Re: permutation mappings

Source: http://www.derkeiler.com/Newsgroups/sci.crypt/2004−09/1044.html

---

From: David Eather (*eather_at_tpg.com.au*)
Date: 09/29/04

```
Date: Wed, 29 Sep 2004 13:39:52 +1000
```

Michael Amling wrote:
> David Eather wrote:
>> Peter Pearson wrote:
>>
>>> duffman wrote:
>>>
>>>> Let PI be a permutation of the integers 0,1,2,3...2^(n−1)
>>>> ...
>>>> ... Show the somewhat unexpected result that over 60% of mappings
>>>> will have at least one fixed point.
>
> That's not true. It fails when n=1, and the probability of at least
> one fixed point is only 50%.
>
>>>>
>>>> any ideas?
>>>
>>> Is this a homework assignment?
>>>
>>> In a mathematical games column long ago, this problem was
>>> presented in another form: what are the odds of winning a
>>> game in which Alice and Bob shuffle decks of cards, then
>>> reveal cards simultaneously. If ever two cards match, Alice
>>> wins, but if they get through the decks without encountering
>>> a match, Bob wins.
>>>
>>> There's a quick and erroneous analysis that gets the right
>>> answer. The only correct derivation I've seen was not quick.
>>>
>>> − Peter Pearson
>>
>> They should get just one match
>
> I agree the expectation value of the number of matches must be 1.
> Proof: If Alice selects a permutation of the cards uniformly at
> random, then it doesn't matter what Bob does with his. He may as well
> leave them in order. If Alice uses a Fisher−Yates shuffle, the
> probability of the the first card she exchanges staying in place is

> exactly 1/n, which becomes the probability of that card matching
> Bob's corresponding card. Thus the contribution of that card to the
> expectation value must be 1/n. But there's nothing special about that
> card. The contribution of each card to the expectation value must be
*> 1/n, hence the total expected number of matches must be n*1/n. QED.*
>
> If the expected number of matches is 1, then the lowest possible
> probability of 0 matches is 0, and that could only happen if the
> probability of having more than one match were 0, which happens only
> when the decks each consists of a single card. When there are at least
> two cards, the probability of at least one match must be less than 1.
> That's an upper limit.
>
> For a two−card deck the probability of zero matches is 1/2.
> With more than two cards, the probability of zero matches must be
> strictly less than 1/2, since the expectation value is 1 and there is
> a nonzero probability of more than 2 matches.
> Offhand the best lower limit I can establish is >50% when more
> than 2 cards in the deck, so I guess the OP will have to do his own
> homework.
>
> −−Mike Amling

The problem is mentioned in (amongst other places) a book called "taking chances − winning with probability" by haigh
I'm not sure if the detail is enough. Just keep thinking homework is fun, homework is fun...