NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer’s or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.
Generating Pseudorandom Numbers From Various Distributions Using C++

by Robert J. Yager
Weapons and Materials Research Directorate, ARL
Generating Pseudorandom Numbers From Various Distributions Using C++

This report documents a set of functions, written in C++, that can be used to generate pseudorandom numbers that have either uniform or normal distributions and pseudorandom integers that have either uniform or Poisson distributions. An implementation of the Mersenne twister algorithm, developed by Matsumoto and Nishimura, is included. The output from the Mersenne twister is used to generate the various distributions through the use of assorted transformation algorithms.
## Contents

Acknowledgments \hspace{1cm} v

1. Introduction \hspace{1cm} 1

2. Generating Pseudorandom Integers Using the Mersenne Twister 19937 Algorithm – The Rand() Function \hspace{1cm} 1
   2.1 Rand() Code \hspace{1cm} 2
   2.2 Rand() Template Classes \hspace{1cm} 2
   2.3 Rand() Parameters \hspace{1cm} 2
   2.4 Rand() Return Value \hspace{1cm} 2
   2.5 Rand() Example \hspace{1cm} 2
   2.6 Comparison of the Rand() Function to Other Mersenne Twister Implementations \hspace{1cm} 3

3. Initializing the Mersenne Twister – The Initialize() Function \hspace{1cm} 4
   3.1 Initialize() Code \hspace{1cm} 4
   3.2 Initialize() Template Classes \hspace{1cm} 4
   3.3 Initialize() Parameters \hspace{1cm} 5

4. Generating Uniformly Distributed Pseudorandom Numbers – The RandU() Function \hspace{1cm} 5
   4.1 RandU() Code \hspace{1cm} 5
   4.2 RandU() Template Classes \hspace{1cm} 6
   4.3 RandU() Parameters \hspace{1cm} 6
   4.4 RandU() Return Value \hspace{1cm} 6
   4.5 RandU() Simple Example \hspace{1cm} 6
   4.6 RandU() Binning Example \hspace{1cm} 6

5. Generating Normally Distributed Pseudorandom Numbers – The RandN() Function \hspace{1cm} 8
   5.1 RandN() Code \hspace{1cm} 8
   5.2 RandN() Template Classes \hspace{1cm} 8
   5.3 RandN() Parameters \hspace{1cm} 8
   5.4 RandN() Return Value \hspace{1cm} 9
Acknowledgments

I would like to thank Mr. Benjamin Flanders and Dr. Benjamin Breech of the U.S. Army Research Laboratory’s Weapons and Materials Research Directorate. Mr. Flanders and Dr. Breech provided technical and editorial recommendations that improved the quality of this report.
INTENTIONALLY LEFT BLANK.
1. Introduction

This report documents a set of functions, written in C++, that can be used to generate pseudorandom numbers that have either uniform or normal distributions and pseudorandom integers that have either uniform or Poisson distributions. An implementation of the Mersenne twister algorithm, developed by Matsumoto and Nishimura (1), is included. The output from the Mersenne twister is used to generate the various distributions through the use of assorted transformation algorithms.

The functions presented here are offered as compiler-independent alternatives to functions defined by the new C++11 standard (2). Although the new standard defines functions for generating pseudorandom numbers with uniform distributions, normal distributions, Poisson distributions, etc., it does not specify which algorithms will be used to generate those pseudorandom numbers. Thus, compilers that conform to the new standard will all generate pseudorandom numbers from the various distributions, but the actual numbers that are generated may differ from compiler to compiler.

The functions presented in this report have been grouped into the yRandom namespace, which is summarized at the end of this report.

2. Generating Pseudorandom Integers Using the Mersenne Twister 19937 Algorithm – The Rand() Function

The Rand() function uses the Mersenne twister 19937 algorithm to generate uniformly distributed pseudorandom integers in the interval \([0,2^{32})\). According to Matsumoto and Nishimura, the algorithm has a period of \(2^{19937}−1\) and passes the Diehard tests for statistical randomness.

The state of the Mersenne twister is stored in an array of 625 32-bit unsigned integers, which is passed as an argument to the Rand() function. The initial state of the Mersenne twister can be set using the Initialize() function (see section 3). The Initialize() function uses a user-supplied 32-bit integer to seed a simple pseudorandom number generator that generates the initial state integers. This effectively allows for the creation of multiple pseudorandom number generators (as many as \(2^{32}\)) that can each produce independent, reproducible sequences of pseudorandom integers.
The code contained in the Rand() function differs from the code that is presented by Matsumoto and Nishimura. To avoid using the modulo operator, their code calculates all of the algorithm’s 624 unsigned state integers once out of every 624 function calls. In contrast, the Rand() function uses the ternary operator to avoid using the modulo operator.

