

Fair gambling with a biased coin

Given a coin such that the two faces show up with probabilities p and q ($p+q=1$), can we generate a fair random sequence of 0s and 1s? If the coin is fair, i.e., $p=1/2$, $q=1/2$, the answer is simple: associate 0 with the one face and 1 with the other, and throw the coin once per digit to be produced. But what if the coin could be biased? Note that we are only given the possibly biased coin, and not the actual p, q -values.

The only thing we can do with the coin is throwing it repeatedly. Our task is to design an experiment with two possible outcomes of equal probability.

Our first observation is that this endeavour is bound to fail if the coin is so extremely biased that one of the faces never shows up — i.e. $p \cdot q = 0$ —, because in that case only one sequence of throws is possible and there cannot be two possible outcomes of the experiment. To phrase it differently: we have to design a deterministic algorithm intended to produce a 0 or a 1 when fed with a sufficiently long sequence of faces, but on a constant input sequence — i.e., all heads or all tails — the algorithm should fail to terminate. Because there are many such

algorithms, we do some more observing.

Our second observation is that it does not matter which side of the coin we call "head" as long as we call the other "tail". The simplest - and therefore standard - way of doing justice to such a binary symmetry is to consider pairs of faces, and to distinguish them according to being a pair of equal faces or a pair of different faces.

The combination of these two observations suggests to investigate the algorithm that starts

```

[[ var x, y: face;
  repeat record throw in (x);
           record throw in (y)
  until x ≠ y
; .....

```

It fails to terminate if $p \cdot q = 0$ - it has been designed that way - and, if $p \cdot q > 0$, it terminates with probability 1. (The expectation value of the number of double throws is $(p \cdot q)^{-1}$.) Moreover it solves our problem, since the above can terminate in two ways, $(x, y) = (\text{head}, \text{tail})$ or $(x, y) = (\text{tail}, \text{head})$, and both outcomes are equally likely.

* * *

It took me very long to design the above solution. After having made the first observation but before

having made the second one, I started to study all sorts of algorithms that failed to terminate on the constant input sequence. And that while the second observation is absolutely standard (vide the bichrome G-graph). I find it shocking that at my age I allowed myself to be lured into the wild search I embarked upon. As soon as I became very stern with myself and told myself not to behave like an uneducated idiot, the above solution was designed.

The problem seems very well known; somehow I had missed it. I was quite thrilled by it! Making a fair "physical" coin is quite hard, for how does one establish that one has one? You cannot test it. Here we have a "mathematical" coin that is fair by construction! Two cheers for mathematics.

Inks Lake State Park,
on the 30th anniversary of my Ph.D.

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA