



**HAL**  
open science

# On the Minimum Number of Completely 3-Scrambling Permutations

Jun Tarui

► **To cite this version:**

Jun Tarui. On the Minimum Number of Completely 3-Scrambling Permutations. 2005 European Conference on Combinatorics, Graph Theory and Applications (EuroComb '05), 2005, Berlin, Germany. pp.351-356, 10.46298/dmtcs.3443 . hal-01184432

**HAL Id: hal-01184432**

**<https://inria.hal.science/hal-01184432>**

Submitted on 14 Aug 2015

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On the Minimum Number of Completely 3-Scrambling Permutations

Jun Tarui

Department of Information and Communication Engineering, University of Electro-Communications  
Chofu, Tokyo 182-8585 Japan tarui@ice.uec.ac.jp

A family  $\mathcal{P} = \{\pi_1, \dots, \pi_q\}$  of permutations of  $[n] = \{1, \dots, n\}$  is *completely  $k$ -scrambling* [Spencer, 1972; Füredi, 1996] if for any distinct  $k$  points  $x_1, \dots, x_k \in [n]$ , permutations  $\pi_i$ 's in  $\mathcal{P}$  produce all  $k!$  possible orders on  $\pi_i(x_1), \dots, \pi_i(x_k)$ . Let  $N^*(n, k)$  be the minimum size of such a family. This paper focuses on the case  $k = 3$ . By a simple explicit construction, we show the following upper bound, which we express together with the lower bound due to Füredi for comparison.

$$\frac{2}{\log_2 e} \log_2 n \leq N^*(n, 3) \leq 2 \log_2 n + (1 + o(1)) \log_2 \log_2 n.$$

We also prove the existence of  $\lim_{n \rightarrow \infty} N^*(n, 3)/\log_2 n = c_3$ . Determining the value  $c_3$  and proving the existence of  $\lim_{n \rightarrow \infty} N^*(n, k)/\log_2 n = c_k$  for  $k \geq 4$  remain open.

## 1 Introduction and Summary

Following Spencer [Sp72] and Füredi [Fü96], call a family  $\mathcal{P} = \{\pi_1, \dots, \pi_q\}$  of permutations of  $[n]$  *completely  $k$ -scrambling* if for any distinct  $x_1, x_2, \dots, x_k \in [n]$ , there exists a permutation  $\pi_i \in \mathcal{P}$  such that  $\pi_i(x_1) < \pi_i(x_2) < \dots < \pi_i(x_k)$ ; or equivalently,  $\pi_i$ 's applied to  $x_1, x_2, \dots, x_k$  produce all  $k!$  orders. This paper focuses on the case  $k = 3$ . Following Füredi [Fü96], say that a family  $\mathcal{P}$  is *3-mixing* if for any distinct  $x, y, z \in [n]$ , there is a permutation  $\pi_i \in \mathcal{P}$  that places  $x$  between  $y$  and  $z$ , i.e., there is a permutation  $\pi_i$  such that either  $\pi_i(y) < \pi_i(x) < \pi_i(z)$  or  $\pi_i(z) < \pi_i(x) < \pi_i(y)$ .

Let  $N^*(n, k)$  be the minimum  $q$  such that completely  $k$ -scrambling  $q$  permutations exist for  $[n]$ . The best known bounds for  $N^*(n, k)$  can be expressed as follows. For arbitrary fixed  $k \geq 3$ , as  $n \rightarrow \infty$ ,

$$\left( \frac{1}{\log_2 e} (k-1)! + o(1) \right) \log_2 n \leq N^*(n, k) \leq \frac{k}{\log_2(k!/(k!-1))} \log_2 n. \quad (1)$$

The coefficient of the upper bound in (1) is  $\Theta(k \cdot k!)$ ; thus the gap between the coefficients of the lower and upper bounds in (1) is  $\Theta(k^2)$ . The upper bound in (1) was shown by Spencer [Sp72] by a probabilistic argument, where one considers the probability that some order among some  $x_1, \dots, x_k$  is never produced by  $q$  independent random permutations. The lower bound in (1) was first proved by Füredi [Fü96] for  $k = 3$ , and was proved for  $k \geq 3$  by Radhakrishnan [Ra03]; entropy arguments are used in both work;

the factor  $\log_2 e$  in the lower bound comes from the fact that  $\int_0^1 H(x)dx = (\log_2 e)/2$ , where  $H(x)$  is the binary entropy function.

