

MATHEMATICAL ASSOCIATION



supporting mathematics in education

84.29 Kruskal's Card Trick

Author(s): John M. Pollard

Source: *The Mathematical Gazette*, Vol. 84, No. 500 (Jul., 2000), pp. 265-267

Published by: The Mathematical Association

Stable URL: <http://www.jstor.org/stable/3621657>

Accessed: 08/01/2009 11:20

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=mathas>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit organization founded in 1995 to build trusted digital archives for scholarship. We work with the scholarly community to preserve their work and the materials they rely upon, and to build a common research platform that promotes the discovery and use of these resources. For more information about JSTOR, please contact support@jstor.org.



The Mathematical Association is collaborating with JSTOR to digitize, preserve and extend access to *The Mathematical Gazette*.

<http://www.jstor.org>

Notes

84.29 Kruskal's card trick

The basic card trick

Martin Gardner [1] describes the following trick, which he calls 'Kruskal's principle'. Take a well-shuffled single pack of cards. Deal it face up in a row, from left to right. Place a pound coin on a card near the right-hand end. Ask a friend to choose a number between 1 and 10. If they choose 4, count to the 4th card from the left. If this is a 7, count on a further seven cards. Continue in this way. When you land on a picture, count five cards. Hopefully, you will land on the coin.

The trick does not always succeed! It only works with probability 'about 5/6' according to [1]. We will confirm the statement, and make some related calculations.

How to do the trick

We give the easiest way. Slight variations are possible. Deal the first card. Suppose it is a 4. Count silently up to 4 as the next four cards are dealt. Using the number reached, start a new count on the next card. Remember that a picture counts as a five. Continue until the count cannot be completed. Place the pound coin on the last card of the previous count.

The original method is slightly different. The first count starts on a small card near the left-hand end of the row, rather than the first card. This is slightly harder to do, and gives no measurable advantage.

If the chosen number is 1, we will certainly land on the coin! But if not, there is still a high probability, as we said. We will next give a simple calculation of this probability.

But first we explain the principle of the trick. If our friend's path, starting from the chosen card, meets our path, starting from the first card, they continue along our path and land on the coin.

A simple calculation

The total value of the whole pack, counting each picture as 5, is:

$$4 \times (1 + 2 + \dots + 10) + 12 \times 5 = 280,$$

so the cards have average value $280/52 \approx 5.38$. Thus both paths involve jumps of average size about 5. A typical card lies on either path with probability about 1/5.

Suppose the trick fails. Then our friend's starting card is not on our path. This occurs with probability about 4/5. Each time they make a jump, they again land on a card not on our path—again with probability about 4/5. They will probably make about 9 jumps. For example, if they start on card 6 and always make jumps of 5, their ninth jump takes them to card 51. Suppose they make 9 jumps. Then they always miss our path with probability:

$$\left(\frac{4}{5}\right)^{10} \approx 0.107.$$

Thus we expect the trick to succeed with probability $1 - 0.107 \approx 0.893$. There are many approximations in this simple method, but it gives us an easy way to see why the trick usually works.

An exact calculation seems difficult (some precise calculations for a related problem are in [3]). Instead we will use computer simulation. Actually we shall consider a second, more complicated, trick. This one is more of an experiment than a trick.

A second trick

Deal the cards and place the pound coin as before. Now place ten pennies on cards 1 to 10. Move forward the left-hand penny by the value of its card. Continue to move the left-hand penny or pile of pennies in this way. Do not move any coins off the end of the row. When the left-hand pile can no longer be moved, it may be possible to move another pile.

At the end of this process, the pennies have become grouped into just a few piles—perhaps a single pile. One of these piles is on the pound—because the penny from card 1 is certainly there.

We can explore what happens by computer simulation. We dealt the cards 10,000 times, using a Psion Series 3a computer (about 0.5 seconds per deal). We obtained the histograms shown below:

n	number of times there are n pennies on pound	number of times there are n piles
1	8	5820
2	145	3973
3	232	206
4	400	1
5	483	0
6	618	0
7	688	0
8	789	0
9	817	0
10	5820	0

The main conclusions are these:

- (i) On average there were 8.54 pennies on the pound. Thus the basic trick succeeds with probability about 0.854, close to $5/6 \approx 0.833$.
- (ii) The most likely outcome (58%) is a single pile of all ten pennies on the pound. Two piles occur with probability 40%, and three with probability 2%. One of these piles is on the pound, usually the largest. More than three piles is very unlikely.

What is the object of the second trick? Presumably, a pile of all ten pennies on the pound. But the probability of this, about 58%, is too low to

be acceptable to conjurors. All the same, it is large enough to be interesting to mathematicians!

How many piles can we get?

We might wonder what is the largest number of piles we can obtain, if we can arrange the cards as we choose. The answer is *six*.

It is quite easy to show that seven piles is not possible. If we do have seven piles, we can choose a set of seven pennies which follow disjoint paths. Make one further jump with each penny. This takes it off the end of the row, so we imagine the row to be extended a little. The extended paths are allowed to meet. What is the minimum total length of the seven extended paths? This arises when the paths start on cards 4 to 10 and all finish on 'card 53'. Then the total length is:

$$7 \times (53 - 7) = 322.$$

The total length of the extended paths is equal to the total value of the cards on those paths. But the total value of the whole pack, counting each picture as 5, is only 280, as we saw in section 3.

So seven piles is not possible. Let us try six piles. Now the total length of the six extended paths is at least:

$$6 \times (53 - 15/2) = 273.$$

There do exist arrangements which achieve exactly this value! We leave the interested reader to find some. Clearly the pennies must start on cards 5 to 10, and finish, after the extra jump, on 'card 53'. The unused cards must have a total value of 7. In my solutions, which have a simple structure, only cards 1 to 4 are unused.

Finally we mention that Kruskal's principle has useful applications in computer science and cryptography. It is employed in the author's 'kangaroo' (or 'lambda') method for computing discrete logarithms [2,3,4]. The essential idea is this. If Kruskal's trick succeeds, and we know the total of the jumps made by each participant, we can deduce our friend's starting point.

I thank the referee for some useful comments.

References

1. M. Gardner, *Mathematical Games*, *Scientific American* (Feb. 1978).
2. J. M. Pollard, Monte Carlo methods for index computation (mod p), *Math. Comp.* **32** (1978) pp. 918-924.
3. J. M. Pollard, Kangaroos, Monopoly and discrete logarithms, *J. Cryptology* (to appear).
4. P. C. van Oorschot and M. J. Wiener, Parallel collision search with cryptanalytic applications, *J. Cryptology* **12** (1999) pp. 1-28.

JOHN M. POLLARD

Tidmarsh Cottage, Manor Farm Lane, Tidmarsh, Reading RG8 8EX