A lower bound for the number of good permutations

Colin Cooper*

May 26, 2000

Abstract

For odd compound natural numbers $t = ns$, we prove an asymptotic lower bound on the number of permutations in S_t which are complete mappings. When $n, s \sim \sqrt{t}$ this lower bound is at least $(\sqrt{t})^{\sqrt{t}}$. The lower bound is constructed algorithmically.

1 Introduction

Let S_n denote the set of $n!$ permutations $\boldsymbol{\sigma} = (\sigma(0), ..., \sigma(i), ..., \sigma(n-1))$ of the symbols $\{0, 1, 2, ..., n-1\}$, where $\sigma(i)$ means $i \to \sigma(i)$.

The use of probability theory to infer the typical structure of permutations has a long and fascinating history. A great variety of asymptotic estimates of the structure of permutations were obtained by V. Gončarov [5] and later by W . Feller [6]. The most famous of these is that the number C of cycles in a uniformly selected permutation has expectation and variance asymptotic to $\log n$ and that the distribution of the random variable $(C - \log n)/\sqrt{\log n}$ tends to the standard normal distribution. The development of the Local Limit theorem for asymptotic distribution of sums of discrete random variables [4] gives a more precise value of the distribution of the central terms of C. The distribution of individual cycles was studied extensively by V. Kolchin in the monograph [8] and more recently [9].

In essence, such problems are of the type: What proportion of the permutations S_n satisfy a property Q and what is the limiting value of this proportion?

*School of Mathematical Sciences, University of North London, London N7 8DB, UK. Research supported by the STORM Research Group

The property G_n with which this paper is concerned may be stated as follows: Let $a+b$ denote the non-negative remainder on division by n. A permutation α has the property of being *good* ($\alpha \in G_n$) if the elements of the sequence $\beta = (\alpha(0)+0, \alpha(1)+1, ..., \alpha(n-1)+(n-1))$ are distinct, so that β is also a permutation.

Apart from the natural elegance of this problem, and the difficulty of obtaining an exact solution, there are also practical applications which we briefly discuss.

In the past, the security of transmitted data has been, on occasions, entrusted to rotor cipher systems. The principle of these systems and their deciphering algorithms is well established and described in [10]. The following summary is taken from [2].

A rotor induces a fixed permutation α of an alphabet of n symbols. The rotor rotates at predetermined intervals, so that at the k-th interval the input x produces the output $\alpha(x+k)-k$ (modulo n). The existence of coincidences of the form

$$\alpha(x+k)-k = \alpha(x+l)-l \tag{1}$$

means that x is given the same transformed values in the intervals k and l.

Such flaws in the structure of α are open to detection by statistical methods. In particular, if x is a frequently occurring letter of the alphabet, then (1) leads to an altered correlation between the output of the cipher system in intervals k and l. Establishing the existence of relations of the type (1) reduces the number of possible solutions for α which must be enumerated.

2 The Problem of Good Permutations

Following the notation of [3], define a *complete mapping* θ on a set X with binary operation $\circ$ as a bijection $\theta : X \to X$ such that the mapping $\eta : X \to X$ defined by $\eta(x) = x \circ \theta(x)$ is again a bijection.

Any group of odd order has a complete mapping (see Theorem 1.4.3 of [3]). Let $(\mathbb{Z}_n, \oplus)$ denote the group of integers under addition modulo n. For $(\mathbb{Z}_n, \oplus)$, n odd, it is trivial to construct n complete mappings based on the identity permutation by cyclically rotating the bottom row. For example, when $n=3$ we have $(0,\ 1,\ 2)$, $(1,\ 2,\ 0)$, $(2,\ 0,\ 1)$. When n is even, it is a theorem of [13] that there are no complete mappings on $(\mathbb{Z}_n, \oplus)$.