2.1 Rand() Code

```cpp
template<class T>T Rand(){//==============================================MERSENNE TWISTER (19937) PRNG
    T I[625]));//<-STATE OF MERSENNE TWISTER (FOR T, USE A 32-BIT UNSIGNED INT)
    T i=I[624],j=i<623?i+1:0,y=I[i]&0x80000000|I[j]&0x7fffffff;
    y=I[i]=I[i<227?i+397:i-227]^y>>1^(y&1)*0x9908b0df,I[624]=j;
    return y^(y^=(y^=(y^=y>>11)<<7&0x9d2c5680)<<15&0xefc60000)>>18;
}}//~~~~~YAGENAUT@GMAIL.COM~~~~~~~~~~~~~~~~~~~~~~~~~LAST~UPDATED~21JAN2014~~~~~~
```

2.2 Rand() Template Classes

T T should be a 32-bit unsigned integer type. Greater than 32-bit unsigned integer types can be used, but performance may suffer.

2.3 Rand() Parameters

I I points to a 625-element array that contains the state of the Mersenne twister algorithm. Each time the Rand() function is called, the array pointed to by I is modified. The initial state of the array should be set using the Initialize() function (see section 3).

2.4 Rand() Return Value

The Rand() function returns uniformly distributed pseudorandom integers in the interval [0,2^{32}).

2.5 Rand() Example

The following example uses the Rand() function to generate one billion pseudorandom integers. The Initialize() function, introduced in section 3, is used to set the initial state of the Mersenne twister.

```cpp
#include <cstdio>
#include <ctime>
#include "y_random.h"

int main(){//<================================EXAMPLE FOR THE yRandom::Rand() FUNCTION
    unsigned I[625]);//<-yRandom::Initialize(I,1);//....state of Mersenne twister
    for(int i=1;i<1000000000;++i)yRandom::Rand(I);
    printf("10^9 pseudorandom numbers generated in %.3f seconds.\nThe 10^9th number is %u.\n",double(clock())/CLOCKS_PER_SEC,yRandom::Rand(I));
}}//~~~~~YAGENAUT@GMAIL.COM~~~~~~~~~~~~~~~~~~~~~~~~~LAST~UPDATED~21JAN2014~~~~~~
```
2.6 Comparison of the Rand() Function to Other Mersenne Twister Implementations

The following example compares the Rand() function to Matsumoto and Nishimura’s genrand() function, as well as to the C++11 built-in Mersenne twister implementation. The example code demonstrates that the three implementations produce identical output (at least for the first $10^9$ values and with a seed value of 1). Note that time values will vary based on computer specifications, compiler, compiler settings, etc.

```cpp
#include <cstdio>
#include <ctime>
#include <random>
#include "matsumoto_nishimura.h"
#include "y_random.h"

int main(){
    double t=0; // elapsed time
    init_genrand(1); // initialize the Matsumoto-Nishimura implementation
    for(int i=1; i<1000000000;++i)genrand();
    printf("Using Matsumoto and Nishimura's genrand():\n");
    printf("  10^9 pseudorandom integers generated in %.3f seconds.\n  The 10^9th number is %u.\n\n", (clock()-t)/CLOCKS_PER_SEC, genrand()), t=clock();
    std::mt19937 g(1); // initialize the C++11 built-in implementation
    for(int i=1; i<1000000000;++i)g();
    printf("Using std::mt19937:\n");
    printf("  10^9 pseudorandom integers generated in %.3f seconds.\n  The 10^9th number is %u.\n\n", (clock()-t)/CLOCKS_PER_SEC, g());
    yRandom::Initialize(I,1); // init. yRandom implementation
    for(int i=1; i<1000000000;++i)yRandom::Rand(I);
    printf("Using yRandom::Rand():\n");
    printf("  10^9 pseudorandom integers generated in %.3f seconds.\n  The 10^9th number is %u.\n\n", (clock()-t)/CLOCKS_PER_SEC, yRandom::Rand(I));
    bool check=true;
    for(int i=0; i<1000000000;++i){
        unsigned x=yRandom::Rand(I);
        if(x!=genrand()||x!=g())check=false;
    }
    printf("\nAre the first 10^9 pseudorandom integers generated by\n  Matsumoto and Nishimura's genrand(), std::mt19937,\n  and yRandom::Rand() identical? %s\n",check?"YES":"NO");
}
```

10^9 pseudorandom numbers generated in 1.778 seconds.
The 10^9th number is 2716480233.
OUTPUT:

Using Matsumoto and Nishimura's genrand():
10^9 pseudorandom integers generated in 3.400 seconds.
The 10^9th number is 2716480233.

