Linear Congruential Generator

- Goal: Generate Un uniform in the interval [0,1)
- Generate Xn in [0,m), Un = Xn/m
- Xn+1 = (a*Xn + c)%m – Linear congruential series
- Four constants required
- X0 (starting value/seed), a (multiplier), c (increment/bias),m (modulus)
- X0 = a = c = 7, m = 10 will give 7, 6, 9, 0, 7, 6, 9, 0, ...
  - Four magic numbers required:

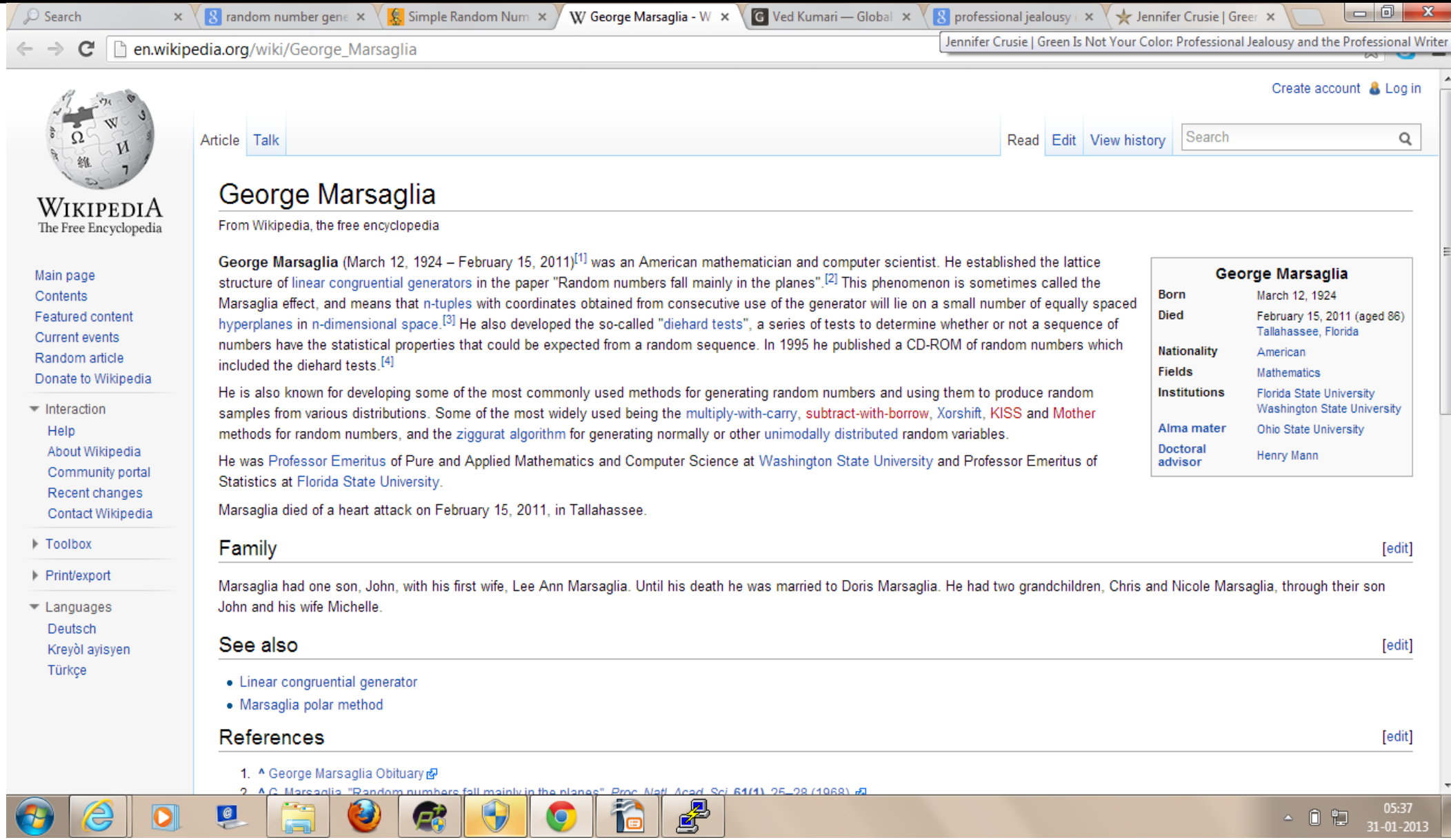
Linear Congruential Generator 2

- Xn+1 =(65539*Xn)%pow(2,31)
- This is essentially RANDU, most popular generator for many years
  - Multiplicative congruential method (Lehman's original method)
  - Mixed congruential method C != 0
- For the math (number theory): http://www.math.cornell.edu/~mec/Winter2009/Luo/Linear%20Congruential%20Generator/linear%20congruential%20gen1.html

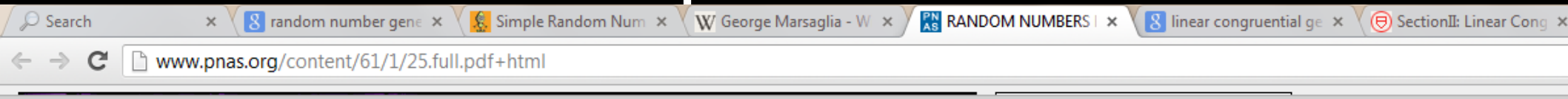
Code for linear congruential generator

```
#include <iostream>
#include <cmath>



double GetUniform()
{
  Static int X0 = 12345, m = 0, Xn = 0;
  m = pow(2,31);
  Xn=X0;
  Xn = (65539*Xn)%m;
  return (double)Xn/(double)m;
}

int main(){

  std::cout<<GetUniform()<<std::endl;

  return 0;
}
```