If we represent $\mathbb{Z}_n$ by the residues $\{0, 1, ..., n-1\}$ then the set of bijections from $\{0, 1, ..., n-1\}$ to $\{0, 1, ..., n-1\}$ is S_n the set of permutations on $\{0, 1, ..., n-1\}$. Let $\boldsymbol{e} = (0, 1, ..., n-1)$. We define addition $\tau = \boldsymbol{e} + \sigma$ by $\tau(i) = (i + \sigma(i)) \mod n$, $(i = 0, 1, ..., n-1)$. Here $x \mod n$ is the non-negative remainder on division by n. We say a permutation σ is *good* if $\tau = \boldsymbol{e} + \sigma$ is in S_n, and denote by G_n the set of good permutations of S_n. Thus a good permutation corresponds to a complete mapping.

It is not clear in what relationship the problem of good permutations stands to the classical probabilistic methods for enumerating permutations outlined in the Introduction, or if a better approach is to treat it as a problem of random allocations (see for example [7]), random functions, or even if the problem is intrinsically number theoretic. In fact studies of the problem have borrowed from all three fields with only partial success.

An asymptotic upper bound on the number $|G_n|$ of good permutations of $n!e^{-cn}$ where c is constant was first proved in [1] for $c = 0.0885$ using probabilistic methods. This bound was later improved to $c = \log\sqrt{2}$ in [11] by a deeper probabilistic analysis of a cycle structure.

For small values on n sampling and enumeration techniques can determine $|G_n|$ and hence c. From these results, the limiting value of c was estimated to be 0.9538 using statistical methods [2]. This accords well with the intuitive value $c = 1$ derived (for example) from the analogous allocation problem, with solution $n!/n^n$, of placing n balls in n boxes so that no box is empty.

Because of the sparsity of G_n within S_n there are no obvious sampling techniques for large n, and it is reasonable to consider an algorithmic method of generating good permutations.

As we mentioned earlier, we can find n good permutations by rotating the bottom row of the identity permutation. Levitskya [12], developed polynomial algorithms of order at least n^2, and also studied some interesting algebraic properties. However no known algorithm finds more than a polynomial number n^a, and it requires considerable effort to increase a beyond a value of 2. The main problem of devising algorithms seems to be that arithmetic modulo n does not support a recursion from $n-2$ to n.

In the case of compound numbers $t = ns$ we use an algorithm to establish a sub-exponential lower bound on G_t. In particular, when $n, s \sim \sqrt{t}$ this lower bound on $|G_t|$ is of the order $(\sqrt{t})^{\sqrt{t}}$. Thus we have the following theorem which is the subject of this paper.

Theorem 1 *Let t be any compound number, $t = ns$. If $t \to \infty$, then provided $s \geq 25\log n$ there exists a positive constant $K > 1$ such that*

$$|G_t| \geq (Ks)^n .$$

The algorithm we consider uses s copies of a good permutation of length n to produce a good permutation of length $t = ns$. For a non-trivial example let $n = 7$, $s = 5$, so that $t = 35$. The permutation $\pi = (0, 1, 3, 5, 2, 6, 4)$ is good in S_7. From the algorithm we can find the good permutation of S_{35} given below.

$$\big(0, 1, 3, 5, 9, 13, 18, 21, 22, 24, 26, 30, 34, 4, 7, 8, 10, 12, 16, 20, 25, 28, 29, 31, 33, 2, 6, 11, 14, 15, 17, 19, 23, 27, 32\big).$$

3 Difference notation for permutations

Let B_n be all sequences of length n on the symbols $\{0, 1, 2, ..., n-1\}$, and let S_n be all permutations on the symbols $\{0, 1, 2, ..., n-1\}$.

Let $r = a \mod n$ denote the non-negative remainder r on division of a by n, and let $b \equiv a \pmod{n}$ denote congruence modulo n. The following property of the remainder operator $\mod n$ is useful. If x, y are integers, then

$$(x + y) \mod n = ((x \mod n) + (y \mod n)) \mod n.$$

We make a convention concerning sequences obtained by arithmetic operations on elements of B_n. Let $\boldsymbol{x} = (x(0), x(1), ..., x(n-1))$ be such a sequence. Unless otherwise stated, we always assume that $\boldsymbol{x}$ satisfies $0 \leq x(i) \leq n-1$. If this is not the case, we reduce the entry $x(i)$ to its non negative remainder mod n.