Using std::mt19937:
10^9 pseudorandom integers generated in 2.231 seconds.
The 10^9th number is 2716480233.

Using yRandom::Rand():
10^9 pseudorandom integers generated in 1.857 seconds.
The 10^9th number is 2716480233.

Are the first 10^9 pseudorandom integers generated by
Matsumoto and Nishimura's genrand(), std::mt19937,
and yRandom::Rand() identical?  YES

3. Initializing the Mersenne Twister – The Initialize() Function

The Initialize() function uses an algorithm presented by Nishimura and Matsumoto (3) to
initialize the 625-element array that is used to store the state of the Mersenne twister algorithm.

3.1 Initialize() Code

```cpp
//<======INITIALIZE STATE OF MERSENNE TWISTER
T I[625],//<--STATE OF MERSENNE TWISTER (FOR T, USE A 32-BIT UNSIGNED INT)
unsigned long s){//<-----------------------------------------SEED [0,2^32)
I[0]=s&0xffffffff,I[624]=0;
for(int i=1;i<624;++i)I[i]=(1812433253*(I[i-1]^I[i-1]>>30)+i)&0xffffffff;
}//@YAGENAUT@GMAIL.COM~~~~~~~~~~~~~~~~~~LAST~UPDATED~21JAN2014~~~~~~
```

3.2 Initialize() Template Classes

T should be a 32-bit unsigned integer type. Greater than 32-bit types can be used,
but performance may suffer.

4
3.3 Initialize() Parameters

I points to storage for a 625-element array that is used to store the state of the Mersenne twister algorithm.

s specifies the seed for the algorithm that is used to generate the initial state of the Mersenne twister algorithm. s can be any value in the interval \([0,2^{32})\).

4. Generating Uniformly Distributed Pseudorandom Numbers – The RandU() Function

The RandU() function can be used to generate uniformly distributed pseudorandom numbers that conform to the probability density function given by equation 1.

\[
f(x) = \begin{cases} 
  1, & \text{for } a < x \leq b \\
  b - a, & \text{for } a \leq x < b \\
  0, & \text{otherwise}
\end{cases}
\]  

(1)

Note that the C++ standards document defines a slightly different probability density function for uniformly distributed pseudorandom numbers \((a \leq x < b)\) rather than \(a < x \leq b\). The decision to exclude the lower bound from the distribution rather than the upper bound was based on the belief that it would be more likely to help the user to avoid a divide-by-zero error.

The RandU() function uses the transformation presented in equation 2, where \(r\) is a uniformly distributed pseudorandom number in the interval \((0,1]\).

\[
x = a + (b - a)r
\]

(2)

Equation 3 can be used to generate \(r\) given \(q\), a uniformly distributed pseudorandom integer in the interval \([0,2^{32})\).

\[
r = \frac{q + 1}{2^{32}}
\]

(3)

4.1 RandU() Code

```cpp
template<class T> double RandU() //======UNIFORMLY DISTRIBUTED PSEUDORANDOM DOUBLE T I[625], //--STATE OF MERSENNE TWISTER (FOR T, USE A 32-BIT UNSIGNED INT) double a, double b) { //----------LOWER & UPPER BOUNDARIES OF DISTRIBUTION return a+(b-a)*(Rand(I)+1.)/4294967296; //..............for a=0 and b=1, (0,1] } //~~~YAGENAUT@GMAIL.COM~~~~~~~~~~~~~~~~~~~~~~~~~LAST~UPDATED~21JAN2014~~~~~~
```
4.2 RandU() Template Classes

T T should be a 32-bit unsigned integer type. Greater than 32-bit types can be used, but performance may suffer.

4.3 RandU() Parameters

I I points to an array that contains the state of the Mersenne twister algorithm.

a a specifies a, the lower bound for the distribution.

b b specifies b, the upper bound for the distribution.

4.4 RandU() Return Value

The RandU() function returns uniformly distributed pseudorandom numbers in the interval (a,b]. Note that, due to limitations inherent in the storage of double precision numbers, the return value is not guaranteed to be distinct from a in all cases (such as when |a| >> |a-b|).

