On the uniform generation of random derangements

J. Ricardo G. Mendonça^{a,b}

^aLPTMS, CNRS, Université Paris-Sud, Université Paris-Saclay, 91405 Orsay CEDEX, France ^bEscola de Artes, Ciências e Humanidades, Universidade de São Paulo, 03828-000 São Paulo, SP, Brazil

Abstract

We show how to generate random derangements with the expected distribution of cycle lengths by two different techniques: random restricted transpositions and sequential importance sampling. The algorithms are simple to understand and implement and possess a performance comparable with those of currently known methods. We measure the mixing time (in the chi-square distance) of the randomized algorithm and our data indicate that $\tau_{mix} \sim O(n \log n)$, where *n* is the size of the derangement. The sequential importance sampling algorithm generates random derangements uniformly in O(n) time but with a small probability O(1/n) of failing.

Keywords: Random permutation, restricted permutation, sequential importance sampling 2010 MSC: 05A05, 65C60, 68R05

1. Introduction

Derangements are permutations $\sigma = \sigma_1 \cdots \sigma_n$ on $n \ge 2$ labels such that $\sigma_i \ne i$ for all i = 1, ..., n. Besides being useful as permutations, derangements are important *per se* in a number of applications like in the testing of software branch instructions and random paths and data randomization and experimental design (Edgington & Onghena, 2007; Sedgewick & Flajolet, 2013). A recent review on the generation of random permutations appeared in Bacher et al. (2017). A well known algorithm to generate random derangements is Sattolo's algorithm, that outputs a random cyclic derangement on *n* labels in O(n) time (Gries & Xue, 1988; Prodinger, 2002; Sattolo, 1986). An explicit O(2n) algorithm to generate random derangements in general (not only cyclic derangements) has been given in Panholzer et al. (2004) and Martínez et al. (2008). Algorithms to generate all *n*-derangements are also known (Baril & Vajnovszki, 2004; Korsh & LaFollette, 2004; Wilson, 2009).

In this letter we propose and test two procedures to generate random derangements with the expected distribution of cycle lengths: one based on the randomization of derangements and the other based on a simple sequential importance sampling scheme. Simulations show that the randomized algorithm samples a derangement uniformly in $O(n \log n)$ time while the sequential importance sampling algorithm does it in O(n) time but with a small probability $\sim O(1/n)$ of failing. The proposed algorithms do not use pre-calculated quantities or auxiliary data structures, being straighforward to understand and implement.

2. Mathematical preliminaries

Let us briefly review some notation and terminology on permutations; for details see Charalambides (2002) and James & Kerber (1981).

We denote the set (that forms a group under the operation of composition) of all permutations on $n \ge 2$ labels $\{1, ..., n\}$ by \mathscr{S}_n . We write an *n*-permutation in one-line notation as $\sigma = \sigma_1 \cdots \sigma_n$, where $\sigma_i = \sigma(i)$. A cycle of length $k \le n$ in a *n*-permutation σ is a sequence of indices $i_1, ..., i_k$ such that $\sigma_{i_1} = i_2, ..., \sigma_{i_{k-1}} = i_k$, and $\sigma_{i_k} = i_1$, completing the cycle. Fixed points are 1-cycles, while transpositions are 2-cycles. An *n*-permutation with a_k cycles of

Email address: jricardo@usp.br (J. Ricardo G. Mendonça)

Preprint submitted to Elsevier

length $k, 1 \le k \le n$, is said to be of type (a_1, \ldots, a_n) , with $\sum_k ka_k = n$. For example, the 9-permutation 174326985 = (8)(6)(34)(2795)(1) has 5 cycles and is of type (3, 1, 0, 1), where we have omitted the trailing $a_5 = a_6 = \cdots = a_9 = 0$.