We can difference a sequence $\boldsymbol{x}$ in B_n modulo n to give the difference diff($\boldsymbol{x}$) where

$$\begin{aligned}
\text{diff}(\boldsymbol{x}) &= (x(1) - x(0), x(2) - x(1), ..., x(0) - x(n-1)) \mod n \\
&= (a(0), a(1), ..., a(n-1)).
\end{aligned}$$

Given a sequence $\boldsymbol{a} = (a(0), a(1), ..., a(n-1))$, satisfying

$$a(0) + a(1) + \cdots + a(n-1) = 0 \mod n$$

then $\boldsymbol{a}$ is a difference sequence of some $\boldsymbol{x} \in B_n$. We can undifference $\boldsymbol{a}$ to n distinct sequences $\boldsymbol{x}$, as follows. Fix $r \in \{0, 1, ..., n-1\}$ and form the partial sums

$$\begin{aligned}
x(0) &= r \mod n, \\
x(1) &= r + a(0) \mod n, \\
x(2) &= r + a(0) + a(1) \mod n, \\
&\cdots \\
x(i) &= r + a(0) + a(1) + \cdots + a(i-1) \mod n, \\
&\cdots \\
x(n-1) &= r + a(0) + \cdots + a(n-2) \mod n.
\end{aligned}$$

The final sum

$$x(0) = r + a(0) + a(1) + \cdots + a(n-1) \mod n = r$$

follows correctly as $\boldsymbol{a}$ is a difference sequence. We note the $x(i)$ are all $0 \leq x(i) \leq n-1$.

When is the sequence $\boldsymbol{a}$ the difference of a permutation $\pi \in S_n$? An obvious necessary condition is that $a(i) \neq 0$, otherwise we would get two identical entries $x(i), x(i+1)$ on un-differencing.

Lemma 2 *Let $\boldsymbol{a} = (a(0), a(1), ..., a(n-1))$, where $0 \leq a(i) \leq n-1$, $i = 0, 1, ..., n-1$. The sequence $\boldsymbol{a}$ is the difference of a permutation $\pi \in S_n$ if and only if*

(i)

$$a(0) + a(1) + \cdots + a(n-1) \equiv 0 \pmod{n}$$

(ii) all other pairs (i, j) $0 \leq i \leq j \leq n-1$, satisfy

$$a(i) + a(i+1) + \cdots + a(j) \not\equiv 0 \pmod{n}.$$

Proof The first condition guarantees $\boldsymbol{a} = \text{diff}(\boldsymbol{x})$ for some $\boldsymbol{x} \in B_n$. We choose the $x(i)$ as described above, so that $0 \leq x(i) \leq n-1$.

Now, if

$$\begin{aligned} x(i) - x(0) &\equiv a(0) + \cdots + a(i-1) \pmod{n} \\ x(j+1) - x(0) &\equiv a(0) + \cdots + a(j) \pmod{n} \end{aligned}$$

then

$$x(j+1) - x(i) \equiv a(i) + \cdots + a(j) \pmod{n}.$$

thus $x(j+1) \neq x(i)$ if and only if $\sum_{k=i}^{j} a(k) \not\equiv 0 \pmod{n}$ if and only if all $x(i)$ are distinct for $i = 0, ..., n-1$.

If all the $x(i)$ are distinct and satisfy $0 \leq x(i) \leq n-1$ then $\boldsymbol{x}$ is a permutation of $\{0, 1, ..., n-1\}$ by the pidgeon hole principle.

□

For simplicity we often choose the permutation π starting with zero, when we undifference a sequence $\boldsymbol{a}$ so that we can talk about a permutation rather than an equivalence class.

