

Re: Random number generation using radioactivity

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-08/1789.html>

From: Michael Jørgensen (*ingen_at_ukendt.dk*)

Date: 08/09/04

Date: Mon, 9 Aug 2004 08:27:33 +0200

<juuitchan@hotmail.com> wrote in message
news:9159d95e.0408082112.428be67b@posting.google.com...
> *I wonder if this would be a good method for random number generation*
> *using radioactive decay:*
>
> *You have a radioactive source and a Geiger counter. This setup is*
> *connected to a computer. The computer's internal timer is good enough*
> *to split the average time between two consecutive decays into several*
> *hundred parts.*
>
> *You take the intervals between successive decays modulo P (P is a*
> *smallish prime number, like 41 or 59). When you get about 30 or so of*
> *these numbers, you concatenate them, read it as a single base- P*
> *number, convert it to decimal, throw away the first 10 or so digits,*
> *and keep the rest as random digits.*

Well, it won't be *exactly* uniform.

Each measured interval follows an known distribution (geometric?) with an average value of around 200 (you wrote "several hundred parts"). Taken modulo 41, we have a random integer in the range $[0, 40]$. The distribution is still not uniform, there will be a substantial bias towards low numbers.

What happens after that I'm not quite sure about. However, if we look at information content, then each measurement gives you approximately 5 bits of information. After collecting 30 values and converting to decimal and throwing away 10 digits we get $(5*30 - 10*3) = 120$ bits of information. That should give you approximately 40 random digits, but keeping the non-uniformity in mind, I would not trust them all to be independent.

Here's an alternate approach, that tries to achieve uniformity:

[disclaimer: This is something I just thought of, while replying to this post. Use at your own risk!]

Take the difference between pairwise measurements. This gives an integer in the range $[-40, 40]$, with a peak at the value 0. Now add together 8 of such

sci.math: Re: Random number generation using radioactivity

values (using a total of 16 measurements). This gives an integer in the range $[-15*40, 15*40]$ which almost follows a normal distribution. You must now normalize, so that the standard deviation becomes 1.

Now if my memory serves me well; if X and Y are normal distributed independent variables, then $\exp(-(X^2 + Y^2))$ is uniformly distributed in the interval $]0,1[$.

-Michael.