Subject: IDL random number generator
Posted by krijger on Fri, 09 May 2003 11:47:02 GMT
View Forum Message <> Reply to Message

Hi,
I know that randomn is pseudo-random, how many numbers can you
generate before the non-randomness kicks in?

Thijs Krijger

Subject: Re: IDL random number generator
Posted by jeyadev on Tue, 13 May 2003 18:54:20 GMT
View Forum Message <> Reply to Message

In article <tandp-1205031112540001@dialup-63.211.240.1.dial1.denver1.level3.net>,
Mike <tandp@mediaone.net> wrote:
>
> A faulty memory led me to describe teh seed as needing to be the largets
> prime number available on the given system. Actually it is the modulus
> value that should be chosen this way. The choice of seed, multiplier and
> modulus numbers is discussed a bit in Numerical Recipes which refers to
> Knuth's book. If you need reliable details readup on it there. Don;t trust
^^^^^^^^^^

> the internet.
^^^^^^^^^^^

Now, *that* is logical conundrum!

What is the poor reader supposed to do?!
--

Surendar Jeyadev jeyadev@wrc.xerox.bounceback.com

Remove 'bounceback' for email address

Subject: Re: IDL random number generator
Posted by David Fanning on Wed, 14 May 2003 23:28:57 GMT
View Forum Message <> Reply to Message

Folks,

You guys might want to check out this Quantum Random
Number Generator. This one takes a LONG time to repeat! :-)

http://www.idquantique.com/qrng.html

Cheers,

David

--
David W. Fanning, Ph.D.
Fanning Software Consulting, Inc.
Phone: 970-221-0438, E-mail: david@dfanning.com
Coyote's Guide to IDL Programming: http://www.dfanning.com/
Toll-Free IDL Book Orders: 1-888-461-0155

Subject: Re: IDL random number generator
Posted by rmoss4 on Thu, 15 May 2003 15:19:54 GMT
View Forum Message <> Reply to Message

That is pretty cool. However, it would not appear to be very useful if you need the ability to replicate your results (e.g. in cases where you would use a known seed value to reproduce a pseudo-random series of numbers). Nevertheless, it's probably as close as one can get to "true" randomness. Ain't physics great?

--
Robert M. Moss, PhD
rmoss4@houston.rr.com
281-856-2017

David Fanning wrote:
> Folks,
>
> You guys might want to check out this Quantum Random
> Number Generator. This one takes a LONG time to repeat! :-)
>
>   http://www.idquantique.com/qrng.html
>
> Cheers,
>
> David
>

Subject: Re: IDL random number generator
Posted by condor on Mon, 19 May 2003 23:51:10 GMT
View Forum Message <> Reply to Message

David Fanning <david@dfanning.com> wrote in message
news:<MPG.192c7f24abbae652989b96@news.frii.com>...
> Folks,
>
> You guys might want to check out this Quantum Random
> Number Generator. This one takes a LONG time to repeat! :-)
>
> http://www.idquantique.com/qrng.html
>
> Cheers,
>
> David

I would mistrust this for the following reasons.

The website states:

> Being deterministic devices, computers are not capable of producing random
> number generators.

That statement is false: any odd soundcard has a noise-generator
(essentially a glorified resistor with a big amplifier attached to it)
that is capable of producing perfectly fine thermal random noise. I've
used that for creating random numbers since back in the days of the
Atari-800 (OK, so I'm dating myself here).

Even if a piece of external hardware was desirable for this process it
could be cobbled together for $5 from a couple resistors, an opAmp for
amplification and an RC high-pass filter (to get rid of slow drifting
in the opAmp). Potentially another opAmp driven open-loop as a
Schmitt-trigger. Gives you clock-free(!) bit-noise.

Anybody who tries to sell a quantum-ANYTHING to make noise(!!) is
direputable from the word 'go' in my eyes.