Lemma 3 *Let $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{v} \in B_n$, the following diagram holds.*

$$\begin{array}{ccccl} \boldsymbol{x} & \xrightarrow{+\boldsymbol{v}} & \boldsymbol{y} & = \boldsymbol{x} + \boldsymbol{v} \mod n \\ {\scriptstyle \text{diff}(\boldsymbol{x})}\big\downarrow & & \big\downarrow{\scriptstyle \text{diff}(\boldsymbol{y})} & \\ \boldsymbol{a} & \xrightarrow{+\boldsymbol{w} = \text{diff}(\boldsymbol{v})} & \boldsymbol{b} & = \boldsymbol{a} + \boldsymbol{w} \mod n \end{array}$$

Proof

$$\begin{aligned} b(i) &= [y(i+1) - y(i)] \mod n \\ &= [(x(i+1) + v(i+1)) \mod n - (x(i) + v(i)) \mod n] \mod n \\ &= [(x(i+1) + v(i+1)) - (x(i) + v(i))] \mod n \\ &= [(x(i+1) - x(i)) \mod n + (v(i+1) - v(i)) \mod n] \mod n \\ &= [a(i) + w(i)] \mod n. \end{aligned}$$

$\square$

Next we ask when is $\boldsymbol{a}$ the difference of a good permutation $\pi \in G_n$?

Lemma 4 *If $\boldsymbol{a}$ is the difference of a permutation $\pi \in S_n$ then $\pi \in G_n$ if and only if*

(i) $a(i) \leq n-2,\ i = 0, 1, ..., n-1,$

(ii) $a(i) + \cdots + a(j) \not\equiv n - (j - i + 1) \pmod n$, *for all pairs* $(i, j) \neq (0, n-1)$.

Proof Let $\boldsymbol{e} = (0, 1, 2, ..., n-1)$, then $\mathrm{diff}(\boldsymbol{e}) = \mathbf{1}$. Let $\boldsymbol{b} = (\boldsymbol{a} + \mathbf{1}) \pmod n$ then $\boldsymbol{b} = \mathrm{diff}(\pi + \boldsymbol{e})$ by the previous theorem.

If $a(i) = n-1$ then $b(i) \equiv a(i) + 1 \equiv 0 \pmod n$ so the sequence $\boldsymbol{b}$ cannot be the difference of a permutation.

If $a(i) \leq n-2$ then $\boldsymbol{b} = \boldsymbol{a} + \mathbf{1} \mod n = \boldsymbol{a} + \mathbf{1}$. If this is the case, the partial sums, taken in the integers, are

$$\begin{aligned} b(i) + \cdots + b(j) &= a(i) + 1 + \cdots + a(j) + 1 \\ &= a(i) + \cdots + a(j) + (j - i + 1) \\ &\not\equiv 0 \pmod n, \end{aligned}$$

unless $(i, j) = (0, n-1)$ when the partial sum satisfies

$$b(0) + b(1) + \cdots + b(n-1) \equiv 0 \pmod n.$$

These are exactly the conditions for $\boldsymbol{b}$ to be the difference of a permutation. $\square$

4 Constructing good permutations as repeated patterns

Under certain conditions, we can construct good permutations in G_{ns} from permutations in G_n. To start with we consider a special case.

Let $\boldsymbol{b} = (b(0), ..., b(n-1))$ be a permutation difference, and let $\boldsymbol{b}[s] = (\boldsymbol{b}, \boldsymbol{b}, ..., \boldsymbol{b})$ be the sequence consisting of s copies of $\boldsymbol{b}$. Let $\theta n = b(0) + \cdots + b(n-1)$ be the sum of the entries $b(i)$ in the *natural numbers.*

Let $\gcd(a, b)$ denote the greatest common divisor of the natural numbers $a,\ b$.

Theorem 5 *Let* $s \in \mathbb{N},\ \pi \in G_n, \mathrm{diff}(\pi) = \boldsymbol{b}$. *If* $\gcd(\theta, s) = 1$ *and* $\gcd(\theta + 1, s) = 1$ *then* $\boldsymbol{b}[s]$ *is the difference of a good permutation* $\gamma \in G_{ns}$.

We will prove the theorem as a series of lemma's.

Lemma 6

$$\gcd(s,\theta)=1 \iff \theta, 2\theta, ..., (s-1)\theta \not\equiv 0 \pmod s$$

Lemma 7 *Let* $\pi \in S_n$, $\text{diff}(\pi)=\boldsymbol{b}$*. If* $\gcd(\theta,s)=1$ *then* $\boldsymbol{b}[s]$ *is the difference of a permutation* $\gamma \in S_{ns}$*.*

Proof Let $\boldsymbol{b}[s]=(a(i): i=0,...,ns-1)$ so that $a(i)=b(l)$ where $i=rn+l,\ 0\le r\le s-1,\ 0\le l\le n-1$.