4.5 RandU() Simple Example

The following example uses the RandU() function to generate and sum one billion uniformly distributed pseudorandom numbers in the interval (2,6].

```cpp
#include <cstdio>
#include <ctime>
#include "y_random.h"

int main(){
    unsigned I[625];
    for(int i=0;i<1000000000;++i)s+=yRandom::RandU(I,2,6);
    printf("10^9 pseudorandom numbers generated and summed in %.3f seconds.\n",s/1000000000);
    return 0;
}
```

OUTPUT:

```
10^9 pseudorandom numbers generated and summed in 8.255 seconds.
Their average is 3.999977.
```

4.6 RandU() Binning Example

The following example uses the RandU() function to generate and bin one billion uniformly distributed pseudorandom numbers in the interval (2,6].
#include <cstdio>
#include "y_random.h"

int main(){
    //=================BINNING EXAMPLE FOR THE yRandom::RandU() FUNCTION
    unsigned I[625];
    yRandom::Initialize(I,1);
    // state of Mersenne twister
    int M=1000000000;
    const int N=11;
    double B[N];
    double E[N+1]={(N-1)/double(M)};
    double C[N+1];
    for(int i=0;i<N+1;++i)C[i]=0;
    for(int i=0;i<N;++i,++C[i],j=0)
        for(double x=yRandom::RandU(I,2,6);x>B[j]&&j<N;++j)
            printf(" COUNT  COUNT
            BIN   ,    (RAW)    ,   (EXPECTED)  ,   %DIFF 
            -------------------
            <= %4.1f     ,",B[0]);
    for(int i=0;i<N+1;++i){
        if(i==0)printf(" <= %4.1f     ,",B[0]);
        else if(i==N)printf(" > %4.1f     ,",B[N-1]);
        else printf(" %4.1f to %4.1f]  ,",B[i-1],B[i]);
        printf("%11d  ,%13.1f
        E[i]>1?printf("  ,%9.4f%%
        printf(" \n");
    }
    return 0;
}

#include <math.h>

OUTPUT:

<table>
<thead>
<tr>
<th>BIN</th>
<th>COUNT (RAW)</th>
<th>COUNT (EXPECTED)</th>
<th>%DIFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 2.0</td>
<td>0</td>
<td>0.0</td>
<td></td>
</tr>
<tr>
<td>( 2.0 to 2.4]</td>
<td>99999019</td>
<td>10000000.0</td>
<td>0.010%</td>
</tr>
<tr>
<td>( 2.4 to 2.8]</td>
<td>100010759</td>
<td>10000000.0</td>
<td>0.010%</td>
</tr>
<tr>
<td>( 2.8 to 3.2]</td>
<td>99997646</td>
<td>10000000.0</td>
<td>0.024%</td>
</tr>
<tr>
<td>( 3.2 to 3.6]</td>
<td>100006913</td>
<td>10000000.0</td>
<td>0.006%</td>
</tr>
<tr>
<td>( 3.6 to 4.0]</td>
<td>100010417</td>
<td>10000000.0</td>
<td>0.010%</td>
</tr>
<tr>
<td>( 4.0 to 4.4]</td>
<td>99979386</td>
<td>10000000.0</td>
<td>0.020%</td>
</tr>
<tr>
<td>( 4.4 to 4.8]</td>
<td>9993880</td>
<td>10000000.0</td>
<td>0.016%</td>
</tr>
<tr>
<td>( 4.8 to 5.2]</td>
<td>9999852</td>
<td>10000000.0</td>
<td>0.003%</td>
</tr>
<tr>
<td>( 5.2 to 5.6]</td>
<td>10004658</td>
<td>10000000.0</td>
<td>0.004%</td>
</tr>
<tr>
<td>( 5.6 to 6.0]</td>
<td>9997670</td>
<td>10000000.0</td>
<td>0.002%</td>
</tr>
<tr>
<td>&gt; 6.0</td>
<td>0</td>
<td>0.0</td>
<td></td>
</tr>
</tbody>
</table>
5. GeneratingNormally Distributed Pseudorandom Numbers – The RandN() Function

The RandN() function can be used to generate normally distributed pseudorandom numbers that conform to the probability density function given by equation 4, where $\mu$ is the mean of the distribution and $\sigma$ is the standard deviation.

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$  \hspace{1cm} (4)

The RandN() function uses the Box-Muller transform (4) to generate normally distributed pseudorandom numbers:

$$x = \mu + \sigma\sqrt{-2\ln(r_a)} \cos(2\pi r_b)$$  \hspace{1cm} (5)

where $r_a$ and $r_b$ are uniformly distributed pseudorandom numbers in the interval (0,1]. Equation 3 can be used to generate $r_a$ and $r_b$ given $q_a$ and $q_b$, two uniformly distributed pseudorandom integers in the interval [0,2$^{32}$).

