Derangements

September 6, 2001

1 Introduction

An absent minded secretary stuffs letters into pre-addressed envelopes at random. What is the probability that none of the letters end up where they are supposed to? It turns out that this probability tends to $1/e$ as the number of envelopes increases. We will see why, as we study this special class of permutations called *derangements*. Studying derangements allows us to visit many of the important themes of this course. An n-derangement is an n-permutation with no singleton cycles. In other words, a derangement is a permutation that does not map any element to itself. The *Combinatorica* function `Derangements` generates all n-derangements in lexicographic order.

```
In[1]:= Derangements[4]

Out[1]= {{2, 1, 4, 3}, {2, 3, 4, 1}, {2, 4, 1, 3}, {3, 1, 4, 2},
         {3, 4, 1, 2}, {3, 4, 2, 1}, {4, 1, 2, 3}, {4, 3, 1, 2}, {4, 3, 2, 1}}
```

Combinatorica also has a function called `DerangementQ` that tests whether a given permutation is a derangement. The code for this function is given below. The function tests to see if any element is mapped on to itself by the permutation. If not, it is a derangement.

```
DerangementQ[p_?PermutationQ] :=
        !(Apply[ Or, Map[( # === p[[#]] )&, Range[Length[p]]] ])
```

```
In[2]:= {DerangementQ[{1, 4, 2, 3}], DerangementQ[{2, 1, 4, 3}]}

Out[2]= {False, True}
```

2 Number of Derangements

The first question we are interested in is: how many n-derangements are there? Let D_n denote the number of n-derangements. $D_1 = 0$ because the only 1-permutation maps 1 to itself and is therefore not a derangement. $D_2 = 1$ since $(2, 1)$ is the only 2-derangement. We will now show that for any $n > 2$

$$D_n = (n-1)D_{n-2} + (n-1)D_{n-1}.$$

In fact, if we define $D_0 = 1$,the above recurrence holds for $n = 2$ as well.

To prove the recurrence we partition the set of n-permutations into two sets. One set A contains the n-derangements in which n occurs in a 2-cycle and the other set B contains those in which n occurs in a larger cycle. Now we define a mapping f_A from A to the set of $(n-2)$-derangements as follows. For any permutation $p \in A$, $f_A(p) = p'$ where p' is obtained by deleting from p the 2-cycle (i, n) containing n and decrementing all elements $i+1, i+2, \ldots, n-1$. p' is an $(n-2)$-permutation and contains no singleton cycles and therefore belongs to the set of $(n-2)$-derangements. The mapping f_A maps exactly $(n-1)$ elements in A onto each $(n-2)$-derangement. To see this observe that for every $(n-2)$-derangement p', the permutation p obtained by incrementing elements $i, i+1, \ldots, n-2$ and adding the cycle (i, n) is mapped onto p'. The possible values of i are 1 through $n-1$ yielding $(n-1)$ distinct p that are mapped onto p' by f_A. Hence the size of the set A is $(n-1)D_{n-2}$.

Now define a similar mapping f_B from the set B into the set of $(n-1)$-derangements as follows. For any permutation $p \in B$, $f_B(p) = p'$ where p' is obtained by simply deleting n from cycle it occurs in. The result is an $(n-1)$-permutation with no singleton cycles. The mapping f_B maps exactly $(n-1)$ elements in B onto each $(n-1)$-derangement. To see this observe that for every $(n-1)$ derangement p', the permutation p obtained by inserting n into each of the $(n-1)$ positions $1, 2, \ldots, (n-1)$ is mapped onto p'. The size of B is therefore $(n-1)D_{n-1}$ and the recurrence follows.