Now let $i\le j$ where $i=rn+l,\ j=r'n+l'$. Consider

$$\begin{aligned} A(i,j) &= a(i)+\cdots+a(j) \\ &= b(l)+\cdots+b(n-1)+\cdots+b(0)+\cdots+b(l'). \end{aligned}$$

We must prove that $A(i,j)\ne 0 \pmod{ns}$. Let $k=r'-r$

$$A(i,j)=\begin{cases} k\theta n & l'=l-1 \quad k>0 \\ k\theta n + b(l)+\cdots+b(l') & l\le l' \quad\quad k\ge 0 \\ k\theta n - (b(l'+1)+\cdots+b(l-1)) & l'<l-1 \quad k>0 \end{cases}$$

Case of $l'=l-1$ *and* $k>0$.

$$\begin{aligned} A(i,j) &= k\theta n \equiv 0 \pmod{ns} \\ &\Rightarrow k\theta \equiv 0 \pmod s \end{aligned}$$

provided $(i,j)\ne(0,ns-1)$ then $k\in\{1,...,s-1\}$ so not possible.

Case of $l\le l'$.

$$\begin{aligned} k\theta n + b(l)+\cdots+b(l') &\equiv 0 \pmod{ns} \\ \Rightarrow k\theta n + b(l)+\cdots+b(l') &= \mu ns \\ \Rightarrow b(l)+\cdots+b(l') &= (\mu s - k\theta)n \\ &\equiv 0 \pmod n \end{aligned}$$

but $\boldsymbol{b}$ is a permutation difference so this is impossible.

Case of $l'<l-1$. This is the same as above. □

Lemma 8 *If* $\boldsymbol{b}$ *is the difference of* $\pi\in G_n$*, then provided* $\gcd(\theta+1,s)=1$, $(\boldsymbol{b}+\mathbf{1})[s]$ *is the difference of a permutation* $\pi=\gamma+\boldsymbol{e}\in S_{ns}$*.*

Proof

$$\mathrm{diff}(\gamma+\boldsymbol{e}) = (\boldsymbol{b}+\boldsymbol{1})[s] \mod sn = (\boldsymbol{b}+\boldsymbol{1})[s]$$

as $b(i) \leq n-2 < ns-1$. Now for $i \leq j$ consider

$$\begin{aligned} B(i,j) &= a(i)+\cdots+a(j)+(j-i+1) \\ &= A(i,j)+(j-i+1), \end{aligned}$$

where

$$j-i+1 = \begin{cases} kn & l'=l-1 \quad k>0 \\ kn+(l'-l+1) & l\leq l' \quad k\geq 0 \\ kn-((l-1)-(l'+1)+1) & l'<l-1 \quad k>0 \end{cases}$$

in the terms of the previous lemma.

Case of $l'=l-1$ *and* $k>0$.

$$\begin{aligned} A(i,j) &= A(i,j)+(j-i+1) \equiv 0 \pmod{ns} \\ &\Rightarrow k\theta n + kn \equiv 0 \pmod{ns} \\ &\Rightarrow k(\theta+1) \equiv 0 \pmod{s} \end{aligned}$$

but $k \in \{1,...,s-1\}$ so not possible.

Case of $l \leq l'$.

$$\begin{aligned} k\theta n + b(l)+\cdots+b(l')+kn+(l'-l+1) &\equiv 0 \pmod{ns} \\ \Rightarrow (k\theta+k)n + b(l)+\cdots+b(l')+(l'-l+1) &= \mu ns \\ \Rightarrow b(l)+\cdots+b(l')+(l'-l+1) &= (\mu s - k\theta - k)n \\ &\equiv 0 \pmod{n} \end{aligned}$$

but $\boldsymbol{b}$ is a good permutation difference so this is impossible.

