

# COMPUTING DERANGEMENT PROBABILITIES OF THE SYMMETRIC GROUP ACTING ON $k$ -SETS

JOHN R. BRITNELL AND MARK WILDON

ABSTRACT. Let  $i(\infty, k)$  be the limiting proportion, as  $n \rightarrow \infty$ , of permutations in the symmetric group of degree  $n$  that fix a  $k$ -set. We give an algorithm for computing  $i(\infty, k)$  and state the values of  $i(\infty, k)$  for  $k \leq 30$ . These values are consistent with a conjecture of Peter Cameron that  $i(\infty, k)$  is a decreasing function of  $k$ .

## 1. INTRODUCTION

The symmetric group  $\text{Sym}_n$  acts on the set of  $k$ -subsets of  $\{1, \dots, n\}$ . Let  $i(n, k)$  be the proportion of permutations in  $\text{Sym}_n$  that fix at least one such  $k$ -subset. Let  $i(\infty, k) = \lim_{n \rightarrow \infty} i(n, k)$ . (We include below a short proof that this limit exists for all  $k \in \mathbf{N}$ .) It was shown by Luczak and Pyber in [3, §3, Lemma] that  $i(n, k) < Ck^{-1/100}$  for some constant  $C$ , uniformly in  $n$ . Thus  $\lim_{k \rightarrow \infty} i(\infty, k) = 0$ . Peter Cameron has conjectured [2] that  $i(\infty, k)$  is a decreasing function of  $k$ . In this note we give an efficient algorithm for computing  $i(\infty, k)$  and use it to prove that Cameron's conjecture is true for  $k \leq 30$ .

We also compute the values of  $i(n, k)$  for all  $n \in \mathbf{N}$  such that  $n \leq 70$ . As a corollary, we find that if  $2k \leq n \leq 70$  then  $i(n, k) < i(n, k + 1)$  if and only if

$$(n, k) \in \left\{ \begin{array}{l} (30, 9), (36, 11), (39, 12), (42, 13), (45, 14), (47, 15), (48, 15), \\ (51, 16), (53, 17), (54, 17), (57, 18), (59, 19), (60, 19), (63, 20), \\ (64, 21), (65, 21), (66, 21), (68, 22), (69, 22), (70, 23) \end{array} \right\}$$

However it is consistent with our data that  $i(n, k) > i(n, k + 1)$  for all  $n$  and  $k$  such that  $k < n/4$ , so these examples do not rule out the approach to Cameron's conjecture through careful estimation of  $i(n, k)$ . (Of course the choice of  $n/4$  is slightly arbitrary: any function  $f : \mathbf{N} \rightarrow \mathbf{N}$  such that  $f(n) \rightarrow \infty$  as  $n \rightarrow \infty$  and  $i(n, k) > i(n, k + 1)$  for all  $n$  and  $k$  with  $k < f(n)$  would suffice.)

Another motivation for this note is recent work of Eberhard, Ford and Green [5]. The main theorem of [5] states that there exist constants  $A$  and  $B$  such that

$$Ak^{-\delta}(1 + \log k)^{-3/2} \leq i(n, k) \leq Bk^{-\delta}(1 + \log k)^{-3/2}$$

for all  $k, n \in \mathbf{N}$ , where  $\delta = 1 - \frac{1 + \log \log 2}{\log 2} \approx 0.0861$ . This paper cites earlier data collected by the present authors, using the algorithm described below, that proves Cameron's conjecture for  $k \leq 23$ .

---

*Date:* November 12, 2015.

*2010 Mathematics Subject Classification.* 05A05, secondary: 05A17, 20B30.

**Outline.** In §2 we recall the necessary background on cycle statistics in permutations. In §3 we describe the ‘Derangement Table Algorithm’ for computing  $i(\infty, k)$ . This algorithm was inspired by a method for calculating  $i(\infty, k)$  by hand, shown to the authors by Peter M. Neumann. In Appendix A we discuss some features of the Haskell implementation of this algorithm. Appendix B gives our data for  $i(\infty, k)$  for  $k \leq 30$ . It is routine to compute  $i(n, k)$  for small values of  $n$  by exhausting over all partitions of  $n$ . Appendices C and D give the values of  $i(n, k)$  and  $1 - i(n, k)$  for  $n \leq 70$  and  $k \leq 35$ .