As for the case  $k = 3$ , Füredi [Fü96] has shown that

$$\frac{2}{\log_2 e} \log_2 n \leq N^*(n, 3) \leq \left( \frac{10}{\log_2 7} \right) \log_2 n + O(1), \quad (2)$$

where the coefficients of  $\log_2 n$  are  $1.38\dots$  and  $3.56\dots$  in (2). The lower bound in (2) is in fact a lower bound for the case where we only require a family to be 3-mixing. No better lower bound for completely 3-scrambling families is known. If a family  $\mathcal{P} = \{\pi_1, \dots, \pi_q\}$  is 3-mixing, by adding to  $\mathcal{P}$  the  $q$  reverse permutations of  $\pi_i$ 's mapping  $x \mapsto n+1-\pi_i(x)$ , we can obtain completely 3-scrambling  $2q$  permutations. Ishigami [Is95] has given an efficient recursive construction of 3-mixing families starting with a 3-mixing family of five permutations of  $\{1, \dots, 7\}$ . Füredi [Fü96] gave the upper bound in (2) by making these observations and doubling the size of Ishigami's 3-mixing family.

In this paper, we first give an improved upper bound for  $N^*(n, 3)$  by a simple construction. Let  $f(q)$  be the maximum  $n$  such that completely 3-scrambling  $q$  permutations exist for  $[n]$ .

### Theorem 1

$$f(q) \geq \binom{\lfloor q/2 \rfloor}{\lfloor q/4 \rfloor}.$$

The following upper bound on  $N^*(n, 3)$  readily follows.

### Corollary 1

$$N^*(n, 3) \leq 2 \log_2 n + (1 + o(1)) \log_2 \log_2 n.$$

It seems natural to conjecture that for every fixed  $k \geq 3$ , as  $n \rightarrow \infty$ ,  $N^*(n, k) = (c_k + o(1)) \log_2 n$  for some  $c_k$ . We show the existence of limit for the case  $k = 3$ :

### Theorem 2

$$\lim_{q \rightarrow \infty} \frac{\log_2 f(q)}{q} = C \text{ exists.}$$

The following immediately follows.

### Corollary 2

$$\lim_{n \rightarrow \infty} \frac{N^*(n, 3)}{\log_2 n} = 1/C = c_3 \text{ exists.}$$

## 2 Proofs

We can identify in a natural way a total order  $\phi$  on  $[n]$  and the permutation of  $[n]$  induced by  $\phi$ ; thus we speak interchangeably in terms of permutations and total orders. In fact for an arbitrary finite set  $U$  with  $n$  elements, we can assume for our purposes that  $U$  is identified with  $[n]$  in an arbitrary fixed way, and speak about permutations of  $U$  in terms of total orders on  $U$ .

**Proof of Theorem 1.** Put  $r = \lfloor q/2 \rfloor$  and let  $\mathcal{F} = \{A_1, A_2, \dots, A_m\}$  be a family of subsets of  $\{1, \dots, r\}$  such that  $A_i \not\subseteq A_j$  for all  $i \neq j$ ; i.e.,  $\mathcal{F}$  is an antichain.

For each point  $x \in \{1, \dots, r\}$ , define two orders  $\phi_x$  and  $\psi_x$  on  $\mathcal{F}$ . In both orders  $\phi_x$  and  $\psi_x$ , the sets  $A_i$  containing the point  $x$  are smaller than all the sets  $A_k$  not containing  $x$ . Among the sets containing  $x$  and among the sets not containing  $x$ : in the order  $\phi_x$ ,  $A_i < A_j$  precisely when  $i < j$ ; in the order  $\psi_x$ , this is reversed, and  $A_i < A_j$  precisely when  $i > j$ .

We claim that for arbitrary distinct  $i, j, k \in [m]$ , there exists an order  $\theta \in \{\phi_1, \psi_1, \phi_2, \psi_2, \dots, \phi_r, \psi_r\}$  such that  $A_i < A_j < A_k$  in the order  $\theta$ . To see the claim fix a point  $x \in (A_i - A_k) \neq \emptyset$ , i.e.,  $x \in A_i$  and  $x \notin A_k$ . Depending on whether  $x \in A_j$  or  $x \notin A_j$ , we specify an order  $\theta$  that produces the ordering  $A_i < A_j < A_k$ .

Case  $x \in A_j$ : Let  $\theta = \phi_x$  if  $i < j$  and let  $\theta = \psi_x$  if  $i > j$ .

Case  $x \notin A_j$ : Let  $\theta = \phi_x$  if  $j < k$  and let  $\theta = \psi_x$  if  $j > k$ .