Case of $l' < l-1$. This is the same as above. □

For example let $n=7$, $s=5$, $\pi=(0,1,3,5,2,6,4)$ then $\mathrm{diff}(\pi)=(1,2,2,4,4,5,3)=\boldsymbol{b}$. Thus $\theta=3$ and $\gcd(3,5)=1$, $\gcd(4,5)=1$ so that $\boldsymbol{b}[s]$ must be the difference of a good permutation of $ns=35$ symbols. Indeed, a corresponding permutation is

$$(0,1,3,5,9,13,18,21,22,24,26,30,34,4,7,8,10,12,16,20,25,28,29,31,33,2,6,11,14,15,17,19,23,27,32).$$

The simplest generalization is to add a fixed pattern $n\boldsymbol{m}$ to $\boldsymbol{b}$. Let $\mu = m(0)+m(1)+\cdots+m(n-1)$,where $m(i) \leq s-1$. Let $b(0)+\cdots+b(n-1)=\theta n$ as before. Typically we require

Type I : $\gcd(\theta,s)=1,\ \gcd(\theta+1,s)=1,\ \mu=\alpha s$

Type II : $\gcd(\theta+\mu, s) = 1$ and $\gcd(\theta+\mu+1, s) = 1$

Theorem 9 *If* $\boldsymbol{b}$ *is the difference of a good permutation in* S_n*, then* $\boldsymbol{c}[s] = (\boldsymbol{b}+n\boldsymbol{m})[s]$ *is the difference of a good permutation in* S_{ns}*, provided one of the conditions above is satisfied.*

Proof

If $\boldsymbol{c}[s] = (c(0), ..., c(ns-1))$ then

$$c(i) + \cdots + c(j) = A(i,j) + M(i,j),$$

where

$$M(i,j) = \begin{cases} kn\mu & l' = l-1 \quad k > 0 \\ kn\mu + n(m(l) + \cdots + m(l')) & l \le l' \quad\quad\; k \ge 0 \\ kn\mu - n(m(l'+1) + \cdots + m(l-1)) & l' < l-1 \quad k > 0 \end{cases}$$

The main case we need to consider is $l-1 = l'$ when

$$A(i,j) + M(i,j) = k\theta n + k\mu n$$

If $k\theta n + k\mu n \equiv 0 \pmod{ns}$ then $k\theta + k\mu \equiv 0 \pmod{s}$ and either

$$\begin{aligned} \mu = \alpha s \quad &\Rightarrow \quad k\theta \equiv 0 \pmod{s} \\ (\theta+\mu, s) = 1 \quad &\Rightarrow \quad k(\theta+\mu) \not\equiv 0 \pmod{s} \end{aligned}$$

leading to the same contradictions as before.

If $\mathrm{diff}(\gamma) = \boldsymbol{c}[s]$ then $\mathrm{diff}(\gamma + \boldsymbol{e}) = (\boldsymbol{c}+\boldsymbol{1})[s]$ as

$$b(i) + nm(i) \le n - 2 + n(s-1) = ns - 2.$$

Now similarly,

$$\begin{aligned} \mu = \alpha s \quad &\Rightarrow \quad k(\theta+1) \equiv 0 \pmod{s} \\ (\theta+\mu+1, s) = 1 \quad &\Rightarrow \quad k(\theta+\mu+1) \not\equiv 0 \pmod{s}. \end{aligned}$$

$\square$

As an example, let $n = 3$, $\pi = (0,1,2)$ so that $\boldsymbol{b} = (1,1,1)$ and $\theta = 1$. Let $s = 3$ and let $\boldsymbol{m} = (0,1,2)$ so that $\mu = 1s$. The Type I pattern is $\boldsymbol{c} = \boldsymbol{b} + 3\boldsymbol{m} = (1,4,7)$ and $\boldsymbol{c}[3]$ gives the good permutation $(0,1,5,3,4,8,6,7,2)$.

5 Proof of Theorem 1

Let $t = ns,\ n \leq s$ We will construct Type I good permutations $\boldsymbol{c}[s] = (\boldsymbol{b}+n\boldsymbol{m})[s]$ based on the n-pattern $\boldsymbol{b} = (1, 1, ..., 1)$, with $\theta = 1$ Thus we require $\gcd(1, s) = 1,\ \gcd(2, s) = 1, \mu = \alpha s$. The first two conditions always hold for s odd. Now

$$\mu = m(0) + m(1) + \cdots + m(n-1) = \alpha s,$$

where $0 \leq m(i) \leq s - 1$. We choose ϵ so that $\alpha = \lfloor n(1-\epsilon) \rfloor$ is a whole number, thus in future we will write $\alpha = n(1-\epsilon)$.