This recurrence can be used to compute the number of derangements, but it turns out that there are two, more elegant formulae for D_n. The first of these is

$$D_n = nD_{n-1} + (-1)^n.$$

To derive this start with the equations

$$\begin{aligned} D_n &= (n-1)D_{n-1} + (n-1)D_{n-2} && (1) \\ D_{n-1} &= (n-2)D_{n-2} + (n-2)D_{n-3} && (2) \end{aligned}$$

To the right hand side of (1) add D_{n-1} and subtract the right hand side of (2). This yields

$$D_n = nD_{n-1} + D_{n-2} - (n-2)D_{n-3} \qquad (3)$$

Now write the equation $D_{n-2} = (n-3)D_{n-3} + (n-3)D_{n-4}$, subtract D_{n-2} from the right hand side of (3) and add $(n-3)D_{n-3} + (n-3)D_{n-4}$. This yields

$$D_n = nD_{n-1} - D_{n-3} + (n-3)D_{n-4}.$$

It is now easy to guess (and prove by induction) the general case

$$D_n = nD_{n-1} + (-1)^j D_{n-j} + (n-j)D_{n-j-1}$$

for $j = 1, 2, \ldots$. Letting $j = n-2$ we get

$$D_n = nD_{n-1} + (-1)^{n-2}D_2 + 2D_1 = nD_{n-1} + (-1)^n.$$

Combinatorica has a function `NumberOfDerangements` that computes the number of n-derangements for a given n. As the code below shows, it is implemented using the recurrence $D_n = nD_{n-1} + (-1)^n$.

```
NumberOfDerangements[0] := 1
NumberOfDerangements[n_Integer?Positive] := n * NumberOfDerangements[n-1] + (-1)^n
```

```
In[3]:= Table[NumberOfDerangements[i], {i, 10}]

Out[3]= {0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961}
```

However, there is simpler way to compute the number of n-derangements. By repeatedly expanding the recurrence $D_n = nD_{n-1} + (-1)^n$ we get

$$D_n = n! + \frac{n!}{1!}(-1)^1 + \frac{n!}{2!}(-1)^2 + \cdots + \frac{n!}{n!}(-1)^n.$$

This can be rewritten as

$$D_n = n!\left(\frac{(-1)^0}{0!} + \frac{(-1)^1}{1!} + \frac{(-1)^2}{2!} + \cdots + \frac{(-1)^n}{n!}\right).$$

Recall that

$$e^x = 1 + \frac{x^1}{1!} + \frac{x^2}{2!} + \cdots$$

and so it follows equation that

$$\lim_{n\to\infty} \frac{D_n}{n!} = e^{-1}.$$

This is proof of the claim we made about the absent minded secretary at the beginning of these notes. Here is an experiment in which the ratio $D_n/n!$ is computed for $n = 1, 2, \ldots, 10$. The value of $1/e$ to the first 6 decimal places is 0.367879 and so by $n = 9$ the values of $1/e$ and $D_n/n!$ match in the first six decimal places.

```
In[4]:= Table[NumberOfDerangements[i]/i!, {i, 10}] // N

Out[4]= {0., 0.5, 0.333333, 0.375, 0.366667, 0.368056, 0.367857, 0.367882,
         0.367879, 0.367879}
```

Does the connection between D_n and e^{-1} help in computing D_n? Yes, says the following experiment. Simply round $n!/e$ and we get D_n.

```
In[5]:= Table[NumberOfDerangements[i] - Round[i!/N[E]], {i, 10}]

Out[5]= {0, 0, 0, 0, 0, 0, 0, 0, 0, 0}
```

To see that rounding $n!/e$ yields D_n consider the "error"

$$\begin{aligned}\left|\frac{n!}{e} - D_n\right| &= n!\left|\frac{(-1)^{n+1}}{(n+1)!} + \frac{(-1)^{n+2}}{(n+2)!} + \cdots\right| \\ &< n!\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right) \\ &< \left(\frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \cdots\right) \\ &= \frac{1}{n}\end{aligned}$$

This tells us that for $n \geq 2$, $|n!/e - D_n| < 1/2$ implying that rounding $n!/e$ gives D_n. For $n = 0$ and $n = 1$ this can be verified separately.