Marsaglia


Search
random number gene
Simple Random Num
George Marsaglia - W
Ved Kumari — Global
professional jealousy
Jennifer Crusie | Gree
Jennifer Crusie | Green Is Not Your Color: Professional Jealousy and the Professional Writer
en.wikipedia.org/wiki/George_Marsaglia
Create account
Log in
Article
Talk
Read
Edit
View history
Search
WIKIPEDIA
The Free Encyclopedia
Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia
Toolbox
Print/export
Languages
Deutsch
Kreyòl ayisyen
Türkçe
George Marsaglia
From Wikipedia, the free encyclopedia
George Marsaglia (March 12, 1924 – February 15, 2011)[1] was an American mathematician and computer scientist. He established the lattice structure of linear congruential generators in the paper "Random numbers fall mainly in the planes".[2] This phenomenon is sometimes called the Marsaglia effect, and means that n-tuples with coordinates obtained from consecutive use of the generator will lie on a small number of equally spaced hyperplanes in n-dimensional space.[3] He also developed the so-called "diehard tests", a series of tests to determine whether or not a sequence of numbers have the statistical properties that could be expected from a random sequence. In 1995 he published a CD-ROM of random numbers which included the diehard tests.[4]
He is also known for developing some of the most commonly used methods for generating random numbers and using them to produce random samples from various distributions. Some of the most widely used being the multiply-with-carry, subtract-with-borrow, Xorshift, KISS and Mother methods for random numbers, and the ziggurat algorithm for generating normally or other unimodally distributed random variables.
He was Professor Emeritus of Pure and Applied Mathematics and Computer Science at Washington State University and Professor Emeritus of Statistics at Florida State University.
Marsaglia died of a heart attack on February 15, 2011, in Tallahassee.
George Marsaglia
Born March 12, 1924
Died February 15, 2011 (aged 86) Tallahassee, Florida
Nationality American
Fields Mathematics
Institutions Florida State University Washington State University
Alma mater Ohio State University
Doctoral advisor Henry Mann
Family
[edit]
Marsaglia had one son, John, with his first wife, Lee Ann Marsaglia. Until his death he was married to Doris Marsaglia. He had two grandchildren, Chris and Nicole Marsaglia, through their son John and his wife Michelle.
See also
[edit]
Linear congruential generator
Marsaglia polar method
References
[edit]
1. ^ George Marsaglia Obituary
2. ^ G. Marsaglia. "Random numbers fall mainly in the planes". Proc. Natl. Acad. Sci. 61(1). 25–28 (1968)
05:37
31-01-2013

Random numbers stay mainly in the plane



RANDOM NUMBERS FALL MAINLY IN THE PLANES

By George Marsaglia

MATHEMATICS RESEARCH LABORATORY, BOEING SCIENTIFIC RESEARCH LABORATORIES, SEATTLE, WASHINGTON

Communicated by G. S. Schairer, June 24, 1968

Virtually all the world's computer centers use an arithmetic procedure for generating random numbers. The most common of these is the multiplicative congruential generator first suggested by D. H. Lehmer. In this method, one merely multiplies the current random integer I by a constant multiplier K and keeps the remainder after overflow:

$$\text{new } I = K \times \text{old } I \quad \text{modulo } M.$$

The apparently haphazard way in which successive multiplications by a large integer K produce remainders after overflow makes the resulting numbers work surprisingly well for many Monte Carlo problems. Scores of papers have reported favorably on cycle length and statistical properties of such generators.

The purpose of this note is to point out that all multiplicative congruential

The purpose of this note is to point out that all multiplicative congruential random number generators have a defect—a defect that makes them unsuitable for many Monte Carlo problems and that cannot be removed by adjusting the starting value, multiplier, or modulus. The problem lies in the "crystalline" nature of multiplicative generators—if n-tuples $(u_1,u_2,\ldots,u_n)$, $(u_2,u_3,\ldots,u_{n+1}),\ldots$ of uniform variates produced by the generator are viewed as points in the unit cube of n dimensions, then *all* the points will be found to lie in a relatively small number of parallel hyperplanes. Furthermore, there are many systems of parallel hyperplanes which contain all of the points; the points are about as randomly spaced in the unit n-cube as the atoms in a perfect crystal at absolute zero.

One can readily think of Monte Carlo problems where such regularity in "random" points in n-space would be unsatisfactory; more disturbing is the possibility that for the past 20 years such regularity might have produced bad, but unrecognized, results in Monte Carlo studies which have used multiplicative generators.

