Adventures in Derangement

The other day I wandered into the edge of a forest, not knowing at the time how vast it actually was. Before I knew it, I was lost. However, since I had only gone a little way in, I was pretty confident that if I searched methodically, I could find my way out. I might even want to sketch a map as I searched. This is the sketch I produced.

It started one morning when, at breakfast, I found no newspaper at hand. All there was on the table to read was a pristine copy of Sheldon Ross' *Introduction to Probability Models*, bound with an attractive cover showing a stand of birch trees. My wife had ordered the book from Amazon some months ago, thinking she might be interested in learning enough about probability to take one of the actuarial exams. Looking through it, I was reminded of a class in probability I had taken in college and, over the years, had largely forgotten.

Problem 12 at the end of Chapter 1 was marked with an asterisk. It asked: suppose there are n men at a party, and each throws his hat into the center of the room. The hats are then mixed up and redistributed to the men at random. Show that the probability that no man gets his own hat back is

$$\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + \frac{(-1)^n}{n!}. \tag{1}$$

Obviously the number of ways to distribute the hats to the n men is $n!$, so if we can find the number b_n of ways to distribute the hats without giving any man his own hat, then the desired probability would be $p_n = b_n/n!$. How to find a formula for b_n? As I later learned, a distribution of hats in which no man gets his own hat is called a "derangement". So what I was looking for was a formula for the number b_n of derangements of n objects.

From the formula (1), it seemed that the inclusion-exclusion principle might be involved. I had seen the principle explained, with a number of examples, in *Counting: the Art of Enumerative Combinatorics* by George E. Martin, a text I had used once for a capstone class. However, I didn't remember it well enough to see how to apply it here. Also, I thought there might be a nice argument relating b_n to b_i for values of i less than n: this might lead to a recurrence relation which could be used to given an inductive proof of the formula (1) for p_n. In other words, I was looking for a "combinatorial proof" of the recurrence relation.

I figured out the values of b_n for the first few values of n, by using the formula (1), and also by writing down the possible ways of redistributing hats to three or four or five people. The values are $b_2 = 1$, $b_3 = 2$, $b_4 = 9$, $b_5 = 44$, $b_6 = 265, \ldots$. By thinking about different ways of distributing the hats, I came up with the recurrence relation

$$b_n = (n-1)\,(b_{n-1} + b_{n-2}) \tag{2}$$

for $n \geq 3$, which was obviously correct, because it fit the values of the sequence up through b_6. However, at this point I got distracted and put the problem aside. When I came back to it a week or so later, I couldn't remember how I had found the recurrence relation, and finally realized that whatever proof I had must have been incorrect. So I sat down and worked out a correct proof this time. My first correct proof was quite long and not fully combinatorial, but after more work I was able to find what is clearly the right proof.

It goes like this. Pick one man, and call him Joe. There are $n-1$ other hats that Joe could receive. Let the owner of the hat Joe receives be called Frank. If it so happens that Frank receives Joe's hat in return, then there are b_{n-2} ways to redistribute the remaining $n-2$ hats among the remaining $n-2$ men, so that none of them get their own hat. This gives a total of $(n-1)b_{n-2}$ derangements of the n hats.

Alternatively, it might happen that Frank does not receive Joe's hat. In this case, take the hat Frank received and give it to Joe, and then take Frank's hat away from Joe and remove Frank and his hat from the room. Now the situation is just as if Frank was never there: there are $n-1$ men and their hats in the room, and no one has their own hat. There are b_{n-1} possible derangements of these $n-1$ hats. Conversely, each of these b_{n-1} derangements produces a derangement of the original n men and their hats: to do this, bring Frank and his hat back into the room, and have Frank switch hats with Joe. So there are exactly b_{n-1} derangements of the n hats in which Joe has Frank's hat but Frank does not have Joe's hat. Since there were $n-1$ ways to choose Frank, this gives $(n-1)b_{n-1}$ possible derangements.

We have now covered all the possibilities: $(n-1)b_{n-2}$ derangements in which Frank exchanges hats with another of the men, and $(n-1)b_{n-1}$ possibilities in which he does not. Adding these two numbers, we get the formula (2) for b_n.

The next step was to use the recurrence relation to show that p_n satisfies (1). I did this using brute force induction, replacing b_k by $k!p_k$ for $k = n, n-1, n-2$ in (2), and using algebra to check that both sides agree. In fact, I had tried doing this on my first attempt at the problem a week earlier, and though the algebra was simple, it was a bit messy, and I still hadn't got the two sides to match after quite a bit of work. This time I sat down and finished it.

At this point I did a Google search to see what I could find about the problem on the internet. The first thing I found was a nice video by Aloha Churchill on YouTube, titled "Hat/Matching Probability Question (Derangement Proof)", in which she explains how to find the formula (1) for p_n using the inclusion-exclusion principle.

