Ling Li, ling@cs.caltech.edu

12.1 Where is my hat?

For convenience, let's number the gentlemen and their hats. The gentlemen are numbered from 1 to n, and the hat of the gentleman i is numbered with i. Let random variable K denote the number of gentlemen that get their own hats back.

Here's a simple way to find out $E(K)$. Let random variable X_i takes value 1 when the i^{th} gentleman gets his own hat, and value 0 when not. We have $K = \sum_{i=1}^{n} X_i$. Since each gentleman receives a random (uniformly chosen) hat, we also have

$$E(X_i) = P(X_i = 1) = \frac{1}{n}.$$

Thus

$$E(K) = E\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} E(X_i) = 1.$$

So averagely, only 1 gentleman gets his own hat. So lucky!

Now look at the Markov inequality, which says the probability that at least half get their own hats back is bounded by

$$P\left(K \geq \frac{n}{2}\right) = P\left(K \geq \left\lceil \frac{n}{2} \right\rceil E(K)\right) \leq \frac{1}{\left\lceil \frac{n}{2} \right\rceil}. \tag{1}$$

Let T be an arbitrary subset of $\{1, 2, \ldots, n\}$ with $|T| = k$. Then

$$P\left(\bigwedge_{i \in T} X_i = 1\right) = \frac{(n-k)!}{n!}, \tag{2}$$

which is the probability that each of the k gentlemen with numbers in set T gets his own hat back. Since there are $\binom{n}{k}$ such set T, we have

$$P(K \geq k) \leq \binom{n}{k} \frac{(n-k)!}{n!} = \frac{1}{k!}.$$

For $k < n$, we even have $P(K \geq k)$ strictly less than $\frac{1}{k!}$. This is because the probability that all gentlemen get their own hats back is included in (2) for all T. Thus

$$P(K \geq k) \leq \binom{n}{k} \frac{(n-k)!}{n!} - P(K = n) = \frac{1}{k!} - \frac{1}{n!}.$$

(We can see this more clearly by the principle of inclusion and exclusion.) Thus for $k = \left\lceil \frac{n}{2} \right\rceil$ and $n \geq 2$, we have $k < n$ and

$$P\left(K \geq \frac{n}{2}\right) = P\left(K \geq \left\lceil \frac{n}{2} \right\rceil\right) \leq \frac{1}{\left\lceil \frac{n}{2} \right\rceil !} - \frac{1}{n!},$$

which is strictly less than the Markov bound (1). So, the Markov bound (1) is loose. (For $n = 1$, it is trivial that the bound which is 1 is loose.)

Another (yet more complicated) way to get $E(K)$. Consider the situation that exactly k gentlemen with numbers in T are lucky enough to get their own hats, and the other $(n-k)$ gentlemen all get wrong hats. Thus, the numbers of the hats the other $(n-k)$ gentlemen get is a *wrong permutation* of the numbers of those $(n-k)$ gentlemen. The number of such wrong permutations, for $(n-k)$ gentlemen, by the principle of inclusion and exclusion, is

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

Taking the combinations of such set T, whose number is $\binom{n}{k}$, into consideration, we get the probability of exact k gentlemen get their own hats is

$$P(K=k)=\binom{n}{k}\frac{(n-k)!}{n!}\left(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^{n-k}\frac{1}{(n-k)!}\right)=\frac{1}{k!}\sum_{i=0}^{n-k}(-1)^i\frac{1}{i!}.$$

Thus the expectation number of the gentlemen who get their own hats is

$$E(K)=\sum_{k=0}^{n}k\cdot P(K=k)=\sum_{k=0}^{n}\left[\frac{k}{k!}\sum_{i=0}^{n-k}\frac{(-1)^i}{i!}\right].$$

We will use a tricky way to calculate $E(K)$. For $|x|<1$, we have

$$\left[\sum_{k=0}^{\infty}\frac{k}{k!}x^k\right]\left[\sum_{i=0}^{\infty}\frac{1}{i!}(-x)^i\right]=\sum_{j=0}^{\infty}\left[\sum_{k=0}^{j}\frac{k}{k!}\frac{(-1)^{j-k}}{(j-k)!}\right]x^j.$$

The sum of the coefficients of the first $(n+1)$ order is

$$\sum_{j=0}^{n}\left[\sum_{k=0}^{j}\frac{k}{k!}\frac{(-1)^{j-k}}{(j-k)!}\right]=\sum_{k=0}^{n}\left[\frac{k}{k!}\sum_{j=k}^{n}\frac{(-1)^{j-k}}{(j-k)!}\right]=\sum_{k=0}^{n}\left[\frac{k}{k!}\sum_{i=0}^{n-k}\frac{(-1)^i}{i!}\right]=E(K).$$

However, we know that

$$\left[\sum_{k=0}^{\infty}\frac{k}{k!}x^k\right]\left[\sum_{i=0}^{\infty}\frac{1}{i!}(-x)^i\right]=x\left(e^x\right)'\cdot e^{-x}=x,$$

so the sum of the coefficients of the first $(n+1)$ order is just 1. That is, $E(K)=1$.