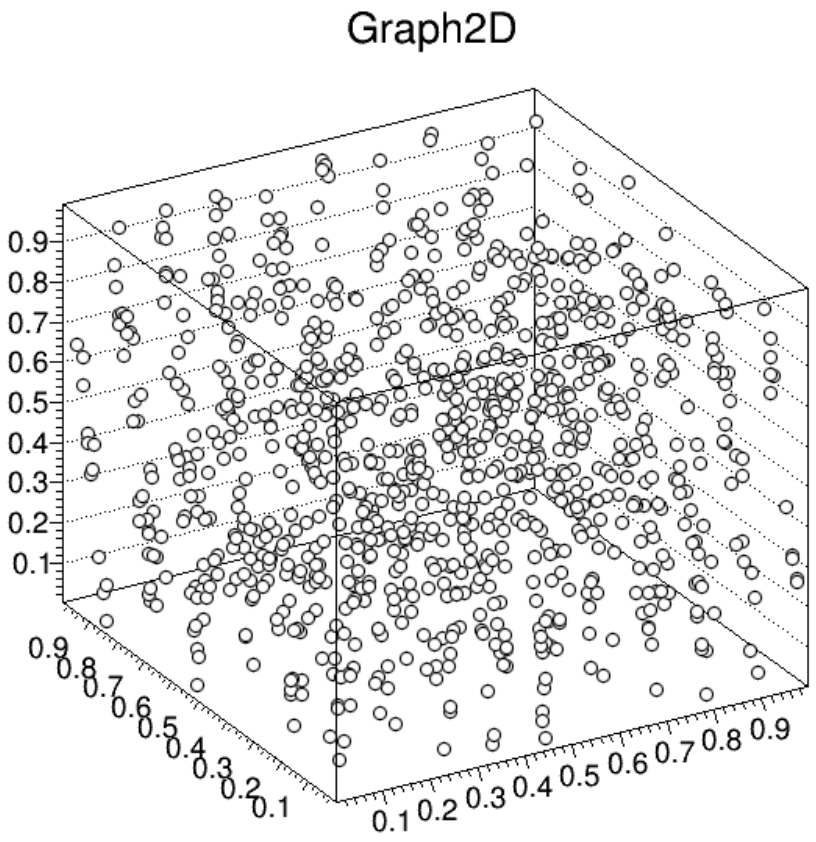
Multiply with carry

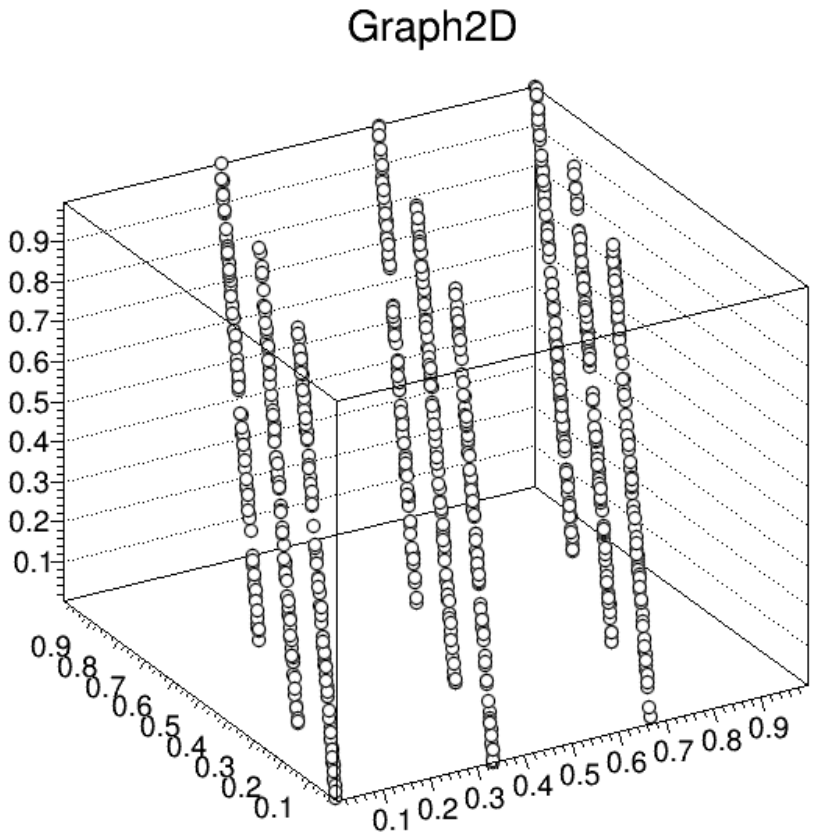
```
 uint GetUint()
{
    m_z = 36969 * (m_z & 65535) + (m_z >> 16);
    m_w = 18000 * (m_w & 65535) + (m_w >>
16);
    return (m_z << 16) + m_w;
}
```

Test of randomness

- Diehard tests (Marsaglia 1995)
- Birthday spacings, parking lot test, the craps test, monkey tests (based on infinite monkey theorem), count the 1's,...
- See eg:http://en.wikipedia.org/wiki/Diehard_tests

Test result: falling on planes





Other distributions from uniform variate

- Uniform random numbers can be used to generate other distributions
- Let x be uniform in (0.,1.), we want a new random number a in (a1,a2) distributed as g(a)
- Conservation of probability:

  g(a)da = f(x)dx; f(x) = 1.

  g(a) = |dx/da|
- If g(a) is desired to be exponential then:
- (1/D)*exp(-a/D) = |dx/da| (D = const parameter)