Clearly under the order  $\theta$ ,  $A_i < A_j < A_k$ . Hence the  $2r$  orders thus defined on  $[m]$  are completely 3-scrambling. We obtain the theorem by taking  $\mathcal{F}$  to be the family of all subsets of  $\{1, \dots, r\}$  with cardinality  $\lfloor r/2 \rfloor = \lfloor q/4 \rfloor$ .  $\square$

**Proof of Theorem 2.** Our proof of Theorem 2 will be basically similar to Füredi's proof [Fü96] of the existence of  $\lim_{q \rightarrow \infty} (\log_2 g(q)) / q$ , where  $g(q)$  is the maximum  $n$  such that 3-mixing  $q$  permutations exist for  $[n]$ . To make a recursive construction go through for scrambling permutations, we introduce and use red-blue colored doubly reversing permutations: Call a family  $\mathcal{P} = \{\pi_1, \dots, \pi_q\}$  of permutations of  $[n]$  2-reversing if there is a coloring  $\chi : \{\pi_1, \dots, \pi_q\} \rightarrow \{\text{red}, \text{blue}\}$  such that for every distinct  $i, j \in [n]$ , there are red  $\pi_\kappa$ , red  $\pi_\lambda$ , blue  $\pi_\mu$ , and blue  $\pi_\nu$  satisfying

$$\pi_\kappa(i) < \pi_\kappa(j), \pi_\lambda(i) > \pi_\lambda(j); \pi_\mu(i) < \pi_\mu(j), \pi_\nu(i) > \pi_\nu(j).$$

For a permutation  $\pi$  of  $[n]$ , let  $\text{reverse}(\pi)$  be the permutation of  $[n]$  mapping  $x \mapsto n + 1 - \pi(x)$ . Let  $\mathcal{P}$  be a family of permutations of  $[n]$  with  $|\mathcal{P}| \geq 3$ . We can easily transform  $\mathcal{P}$  to a 2-reversing family by adding at most two permutations as follows. Arbitrarily fix two distinct permutations  $\sigma, \tau \in \mathcal{P}$  such that  $\tau \neq \text{reverse}(\sigma)$ ; such  $\sigma$  and  $\tau$  exist since  $|\mathcal{P}| \geq 3$ ; add  $\text{reverse}(\sigma)$  and  $\text{reverse}(\tau)$  to  $\mathcal{P}$ ; color  $\sigma$  and  $\text{reverse}(\sigma)$  red; color  $\tau$  and  $\text{reverse}(\tau)$  blue; color the remaining permutations arbitrarily.

Let  $f^*(q)$  be the maximum  $n$  such that completely 3-scrambling and 2-reversing  $q$  permutations exist for  $[n]$ . By definition and from the discussion above we have

$$f^*(q) \leq f(q) \leq f^*(q + 2). \tag{3}$$

### Claim 1

$$f^*(q + r) \geq f^*(q)f^*(r).$$

For the moment we assume that Claim 1 holds and go on to derive Theorem 2.

The sequence  $(1/q) \log_2 f^*(q)$  is bounded above. From this and Claim 1 it follows by classical calculus (Fekete's theorem) that

$$\lim_{q \rightarrow \infty} \frac{1}{q} \log_2 f^*(q) = \limsup_{q \rightarrow \infty} \frac{1}{q} \log_2 f^*(q).$$

From (3) it now follows that

$$\lim_{q \rightarrow \infty} \frac{1}{q} \log_2 f(q) = \lim_{q \rightarrow \infty} \frac{1}{q} \log_2 f^*(q).$$

Thus we are left to prove Claim 1.

Let  $\mathcal{S} = \{\sigma_1, \dots, \sigma_q\}$  and  $\mathcal{T} = \{\tau_1, \dots, \tau_r\}$  be completely 3-scrambling and 2-reversing families of permutations of  $[l]$  and  $[m]$  respectively. Assume that both families are validly red-blue colored. Let  $U = \{(i, j) : 1 \leq i \leq l, 1 \leq j \leq m\}$ ; think of  $U$  as a matrix with  $l$  rows and  $m$  columns. We will show that we can define  $q + r$  orders on  $U$  that are completely 3-scrambling and 2-reversing. Note that from this Claim 1 follows.