## 2. THE LIMITING DISTRIBUTION OF $k$ -CYCLES IN PERMUTATIONS

Let  $X_k^{(n)}(\pi)$  be the number of  $k$ -cycles in the permutation  $\pi$ , chosen uniformly at random from  $\text{Sym}_n$ . Let  $X_1, X_2, \dots$  be independent Poisson random variables such that  $X_k$  has mean  $1/k$ . The following proposition is well known. It is proved as Theorem 1 in [1].

**Proposition 1.** *Let  $m \in \mathbf{N}$ . As  $n \rightarrow \infty$ ,*

$$(X_1^{(n)}, \dots, X_m^{(n)}) \xrightarrow{\text{dist}} (X_1, \dots, X_m).$$

For  $n \in \mathbf{N}$ , let  $P^{(n)}$  be the random partition having exactly  $X_j^{(n)}$  parts of size  $j$  for each  $j \in \{1, \dots, k\}$ . It is clear that  $i(\infty, k)$  is the limit as  $n \rightarrow \infty$  of the probability that  $P^{(n)}$  has a subpartition of size  $k$ . It follows from Proposition 1 that  $i(\infty, k)$  exists, and is equal to the probability that the random partition  $(1^{X_1}, 2^{X_2}, \dots, k^{X_k})$  with exactly  $X_j$  parts of size  $j$  has a subpartition of size  $k$ .

## 3. THE DERANGEMENTS TABLE ALGORITHM

The input of the Derangements Table Algorithm is a natural number  $k$ . We call elements of  $\mathbf{N}_0^k$  *rows*, and elements of  $\mathbf{N}_0^\ell$  for  $\ell \leq k$  *partial rows*. Say that a partial row  $(m_1, \dots, m_\ell)$  is *k-free* if the partition  $(1^{m_1}, \dots, \ell^{m_\ell})$  has no subpartition of size  $k$ . The output of the algorithm is a list in lexicographic order from greatest to least of all  $k$ -free rows  $(m_1, \dots, m_k)$  with  $m_j \leq k/j$  for each  $j$ .

**Constructing  $k$ -free rows.** The algorithm’s internal state is a partial row  $r$ . At the start,  $r$  is set to  $(k - 1)$ .

- (A) [Building a partial row] Suppose  $r = (m_1, \dots, m_\ell)$ .
- (1) If  $\ell = k$  then output  $r$  [ $r$  is a row] and go to (B).
  - (2) Else, set  $j = \ell + 1$ . Take  $m$  maximal such that  $0 \leq m < k/j$  and the partial row  $(m_1, \dots, m_\ell, m)$  is  $k$ -free. Set  $r$  equal to  $(m_1, \dots, m_\ell, m)$  and repeat (A).
- (B) [Begin a new partial row]
- (1) If  $r = (0, \dots, 0) \in \mathbf{Z}^k$  then terminate.
  - (2) Else, we have  $r = (m_1, \dots, m_j, 0, \dots, 0) \in \mathbf{Z}^k$  where  $m_j \geq 1$ . Set  $r$  to  $(m_1, \dots, m_j - 1)$  and go to (A).

The details of the implementation of Step (A2) are key to the speed of the algorithm. We describe the feature of the greatest mathematical interest here and leave the other refinements to Appendix A.

Say that a partition  $\lambda$  of  $n$  is  $t$ -universal if  $\lambda$  has subpartitions of all numbers  $s \leq t$ . There is a surprisingly simple characterization of universal partitions.

**Proposition 2.** *The partition  $(1^{m_1}, 2^{m_2}, \dots, \ell^{m_\ell})$  is  $t$ -universal if and only if*

$$\sum_{j=1}^s jm_j \geq s$$

for all  $s \in \{1, \dots, t\}$ .

*Proof.* The condition is obviously necessary. Suppose that it holds. Let  $s \leq t$  be given. By hypothesis we have  $\sum_{j=1}^s jm_j \geq s$ . Let  $q$  be greatest such that  $q \leq s$  and  $m_q \neq 0$ . Let  $m'_j = m_j$  if  $j \neq q$  and let  $m'_q = m_q - 1$ . We consider two cases.

- (i) Suppose  $s - q \geq q$ . We first show that the partition  $(1^{m'_1}, \dots, q^{m'_q})$  is  $(s - q)$ -universal. Let  $u \leq s - q$  be given. If  $u < q$  then  $\sum_{j=1}^u jm'_j = \sum_{j=1}^u jm_j \geq u$ . If  $u \geq q$  then we have

$$\sum_{j=1}^u jm'_j = \sum_{j=1}^q jm'_j = \sum_{j=1}^q jm_j - q = \sum_{j=1}^s jm_j - q \geq s - q \geq u.$$

Hence, by induction,  $(1^{m'_1}, \dots, q^{m'_q})$  is  $(s - q)$ -universal. In particular it has a subpartition of size  $s - q$ . Since  $(1^{m_1}, \dots, q^{m_q})$  has an extra part of size  $q$ , it has a subpartition of size  $s$ .

- (ii) If  $s - q < q$  then  $\sum_{j=1}^u jm'_j = \sum_{j=1}^u jm_j$  for any  $u \leq s - q$ . By hypothesis  $\sum_{j=1}^u jm_j \geq u$ , so by induction the partition  $(1^{m'_1}, \dots, q^{m'_q})$  is  $(s - q)$ -universal. The proof finishes as in (i).  $\square$

In Step (A2) of the algorithm we test whether each partial row is  $k$ -universal using the criterion in Proposition 2. Any partial row that passes this test can immediately be discarded.

**Computation of  $i(\infty, k)$  given the table.** Let  $p(\infty, k) = 1 - i(\infty, k)$ . Let  $r = (m_1, \dots, m_k)$  be a row of the table. For each  $j$ , define

$$x_j(r) = \begin{cases} e^{-1/j} \frac{1}{j^{m_j} m_j!} & \text{if } m_j < \lfloor k/j \rfloor \\ 1 - e^{-1/j} \sum_{0 \leq i < \lfloor k/j \rfloor} \frac{1}{j^i i!} & \text{if } m_j = \lfloor k/j \rfloor. \end{cases}$$

**Lemma 3.** *For each  $k \in \mathbf{N}$ , the limiting probability  $p(\infty, k)$  is equal to the sum of  $x_1(r) \dots x_k(r)$  over every row of the table produced by the Derangements Table Algorithm with input  $k$ .*

*Proof.* Let  $r = (m_1, \dots, m_k)$  be a row of the table. Let  $J = \{j \in \{1, \dots, k\} : m_j = \lfloor k/j \rfloor\}$ . Note that any partition  $(1^{m'_1}, \dots, k^{m'_k})$  such that  $m'_i = m_i$  if  $i \notin J$  is  $k$ -free. Each partition of this form with  $m'_j < m_j$  for some  $j \in J$  corresponds to a row appearing later in the table. Thus  $r$  must account precisely for the partitions with *at least*  $\lfloor k/j \rfloor$  parts of size  $j$  for every  $j \in J$ , and with *exactly*  $m_i$  parts of size  $i$  for every  $i \notin J$ . The correct contribution from  $r$  to  $p(\infty, k)$  is therefore  $x_1(r) \dots x_k(r)$ .  $\square$

**Example.** The Derangements Table Algorithm can readily be implemented by hand for small values of  $k$ . As an illustration, the table for  $k = 4$  is shown below.

| 1 | 2 | 3 | 4 | probability                         |          |
|---|---|---|---|-------------------------------------|----------|
| 3 | 0 | 0 | 0 | $\frac{1}{6}e^{-25/12}$             | 0.020752 |
| 2 | 0 | 0 | 0 | $\frac{1}{2}e^{-25/12}$             | 0.062257 |
| 1 | 1 | 0 | 0 | $\frac{1}{2}e^{-25/12}$             | 0.062257 |
| 1 | 0 | 0 | 0 | $e^{-25/12}$                        | 0.124514 |
| 0 | 1 | 1 | 0 | $\frac{1}{2}e^{-7/4}(1 - e^{-1/3})$ | 0.024630 |
| 0 | 1 | 0 | 0 | $\frac{1}{2}e^{-25/12}$             | 0.062257 |
| 0 | 0 | 1 | 0 | $e^{-7/4}(1 - e^{-1/3})$            | 0.049259 |
| 0 | 0 | 0 | 0 | $e^{-25/12}$                        | 0.124514 |

For example, the exact probability for the row  $(0, 1, 1, 0)$ , accounting for all partitions of the form  $(2, 3^a)$  with  $a \geq 1$ , is  $e^{-1}e^{-1/2}\frac{1}{2}(1 - e^{-1/3})e^{-1/4}$ . The only other row having a multiplicity  $m_j$  such that  $m_j = \lfloor k/j \rfloor$  is  $(0, 0, 1, 0)$ . Thus all remaining rows contribute a rational multiple of  $e^{-1-1/2-1/3-1/4} = e^{-25/12}$  to the limiting probability. One finds that

$$p(\infty, 4) = \frac{3}{2}(1 - e^{-1/3})e^{-7/4} + \frac{11}{3}e^{-25/12} \approx 0.530442.$$

#### APPENDIX A: HASKELL IMPLEMENTATION

The Derangements Table Algorithm has been implemented in Haskell [4]. The arXiv submission of this paper includes the relevant files: `DerangementsTable.hs` and `Main.hs`.