Acceptance—rejection method

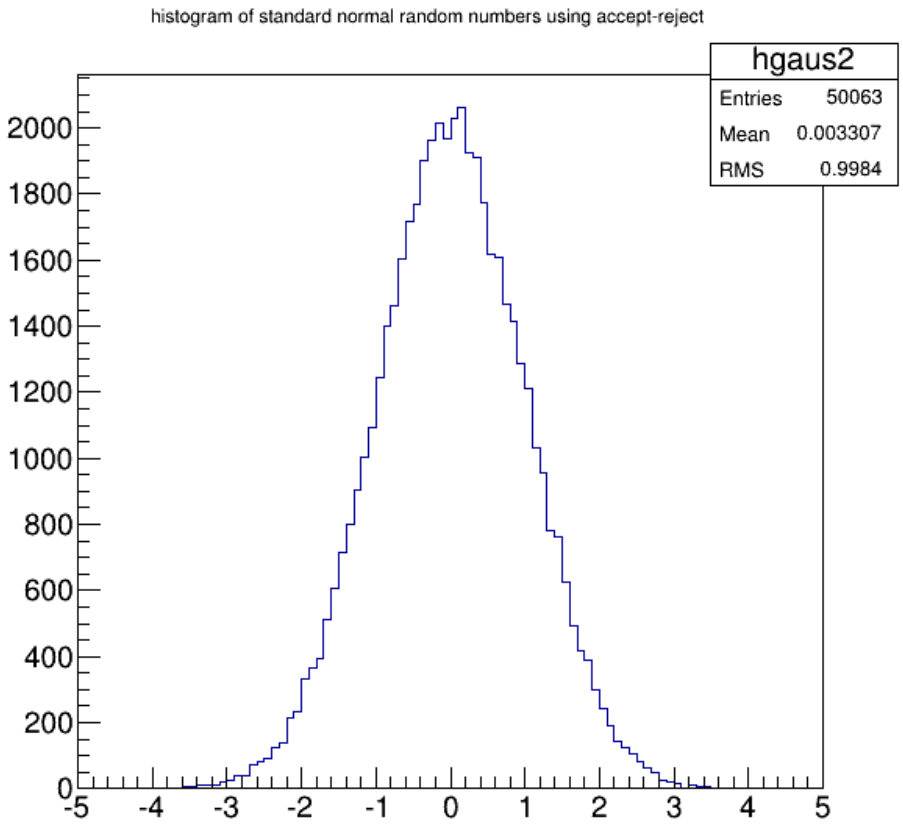
- Due to Von Neumann

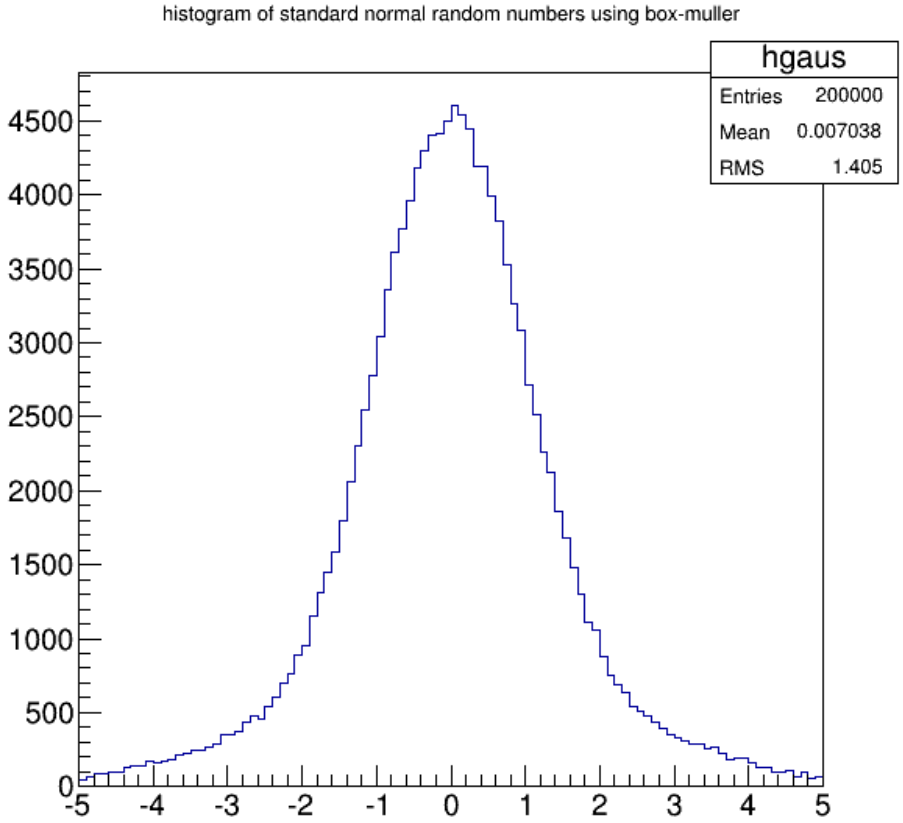
(1) Generate a random number x, uniformly distributed between $x_{\min}$ and $x_{\max}$, i.e. $x = x_{\min} + r_1(x_{\max} - x_{\min})$ where r_1 is uniformly distributed between 0 and 1.

(2) Generate a second independent random number u uniformly distributed between 0 and $f_{\max}$, i.e. $u = r_2 f_{\max}$.

(3) If $u < f(x)$, then accept x. If not, reject x and repeat.

Gaussian random numbers





Box muller method

A NOTE ON THE GENERATION OF RANDOM NORMAL DEVIATES[1]

By G. E. P. Box and Mervin E. Muller

Princeton University

1. Introduction. Sampling experiments often require the generation of large numbers of random normal deviates. When an electronic computer is used it is desirable to arrange for the generation of such normal deviates within the machine itself rather than to rely on tables. Pseudo random numbers can be generated by a variety of methods within the machine and the purpose of this note is to give what is believed to be a new method for generating normal deviates from independent random numbers. This approach can be used on small as well as large scale computers. A detailed comparison of the utility of this approach with other known methods (such as: (1) the inverse Gaussian function of the uniform deviates, (2) Teichroew's approach, (3) a rational approximation such as that developed by Hastings, (4) the sum of a fixed number of uniform deviates and (5) rejection-type approach), has been made elsewhere [1] by one of the authors (M.M.). It is shown that the present approach not only gives higher accuracy than previous methods but also compares in speed very favourably with other methods.

