

Re: Please help me to find a mistake here

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg00999.html>

- *From:* matt271829-news@xxxxxxxxxxxxx
 - *Date:* 6 Jul 2006 10:37:43 -0700
-

valery wrote:

matt271829-news@xxxxxxxxxxxxx wrote:

Anyway, FWIW, making some simplifying assumptions (that seem entirely reasonable since 71 is so much smaller than 2^{32}), I make the probability of event E equal to about $1.76E-10$. I think this is slightly different from James Waldby's answer. I did it in a slightly more elaborate way, but with these particular numbers I would have thought the answers should differ by only an imperceptible amount. I'm not sure at the moment why the answers differ as much as they do, but if I get a following wind I might try to pick through it and figure it out.

$1.76E-10$ sounds just perfect! it passes reality check and is very well aligned with my experiment (taking your numbers gives us about 0.58 probability that event E occurs at least once per 2^{32} attempts). Could you post your formulas, please? (with some explanations if possible ;-).

-Valery.

<http://www.harper.no/valery>

How do you get 0.58? I make $1 - (1 - 1.76E-10)^{(2^{32})}$ equal to about 0.53... Incidentally, I don't think that your eight-out-of-twelve experimental result is particularly diagnostic when discriminating between the various suggested answers. With such a small number of trials the experimental results are consistent with a fairly wide range of actual probabilities.

Anyway. As understand it, to calculate $\Pr(E)$, the probability of event E, we need to select 71 different numbers randomly from the numbers 0 to $2^{32} - 1$, and find the probability that at least two pairs differ by exactly one bit. I will let $k = 71$ and $n = 32$. The exact answer looks rather difficult to compute (unless I'm missing something obvious), but as a simplification one can assume that all the pairs in the set of k numbers can be considered independently.

Re: Please help me to find a mistake here

The simplest way to do this is something along the lines of the method that I think James Waldby used, and I'll use some of his notation for consistency. The probability that any individual pair of (distinct) numbers does NOT differ by exactly one bit is, as far as