We note two refinements to the basic version of the algorithm presented above.

- (1) In any row the  $k$ -th element, corresponding to cycles of length  $k$ , is always zero. It therefore suffices to work with rows and partial rows of length at most  $k - 1$ , scaling by  $\exp(-1/k)$  to account for the  $k$ -cycles.
- (2) Suppose that  $r$  is a partial row of length  $\ell$  and  $d \in \mathbf{N}$  is such that (i)  $n$  is not divisible by  $d$ , and (ii) for each  $j \in \{1, \dots, \ell\}$ , either  $j$  is divisible by  $d$ , or  $a_j = 0$ . Then  $r$  is clearly  $k$ -free. Applying this trick to the partial rows considered in Step A2 when finding  $m$  gives a surprisingly large speed-up. For example, when  $k = 25$ , it reduces the running time from approximately 44 minutes to approximately 12 minutes.

If a partial row is neither  $k$ -universal, nor meets the condition for the divisibility check, then an exhaustive search is made for subpartitions of size  $k$  using the function `subpartitionSizes`. This accounts for the majority of the running time. For example, when  $k = 25$ , 5240351 partial rows are considered; of these 103189 are  $k$ -universal and 2041735 are ruled out by divisibility, leaving 3095427 on which a full test must be made. The final table has 2 235 240 rows.

The values shown in Appendix B take about 72 hours to compute on one core of a 2.7GHz Intel i5.

The key functions in `DerangementsTable.hs` are reproduced below.

```

universality ms = case as' of [] -> 0
                    otherwise -> s
  where ss = zip [1..] $ partialSums [a*m | (a,m) <- zip [1..] ms]
        (as', _) = span (uncurry (<=)) ss
        (a, s) : _ = reverse as'

partialSums = scanl1 (+)

subpartition k ms
  | universality ms >= k    = True
  | divisibilityTest k ms  = False
  | otherwise = k 'elem' (subpartitionSizes $ zip [1..] ms)

divisibilityTest k ms =
  let test c = k 'mod' c /= 0
      && and [j 'mod' c == 0 || m == 0 | (j,m) <- zip [1..] ms]
  in or [test c | c <- [2..k 'div' 2]]

subpartitionSizes [] = [0]
subpartitionSizes ((a, m) : ams)
  = [1*a + y | 1 <- [0..m], y <- subpartitionSizes ams]

Clearly the subpartition function can also be used to compute the finite derangement probabilities  $i(n, k)$  and  $p(n, k) = 1 - i(n, k)$ . The values shown in Appendices B and C take about 24 hours to compute on one core of a 2.7 GHz Intel i5. The relevant code is reproduced below.

fixesSet k ms | universality ms >= k = True
              | otherwise = subpartition k ms

centralizerSize ms = product [f (x, m) | (x,m) <- zip [1..] ms]
  where f (x, m) = let x' = toInteger x
                    m' = toInteger m
                  in x'^m' * factorial m'

finiteTable n k = [(ms, subpartition k ms, centralizerSize ms)
                  | xs <- partitions n,
                    let ms = toMultiplicities n xs]

sumStrict = foldl1' (+)

i n k = sumStrict [1 % c | (_, True, c) <- finiteTable n k]

```

APPENDIX B:  $i(\infty, k)$  FOR  $k \leq 30$ 

In the table below probabilities are rounded to 8 decimal places. These probabilities were computed using MATHEMATICA to add up the contributions given by Lemma 3 from each row of the table produced by the Derangements Table Algorithm, requiring an exact answer to 20 decimal places. The number of rows of the table is also given.

