Subject: Re: IDL random number generator
Posted by James Kuyper on Sun, 11 May 2003 06:30:46 GMT
View Forum Message <> Reply to Message

Mike wrote:

```
>
> In article <3EBBB786.9C52F5F3@saicmodis.com>, James Kuyper
> <kuyper@saicmodis.com> wrote:
>
>> 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
>                                                ^
>                                                |  and the seed
>
>> 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
>
> The best pseudorandom number generator (congruence method and seed chosen
> to be the largest prime ineteger representable in a word) will have a
> period equal to the seed value.
```

The seed value? Thus, if the seed value is 1, it repeats indefinitely? I
think you're mistaken on that.

My understanding is that, if care is taken it choosing the parameters of
the algorithm, the period is precisely the best that it could be,
independent of the seed value chosen. It's 2^n-1, where n is the number
of bits in the seed. However, there are other algorithms that set up an
initial state which is much larger than the seed itself, often
represented as a array of integers. Ideally, such generators could have
a period as long as 2^(n*m), where m is the number of n-bit integers in

the array. Let 'm' be as small as 128, and you've got a period that could never possibly be measured before the machines they run on become obsolete.