5.1 RandN() Code

```cpp
#include <cmath>

template<class T> double RandN(T I[625], double m, double s) {
    return m + s * std::sqrt(-2 * std::log((Rand(I)+1.)/4294967296)) * std::cos(1.4629180792671596E-9*(Rand(I)+1.));
}
```

5.2 RandN() Template Classes

- **T** should be a 32-bit unsigned integer type. Greater than 32-bit types can be used, but performance may suffer.

5.3 RandN() Parameters

- **I** points to an array that contains the state of the Mersenne twister algorithm.
- **m** specifies $\mu$, the mean of the distribution.
- **s** specifies $\sigma$, the standard deviation of the distribution.
5.4 RandN() Return Value

The RandN() function returns normally distributed pseudorandom numbers.

5.5 RandN() Simple Example

The following example uses the RandN() function to generate and sum one billion normally distributed pseudorandom numbers with $\mu = 4$ and $\sigma = 0.5$.

```c
#include <cstdio>
#include <ctime>
#include "y_random.h"

int main(){
    unsigned I[625];
    yRandom::Initialize(I,1);
    double s=0;
    for(int i=0;i<1000000000;++i)s+=yRandom::RandN(I,4,.5);
    printf("10^9 pseudorandom numbers generated and summed in %.3f seconds.\n",
           double(clock())/CLOCKS_PER_SEC,s/1000000000);
}
```

OUTPUT:

10^9 pseudorandom numbers generated and summed in 46.213 seconds.
Their average is 3.999998.

5.6 RandN() Binning Example

The following example uses the RandN() function to generate and bin one billion normally distributed pseudorandom numbers with $\mu = 4$ and $\sigma = 0.5$. The Erf() function is an implementation of an algorithm presented by Abramowitz and Stegun (5).
#include <stdio.h>
#include "y_random.h"

inline double Erf(double x)
{  
    double t=1/(1+.3275911*fabs(x));
    double a[]={.254829592,-.284496736,1.421413741,-1.453152027,1.061405429};
    double s=0;  
    for(int i=0;i<5;++i)s+=a[i]*pow(t,i+1); 
    return (x<0?1:1-s*exp(-x*x));
}

int main()
{  
    unsigned I[625];
    yRandom::Initialize(I,1);
    int M=100000000;
    const int N=11;
    double B[N];
    for(int i=0;i<N;++i)B[i]=4*double(i)/(N-1)+2;
    double E[N+1]={0};
    for(int i=0;i<N+1;++i)C[i]=0;
    for(int i=0;i<M;++i,++C[j],j=0)
    {
        for(double x=yRandom::RandN(I,4,.5);x>B[j]&&j<N;++j);
    }
    printf("BIN , (RAW) , (EXPECTED) , %DIFF \n ");
    printf("\n");
    for(int i=0;i<N+1;++i){
        if(i==0)printf("<= %4.1f \n",B[0]);
        else if(i==N)printf("> %4.1f \n",B[N-1]);
        else printf("%4.1f to %4.1f\n",B[i-1],B[i]);
    }
}

OUTPUT:

<table>
<thead>
<tr>
<th>BIN</th>
<th>COUNT (RAW)</th>
<th>COUNT (EXPECTED)</th>
<th>%DIFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 2.0</td>
<td>31839</td>
<td>31686.0</td>
<td>0.4827%</td>
</tr>
<tr>
<td>(2.0 to 2.4)</td>
<td>655830</td>
<td>655516.1</td>
<td>0.0479%</td>
</tr>
<tr>
<td>(2.4 to 2.8)</td>
<td>7507620</td>
<td>7510327.1</td>
<td>0.0360%</td>
</tr>
<tr>
<td>(2.8 to 3.2)</td>
<td>46597020</td>
<td>46601762.1</td>
<td>0.0102%</td>
</tr>
<tr>
<td>(3.2 to 3.6)</td>
<td>157066122</td>
<td>157056047.3</td>
<td>0.0064%</td>
</tr>
<tr>
<td>(3.6 to 4.0)</td>
<td>288150018</td>
<td>288144661.9</td>
<td>0.0019%</td>
</tr>
<tr>
<td>(4.0 to 4.4)</td>
<td>288145262</td>
<td>288144660.9</td>
<td>0.0002%</td>
</tr>
<tr>
<td>(4.4 to 4.8)</td>
<td>157043835</td>
<td>157056047.3</td>
<td>0.0078%</td>
</tr>
<tr>
<td>(4.8 to 5.2)</td>
<td>46607503</td>
<td>46601762.1</td>
<td>0.0123%</td>
</tr>
<tr>
<td>(5.2 to 5.6)</td>
<td>7508108</td>
<td>7510327.1</td>
<td>0.0295%</td>
</tr>
<tr>
<td>(5.6 to 6.0)</td>
<td>655295</td>
<td>655516.1</td>
<td>0.0337%</td>
</tr>
<tr>
<td>&gt; 6.0</td>
<td>31558</td>
<td>31686.0</td>
<td>0.4041%</td>
</tr>
</tbody>
</table>
6. Generating Uniformly Distributed Pseudorandom Integers – The RandI() Function