We derived the formula $D_n = \sum_{i=0}^{n}(-1)^i n!/i!$ from the recurrence $D_n = nD_{n-1} + (-1)^n$, which in turn we derived from the recurrence $D_n = (n-1)D_{n-1} + (n-2)D_{n-2}$. A more direct way of deriving this formula uses the *inclusion-exclusion principle*. This is an important technique in combinatorics, useful for counting various combinatorial objects. Let X be a finite set and let $X_1, X_2, \ldots, X_n$ be subsets of X. For any set $I \subseteq [n]$ of indices, let $X_I = \cap_{i\in I} X_i$. The inclusion-exclusion principle states that

$$\left|X - \bigcup_{i\in[n]} X_i\right| = \sum_{I\subseteq[n]} (-1)^{|I|}|X_I|.$$

This is easy to prove by induction and is left as an exercise for you. To use this to derive a formula for D_n, let X be the set of n-permutations and for each $i \in [n]$, let X_i be the set of n-permutations in which i appears as a singleton cycle. Clearly, $\cup_{i\in[n]}X_i$ is the set of n-permutations which contain at least one singleton cycle. Therefore, $X - \cup_{i\in[n]}X_i$ is the set of n-derangements and $D_n = |X - \cup_{i\in[n]}X_i|$. The set X_I is the set of n-permutations in which each element in I appears in a singleton. So elements in I are "fixed" while the other $(n - |I|)$ elements can be permuted. This implies that $|X_I| = (n - |I|)!$. There are $\binom{n}{|I|}$ subsets of $[n]$ of size $|I|$ and therefore

$$\sum_{I\subseteq[n]} (-1)^{|I|}|X_I| = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)! = \sum_{i=0}^{n}(-1)^i\frac{n!}{i!}.$$

3 Maximum Change Permutations

What we have learned thus far about derangements proves useful in the solution of the following enumeration problem.

> Can n-permutations be listed in an order in which for any pair p and q of consecutive permutations, p and q differ in every position.

In other words, we want to list n-permutations in "maximum change order," that is, in an order in which going from one permutation to the next requires moving every element.

Just as we did when we wanted to list permutations in minimum change order, let us start by defining a graph $P_n = (V_n, E_n)$ in which V_n is the set of all n-permutations and E_n contains edges connecting pairs of permutations that differ in all positions. The question "can n-permutations be listed in maximum change order?" is therefore equivalent to the question "does P_n contain a Hamiltonian path?" Let us first explore the structure of P_n before attempting to tackle the problem of determining whether it contains a Hamiltonian path. How many neighbors does a vertex in P_n have? The answer is $\langle n!/e\rangle$[1] because a pair of permutations p and q are neighbors if and only if $p^{-1} \times q$ is an n-derangement. Thus for each n-derangement d, p has a neighbor $p \times d$. This connection between P_n and derangements is used to construct the graph P_n in the *Mathematica* code below.

```
P[n_Integer?Positive] :=
   MakeGraph[Permutations[n],
             DerangementQ[Permute[InversePermutation[#1],  #2]]&,
             Type -> Undirected
   ]
```

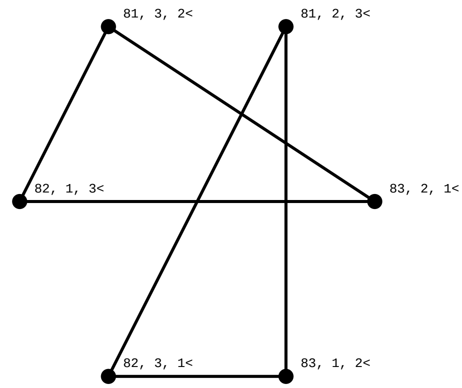
In the following experiment P_4 is constructed and the degrees of the vertices in P_4 are listed. Each vertex has 9 neighbors and this is as predicted by $D_4 = 9$.

```
In[6]:= Degrees[ P[4] ]

Out[7]= {9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9}
```

Here is P_3 constructed by calling the function `P` defined above.