The number of *n*-permutations with *k* cycles is given by the unsigned Stirling number of the first kind $\binom{n}{k}$. We have $\binom{n}{n} = 1$, counting just the identity permutation $(1)(2)\cdots(n)$, $\binom{n}{n-1} = \binom{n}{2}$, counting *n*-permutations of n-2 fixed points, that can be taken in $\binom{n}{n-2} = \binom{n}{2}$ different ways, plus a transposition of the remaining two labels, and $\binom{n}{1} = (n-1)!$, the number of 1-cycle (or cyclic) *n*-derangements. It can be shown that $\binom{n}{2} = (n-1)!H_{n-1}$, where H_n is the *n*-th harmonic number. Other useful formulae involving Stirling numbers of the first kind are $\binom{0}{0} = 1$, $\binom{n}{0} = 0$, and the recursion relation

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$
 (1)

Obviously, $\begin{bmatrix} n \\ 1 \end{bmatrix} + \dots + \begin{bmatrix} n \\ n \end{bmatrix} = n!.$

Let us denote the set (that does not form a group) of all *n*-derangements by \mathcal{D}_n . It is well known that

$$|\mathcal{D}_n| = n! \left(1 - \frac{1}{1!} + \dots + \frac{(-1)^n}{n!} \right) = \left\lfloor \frac{n! + 1}{e} \right\rfloor, \quad n \ge 1,$$
(2)

the so-called *rencontres* numbers (OEIS A000166). Let us also denote the set of *k*-cycle *n*-derangements, irrespective of their type, by $\mathscr{D}_n^{(k)}$. Note that $\mathscr{D}_n^{(k)} = \varnothing$ for $k > \lfloor n/2 \rfloor$. If we want to generate random *n*-derangements uniformly over $\mathscr{D}_n = \mathscr{D}_n^{(1)} \cup \cdots \cup \mathscr{D}_n^{(\lfloor n/2 \rfloor)}$, we must be able to generate *k*-cycle random *n*-derangements with probabilities

$$\mathbb{P}(\boldsymbol{\sigma} \in \mathscr{D}_n^{(k)}) = \frac{|\mathscr{D}_n^{(k)}|}{|\mathscr{D}_n|}.$$
(3)

To calculate these probabilities we need to determine $|\mathscr{D}_n^{(k)}|$. Perusal of the inclusion-exclusion principle furnishes

$$|\mathscr{D}_n^{(k)}| = \sum_{j=0}^k (-1)^j \binom{n}{j} \binom{n-j}{k-j}.$$
(4)

Equation (4) recovers $|\mathscr{D}_n^{(1)}| = {n \brack 1} = (n-1)!$, while we find that $|\mathscr{D}_n^{(2)}| = (n-1)!(H_{n-2}-1)$ for $n \ge 2$. Accordingly, already for small n (say, $n \ge 8$) we have $\mathbb{P}(\sigma \in \mathscr{D}_n^{(1)}) \simeq e/n$ and $\mathbb{P}(\sigma \in \mathscr{D}_n^{(2)}) \simeq (H_{n-2}-1)e/n$.

3. Generating random derangements by random transpositions

Our first approach to generate random *n*-derangements correctly distributed over \mathscr{D}_n consists in taking an initial cyclic *n*-derangement and to scramble it by random restricted transpositions enough to obtain the required distribution. By restricted transpositions we mean swaps $\sigma_i \leftrightarrow \sigma_j$ avoiding pairs for which $\sigma_i = j$ or $\sigma_j = i$. Algorithm 1 describes the generation of random *n*-derangements according to this idea, where $mix \ge n/2$ is a constant establishing the amount of restricted transpositions to be attempted and *rnd* is a computer generated pseudorandom uniform deviate in (0, 1).

The initial derangement in Algorithm 1 does not need to be cyclic, but this minimizes the risk of a careless implementation botching up the algorithm. We always start with the cycle $23 \cdots n1$. The minimum number of transpositions necessary to turn a cyclic *n*-derangement into a *k*-cycle *n*-derangement is k - 1, $1 \le k \le \lfloor n/2 \rfloor$, since transpositions of labels that belong to the same cycle split it into two cycles,

$$(ab)(i_1\cdots i_{a-1}i_ai_{a+1}\cdots i_{b-1}i_bi_{b+1}\cdots i_k) = (i_1\cdots i_{a-1}i_bi_{b+1}\cdots i_k)(i_{a+1}\cdots i_{b-1}i_a),$$
(5)

and, conversely, transpositions involving labels of different cycles join them into a single one.

Remark 1. Algorithm 1 is applicable only for $n \ge 4$, as it is not possible to connect the even permutations 231 and 312 by a single transposition.

