Is it possible to simulate a fair coin with a finite number of tossing of a biased one?

It is a classic problem to simulate a fair coin with a biased one.

According to Fair Coin (wiki),

> John von Neumann gave the following procedure:
>
> 1. Toss the coin twice.
> 2. If the results match, start over, forgetting both results.
> 3. If the results differ, use the first result, forgetting the second.

In the worst case, the procedure may not terminate.

Problem: Is it possible to design an algorithm which guarantees termination in the worst case? What is the technique to solve such an impossibility problem?

proof-techniques probability-theory randomized-algorithms randomness probabilistic-algorithms

asked 22 hours ago
hengxin
6,810 13 46

2 No, it's not possible, even when you know the bias of the coin to be, say, 1/3. – Yuval Filmus 16 hours ago

1 Answer

No, it's not possible. Suppose the bias of the coin is $1/3$, and suppose you could guarantee termination. Then there would be some n such that this always terminates after n coin flips. Let S denote the set of flip-sequences that causes your algorithm to output 0 (so that $\overline{S}$ is the set of flip-sequences that causes your algorithm to output 1). The probability of your algorithm outputting 0 is equal to the probability of getting a flip-sequence in S, which is a sum of the form

$$\sum_{x \in S} \frac{a_x}{3^n}$$

where each a_x is an integer. Thus the probability of outputting 0 has the form $b/3^n$ where b is an integer. We want this to be $1/2$, for your algorithm to produce an unbiased bit of output. However since 3^n is odd, there is no integer b such that $b/3^n = 1/2$. Therefore, no such algorithm can exist.

answered 16 hours ago
D.W. ♦
95.3k 11 109 255

2 See this question and its answer for an extension of this argument that works for all rational biases (other than 1/2). – Yuval Filmus 9 hours ago

Answer Your Question