By Theorem 5.5 (ii)

$$w(n+1)_{ij} = v_{n+1,k}(X_{ij})$$
$$= \sum_{*} v_{n,k}(X_{sj}) \quad \text{(where } \sum_{*} \text{ represents the sum over all } s \in \{1, 2, \cdots, t\} \text{ such}$$
$$\text{that } R_i^* \text{ is a subset of } R_s\text{)},$$
$$= \sum_{s=1}^{t} h_{is} v(n)_{sj},$$

i.e., $W(n+1) = H(k, r).W(n) = H(k, r)^{n-k+1}$ for every $n \geqq k$.

Now suppose $n = 2k-2$. Then, by Theorem 5.6, and because of the chosen labeling, $u_k(X_{ij}) = v_{2k-2,k}(X_{ji}) = w(2k-2)_{ji}$. Thus, by Theorem 5.4 we have

$$a(n, k, r) = \sum_{E \in \mathbb{E}(k,r)} u_k(E) v_{n,k}(E)$$
$$= \sum_{i=1}^{t} \sum_{j=1}^{t} u_k(X_{ij}).v_{n,k}(X_{ij})$$
$$= \sum_{i=1}^{t} \sum_{j=1}^{t} w(2k-2)_{ji}.w(n)_{ij}$$
$$= \text{Trace}\,(W(n).W(2k-2))$$
$$= \text{Trace}\,(H(k, r)^{n-k+1}.H(k, r)^{k-1})$$
$$= \text{Trace}\,(H(k, r)^n). \qquad \square$$

Corollaries 4.5 and 4.6(i) are immediate from Theorem 4.4. We now prove the asymptote for $a(n, k, r)$ given in Corollary 4.6(ii).

Proof of Corollary 4.6(ii).

$$a(n, k, r)/(q_s)^n = \sum_{i=1}^{t} \left(\frac{q_i}{q_s}\right)^n$$
$$= \sum_{\substack{i=1 \\ i \neq s}}^{t} \left(\frac{q_i}{q_s}\right)^n + 1.$$

Now

$$\left| \sum_{\substack{i=1 \\ i \neq s}}^{t} \left(\frac{q_i}{q_s}\right)^n \right| \leqq \sum_{\substack{i=1 \\ i \neq s}}^{t} \left|\frac{q_i}{q_s}\right|^n \leqq (t-1).d^n$$

where $d = \max_{i \neq s} (|q_i/q_s|) < 1$. Finally, note that $(t-1).d^n$ can be made arbitrarily small given sufficiently large n, and the result follows. $\square$

To establish 4.7 and 4.8 we need to examine the matrix $H(k, 1)$. In fact we have

LEMMA 5.7. *Suppose* $r = 1$ *and* $k \geqq 2$. *Then if the labeling* $(R_1, R_2, \cdots, R_t)$ *is chosen so that* $R_i = \{1 - i\}$, *then* $H(k, 1)$ *is the* $k-1$ *by* $k-1$ *matrix*

$$\begin{bmatrix} 1 & 1 & 1 & \cdots\cdots & 1 \\ & & & & 0 \\ & & & & 0 \\ & & I_{k-2} & & \vdots \\ & & & & 0 \end{bmatrix}$$

where I_{k-2} *is the* $k-2$ *by* $k-2$ *identity matrix.*

Proof. First note that $\{0\}^*$ is empty, and hence $h_{1j} = 1$ for every j. Second, note that if $i < 0$, then $\{i\}^* = \{i + 1\}$, and so if $i > 1$ then $h_{ij} = 1$ if and only if $j = i - 1$. □

Hence, for the case $r = 1$, $H(k, 1)$ is already in Frobenius normal form, and as in [9, p. 297] the characteristic equation of $H(k, 1)$ is

$$x^{k-1} - \sum_{i=0}^{k-2} x^i = 0.$$

This gives Result 4.7 as an immediate corollary. We can also now prove the final result from § 4.

Proof of Theorem 4.8. As before let $r = 1$ and $k \geqq 2$. Then we claim that if $1 \leqq i \leqq k - 1$, then $H(k, r)^i =$

$$\begin{bmatrix} & \mathbf{d}_i & \\ & \mathbf{d}_{i-1} & \\ & \vdots & \\ & \mathbf{d}_1 & \\ I_{k-i-1} & & O_{k-i-1,i} \end{bmatrix}$$

where I_{k-i-1} is the $(k - i - 1)$ by $(k - i - 1)$ identity matrix, $O_{k-i-1,i}$ is the $(k - i - 1)$ by i all-zero matrix and $\mathbf{d}_i = (d_{i1}, d_{i2}, \cdots, d_{i(k-1)})$ satisfies $d_{ij} = 2^{i-1}$, $1 \leqq j \leqq k - i$.

By Lemma 5.7 this is clearly true for $i = 1$, and by induction (and by examination of $H(k, 1)$) we need only observe that

$$d_{ij} = \sum_{s=1}^{i-1} d_{sj} + \begin{cases} 1 & \text{if } j \leqq k-i, \\ 0 & \text{if } j > k-i. \end{cases}$$

Hence, if $j \leqq k - i$,

$$d_{ij} = \sum_{s=1}^{i-1} 2^{s-1} + 1 \quad \text{(by the inductive hypothesis)}$$

$$= 2^{i-1}.$$

Thus,

$$\text{Trace } (H(k, r)^i) = d_{i1} + d_{(i-1)2} + \cdots + d_{1i} \quad (i \leqq k-1)$$

$$= 2^{i-1} + 2^{i-2} + \cdots + 2^0$$

$$= 2^i - 1.$$ □

Note also that $a(1, k, r) = 1$ for every k and r since R^* is contained in R iff $R = \{-r + 1, -r + 2, \cdots, 0\}$, and thus $H(k, r)$ always has a unique nonzero diagonal entry.

6. Tabulations of computed values. The papers of Metropolis, Stein and Stein [9], and Minc [10], contain extensive tables of values for $a(n, k)$ for $k \leqq 9$; [9] also contains tables of the characteristic equations for $H(k, r)$ and approximate values for the maximal eigenvalue of $H(k, r)$, again for $k \leqq 9$.

Using Theorem 4.4, together with a set of multiprecision routines written by Dave Levin running on a VAX = 11/750 minicomputer, we have been able to verify all the existing tabulations of $a(n, k)$ and $a(n, k, r)$, and to also produce the following tables of values for $k = 10$, 11 and 12 and $1 \leqq n \leqq 50$. (See Tables 1–3.) Note that, as in the remarks following Corollary 4.6 in § 4, we define $a(n, k, r)$ to be the trace of $H(k, r)^n$ for every $n \geqq 1$, and, in the natural way, we define $a(n, k)$ to be the sum of the $a(n, k, r)$ for every $n \geqq 1$.

TABLE 1
$a(n, 10)$ $(1 \leqq n \leqq 50)$

n	$a(n, 10)$
1	10
2	50
3	226
4	962
5	3840
6	16130
7	65698
8	258690
9	986410
10	3628800
11	14684570
12	59216642
13	238282730
14	957874226
15	3850864416
16	15498424578
17	62494094138
18	252579461906
19	1023207993178
20	4152609019392
21	16866126115498
22	68562634725426
23	278965798055154
24	1136049057102978
25	4630217243007040
26	18885572768497186
27	77080942110390418
28	314787782093356610
29	1286217554205276682
30	5257934625513024000
31	21503218756525334970
32	87975626996492343810
33	360060541514858306810
34	1474102716437359422226
35	6036778093871268296928
36	24728373540667369577474
37	101318258384798761261866
38	415213810742569786850322
39	1701918744817772671844282
40	697719196611803588269312 0
41	2860816126328619998058413 8
42	1173167306977168715696168 18
43	4811546175049453514216314 90
44	1973597676853638993657364034
45	8096120287083522358723474560
46	3321507353442208488228981 5106
47	1362791567535790835768672462 10
48	5591856468242986518238165880 34
49	2294624949149162154512316665962
50	941658879830096965347414574720 0

7. Developments of the basic problem. The determination of $a(n, k)$ is only one of many problems associated with the design of a sliding window time element scrambler of the type described in § 3 above. There is also the fundamental problem of choosing n and k, and designing the method to be used to select permutations from $A(n, k)$.