Algorithm 1 Random derangements by random restricted transpositions

Require: Cyclic *n*-derangement $\sigma_1 \cdots \sigma_n$ 1: *mix* \leftarrow number of restricted transpositions to attempt 2: **for** s = 1 **to** *mix* **do** 3: $i \leftarrow \lceil rnd \cdot n \rceil, j \leftarrow \lceil rnd \cdot n \rceil$ 4: **if** $(\sigma_i \neq j) \land (\sigma_j \neq i)$ **then** 5: swap $\sigma_i \leftrightarrow \sigma_j$ 6: **end if** 7: **end for**

Table 1: Proportion of *n*-derangements in $\mathscr{D}_n^{(k)}$ observed in 10¹⁰ samples generated by Algorithms 1 and 2 for n = 64. Data for Algorithm 2 are based on a run that performed with a ratio of completed/attempted derangements of 0.985471. The notation n_{-a} reads $n \times 10^{-a}$. The last line of the table gives runtimes for comparison.

Cycles	Algorithm	orithm 1, nr. restricted transpositions attempted			Algorithm 2	Exact
k	n/2	n	2n	n log n		Eqs. (2)–(4)
1	0.048055	0.042933	0.042479	0.042473	0.042475	0.042473
2	0.160153	0.158395	0.157691	0.157679	0.157684	0.157677
3	0.278164	0.260129	0.258787	0.258765	0.258788	0.258772
4	0.241317	0.252739	0.253304	0.253305	0.253306	0.253301
5	0.167413	0.167189	0.167621	0.167639	0.167622	0.167635
6	0.070203	0.079498	0.080390	0.080402	0.080389	0.080400
7	0.026470	0.028825	0.029192	0.029195	0.029196	0.029200
8	0.006457	0.008087	0.008269	0.008274	0.008272	0.008274
9	0.001498	0.001 821	0.001868	0.001869	0.001868	0.001869
10	2.317_{-4}	3.292_{-4}	3.416_{-4}	3.418_{-4}	3.412_{-4}	3.417_{-4}
11	3.523_{-5}	4.914_{-5}	5.109_{-5}	5.120_{-5}	5.103_{-5}	5.116_{-5}
12	3.619 ₋₆	5.997_{-6}	6.322_{-6}	6.301_{-6}	6.354_{-6}	6.326_{-6}
13	3.639_{-7}	6.215_{-7}	6.493_{-7}	6.301_{-7}	6.507_{-7}	6.499_{-7}
14	2.53_{-8}	4.83_{-8}	5.40_{-8}	5.57_{-8}	5.44_{-8}	5.569_{-8}
15	1.2_{-9}	4.6_{-9}	3.1_9	3.0_9	4.1_{-9}	3.989_{-9}
16	2_{-10}	4_{-10}	1_{-10}	3_{-10}	1_{-10}	2.390_{-10}
runtime (sec)	9357	11298	15068	25238	18954	_

We run Algorithm 1 for different values of $mix \ge n/2$ and collect data. Our results appear in Table 1. We choose n = 64 because the difference between 2n = 128 and $n \log n = 266$ is significant in this case. From Table 1 we clearly see that mix = n/2 random restricted transpositions are unable to lead the initial cyclic derangement into higher k-cycle derangements—there is an excess of probability mass in the lower k-cycle sets with k = 1, 2, and 3. The same imbalance can be noted, although less clearly, with mix = n random restricted transpositions. Figures for derangements of higher cycle number fluctuate more due to the finite size of the sample. However, while the difference between trying to scramble the initial cyclic *n*-derrangement by *n* and 2n restricted transpositions is significant, the difference between attempting 2n or $n \log n$ restricted transpositions is much less pronounced. Our data suggest that Algorithm 1 can efficiently generate a random *n*-derangement correctly distributed on \mathcal{D}_n in O(2n) time employing of the order of 4n pseudorandom numbers in the process. This is further discussed in Section 5.