Let  $x = (i, j)$  and  $y = (i', j')$  be distinct elements of  $U$ . For  $k = 1, \dots, q$ , define the order  $\tilde{\sigma}_k$  using  $\sigma_k$  in a row-major form as follows: if  $i \neq i'$ , order  $x$  and  $y$  according to the order of  $\sigma_k(i)$  and  $\sigma_k(i')$ . When  $i = i'$ : if  $\sigma_k$  is red,  $(i, j) < (i, j') \iff j < j'$ ; if  $\sigma_k$  is blue,  $(i, j) < (i, j') \iff j > j'$ . Similarly for  $k = 1, \dots, r$ , define the order  $\tilde{\tau}_k$  on  $U$  in a column-major form: when  $j \neq j'$ ,  $x < y \iff \tau_k(j) < \tau_k(j')$ ; when  $j = j'$ : if  $\tau_k$  is red,  $(i, j) < (i', j) \iff i < i'$ ; if  $\tau_k$  is blue,  $(i, j) < (i', j) \iff i > i'$ . As for colors, let  $\tilde{\sigma}_k$  and  $\tilde{\tau}_k$  inherit the colors of  $\sigma_k$  and  $\tau_k$ .

**Claim 2** The family  $\mathcal{F} = \{\tilde{\sigma}_1, \dots, \tilde{\sigma}_q, \tilde{\tau}_1, \dots, \tilde{\tau}_r\}$  is completely 3-scrambling and 2-reversing.

To see Claim 2, let  $x_1 = (i_1, j_1), x_2 = (i_2, j_2), x_3 = (i_3, j_3)$  be distinct elements of  $U$ . If  $i_1, i_2, i_3$  are all distinct,  $\sigma_k$ 's produce all six orderings of  $i_1, i_2, i_3$ , and hence  $\tilde{\sigma}_k$ 's produce all six orderings of  $x_1, x_2, x_3$ . Similar arguments with  $\tau_k$ 's and  $\tilde{\tau}_k$ 's apply for the case when  $j_1, j_2, j_3$  are all distinct.

The remaining case is when  $|\{i_1, i_2, i_3\}| = |\{j_1, j_2, j_3\}| = 2$ . We write, e.g., 231 to express the ordering  $x_2 < x_3 < x_1$ . Assume that

$$x_1 = (i, j), x_2 = (i, j'), x_3 = (i', j), \quad i \neq i', j \neq j'.$$

We will see that all six orderings of  $x_1, x_2, x_3$  are produced by checking that (1) all the four orders in which  $x_3$  is smallest or largest, i.e., 312, 321, 123, 213 are produced and that (2) all the four orders in which  $x_2$  is smallest or largest are produced.

A red  $\tilde{\sigma}_\kappa$  and a blue  $\tilde{\sigma}_\mu$  satisfying  $\sigma_\kappa(i) < \sigma_\kappa(i')$  and  $\sigma_\mu(i) < \sigma_\mu(i')$  produce 123 and 213 respectively. Similarly, a red  $\tilde{\sigma}_\lambda$  and a blue  $\tilde{\sigma}_\nu$  satisfying  $\sigma_\lambda(i) > \sigma_\lambda(i')$  and  $\sigma_\nu(i) > \sigma_\nu(i')$  produce 312 and 321 respectively. Thus all the four orders in which  $x_3$  is smallest or largest are produced. Similarly, two red  $\tilde{\tau}$ 's and two blue  $\tilde{\tau}$ 's ordering  $j$  and  $j'$  in both directions produce the four orders in which  $x_2$  is smallest or largest.

Finally, if  $x = (i, j)$  and  $y = (i', j')$  are distinct points in  $U$ , either (i)  $i \neq i'$  or (ii)  $j \neq j'$ . The 2-reversing condition is satisfied by  $\tilde{\sigma}_k$ 's in case (i) and by  $\tilde{\tau}_k$ 's in case (ii).  $\square$

## Acknowledgements

The author thanks the anonymous referees for helpful comments.

## References

- [Fü96] Z. Füredi. Scrambling Permutations and Entropy of Hypergraphs, *Random Structures and Algorithms*, vol. 8, no. 2, pp. 97–104, 1996.
- [Is95] Y. Ishigami. Containment Problems in High-Dimensional Spaces, *Graphs and Combinatorics*, vol. 11, pp. 327–335, 1995.
- [Ra03] J. Radhakrishnan. A Note on Scrambling Permutations, *Random Structures and Algorithms*, vol. 22, no. 4, pp. 435–439, 2003.
- [Sp72] J. Spencer. Minimal Scrambling Sets of Simple Orders, *Acta Mathematica Hungarica*, vol. 22, pp. 349–353, 1972.