TABLE 2
$a(n, 11)$ $(1 \leqq n \leqq 50)$

n	$a(n, 11)$
1	11
2	61
3	299
4	1393
5	6331
6	27949
7	126095
8	554177
9	2368847
10	9864101
11	39916800
12	176214841
13	775596313
14	3407118041
15	14951584189
16	65598500129
17	287972983669
18	1265785879297
19	5573449326001
20	24588660672953
21	108681408827381
22	481065936784384
23	2130831306657527
24	9445455128274737
25	41902710214254531
26	186040589545320129
27	826626380784149855
28	3675606432528120601
29	16354817596119737239
30	72817892293114361249
31	324404970589895718419
32	1446036425685642910913
33	6449154750576695662848
34	2877732287498099720 1469
35	1284735488437529001 17725
36	5738316970827342300 11665
37	2564217910410345862799157
38	1146350807497565794429 7053
39	5127026800110397281290 8657
40	2293996921254168380941 66177
41	1026818034189449323389052049
42	459792756935027542077070 2533
43	205965068355244842407458 27169
44	92295992963140763623590913024
45	413737754483439976252567341907
46	185530733306953534822909244 8661
47	83224367427938527266613667 13051
48	373443371842024862721257015 83553
49	167623315461313026160891570970211
50	752619449962479689980066343390501

As before we let

$$A(n,k) = \{\pi \in S_n : \overline{i\pi} \in \{\bar{i}, \overline{i+1}, \cdots, \overline{i+k-1}\} \text{ for every } i\}.$$

Another secondary problem, similar to the $a(n, k)$ evaluation problem, concerns choosing

TABLE 3
$a(n, 12)$ $(1 \leqq n \leqq 50)$

n	$a(n, 12)$
1	12
2	72
3	384
4	1944
5	9812
6	46080
7	227680
8	1100680
9	5199648
10	24011832
11	108505112
12	479001600
13	2290792932
14	10927434464
15	52034548064
16	247524019720
17	1177003136892
18	5598118158336
19	26647751359904
20	127007092256024
21	606269105086336
22	2898753047375312
23	13880706183899752
24	66544727442343936
25	319198916117248012
26	1532071808279181592
27	7358305929283036608
28	35363678926464144632
29	170062683110076661012
30	818309438846696002560
31	3939711747851871915248
32	18977103341489089532424
33	91452381430150298900000
34	440902914787573840187976
35	2126473158349980849520200
36	10259701680625467679872000
37	4951743355272467510215754O
38	23906751464024176285386l328
39	1154549828245379314130268192
40	5577319090541480294809775880
41	26949490191171589347220311676
42	130250684430090783496906489856
43	629660737886339608173390416560
44	3044553776812595993002687353336
45	14723969563417452202403843439488
46	71220434757273136282267411587712
47	344554065382463547747151575797784
48	1667163251724747083829231695497216
49	8067930334499348958454566728595916
50	39048557417232324389011734475683432

permutations suitable for use from $A(n, k)$. Clearly not every permutation in $A(n, k)$ is suitable for use as a scrambling pattern; consider the permutation $\pi \in S_n$ which satisfies $i\pi = i - 1$ $(2 \leqq i \leqq n)$ and $1\pi = n$. Then $\pi \in A(n, k)$ for every $k \geqq 1$, but the transmitted

speech enciphered using π will, in effect, not be permuted at all, and a device using such a permutation will offer no security at all.

The basic problem is what is commonly known as *residual intelligibility*. This term refers to the amount of intelligible information remaining in the analogue signal after it has been scrambled. Clearly, different permutations from $A(n, k)$ will have different residual intelligibilities, and it is thus desirable to have some method of choosing permutations from $A(n, k)$ which leave the minimum residual intelligibility.

In order to assess the level of residual intelligibility associated with a permutation, it is necessary to perform a large number of experiments to try to assess the amount of decipherable information remaining in speech after encryption using the permutation. Such experiments have been performed, and the results of these experiments have led us to conclude that the most important extra criterion that a permutation $\pi \in A(n, k)$ should satisfy in order to minimise the residual intelligibility is that

$$\overline{i\pi + 1} \neq \overline{(i+1)\pi}, \quad 1 \leqq i \leqq n-1 \quad \text{and} \quad \overline{n\pi + 1} \neq \overline{1\pi}.$$

This ensures that no two originally consecutive segments remain consecutive after encryption.