Remark 2. It is a classic result that $O(n \log n)$ transpositions are needed before a shuffle becomes "sufficiently random" (Aldous & Fill, 2002; Diaconis, 1988; Levin & Peres, 2017). A similar analysis for random restricted transpositions over derangements is complicated by the fact that derangements do not form a group. Recently, the analysis of the spectral gap of the Markov transition kernel of the process of restricted transpositions over derangements provided the bound $mix > Cn + an \log n^2$, with a > 0 and $C \ge 0$ a decreasing continuous function (Smith, 2015). This bound results from involved estimations and approximations and may not be very accurate. Related results appear in the remarkable (and difficult) paper by Hanlon (1996). We are not aware of other rigorous results on this particular problem.

Algorithm 2 Random derangements by sequential importance sampling

1: $J \leftarrow \{1, \ldots, n\}, d \leftarrow 0$ 2: for i = 1 to n - 1 do choose $j \in J \setminus \{i\}$ uniformly at random 3: 4: $\sigma_i \leftarrow j$ 5: $J \leftarrow J \setminus \{j\}$ $d \leftarrow d + 1\!\!1 \{j = n\}$ 6: 7: end for 8: **if** *d* > 0 **then** 9: $\sigma_n \leftarrow$ the remaining label $j \in J$ 10: else 11: fail 12: end if

4. Sequential importance sampling of derangements

Algorithm 2 describes a sequential importance sampling (SIS) algorithm to generate random derangements inspired by the analogous problem of sampling contingency tables with restrictions (Chen et al., 2005; Diaconis et al., 2001) as well as the problem of estimating the permanent of a matrix (Jerrum et al., 2004; Kuznetsov, 1996; Rasmussen, 1994)—namely, the permanent of the $n \times n$ matrix with 0 on the diagonal and 1 elsewhere.

In the *i*-th iteration of the loop in Algorithm 2 (lines 2–7), σ_i can pick (lines 3–4) one of

$$|J_i| = n - i + \sum_{j=1}^{i-1} \mathbb{1}\{\sigma_j = n\}$$
(6)

available labels, where the indicator function $1\!\!1 \{P\} = 1$ if *P* is true and 0 otherwise—i. e., σ_i can choose among either n-i or n-i+1 labels, depending on whether in the *i*-th iteration label *i* itself has already been picked. Note that J_i is never empty during the execution of the algorithm. This guarantees the construction of the *n*-derangement till the last but one element σ_{n-1} . The *n*-derangement will be completed only if the last remaining label $j \neq n$, such that σ_n does not pick *n*. Variable *d* (line 6) monitors this event: if after n-1 choices no one picked label *n*, d = 0 and the derangement failed. The probability that Algorithm 2 fails is thus given by

$$\mathbb{P}(\sigma_n = n) = \mathbb{P}(\sigma_1 \neq n) \mathbb{P}(\sigma_2 \neq n \mid \sigma_1 \neq n) \cdots \mathbb{P}(\sigma_{n-1} \neq n \mid \sigma_1 \neq n, \dots, \sigma_{n-2} \neq n).$$
(7)

Now, $\mathbb{P}(\sigma_i \neq n \mid \cdots) = 1 - \mathbb{P}(\sigma_i = n \mid \cdots)$ with (Algorithm 2, line 3)

$$\mathbb{P}(\sigma_i = n \mid \cdots) = \mathbb{E}\left(\frac{1}{|J_i|}\right) = \frac{1}{\mathbb{E}(|J_i|)},\tag{8}$$

and since

$$\mathbb{E}(|J_i|) = \mathbb{E}\left(n - i + \sum_{j=1}^{i-1} \mathbb{1}\left\{\sigma_j = n\right\}\right) = n - i + \frac{i-1}{n}$$

$$\tag{9}$$

we deduce that Algorithm 2 fails with probability

$$\mathbb{P}(\sigma_n = n \mid \dots) = \prod_{i=1}^{n-1} \frac{(n-1)(n-i) - 1}{n(n-i) + i - 1} \sim O\left(\frac{1}{n}\right).$$
(10)

According to (10), for n = 64 Algorithm 2 fails with probability 0.014492; compare this figure with the observed failure rate 1 - 0.985471 = 0.014529 given in Table 1.