The RandI() function can be used to generate uniformly distributed pseudorandom integers that conform to the probability density function given by equation 6.

\[ f(k) = \begin{cases} \frac{1}{b-a+1}, & \text{for } a \leq k \leq b \\ 0, & \text{otherwise} \end{cases} \]  

(6)

The RandI() function uses the transformation presented in equation 7, where \( q \) is a uniformly distributed pseudorandom integer in the interval \([0,2^{32})\).

\[ k = a + \text{trunc} \left( \frac{q}{2^{32}} (b - a + 1) \right) \]  

(7)

6.1 RandI() Code

```cpp
#include <iostream>
#include <stdlib.h>

typedef long int T;

T RandI(T I[625], long a, long b)
{
    return a + T(Rand(I)/4294967296.*(b-a+1));
}
```

6.2 RandI() Template Classes

- **T** should be a 32-bit unsigned integer type. Greater than 32-bit types can be used, but performance may suffer.

6.3 RandI() Parameters

- **I** points to an array that contains the state of the Mersenne twister algorithm.
- **a** specifies \( a \), the lower bound for the distribution.
- **b** specifies \( b \), the upper bound for the distribution.

6.4 RandI() Return Value

The RandI() function returns a uniformly distributed pseudorandom integer in the interval \([a,b]\).

6.5 RandI() Simple Example

The following example uses the RandI() function to generate and sum one billion uniformly distributed pseudorandom integers in the interval \([-5,4]\).
#include <cstdio>
#include <ctime>
#include "y_random.h"

int main(){
    #<==================SIMPLE EXAMPLE FOR THE yRandom::RandI() FUNCTION
    unsigned I[625];/*<-*/yRandom::Initialize(I,1);/..state of Mersenne twister
double s=0;/*/for(int i=0;i<1000000000;++i)s+=yRandom::RandI(I,-5,4);
    printf("10^9 pseudorandom numbers generated and summed in %.3f seconds.\n"                
        "Their average is %f.\n\n",double(clock())/CLOCKS_PER_SEC,s/1000000000);
};//~~~~~~YAGENAUT@GMAIL.COM~~~~~~~~~~~~~~~~~~~~~~~~~LAST~UPDATED~21JAN2014~~~~~~

OUTPUT:

10^9 pseudorandom numbers generated and summed in 10.140 seconds.
Their average is -0.500057.

6.6 RandI() Binning Example

The following example uses the RandI() function to generate and bin one billion uniformly distributed pseudorandom integers in the interval [-5,4].

```cpp
#include <cstdio>
#include "y_random.h"

int main(){
    #<=================BINNING EXAMPLE FOR THE yRandom::RandI() FUNCTION
    int M=1000000000; /**<number of random numbers to generate
    const int N=11; /**<number of bins (not counting overflow bin)
    double B[N]; /**<for(int i=0;i<N;++i)B[i]=i-6; /**<bins
    double E[N+1]={0}; /**<for(int i=1;i<N;++i)E[i]=M/(N-1.); /**<expected counts
    int C[N+1]; /**<for(int i=0;i<N+1;++i)C[i]=0; /**<raw counts
    for(int i=0,j=0;i<M;++i,++C[j],j=0)
        for(double x=yRandom::RandI(I,-5,4);x>B[j]&&j<N;++j)
            printf("                                 COUNT
      BIN       ,    (RAW)    ,   (EXPECTED)  ,   %%DIFF
      -----------------------------------------
      %11d  ,%13.1f
          %9.4f%%\n        
    for(int i=0;i<N+1;++i){
        if(i==0)printf(" <= %4.1f  ,",B[0]);
        else if(i==N)printf(" > %4.1f   ,",B[N-1]);
        else printf(" (%4.1f to %4.1f]  ,",B[i-1],B[i]);
        printf("%11d ,%13.1f",C[i],E[i]);
        E[i]>0.1?printf(" ,%9.4f%%\n",fabs(E[i]-C[i])/E[i]*100):printf("\n");
};//~~~~~~YAGENAUT@GMAIL.COM~~~~~~~~~~~~~~~~~~~~~~~~~LAST~UPDATED~21JAN2014~~~~~~
```
7. Generating Poisson-Distributed Pseudorandom Integers – The RandP() Function