Subject: Re: IDL random number generator
Posted by rmoss4 on Tue, 20 May 2003 04:18:07 GMT
View Forum Message <> Reply to Message

Big Bird wrote:
> David Fanning <david@dfanning.com> wrote in message
news:<MPG.192c7f24abbae652989b96@news.frii.com>...
>
>> Folks,
>>
>> You guys might want to check out this Quantum Random
>> Number Generator. This one takes a LONG time to repeat! :-)

>>
>>   http://www.idquantique.com/qrng.html
>>
>> Cheers,
>>
>> David
>
>
> I would mistrust this for the following reasons.
>
> The website states:
>
>
>> Being deterministic devices, computers are not capable of producing random
>> number generators.
>
>
> That statement is false: any odd soundcard has a noise-generator
> (essentially a glorified resistor with a big amplifier attached to it)
> that is capable of producing perfectly fine thermal random noise. I've
> used that for creating random numbers since back in the days of the
> Atari-800 (OK, so I'm dating myself here).
>
> Even if a piece of external hardware was desirable for this process it
> could be cobbled together for $5 from a couple resistors, an opAmp for
> amplification and an RC high-pass filter (to get rid of slow drifting
> in the opAmp). Potentially another opAmp driven open-loop as a
> Schmitt-trigger. Gives you clock-free(!) bit-noise.
>
> Anybody who tries to sell a quantum-ANYTHING to make noise(!!) is
> direputable from the word 'go' in my eyes.

Thermal random noise is itself quantum in nature. Though not stated very precisely, I think the web site is referring to computer software (as opposed to hardware) as being deterministic and therefore non-random. I agree with you though that there are less expensive ways of making noise :)

--
Robert M. Moss, PhD

Subject: Re: IDL random number generator
Posted by James Kuyper on Tue, 20 May 2003 14:30:43 GMT
View Forum Message <> Reply to Message

Big Bird wrote:
>
> David Fanning <david@dfanning.com> wrote in message

news:<MPG.192c7f24abbae652989b96@news.frii.com>...
>> Folks,
>>
>> You guys might want to check out this Quantum Random
>> Number Generator. This one takes a LONG time to repeat! :-)
>>
>> http://www.idquantique.com/qrng.html
>>
>> Cheers,
>>
>> David
>
> I would mistrust this for the following reasons.
>
> The website states:
>
>> Being deterministic devices, computers are not capable of producing random
>> number generators.
>
> That statement is false: any odd soundcard has a noise-generator
> (essentially a glorified resistor with a big amplifier attached to it)
> that is capable of producing perfectly fine thermal random noise. I've
> used that for creating random numbers since back in the days of the
> Atari-800 (OK, so I'm dating myself here).

It's an exagerration, rather than being false. Their real point was that
the standard random number generators are not truly random, and can't be
truly random as long as they are entirely based in software.

> Even if a piece of external hardware was desirable for this process it
> could be cobbled together for $5 from a couple resistors, an opAmp for
> amplification and an RC high-pass filter (to get rid of slow drifting
> in the opAmp). Potentially another opAmp driven open-loop as a
> Schmitt-trigger. Gives you clock-free(!) bit-noise.
>
> Anybody who tries to sell a quantum-ANYTHING to make noise(!!) is
> direputable from the word 'go' in my eyes.

Thermal noise is not as fundamentally random as the quantum fluctuations
that determine radioactive decay. Among other things, your circuit will
pick up and therefore be influenced by EM radiation, which is not
random, and since it's thermal noise you're looking at, it will be
influenced by the temperature. I'll admit, it's a subtle difference, but
if you were doing serious scientific work using those random numbers,
it's one you should worry about when designing the program.

Subject: Re: IDL random number generator
Posted by tandp on Wed, 21 May 2003 02:54:23 GMT
View Forum Message <> Reply to Message

> influenced by the temperature. I'll admit, it's a subtle difference, but
> if you were doing serious scientific work using those random numbers,
> it's one you should worry about when designing the program.

For scientific work a pseudorandom number generator should be sufficient as long as it is well designed, i.e. has cycle longer than the number of values it will be rquired to generate and generates data that has a prescribed mean (usually zero). It should conform to the probablility distribution it is designed for. A random number generator of values from a uniform distribution should be verifiable as generating data with a zro mean and have a frequency spectrum indistiguishable from white noise.