[1] The function $\langle\cdot\rangle$ is being used here to denote "rounding."



P_3 is not even connected! It seems like we are done, having answered the question in the negative. But, it turns out that P_3 is an exception and we now show that P_n is connected for all $n > 3$. Showing this is equivalent to showing that for any pair of n-permutations p and q, there is a sequence of derangements $d_1, d_2, \ldots, d_k$ such that

$$p \times d_1 \times d_2 \times \cdots \times d_k = q.$$

We already know that for any n-permutations p and q, there is a sequence of transpositions $t_1, t_2, \ldots, t_\ell$ such that

$$p \times t_1 \times t_2 \times \cdots \times t_\ell = q.$$

Therefore, if we show that *any* transposition can be expressed as a product of derangements, we are done. Now observe that if one transposition can be expressed as a product of derangements, any transposition can. This allows us to focus on the specific problem of showing that the transposition $t = ((1,2))$ can be expressed as a product of derangements. For odd n with $n \geq 5$, let $d = ((1,2),(3,4,5,\ldots,n))$. Then d^{n-2} (the product of $(n-2)$ d's) equals t. For even n with $n \geq 6$, let $d' = ((1,2),(3,n-1,n-3,\ldots,5),(4,n,n-2,\ldots,6))$. Then $d' \times d^{n-4}$ equals t. This completes our proof for $n \geq 5$. The case of $n = 4$ can be verified explicitly. Specifically, we note that

$$((1,2)) = ((1,3,2,4)) \times ((1,4,3,2)) \times ((1,4,3,2)).$$

All permutations in the equation above are written in cycle structure form.

The above proof shows that the *diameter* of P_n, that is the maximum distance between any pair of vertices in the graph is at most $(n-1)(n-2)$. This is because between any two permutations there is a path of transpositions that is at most $(n-1)$ edges long. Each edge corresponding to a transposition can be replaced by a path of derangements of length at most $(n-2)$. This leads to a maximum path length of $(n-1)(n-2)$. However, this seems to be a gross overestimate. The following experiment tells us that the diameters of P_4 and P_5, are 2! Is this a coincidence or can you prove this in general? If true in general, it means that 2 derangements suffice to take any permutation to any other permutation.

```
In[7]:= g = P[4]; h = P[5]; {Diameter[g], Diameter[h]}

Out[7]= {2, 2}
```

The following experiment shows that P_4 is not only connected, it has a Hamiltonian cycle as well.

```
In[8]:= HamiltonianQ[P[4]]

Out[8]= True
```

This is not a mere coincidence, and we will be able to appeal to a certain theorem by Jackson and show that P_n is Hamiltonian for all $n > 3$. One of the simplest sufficient conditions for Hamiltonicity of a graph was proved by Dirac in 1952. Dirac's theorem says that any n-vertex graph with at least 3 vertices, whose minimum vertex degree is at least $n/2$ is Hamiltonian. Dirac's Theorem does not apply to P_n because the degree of any vertex in P_n $\langle n!/e \rangle$. This quantity is greater than $n!/3$ but smaller than $n!/2$. Jackson in 1980 proved a stronger sufficient condition for k-regular graphs. Jackson's theorem says that any k-regular biconnected graph with at most $3k$ vertices is Hamiltonian. In other words, if an n-vertex graph is regular, biconnected, and every vertex has at least $n/3$ neighbors, then it is Hamiltonian. P_n is regular and every vertex has at least $n!/3$ neighbors. The fact that it is biconnected for all $n > 3$ is not hard to show and I leave that as an exercise. The conditions plus Jackson's theorem implies that P_n is Hamiltonian for all $n > 3$ and from this it follows that n-permutations can be listed in maximum change order for any $n > 3$. The interesting thing about this result is that it proves the existence of a Hamiltonian cycle without providing an algorithm for constructing such a thing. It seems that no one knows of a simple algorithm to list permutations in maximum change order.