| $k$ | $i(\infty, k)$ | rows( $k$ ) | $k$ | $i(\infty, k)$ | rows( $k$ ) |
|-----|----------------|-------------|-----|----------------|-------------|
| 1   | 0.63212056     | 1           | 16  | 0.33807249     | 8420        |
| 2   | 0.55373968     | 2           | 17  | 0.33297333     | 19553       |
| 3   | 0.49658324     | 4           | 18  | 0.32907588     | 23586       |
| 4   | 0.46955773     | 8           | 19  | 0.32472908     | 61470       |
| 5   | 0.44145770     | 15          | 20  | 0.32132422     | 71413       |
| 6   | 0.42505870     | 29          | 21  | 0.31750065     | 193303      |
| 7   | 0.40848113     | 53          | 22  | 0.31449862     | 216928      |
| 8   | 0.39727771     | 93          | 23  | 0.31110428     | 508502      |
| 9   | 0.38516443     | 187         | 24  | 0.30842280     | 532542      |
| 10  | 0.37687192     | 305         | 25  | 0.30538904     | 2235240     |
| 11  | 0.36773064     | 561         | 26  | 0.30295361     | 1817364     |
| 12  | 0.36119415     | 916         | 27  | 0.30021508     | 5143197     |
| 13  | 0.35396068     | 2067        | 28  | 0.29801340     | 4961040     |
| 14  | 0.34855007     | 2782        | 29  | 0.29550915     | 17517544    |
| 15  | 0.34256331     | 5670        | 30  | 0.29348611     | 12022223    |

Question 1 in [5] asks if there is a constant  $C$  such that  $i(\infty, k) \sim Ck^{-\delta}(\log k)^{-3/2}$ . The ratio of the two sides is shown below for  $1 \leq k \leq 30$ . If Question 1 has an affirmative answer then the ratio converges to  $C$  as  $k \rightarrow \infty$ .

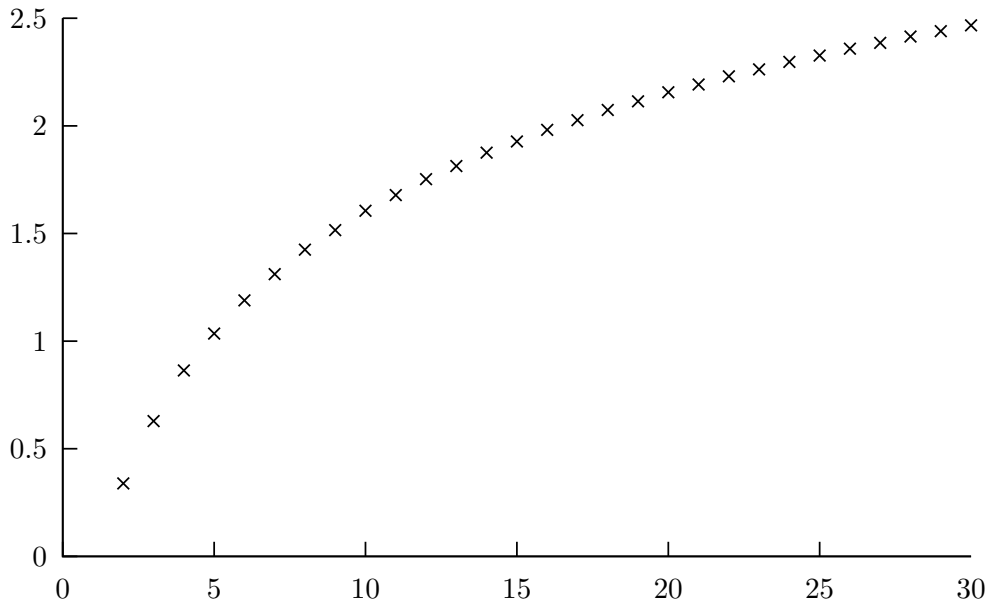


FIGURE 1.  $i(\infty, k) / k^{-\delta} (\log k)^{-3/2}$  for  $2 \leq k \leq 30$







## ACKNOWLEDGEMENTS

The authors thank Sean Eberhard for helpful comments and Jasdeep Kochhar for helpful comments and corrections.

## REFERENCES

- [1] Richard Arratia and Simon Tavaré, *The cycle structure of random permutations*, Ann. Probab. **20** (1992), no. 3, 1567–1591.
- [2] Peter Cameron, [cameroncounts.wordpress.com/2010/11/15/derangements-2/](http://cameroncounts.wordpress.com/2010/11/15/derangements-2/), posted on 15/11/2010, accessed October 2015.
- [3] Tomasz Łuczak and László Pyber, *On random generation of the symmetric group*, Combin. Probab. Comput. **2** (1993), no. 4, 505–512.
- [4] Simon Peyton Jones et al., *The Haskell 98 language and libraries: The revised report*, Journal of Functional Programming **13** (2003), no. 1, 0–255, <http://www.haskell.org/definition/>.
- [5] Sean Eberhard, Kevin Ford and Ben Green, *Permutations fixing a  $k$ -set*, arXiv:1507.04465 (July 2015), 17 pages.