Thus, if we let

$$B(n,k) = \{\pi \in A(n,k) : \overline{i\pi + 1} \neq \overline{(i+1)\pi}, 1 \leqq i \leqq n-1 \quad \text{and} \quad \overline{n\pi + 1} \neq \overline{1\pi}\}$$

and $b(n, k) = |B(n, k)|$, then choosing permutations from $B(n, k)$ considerably reduces the probability of π leaving a high level of residual intelligibility in the scrambled speech. For a more detailed description of the experimental results and permutation evaluation procedures (see [3] and [4]).

Once we have made this definition, it is clearly important that some estimate be obtained for the size of $b(n, k)$. However, few results appear to exist on this problem, and the following summarises the results currently known to the authors.

THEOREM 7.1. (i) $b(n, 1) = b(n, 2) = 0$ *for every* n,

(ii) $b(n, 3) = b(n-2, 3) + b(n-3, 3)$, $n \geqq 6$, $b(3, 3) = 3$, $b(4, 3) = 2$, $b(5, 3) = 5$,

(iii) $b(n, 4) = 2b(n, 3)$, $n \geqq 4$,

(iv) $b(n, n) = n.\sum_{i=1}^{n-1} (-1)^{i-1}.a(n-i, n-i-1)$, $n \geqq 2$.

Theorem 7.1(i) is trivial. Parts (ii) and (iii) have been obtained independently by Dr. Keith Lloyd and the authors. Part (iv) is based on a recurrence relation due to Stacey [8], which says that $b(n+3, n+3) = n.b(n+2, n+2) + 2.(n+1).b(n+1, n+1) + (n+1).b(n, n)$. The solution to this recurrence to give (iv) can be found in [7, Ex. 15.5.10]. For further references to (iv) see also [16, Exercise 21, p. 160] and [16, Exercise 8, p. 172]. We now give a proof of (ii) and (iii).

In order to prove these two results, we first need some preliminary definitions. Let

$$B(n,k,r) = \{\pi \in B(n,k) : \pi \in A(n,k,r)\}.$$

As for Lemmas 4.2 and 4.3 we immediately have

LEMMA 7.2.

$$b(n,k) = \sum_{r=0}^{k-1} b(n,k,r).$$

Proof. Immediate from the definition. □

LEMMA 7.3. (i) $b(n, k, r) = b(n, k, k-1-r)$, $0 \leqq r \leqq k-1 \leqq n-1$.

(ii) $b(n, k, 0) = b(n, k, k-1) = 0$, $0 \leqq k-1 \leqq n-1$.

Proof. (i) As for the proof of Lemma 4.3(i), we define the function ϕ_k which maps S_n into S_n by

$\phi_k(\pi)$ maps i to $(n+1) - s\pi$ where $s \in \{1, 2, \cdots, n\}$ and $\bar{s} = \overline{-i-k+2}$.

We claim that ϕ_k is a one-to-one mapping from $B(n, k, r)$ into $B(n, k, k-1-r)$. This will establish the result. By the proof of Lemma 4.3(i) we have shown that ϕ_k is one to one and that if $\pi \in B(n, k, r)$ then $\phi_k(\pi) \in A(n, k, k-1-r)$; hence we need only show that $\phi_k(\pi) \in B(n, k)$ in order to establish the above claim, and thence the desired result. Now if i and j satisfy $\overline{i+1} = \bar{j}$, $i, j \in \{1, 2, \cdots, n\}$, then $i\phi_k(\pi) + 1 = n + 2 - t\pi$, and $j\phi_k(\pi) = n + 1 - s\pi$, where, by definition, $\overline{s+1} = \bar{t}$. But $\pi \in B(n, k, r)$, and because s and t satisfy $\overline{s+1} = \bar{t}$, we know $\overline{s\pi+1} \neq \bar{t}$. Hence $\overline{i\phi_k(\pi)+1} \neq \overline{j\phi_k(\pi)}$, and thus $\phi_k(\pi) \in B(n, k)$.