The RandP() function can be used to generate Poisson distributed pseudorandom integers that conform to the probability density function given by equation 8, where $\mu$ is the mean of the distribution.

$$f(k) = \frac{\mu^k e^{-\mu}}{k!} \tag{8}$$

The RandP() function uses a transformation described by Knuth (6) to generate Poisson-distributed pseudorandom integers by finding the largest $k$ that satisfies equation 9.

$$\prod_{i=0}^{k} r_i > e^{-\mu} \tag{9}$$

where $r_i$ is a uniformly distributed pseudorandom number in the interval (0,1]. Equation 3 can be used to generate each $r_i$ given $q_i$, a uniformly distributed pseudorandom integer in the interval [0,2^{32}).

Note that the for large $\mu$, the RandP() function is slow. This problem can be overcome by making use of the fact that, for large $\mu$, Poisson distributions are approximately normal.
7.1 RandP() Code

```cpp
#include <cstdlib>
#include <ctime>
#include "y_random.h"

int main(){
    //SIMPLE EXAMPLE FOR THE yRandom::RandP() FUNCTION
    unsigned I[625];
    yRandom::Initialize(I,1);
    double s=0;
    for(int i=0;i<100000000;++i)s+=yRandom::RandP(I,1);
    printf("10^9 pseudorandom numbers generated and summed in %.3f seconds.\n" "Their average is %f.\n",double(clock())/CLOCKS_PER_SEC,s/100000000);
}
```

7.2 RandP() Template Classes

T should be a 32-bit unsigned integer type. Greater than 32-bit types can be used, but performance may suffer.

7.3 RandP() Parameters

- I points to an array that contains the state of the Mersenne twister algorithm.
- m specifies \( \mu \), the mean of a Poisson distribution.

7.4 RandP() Return Value

The RandP() function returns a Poisson-distributed pseudorandom unsigned integer.

7.5 RandP() Simple Example

The following example uses the RandP() function to generate and sum one billion Poisson-distributed pseudorandom integers with \( \mu = 1 \).

```cpp
#include <cstdlib>
#include <ctime>
#include "y_random.h"

int main(){
    //SIMPLE EXAMPLE FOR THE yRandom::RandP() FUNCTION
    unsigned I[625];
    yRandom::Initialize(I,1);
    double s=0;
    for(int i=0;i<100000000;++i)s+=yRandom::RandP(I,1);
    printf("10^9 pseudorandom numbers generated and summed in %.3f seconds.\n" "Their average is %f.\n",double(clock())/CLOCKS_PER_SEC,s/100000000);
}
```

OUTPUT:

10^9 pseudorandom numbers generated and summed in 35.708 seconds.
Their average is 1.000013.
7.6 RandP() Binning Example

The following example uses the RandP() function to generate and bin one billion Poisson distributed pseudorandom integers with $\mu = 1$.

```
#include <cstdio>  
#include "y_random.h"  

int main(){  
  //.....................................................printf()  
  //..................................................yRandom
  unsigned I[625];  
  //...........................................expected counts  
  #include <y_random.h>  
  #include <cstdio>  
  #define MARK "\n"  
  #define COUNT '"'

  int M=1000000000;  
  //...........................................expected counts  
  int N=11;  
  //...........................................expected counts  
  double B[N];  
  //...........................................expected counts  
  double E[N+1]={0};  
  //...........................................expected counts  
  double F=1;  
  //...........................................expected counts  
  for(int i=0;i<N;++i)B[i]=i;  
  //...........................................expected counts

  for(int i=0;i<N+1;++i){  
    printf("COUNT
    BIN , (RAW) , (EXPECTED) , %DIFF \n " );  
    printf(" COUNT\n " );

    if(i==0)printf(" <= %4.1f ,",B[0]);
    else if(i==N)printf(" > %4.1f ,",B[N-1]);
    else printf(" (%4.1f to %4.1f] ,",B[i-1],B[i]);

    double E=B[N-1]-B[0];

    printf("%11d ,%13.1f" ,E,C[i]);
    printf(" ,%9.4f%%\n",fabs(C[i]-E[i])/E[i]*100);printf("\n");
}
```