2. Method. The following approach may be used to generate a pair of random deviates from the same normal distribution starting from a pair of random numbers.

Method: Let U_1, U_2 be independent random variables from the same rectangular density function on the interval (0, 1). Consider the random variables:

$$X_1 = (-2 \log_e U_1)^{1/2} \cos 2\pi U_2$$
$$X_2 = (-2 \log_e U_1)^{1/2} \sin 2\pi U_2 \tag{1}$$

Received October 30, 1957; revised January 31, 1958.

[1] Prepared in connection with research sponsored by the Office of Ordnance Research, U. S. Army; Statistical Techniques Research Group, Princeton University, Contract No. DA 36-034-ORD 2297.

Box muller method 2

Then (X_1, X_2) will be a pair of independent random variables from the same normal distribution with mean zero, and unit variance.

Justification: From (1) (giving attention to principal values), one obtains at once the inverse relationships:

$$U_1 = e^{\frac{-(X_1^2 + X_2^2)}{2}} \cdot$$

$$U_2 = -\frac{1}{2\pi} \arctan \frac{X_2}{X_1}.$$

It follows that the joint density of X_1, X_2 is

$$f(X_1, X_2) = \frac{1}{2\pi} e^{\frac{-(X_1 + X_2)}{2}} = \frac{1}{\sqrt{2\pi}} e^{\frac{-X_1^2}{2}} \cdot \frac{1}{\sqrt{2\pi}} e^{\frac{-X_2^2}{2}} = f(X_1) f(X_2);$$

thus the desired conclusions, including the independence of X_1 and X_2 is obtained.

The above approach is motivated by the following considerations: the probability density of $f(X_1, X_2)$ is constant on circles, so $\Theta = \arctan X_2/X_1$ is uniformly distributed $(0, 2\pi)$. Further, the square of the length of the radius vector $r^2 = X_1^2 + X_2^2$ has a Chi-squared distribution with two degrees of freedom. If U has a rectangular density on $(0, 1)$ then $-2 \log_e U$ has a Chi-squared distribution with two degrees of freedom. Proceeding in the reverse order we arrive at (1).

3. Generalizations and other random variables. Observations from the Chi-squared distribution with $2k$ degrees of freedom can of course be generated by adding together the k terms, $\sum_{i=1}^{k} (-2 \log_e U_1)$ and for Chi-squared with $2k + 1$ degrees of freedom one may add the square of a normal deviate generated by the above method. Deviates from the F-distribution and for the t-distribution are obtained by calculating the appropriate ratio of deviates generated as above. From independent random normal deviates well known methods can of course be used to generate n-dimensional normal deviates with arbitrary means and variance-covariance matrix.

4. Convenience and accuracy. The method suggested here grew out of the desire to have a way of generating normal deviates which would be reliable in the tails of the distribution. Since most computing centers have library programs to compute values of trigonometric functions, logarithms, and square roots this approach requires little additional machine program writing. The accuracy obtained depends essentially on the precision of the available library programs, whereas that of other methods cannot readily be increased.

- Annals of mathematical statistics, vol. 29, 1958

Usfulness of randomness

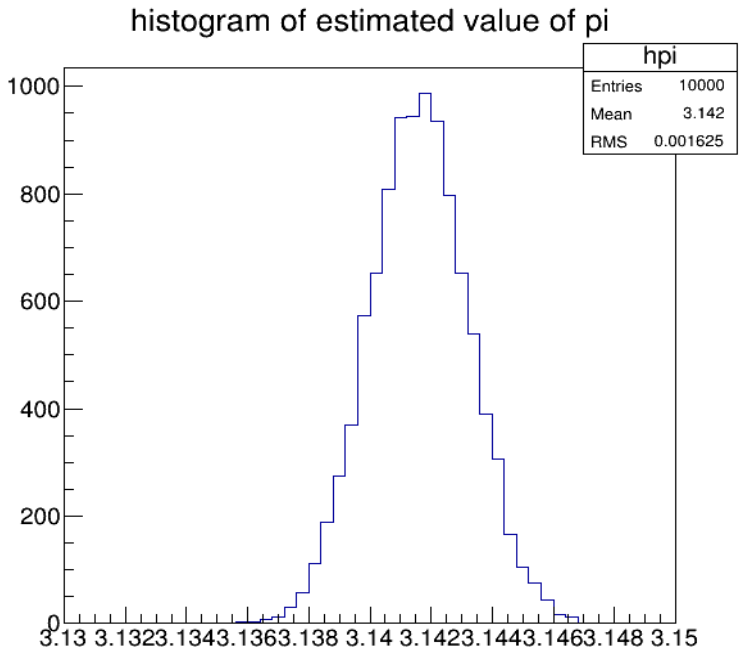
- What is the probability of getting two sixes in 10 throws of a fair dice?
- Example code dicethrow

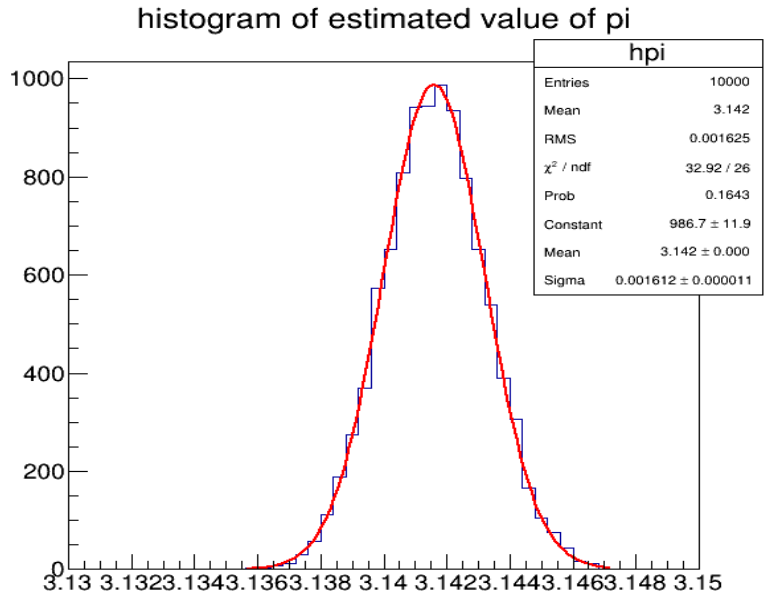
Random to estimate not random

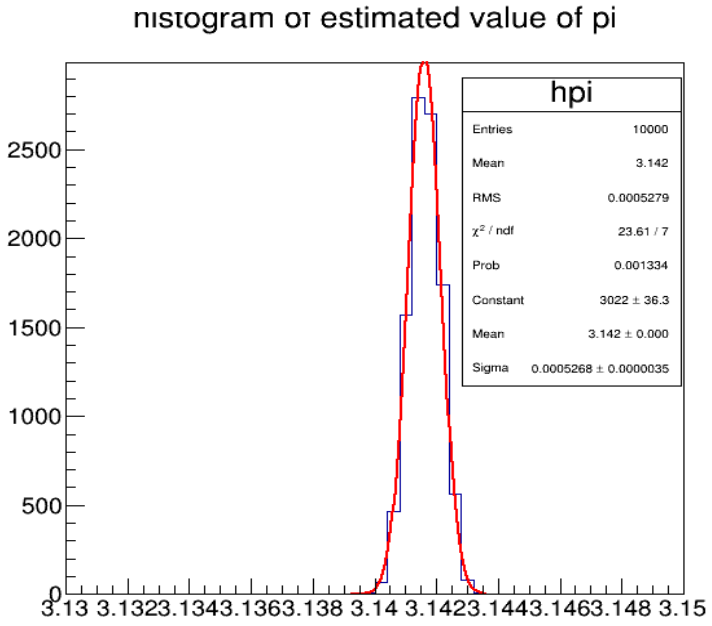
- The earliest values of π were experimentally measured. In the Egyptian Rhind Papyrus, which is dated about 1650 BC, there is good evidence for $4 \times (8/9)2 = 3.16$ as a value for π.
- A little known verse of the Bible reads
- And he made a molten sea, ten cubits from the one brim to the other: it was round all about, and his height was five cubits: and a line of thirty cubits did compass it about. (I Kings 7, 23)
- It occurs in a list of specifications for the great temple of Solomon, built around 950 BC, it gives $\pi = 3$. Egyptian and Mesopotamian values of $25/8 = 3.125$ and $\sqrt{10} = 3.162$ have been traced to much earlier dates.
- The first theoretical calculation seems to have been carried out by Archimedes of Syracuse (287-212 BC). He obtained the approximation $223/71 < \pi < 22/7$.
- $\pi/4 = 1 - 1/3 + 1/5 - 1/7 + \ldots$ Leibinitz (1646-1716)

To read on...
http://www-history.mcs.st-and.ac.uk/HistTopics/Pi_through_the_ages.html

Estimate of pi







Measurements and errors

- One can use random numbers for difficult multidimentional integration
- What we will get is an estimate of the integral
  - There will be error
  - How confident are we in the answer?
  - What can we say about the true value, given an estimate

Simulating the alcoholic (1d random walk)

- Bernoulli process: A Bernoulli trial is an experiment with two and only two possible outcomes. A random variable X has a Bernoulli (p) distribution if

  X = 1 with probability p 0<= p <=1

  = 0 with probability 1-p,

- Let the n-th step of alcoholic be Xn, Xn is Bernoulli(p=0.5) distributed
- Let dn =1 or -1 for step to right or left
- Dn = sum (di), i = 1 to n
- Dn = r -l (r = total number of steps to right/left)

  = 2r - n

Ref: Casella, Berger, Statistical Inference, 2nd ed.

Pascal's triangle

The Symmetric Random Walk

$n \setminus x$	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					$\frac{1}{2}$	0	$\frac{1}{2}$				
2				$\frac{1}{4}$	0	$\frac{2}{4}$	0	$\frac{1}{4}$			
3			$\frac{1}{8}$	0	$\frac{3}{8}$	0	$\frac{3}{8}$	0	$\frac{1}{8}$		
4		$\frac{1}{16}$	0	$\frac{4}{16}$	0	$\frac{6}{16}$	0	$\frac{4}{16}$	0	$\frac{1}{16}$	
5	$\frac{1}{32}$	0	$\frac{5}{32}$	0	$\frac{10}{32}$	0	$\frac{10}{32}$	0	$\frac{5}{32}$	0	$\frac{1}{32}$

Source: Random walk for dummies, Richard Monte

Bootstrapping and jackknife

- Estimate the variance of an estimator from the data itself
- Non parametric method
- Suppose you have n data entries
- Make another dataset by drawing n times from the data with replacement --> you have got another sample made from the date : the bootstrap sample
- Estimate the statistic again. Keep repeating k times
- This will give you k values of the statistic
- From this you can now calculate the variance of the statistic
- D-delete jackknife is a variation of this procedure.