(ii) This part is trivial. □

We can now give the following lemma.

LEMMA 7.4. $B(n, k, k-2) = B(n, 3, 1)$, $k \geqq 3$.

Proof. We first show that if $1 \leqq r < k < n$, then $A(n, k-1, r-1)$ is a subset of $A(n, k, r)$. Suppose that $\pi \in A(n, k-1, r-1)$. Then, by definition, $\pi \in A(n, k-1)$ and hence $\pi \in A(n, k)$. Thus, by Lemma 4.1, we need only show that $|X_k(\pi, i)| = r$ for some $i \in \{1, 2, \cdots, n\}$.

Now $\pi \in A(n, k-1, r-1)$, and hence $|X_{k-1}(\pi, n-k+3)| = r-1$. By definition, $X_{k-1}(\pi, n-k+3)$ is a subset of $X_k(\pi, n-k+2)$, and

$$X_k(\pi, n-k+2) - X_{k-1}(\pi, n-k+3) = \{(n-k+2)\pi\},$$

since $\pi \in A(n, k-1)$. Thus:

$$|X_k(\pi, n-k+2)| = r-1+|\{(n-k+2)\pi\}| = r,$$

and hence $A(n, k-1, r-1)$ is a subset of $A(n, k, r)$. This immediately implies that $B(n, 3, 1)$ is a subset of $B(n, k, k-2)$, $k \geqq 3$.

We now show that $B(n, k, k-2)$ is a subset of $B(n, 3, 1)$, $k \geqq 3$, and the result follows.

Clearly, if $k = 3$, then the claim is automatically true, and so we suppose $k \geqq 4$. Now choose $\pi \in B(n, k, k-2)$, and suppose $\pi \notin B(n, 3)$, i.e., suppose there exists an $h \in \{1, 2, \cdots, n\}$ for which $\overline{h\pi} = \overline{h+s}$, where $3 \leqq s \leqq k-1$.

Now, by definition, $|X_k(\pi, i)| = k-2$, for every $i \in \{1, 2, \cdots, n\}$. Let $x, y \in \{1, 2, \cdots, n\}$ satisfy $\bar{x} = \overline{h-k+3}$ and $\bar{y} = \overline{h-k+4}$. Since

$$\overline{h\pi} \notin \{\bar{h}, \overline{h+1}, \overline{h+2}\}$$

we have: $h\pi \notin X_k(\pi, x)$ and $h\pi \notin X_k(\pi, y)$. But

$$|X_k(\pi, x)| = |X_k(\pi, y)| = k-2,$$

and hence if $u, v \in \{1, 2, \cdots, n\}$ satisfy $\bar{u} = \overline{h+1}$ and $\bar{v} = \overline{h+2}$ then $u\pi = u$ and $v\pi = v$. But since $\bar{v} = \overline{u+1}$ this contradicts the definition of $B(n, k)$ and hence $\pi \in B(n, 3)$. The result now follows by our observing that $B(n, 3) = B(n, 3, 1)$, since $B(n, 3, 0)$ and $B(n, 3, 2)$ are empty by Lemma 7.3(ii). □

Now since $b(n, 4) = b(n, 4, 1) + b(n, 4, 2)$ (by Lemmas 7.2 and 7.3(ii)), and since $b(n, 4, 1) = b(n, 4, 2)$ (by Lemma 7.3(i)), we know that $b(n, 4) = 2b(n, 4, 2)$. But $b(n, 4, 2) = b(n, 3, 1)$ (by Lemma 7.4), and hence $b(n, 4) = 2b(n, 3, 1)$, establishing Theorem 7.1(iii). It remains for us to prove the recurrence of Theorem 7.1(ii), noting that the initial values of $b(n, 3)$ for $n \leqq 5$ can be verified by hand.

Proof of Theorem 7.1(ii). We first introduce some notation.