Ling Li, ling@cs.caltech.edu

12.2 $GF(p^k)$

For distinct $b_1, b_2, b_3, b_4 \in GF(p)$, let

$$\mathbf{B} = \begin{pmatrix} 1 & b_1 & b_1^2 & b_1^3 \\ 1 & b_2 & b_2^2 & b_2^3 \\ 1 & b_3 & b_3^2 & b_3^3 \\ 1 & b_4 & b_4^2 & b_4^3 \end{pmatrix}.$$

The Vandermonde determinant theorem gives

$$\det(\mathbf{B}) = \prod_{i=1}^{3} \prod_{j=i+1}^{4} (b_i - b_j) \neq 0.$$

Thus in $GF(p)$, $\mathbf{B}$ is invertible and $f : \mathbf{x} \mapsto \mathbf{Bx}$ is a 1-1 map on function, from $GF(p)^4$ to $GF(p)^4$ (in fact, $GF(p^4)$ to $GF(p^4)$, if we take the tuple as a single element). Especially, since here $X_b = a_3 b^3 + a_2 b^2 + a_1 b + a_0$, we have

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} X_{b_1} \\ X_{b_2} \\ X_{b_3} \\ X_{b_4} \end{pmatrix} = \mathbf{B} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}, \text{ and } \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \mathbf{B}^{-1} \begin{pmatrix} X_{b_1} \\ X_{b_2} \\ X_{b_3} \\ X_{b_4} \end{pmatrix} = \mathbf{B}^{-1} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix},$$

meaning that there is a 1-1 mapping between the set of degree 3 polynomials over $GF(p)$ and the set of four-element tuples (c_1, c_2, c_3, c_4). Thus

$$P(X_{b_1} = c_1 \wedge X_{b_2} = c_2 \wedge X_{b_3} = c_3 \wedge X_{b_4} = c_4) = P(a_1, a_2, a_3, a_4) = p^{-4}.$$

So the random variables X_{b_1}, X_{b_2}, X_{b_3}, X_{b_4} are uniform and 4-wise independent.

Ling Li, ling@cs.caltech.edu

12.3 To be a millionare

It is neither better nor worse, on average, to switch.

First, I want to point out why the host's conclusion is wrong. Yes, when I picked an envelope, it is equally probable to have the large check or small check. However, if the large check was selected, the total amount of those two checks is $x + \frac{x}{2} = \frac{3x}{2}$; If the small check was selected, the total amount is $x + 2x = 3x$. They are different in terms of x. Since the total amount has already been decided before I selected an envelope, we can not fix x as the value I selected for the calculation of the expected winnings. We have already entered into the world of posterior probability.

Then, I give a way to calculate the expected value after a switch. Suppose the two checks are x_0 and x_1. The one I chose may be x_1, may be x_2. So the expected value of winning is

$$\frac{1}{2}(x_1 + x_2),$$

which is the same as that of not switching.

The tricky part of this problem is that there are different conditions for such switching, and they may give different answers. For example, we assumed that the total amount is a constant in the above analysis. However, we can also assume that the total amount is not an issue — it need not to be a constant. The problem can be redefined as below:

The host chooses $x \in_U [0, T]$, where T is a positive constant, and writes two checks, one with x dollars, the other $2x$ dollars. You choose one of them and find out it is y dollars. Here y is one of x or $2x$, not fixed. Then you are asked to switch or not to switch. What's your strategy to earn more money?

For this problem, the performance of always not switching is the same as that of always switching. However, we can use another strategy.*

Strategy-Z: Randomly choose T' as a guess for T. With fixed T', always switch if $y \leq T'$ and always not if $y > T'$.

OK, I do not want to prove anything about this strategy-Z. However, simulations show that the average performance of this strategy is better (or not worth) than the previous two strategies. And if $T' = T$, the ratio of this one to those two is a little higher that 5/4.

*Alexander Nicholson discussed this strategy with me.