Next I found several posts on the topic at MathStackExchange. In the top-rated answer to the question 83380, a simpler way to get to (1) from the recurrence relation was presented. First, subtract nb_{n-1} from both sides of (2) and rearrange to get

$$b_n - nb_{n-1} = -\left(b_{n-1} - (n-1)b_{n-2}\right),$$

which, together with the fact that $b_3 - 3b_2 = -1$, immediately leads to the simpler recurrence relation

$$b_n = nb_{n-1} + (-1)^n \tag{3}$$

for $n \geq 3$. Dividing both sides by $n!$ gives

$$p_n = p_{n-1} + \frac{(-1)^n}{n!},$$

which proves (1).

Finally, I went to the Online Encyclopedia of Integer Sequences and entered the list "$1, 2, 9, 44, 265$" into the search bar. This brought up the entry "A000166: Subfactorial or rencontres numbers, or derangements: number of permutations of n elements with no fixed points". It was here that it became apparent how deep the forest was that I had wandered into. There was a long list of comments, describing various incarnations of the sequence. For example, one comment says that b_n counts "the number of wedged $(n-1)$-spheres in the homotopy type of the Boolean complex of the complete graph K_n"; while another refers to "a family of recurrences found by Malin Sjödahl for a combinatorial problem for certain quark and gluon diagrams".

The comments were followed by an even longer list of references, formulas, and examples. It turns out the problem has a long history, and was solved and re-solved several times in the 18th century by Jean and Nicolas Bernoulli, Montmort, de Moivre, and Euler, among others (see the notes below for online references to the sources). But now that we have found our way out into the light again after our first venture into the forest, let's postpone our further exploration to another time!

NOTES:

- I assumed the asterisk meant the problem was a difficult one. Later I realized that it actually meant that the solution to the problem was given at the end of the book. In fact, the exclusion-inclusion principle is covered in Chapter 1, and as an example, the problem is solved there for $n = 3$ — which essentially explains the solution of the problem for general n as well. If I had read that example first, I might not have ever given the problem a second thought!

- Aloha Churchill's YouTube video is at:

  `https://www.youtube.com/watch?v=1QAzjQWCk48` .

- In the same answer to question 83380 on MathematicsStackExchange that is mentioned above, it is proved that b_n is actually the nearest integer to $n!/e$.

- The Online Encyclopedia of Integer Sequences is at `https://oeis.org` .

- For a glimpse of the type of analysis that Malin Sjödahl does, see her paper on arXiv at:

  `https://arxiv.org/pdf/1503.00530` .

- The history of the problem I had found in Ross' textbook dates back to Nicholas Bernoulli and Leonhard Euler, among others.

  In Euler's paper "Solutio quaestionis curiosae ex doctrina combinationum" or "The solution of a curious question in the doctrine of combinatorics", written in 1779, four years before his death, and published posthumously in *Mémoires de l'académie des sciences de St.-Petersbourg*, Volume 3, 1811, pp. 57–64, he proved both recurrence relations (2) and (3), with essentially the same proofs I gave above. This paper is available, both in the original Latin, and in an English translation, at

  `https://scholarlycommons.pacific.edu/euler-works/738`

  However, it seems the problem had been more or less solved much earlier. Pierre Renard de Montmort corresponded with Jean Bernoulli about it, and Nicolas Bernoulli added some commentary, in 1710. See the account in "Diverse problems concerning the game of treize", an extract of Montmort's *Essay d'Analyse sur les Jeux de Hasard*, 2nd edition of 1713, pp. 130-143, and accompanying excerpts of the correspondence, in:

  `http://www.probabilityandfinance.com/`

  `pulskamp/Montmort/essai_treize_98_114.pdf` .

  Abraham de Moivre also solves the problem in his book *The Doctrine of Chances*, 3rd edition 1756. It appears as Problem XXXV on pages 109–117. See:

  `http://www.probabilityandfinance.com/pulskamp/`

  `Moivre/doctrine%20of%20chances%20prob%2035_36-derangements.pdf`

- Richard Stanley, in Volume 1 of his comprehensive text *Enumerative Combinatorics*, features this problem prominently, stating it at the beginning of Chapter 1, and giving a complete treatment near the beginning of Chapter 2. Stanley credits Montmort with the first solution of the problem.

  He also mentions that the recurrence relation (3) can be given a direct combinatorial proof (as opposed to the proof I gave above, in which first (2) is proved combinatorially and then some algebra is used to derive (3)). Stanley leaves the task of finding a combinatorial proof of (3) as an exercise for the reader. I haven't found such a proof yet myself.