Suppose $n \geqq 3$. Let

$$Q(n) = \{\pi \in B(n, 3) : 1\pi = 1\} \quad \text{and} \quad q(n) = |Q(n)|.$$

Also define

$$Q_1(n) = \{\pi \in Q(n) : 3\pi = 3\} \quad \text{and} \quad q_1(n) = |Q_1(n)|,$$

$$Q_2(n) = \{\pi \in Q(n) : 3\pi \neq 3\} \quad \text{and} \quad q_2(n) = |Q_2(n)|.$$

Then $Q(n)$ is equal to the disjoint union of $Q_1(n)$ and $Q_2(n)$, and we have

$$q(n) = q_1(n) + q_2(n), \qquad n \geq 3. \tag{1}$$

We also need the notion of a displacement vector. Choose $\pi \in S_n$, and let $\mathbf{d} = (d_1, d_2, \cdots, d_n)$ satisfy:

$$d_i \in \{0, 1, \cdots, n-1\} \quad \text{and} \quad \bar{d}_i = \overline{i\pi - i} \quad \text{for every } i \in \{1, 2, \cdots, n\}.$$

Then we call $\mathbf{d}$ the displacement vector of π. Note that permutations in $Q_1(n)$ and $Q_2(n)$ have displacement vectors of the form $(0, 2, \cdots)$ and $(0, 1, 2, \cdots)$, respectively.

Now suppose $n \geq 5$. We define the mapping ϕ_1 from $Q_1(n)$ into $Q(n-2)$ as follows. If $\pi \in Q_1(n)$ has displacement vector

$$(0, 2, d_3, d_4, \cdots, d_n)$$

then let $\phi_1(\pi)$ be the permutation having displacement vector

$$(d_3, d_4, \cdots, d_n).$$

It is straightforward to show that ϕ_1 is well defined and both one to one and onto. We have thus shown:

$$q_1(n) = q(n-2), \qquad n \geq 5. \tag{2}$$

Next suppose $n \geq 6$. We define the mapping ϕ_2 from $Q_2(n)$ into $Q(n-3)$ as follows. If $\pi \in Q_2(n)$ has displacement vector

$$(0, 1, 2, d_4, d_5, \cdots, d_n)$$

then let $\phi_2(\pi)$ be the permutation having displacement vector

$$(d_4, d_5, \cdots, d_n).$$

It is straightforward to show that ϕ_2 is well-defined and both one to one and onto. We have thus shown:

$$q_2(n) = q(n-3), \qquad n \geq 6. \tag{3}$$

Next suppose $n \geq 4$ and define a third mapping ϕ_{12} from $Q_1(n-1)$ into $Q_2(n)$ as follows. If $\pi \in Q_1(n-1)$ has displacement vector

$$(0, 2, d_3, d_4, \cdots, d_{n-1})$$

then let $\phi_{12}(\pi)$ be the permutation having displacement vector

$$(0, 1, 2, d_3, d_4, \cdots, d_{n-1}).$$

Again it is straightforward to show that ϕ_{12} is well defined and both one to one and onto. We then have

$$q_1(n-1) = q_2(n), \qquad n \geq 4. \tag{4}$$

Finally suppose $n \geq 3$. If $\mathbf{d}$ is the displacement vector of $\pi \in B(n, 3)$, and if $\pi^* \in B(n, 3)$ has displacement vector $\mathbf{d}^* = (d_{s+1}, d_{s+2}, \cdots, d_n, d_1, d_2, \cdots, d_s)$, then we

call π^* the s-fold cyclic shift of π. We now let

$$Q_{11}(n) = \{\pi^* : \pi^* = \text{the 1-fold cyclic shift of some } \pi \in Q_1(n)\},$$

$$Q_{21}(n) = \{\pi^* : \pi^* = \text{the 1-fold cyclic shift of some } \pi \in Q_2(n)\},$$

$$Q_{22}(n) = \{\pi^* : \pi^* = \text{the 2-fold cyclic shift of some } \pi \in Q_2(n)\}.$$