Ref: Effron and Tibshirani

Try at home

- Generate binomial distribution on computer
- Check its poisson and normal limits
- Pseudo experiment: linear fit with computer generated data of resistance vs. temperature. Estimate slope and intercept by chi-square minimization.
- Find the distribution of the estimated slope and intercept

Monte Carlo method: basic theorem

Taken from: numerical recipes in C

Suppose that we pick N random points, uniformly distributed in a multidimensional volume V. Call them $x_1, \ldots, x_N$. Then the basic theorem of Monte Carlo integration estimates the integral of a function f over the multidimensional volume,

$$\int f \, dV \approx V \langle f \rangle \pm V \sqrt{\frac{\langle f^2 \rangle - \langle f \rangle^2}{N}} \tag{7.6.1}$$

Here the angle brackets denote taking the arithmetic mean over the N sample points,

$$\langle f \rangle \equiv \frac{1}{N} \sum_{i=1}^{N} f(x_i) \qquad \langle f^2 \rangle \equiv \frac{1}{N} \sum_{i=1}^{N} f^2(x_i) \tag{7.6.2}$$

- There is no guarantee that error is Gaussian distributed, so the estimated error is only approximate

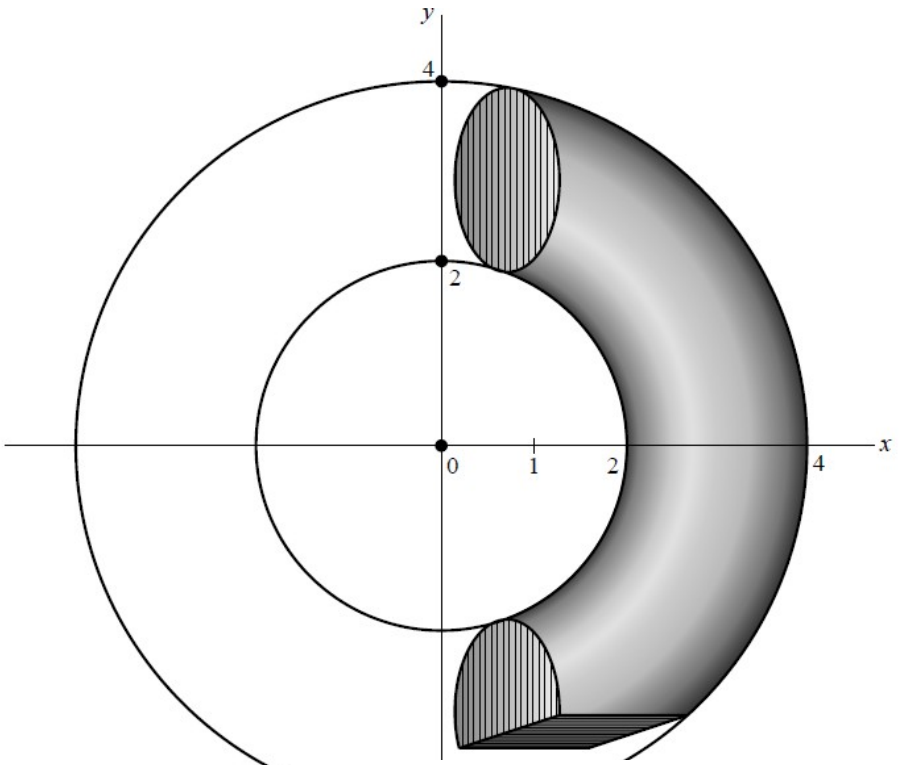
An example integration

- We want to evaluate mass and center of mass

$$\int \rho \, dx \, dy \, dz \qquad \int x\rho \, dx \, dy \, dz \qquad \int y\rho \, dx \, dy \, dz \qquad \int z\rho \, dx \, dy \, dz$$

- Limits can not be written easily, analytically
- MC integration is useful

$$z^2 + \left(\sqrt{x^2 + y^2} - 3\right)^2 \leq 1$$



$$x \geq 1 \qquad y \geq -3$$

```
#include "nrutil.h"
...
n=...                                   Set to the number of sample points desired.
den=...                                 Set to the constant value of the density.
sw=swx=swy=swz=0.0;                     Zero the various sums to be accumulated.
varw=varx=vary=varz=0.0;
vol=3.0*7.0*2.0;                        Volume of the sampled region.
for(j=1;j<=n;j++) {
    x=1.0+3.0*ran2(&idum);              Pick a point randomly in the sampled re-
    y=(-3.0)+7.0*ran2(&idum);               gion.
    z=(-1.0)+2.0*ran2(&idum);
    if (z*z+SQR(sqrt(x*x+y*y)-3.0) < 1.0) {     Is it in the torus?
        sw += den;                      If so, add to the various cumulants.
        swx += x*den;
        swy += y*den;
        swz += z*den;
        varw += SQR(den);
        varx += SQR(x*den);
        vary += SQR(y*den);
        varz += SQR(z*den);
    }
}
w=vol*sw/n;                             The values of the integrals (7.6.5),
x=vol*swx/n;
y=vol*swy/n;
z=vol*swz/n;
dw=vol*sqrt((varw/n-SQR(sw/n))/n);      and their corresponding error estimates.
dx=vol*sqrt((varx/n-SQR(swx/n))/n);
dy=vol*sqrt((vary/n-SQR(swy/n))/n);
dz=vol*sqrt((varz/n-SQR(swz/n))/n);
```