5. Mixing times of the restricted transpositions shuffle

To shed some light on the question of how many random restricted transpositions are necessary to generate random derangements uniformly over \mathcal{D}_n , we investigate the convergence of Algorithm 1 numerically. This can be done by monitoring the evolution of the empirical probabilities observed along the run of the algorithm towards the exact probabilities given by (3)–(4).

Let v be the measure that puts mass $|\mathscr{D}_n^{(k)}|/|\mathscr{D}_n|$ on the set $\mathscr{D}_n^{(k)}$ and μ_t be the empirical measure

$$\boldsymbol{\mu}_{t}(k) = \frac{1}{t} \sum_{s=1}^{t} \mathbf{1}\{\boldsymbol{\sigma}_{s} \in \mathscr{D}_{n}^{(k)}\},\tag{11}$$

where σ_s is the derangement obtained after attempting *s* restricted transpositions by Algorithm 1 on a given initial derangement σ_0 . The chi-square distance between *v* and μ_t is given by

$$d(t) = \|\mu_t - \nu\|_{2,\nu} = \sum_{k=1}^{\lfloor n/2 \rfloor} \frac{\left[\mu_t(k) - \nu(k)\right]^2}{\nu(k)}.$$
(12)

Distance d(t) allows us to define $\tau_{mix}(\varepsilon)$ of the process as the time it takes for μ_t to fall within distance ε of v,

$$\tau_{\min}(\varepsilon) = \min\{t \ge 0 : d(t) < \varepsilon\}.$$
(13)

It is usual to define *the* mixing time τ_{mix} by setting $\varepsilon = \frac{1}{4}$ or $\varepsilon = e^{-1}$, a figure reminiscent of the spectral analysis of Markov chains. In what follows we set $\varepsilon = \frac{1}{4}$.

Starting with a cyclic derangement, i. e., with $\mu_0(1) = 1$ and all other $\mu_0(k) = 0$, we run Algorithm 1 and measure d(t) for some time. Figure 1 displays the average $\langle d(t) \rangle$ over 10⁶ runs for n = 128. The behavior of $\langle d(t) \rangle$ does not show any sign of the cutoff phenomenon (Aldous & Fill, 2002; Diaconis, 1988; Levin & Peres, 2017). Our data indicate that

$$\tau_{\rm mix} \sim O(n\log n),\tag{14}$$

which roughly agrees with the bound given in Smith (2015). Table 2 lists data for derangements of larger sizes; all seem to behave like $O(n \log n)$ to leading order.

6. Summary

While a simple acception-rejection algorithm generates random derangements in O(n) with an acceptance rate of $\sim e^{-1} \simeq 0.367$, thus being $O(e \cdot n)$ (the cost of verifying if the permutation generated is a derangement is negligible), Sattolo's O(n) algorithm only generates cyclic derangements, and Martínez-Panholzer-Prodinger algorithm, with



Figure 1: Chi-square distance $\langle d(t) \rangle$ (averaged over 10⁶ runs) between the empirical measure μ_t and the stationary measure ν of the process defined by Algorithm 1 for n = 128 with $\mu_0(1) = 1$. The dotted line indicates the level $\frac{1}{4}$, that meets $\langle d(t) \rangle$ at $t = \tau_{\text{mix}} = 861$.

Table 2: Measured mixing time τ_{mix} compared to $n \log n$.

$ au_{ m mix}$	$n\log n$	$\tau_{\rm mix}/n\log n$
543	266	2.04
861	621	1.39
1 3 9 6	1420	0.98
2085	3194	0.65
3347	7098	0.47
	$ filt au_{mix} ext{543} ext{861} ext{1396} ext{2085} ext{3347} ext{347}$	$\begin{array}{c c} \tau_{\rm mix} & n\log n \\ \hline 543 & 266 \\ 861 & 621 \\ 1396 & 1420 \\ 2085 & 3194 \\ 3347 & 7098 \end{array}$

guaranteed uniformity, is $2n + O(\log^2 n)$, we described two procedures that are competitive for the efficient generation of random derangements. We found, empirically (Tables 1 and 2), that $O(n \log n)$ random restricted transpositions suffice to spread an initial *n*-derangement correctly over \mathcal{D}_n with the expected distribution of cycle lengths. In terms of the amount of pseudorandom numbers employed, Algorithm 1 employs of the order of $2n \log n$ pseudorandom numbers and Algorithm 2 (SIS) employs n + O(1) pseudorandom numbers to generate an *n*-derangement uniformly distributed over \mathcal{D}_n . The advantage of the SIS algorithm is obvious.