If we consider a scheme for allocating αs balls into n boxes the expected occupancy of a box is $\alpha s/n = s(1-\epsilon)$, thus

$$\lambda = \Pr(\text{ Some box has occupancy } \geq s) \leq n \exp\left(-\frac{\epsilon^2}{3} s(1-\epsilon)\right),$$

follows from the Chernoff bound for binomial tails.

Let $s > 25 \log n$ then when $\epsilon \sim \frac{1}{2}$, $\lambda = n^{-1/25}$ is strictly less than 1. Of the $\rho = \binom{n+\alpha s-1}{n-1}$ occupancy schemes, $\boldsymbol{m} = (x(0), ..., x(n-1))$, at least $(1-\lambda)\rho$ satisfy $x(i) \leq s-1,\ (i = 0, 1, ..., n-1)$ and can be used to construct distinct Type I patterns $\boldsymbol{c}[s]$ using s copies of $\boldsymbol{b} + n\boldsymbol{m}$, where $\boldsymbol{c}[s]$ is the difference of a good permutation in S_{ns}.

Crudely,

$$\binom{n-1+n(1-\epsilon)s}{n-1} \geq \frac{A}{\sqrt{ns}} \left(\frac{se}{2}\right)^n,$$

for some positive constant A, when $\epsilon \sim \frac{1}{2}$. This completes the proof of Theorem 1.

6 Concluding remarks

For the case of certain compound numbers $t = ns$, we have improved the lower bound on the number of good permutations on t symbols from a polynomial power of t to an sub-exponential one, $\exp(n \log s)$. However the exponent is sublinear in $t! \sim \exp(t \log t/e)$ the size of S_t. Moreover no such construction exists for prime t.

Enumeration for small t suggests that most good permutations do not have differences which are repeated patterns, so it is indicative of the density of good permutations that such a sparse subclass is large.

References

[1] Cooper, C. and Kovalenko, I.N. (1995) *An upper bound for the number of complete mappings.* Theory of Probability and Mathematical Statistics. 53, 69-75 (in Russian).

[2] Cooper C, Gilchrist R, Kovalenko I.N. and Novakovic D. (1999) *Deriving the number of good permutations with applications to cryptography.* Cybernetics and Systems Analysis 5, 10-16.

[3] Dénes, J. and Keedwell, A.D. (1974) *Latin Squares and Their Application.* English University Press.

[4] Gnedenko B.V. and Kolmogorov A. N. (1954) *Limit distributions for sums of independent random variables.* Addison-Wesley, Reading MA.

[5] Gončarov V. (1944) *Du domaine d'analyse combinatoire.* Bulletin de l'Académie Sciences URSS, Sér. Math. 8, 3-48 (in Russian, French summary).

[6] Feller W. (1945) *The fundamental limit theorems in probability.* Bulletin of AMS 51, 800-832.

[7] Kolchin V.F, Sevast'yanov B. A and Christyakov V.P (1978) *Random allocations.* Wiley, New York.

[8] Kolchin V. F. (1986) *Random Mappings.* Optimization Software, New York.

[9] Kolchin V. F. (1999) *Random Graphs.* (Encyclopedia of mathematics and its applications; v 53) Cambridge University Press, Cambridge.

[10] Konheim R. (1991) *Cryptography, a primer.* Wiley, Chichester.

[11] Kovalenko, I.N. (1995) *On an upper bound for the number of complete mappings.* Cybernetics and Systems Analysis. 1, 81-85 (in Russian).

[12] Levitskya, A.A. (1996) *A combinatorial problem concerning the class of permutations over the ring* $\mathbb{Z}_n$ *of residuals modulo n (for odd n).* Problems of Control and Informatics. 5, 99-109.

[13] Paige, L.J. (1951) *Complete mappings of finite groups.* Pacific J. Math 1, 111-116.