Nonuniform density torus

- What will you do if $\rho(x, y, z) = e^{5z}$
- Define den = exp (5.*z) and do weighted average?
- Very inefficient, points will be wasted in low density region
- Importance sampling:

$$ds = e^{5z} dz \qquad \text{so that} \qquad s = \frac{1}{5} e^{5z}, \quad z = \frac{1}{5} \ln(5s) \qquad (7.$$

Then $\rho dz = ds$, and the limits $-1 < z < 1$ become $.00135 < s < 29.682$.

```
#include "nrutil.h"
...
n=...                                   Set to the number of sample points desired.
sw=swx=swy=swz=0.0;
varw=varx=vary=varz=0.0;
ss=0.2*(exp(5.0)-exp(-5.0))             Interval of s to be random sampled.
vol=3.0*7.0*ss                          Volume in x,y,s-space.
for(j=1;j<=n;j++) {
    x=1.0+3.0*ran2(&idum);
    y=(-3.0)+7.0*ran2(&idum);
    s=0.00135+ss*ran2(&idum);           Pick a point in s.
    z=0.2*log(5.0*s);                   Equation (7.6.7).
    if (z*z+SQR(sqrt(x*x+y*y)-3.0) < 1.0) {
        sw += 1.0;                      Density is 1, since absorbed into definition
        swx += x;                           of s.
        swy += y;
        swz += z;
        varw += 1.0;
        varx += x*x;
        vary += y*y;
        varz += z*z;
    }
}
w=vol*sw/n;                             The values of the integrals (7.6.5),
x=vol*swx/n;
y=vol*swy/n;
z=vol*swz/n;
dw=vol*sqrt((varw/n-SQR(sw/n))/n);      and their corresponding error estimates.
dx=vol*sqrt((varx/n-SQR(swx/n))/n);
dy=vol*sqrt((vary/n-SQR(swy/n))/n);
dz=vol*sqrt((varz/n-SQR(swz/n))/n);
```

Importance Sampling

$$I \equiv \int f\,dV = \int \frac{f}{p}\,p dV \approx \left\langle \frac{f}{p} \right\rangle \pm \sqrt{\frac{\langle f^2/p^2 \rangle - \langle f/p \rangle^2}{N}}$$ with $$\int p\,dV = 1$$

What is the optimal choice of p? Make f/p as flat as possible

$$S \equiv \left\langle \frac{f^2}{p^2} \right\rangle - \left\langle \frac{f}{p} \right\rangle^2 \approx \int \frac{f^2}{p^2}\,p dV - \left[\int \frac{f}{p}\,p dV\right]^2 = \int \frac{f^2}{p}\,dV - \left[\int f\,dV\right]^2$$

Minimize variance subject to the constraint of probability conservation

$$0 = \frac{\delta}{\delta p}\left(\int \frac{f^2}{p}\,dV - \left[\int f\,dV\right]^2 + \lambda \int p\,dV\right)$$

Results in

$$p = \frac{|f|}{\sqrt{\lambda}} = \frac{|f|}{\int |f|\,dV}$$

Stratified sampling

- Subdivide in regions and throw points
- For two equal regions with same number of points

$$\langle f \rangle' \equiv \frac{1}{2}\left(\langle f \rangle_a + \langle f \rangle_b\right)$$

$$\begin{aligned}\mathrm{Var}\left(\langle f \rangle'\right) &= \frac{1}{4}\left[\mathrm{Var}\left(\langle f \rangle_a\right) + \mathrm{Var}\left(\langle f \rangle_b\right)\right] \\ &= \frac{1}{4}\left[\frac{\mathrm{Var}_a\left(f\right)}{N/2} + \frac{\mathrm{Var}_b\left(f\right)}{N/2}\right] \\ &= \frac{1}{2N}\left[\mathrm{Var}_a\left(f\right) + \mathrm{Var}_b\left(f\right)\right]\end{aligned}$$

$$\mathrm{Var}\left(f\right) = \frac{1}{2}\left[\mathrm{Var}_a\left(f\right) + \mathrm{Var}_b\left(f\right)\right] + \frac{1}{4}\left(\langle\langle f \rangle\rangle_a - \langle\langle f \rangle\rangle_b\right)^2$$

- For unequal number of points in two regions a and b

$$\mathrm{Var}\left(\langle f \rangle'\right) = \frac{1}{4}\left[\frac{\mathrm{Var}_a\left(f\right)}{N_a} + \frac{\mathrm{Var}_b\left(f\right)}{N - N_a}\right]$$

Stratified sampling (2)

$$\mathrm{Var}\left(\langle f\rangle'\right) = \frac{1}{4}\left[\frac{\mathrm{Var}_a\left(f\right)}{N_a} + \frac{\mathrm{Var}_b\left(f\right)}{N - N_a}\right]$$

which is minimized (one can easily verify) when

$$\frac{N_a}{N} = \frac{\sigma_a}{\sigma_a + \sigma_b}$$

- Similar for region b, which then gives,

$$\mathrm{Var}\left(\langle f\rangle'\right) = \frac{\left(\sigma_a + \sigma_b\right)^2}{4N}$$