Acknowledgments

The author acknowledges partial financial support from FAPESP (Brazil) through grant No. 2017/22166-9.

References

References

- Aldous, D., Fill, J. A., 2002. Reversible Markov Chains and Random Walks on Graphs. http://www.stat.berkeley.edu/~aldous/RWG/book.html.
- Bacher, A., Bodini, O., Hwang, H.-K., Tsai, T.-H., 2017. Generating random permutations by coin tossing: Classical algorithms, new analysis, and modern implementation. ACM Trans. Algorithms 13 (2), 24.
- Baril, J. L., Vajnovszki, V., 2004. Gray code for derangements. Discrete Appl. Math. 140 (1-3), 207-221.
- Charalambides, C. A., 2002. Enumerative Combinatorics. Chapman & Hall/CRC, Boca Raton.
- Chen, Y., Diaconis, P., Holmes, S. P., Liu, J. S., 2005. Sequential Monte Carlo methods for statistical analysis of tables. J. Am. Stat. Assoc. 100 (469), 109–120.
- Diaconis, P., 1988. Group Representations in Probability and Statistics. IMS, Hayward.
- Diaconis, P., Graham, R. L., Holmes, S. P., 2001. Statistical problems involving permutations with restricted positions, in: de Gunst, M., Klaassen, C., Van der Vaart, A. (Eds.), State of the Art in Probability and Statistics: Festschrift for Willem R. van Zwet. IMS, Beachwood, pp. 195–222. Edgington, E. S., Onghena, P., 2007. Randomization Tests, fourth ed. Chapman & Hall/CRC, Boca Raton.

Gries, D., Xue, J., 1988. Generating a random cyclic permutation. BIT Numer. Math. 28 (3), 569–572.

Hanlon, P., 1996. A random walk on the rook placements on a Ferrer's board. Electron. J. Comb. 3 (2), 26.

James, G. D., Kerber, A., 1981. The Representation Theory of the Symmetric Group. Addison-Wesley, Reading.

- Jerrum, M., Sinclair, A., Vigoda, E., 2004. A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. J. ACM 51 (4), 671–697.
- Korsh, J. F., LaFollette, P. S., 2004. Constant time generation of derangements. Inf. Process. Lett. 90 (4), 181–186.
- Kuznetsov, N. Y., 1996. Computing the permanent by importance sampling method. Cybern. Syst. Anal. 32 (6), 749-755.
- Levin, D., Peres, Y., 2017. Markov Chains and Mixing Times, second ed. AMS, Providence.
- Martínez, C., Panholzer, A., Prodinger, H., 2008. Generating random derangements, in: Sedgewick, R., Szpankowski, W. (Eds.), 2008 Proc. Fifth Workshop on Analytic Algorithmics and Combinatorics – ANALCO. SIAM, Philadelphia, pp. 234–240.
- Mendonça, J. R. G., 2018. Restricted permutations for the symmetric simple exclusion process in discrete time over graphs. arXiv:1806.09227.

Panholzer, A., Prodinger, H., Riedel, M., 2004. Measuring post-quickselect disorder. J. Iran. Stat. Soc. 3 (2), 219-249.

Prodinger, H., 2002. On the analysis of an algorithm to generate a random cyclic permutation. Ars Comb. 65, 75–78.

Rasmussen, L. E., 1994. Approximating the permanent: A simple approach. Random Struct. Algor. 5 (2), 349-361.

Sattolo, S., 1986. An algorithm to generate a random cyclic permutation. Inf. Process. Lett. 22 (6), 315–317.

Sedgewick, R., Flajolet, P., 2013. An Introduction to the Analysis of Algorithms, second ed. Addison-Wesley, Upper-Saddle River.

Smith, A., 2015. Comparison theory for Markov chains on different state spaces and application to random walk on derangements. J. Theor. Probab. 28 (4), 1406–1430.

Wilson, M. C., 2009. Random and exhaustive generation of permutations and cycles. Ann. Comb. 12 (4), 509-520.