Subject: Re: IDL random number generator
Posted by Matt Feinstein on Mon, 12 May 2003 18:06:37 GMT
View Forum Message <> Reply to Message

On 12 May 2003 02:29:54 -0700, krijger@astro.uu.nl wrote:

> James Kuyper <kuyper@saicmodis.com> wrote in message
news:<3EBBB786.9C52F5F3@saicmodis.com>...
>> krijger@astro.uu.nl wrote:
>>>
>>> Hi,
>>> I know that randomn is pseudo-random, how many numbers can you
>>> generate before the non-randomness kicks in?
>>>
>>> Thijs Krijger
>>
>> None. The non-randomness is there from the very beginning. You could
>> make a true random number generator by running it off of the radioactive
>> decay of atoms, or some similar hardware-based approach. However,
>> software random number generators are absolutely deterministic, once
>> you've set up the seed. You can set the seed form a clock setting, which
>> means that the precise sequence of random numbers generated depends upon
>> the precise time at which the program reads the clock. But even the very
>> first number can be absolutely predicted from the seed value.
>>
>> Every random number generator has a period, after which it starts
>> repeating the same exact sequence. How long that period is depends upon
>> the quality of the algorithm used. Commonly used algorithms have periods
>> in the range of 100,000 numbers or better. Very sophisticated generators
>> can have periods that are so long that your computer will become
>> obsolete before the sequence repeats.
>
> So, if in IDL I use the data=randomn(seed,N), then how big can N be
> (and I can make the claim that the numbers are still random (compared
> to each other))?
>
> Thijs Krijger

The period of a reasonable random number generator should be at least
2^32 (around four billion) and could be larger-- you need to know the
details of the algorithm to be sure. Table 1 in Knuth's chapter on
random numbers has one with an effective modulus of 2^1376, which is a
pretty big number by most standards. It's worth pointing out that the
subject of random number generators has been worked over rather
heavily since the 60's, when some notorious algorithms produced
numbers that weren't very random. Modern algorithms must pass a
battery of stringent tests for non-correlation and non-periodicity in
all low dimensions. The moral is that you can't select a random number

generator at random.

Matt Feinstein

--
The Law of Polarity: The probability of wiring a battery with
the correct polarity is (1/2)^N, where N is the number of times
you try to connect it.