OUTPUT:

```
<table>
<thead>
<tr>
<th>BIN</th>
<th>COUNT (RAW)</th>
<th>COUNT (EXPECTED)</th>
<th>%DIFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 0.0</td>
<td>367886090</td>
<td>367879441.2</td>
<td>0.0018%</td>
</tr>
<tr>
<td>( 0.0 to 1.0]</td>
<td>367871283</td>
<td>367879441.2</td>
<td>0.0022%</td>
</tr>
<tr>
<td>( 1.0 to 2.0]</td>
<td>183939720.6</td>
<td>183939720.6</td>
<td>0.0066%</td>
</tr>
<tr>
<td>( 2.0 to 3.0]</td>
<td>61312840.2</td>
<td>61312840.2</td>
<td>0.0140%</td>
</tr>
<tr>
<td>( 3.0 to 4.0]</td>
<td>15328310.0</td>
<td>15328310.0</td>
<td>0.0250%</td>
</tr>
<tr>
<td>( 4.0 to 5.0]</td>
<td>3065662.0</td>
<td>3065662.0</td>
<td>0.0674%</td>
</tr>
<tr>
<td>( 5.0 to 6.0]</td>
<td>510943.7</td>
<td>510943.7</td>
<td>0.1397%</td>
</tr>
<tr>
<td>( 6.0 to 7.0]</td>
<td>72992.0</td>
<td>72992.0</td>
<td>0.1577%</td>
</tr>
<tr>
<td>( 7.0 to 8.0]</td>
<td>9124.0</td>
<td>9124.0</td>
<td>0.7781%</td>
</tr>
<tr>
<td>( 8.0 to 9.0]</td>
<td>1013.8</td>
<td>1013.8</td>
<td>1.4576%</td>
</tr>
<tr>
<td>( 9.0 to 10.0]</td>
<td>101.4</td>
<td>101.4</td>
<td>10.4779%</td>
</tr>
<tr>
<td>&gt; 10.0</td>
<td>9.2</td>
<td>9.2</td>
<td>30.2061%</td>
</tr>
</tbody>
</table>
```
8. **Code Summary**

A summary sheet is provided at the end of this report. It presents the yRandom namespace, which contains the six functions that are described in this report.
**yRandom Summary**

**RandU() Probability Density Function and Simple Example**

\[ f(x) = \frac{1}{b-a} \]

for \( a \leq x \leq b \)

0, otherwise

**RandU() Example**

```
#include <cstdio>

int main(){
  double a=0, b=1;
  double P=1, E=exp(-2*log((RandU()+1.)/4294967296));
  double M=1000000000;
  for(int i=0;i<N;++i)E[i]=(.5*(1+Erf((B[i]-M)/sqrt(2*M))));
  printf("\n Their average is \%.0f,\n double(clock())/CLOCKS_PER_SEC\n", E[N]);
  return E[N];
}
```

**Output:**

10^9 pseudorandom numbers generated and summed in 8.255 seconds. Their average is 1.000013.

**RandI() Probability Density Function and Simple Example**

\[ f(k) = \frac{1}{\Gamma(k) \sigma^k} e^{-\frac{(k-\mu)^2}{2\sigma^2}} \]

for \( \mu \leq k < \mu + \sigma \sqrt{2 \ln 2} \)

0, otherwise

**RandI() Example**

```
#include <cstdio>

int main(){
  double a=0, b=1;
  double P=1, E=exp(-2*log((RandI()+1.)/4294967296));
  double M=1000000000;
  for(int i=0;i<N;++i)E[i]=(.5*(1+Erf((B[i]-M)/sqrt(2*M))));
  printf("\n Their average is \%.0f,\n double(clock())/CLOCKS_PER_SEC\n", E[N]);
  return E[N];
}
```

**Output:**

10^9 pseudorandom numbers generated and summed in 64.213 seconds. Their average is 1.000013.

---

For more examples and detailed explanations, refer to the documentation and source code provided in the original text.
9. References


<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Title</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFENSE TECHNICAL INFORMATION CTR</td>
<td>DIRECTOR</td>
<td>US ARMY RESEARCH LAB</td>
</tr>
<tr>
<td></td>
<td>(PDF)</td>
<td>(PDF)</td>
<td>RDRL CIO LL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IMAL HRA MAIL &amp; RECORDS MGMT</td>
</tr>
<tr>
<td>1</td>
<td>GOVT PRINTG OFC</td>
<td>A MALHOTRA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(PDF)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>RDRL WML. A</td>
<td>R YAGER</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(PDF)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>