It is straightforward to show that all elements of $Q_{11}(n)$, $Q_{21}(n)$ and $Q_{22}(n)$ have displacement vectors of the forms: $(2, 0, \cdots, 0)$, $(1, 2, 0, \cdots)$ and $(2, 0, \cdots, 1)$, respectively. Hence the five sets

$$Q_1(n), Q_{12}(n), Q_2(n), Q_{21}(n), Q_{22}(n)$$

are all disjoint; moreover, every element of $B(n, 3)$ is in one of these sets. This immediately gives

$$b(n, 3) = 2q_1(n) + 3q_2(n), \qquad n \geqq 3. \tag{5}$$

We can now combine the above results to obtain the desired recurrence. Suppose $n \geqq 6$. Then:

$$\begin{aligned} b(n,3) &= 2q_1(n) + 3q_2(n) \quad \text{by (5)} \\ &= 2q(n-2) + 3q(n-3) \quad \text{by (2) and (3)} \\ &= 2q_1(n-2) + 2q_2(n-2) + 3q_1(n-3) + 3q_2(n-3) \quad \text{by (1)} \\ &= 2q_1(n-2) + 3q_2(n-2) + 2q_1(n-3) + 3q_2(n-3) \quad \text{by (4)} \\ &= b(n-2,3) + b(n-3,3) \quad \text{by (5).} \end{aligned}$$

□

Acknowledgments. The authors would like to acknowledge the assistance and encouragement of Racal Comsec Ltd. and Racal Research Ltd. The authors would also like to thank Dr. Keith Lloyd for his help in discovering the history of the problem.

REFERENCES

[1] H. J. BEKER, *Analogue speech security systems*, in Cryptography: Proc. Workshop on Cryptography, Burg Feuerstein 1982, Lecture Notes in Comput. Sci., 149, Springer–Verlag, Berlin, New York, 1983, pp. 130–146.

[2] ———, *Options available for speech encryption*, Radio Electron. Engineer, 54 (1984), pp. 35–40.

[3] H. J. BEKER AND F. C. PIPER, *Secure Speech Communications*, Academic Press, London, 1985.

[4] A. J. BROMFIELD AND C. J. MITCHELL, *Permutation selector for a sliding window time element scrambler*, preprint.

[5] M. R. GAREY AND D. S. JOHNSON, *Computers and Intractability*, W. H. Freeman, San Francisco, 1979.

[6] I. KAPLANSKY AND J. RIORDAN, *The Problème des Ménages*, Scripta Math., 12 (1946), pp. 113–124.

[7] W. LEDERMANN, (ed.), *Handbook of Applicable Mathematics, Volume* 5: *Geometry and Combinatorics*, John Wiley, New York, 1985.

[8] E. K. LLOYD, Private communication, May 1982.

[9] N. METROPOLIS, M. L. STEIN AND P. R. STEIN, *Permanents of cyclic* (0, 1) *matrices*, J. Combin. Theory, 7 (1969), pp. 291–321.

[10] H. MINC, *Permanents of* (0, 1)*-Circulants*, Canad. Math. Bull., 7 (1964), pp. 253–263.

[11] ———, *Permanents*, Addison–Wesley, Reading, MA, 1978.

[12] C. J. MITCHELL AND F. C. PIPER, *A classification of time element speech scramblers*, J. Institut. Electron. Radio Engineers, 55 (1985), pp. 391–396.

[13] W. O. J. MOSER, *The number of very reduced* $4 \times n$ *Latin rectangles*, Canad. J. Math., 19 (1967), pp. 1011–1017.

[14] J. RIORDAN, *Discordant permutations*, Scripta Math., 20 (1954), pp. 14–23.
[15] J. TOUCHARD, *Permutations discordant with two given permutations*, Scripta Math., 19 (1953), pp. 109–119.
[16] A. TUCKER, *Applied Combinatorics*, John Wiley, New York, 1980.
[17] L. G. VALIANT, *The complexity of computing the permanent*, Theoret. Comput. Sci., 8 (1979), pp. 189–201.
[18] ———, *The complexity of enumeration and reliability problems,* SIAM J. Comput., 8 (1979), pp. 410–421.
[19] E. G. WHITEHEAD, *Four-discordant permutations*, J. Austral. Math. Soc. Ser. A, 28 (1979), pp. 369–377.
[20] K. YAMAMOTO, *Structure polynomial of Latin rectangles and its application to a combinatorial problem*, Mem. Fac. Sci. Kyusyu Univ. Ser. A, 10 (1956), pp. 1–13.