Tina's Random Number Generators Reference Manual

Generated by Doxygen 1.2.15

Mon Apr 21 16:27:50 2003

Contents

1 Tina's Random Number Generators' User Manual

Tina's Random Number Generators (TRNG) is a C^{++} parallel pseudo random number generators package.

1.0.1 Introduction

A lot of tasks in scientific computing can only be tackled by the power of parallel computers. Especially Monte Carlo simmulations are often well suited for parallel computers because of the inherent parallelism of these problems.

A straight forward way to generate pseudo random numbers in a parallel environment is to use the same serial pseudo random number generator on every processor but with (randomly chosen) different seeds or the same generator type but with different parameter sets. These methods are quiet arbitrary and it is not possible to enshure in every case that there are no correlations between the pseudo random number sequences.

To create a good pseudo random number generator for parallel applications we take an excellent sequential pseudo random number generator and distribute its numbers in a *well defined* way over the parallel jobs. There are two different approaches in distributing the numbers.

- **Sequence splitting** The sequential generator's series is split into different contiguous subsequences, which are distributed over the processors. The pseudo random number series r_i of a sequential generator is split into p non overlapping contiguous subsequences with k elements in each subsequence.

  $$\begin{aligned} s_{0,i} &= r_i \\ s_{1,i} &= r_{i+k} \\ &\dots \\ s_{p-1,i} &= r_{i+(p-1)k} \end{aligned} \qquad i = 0, 1, \dots, k-1$$

  For a performand implementation it is necessary that r_{i+k} can be easy calculated from r_i even for large k.

- **Leapfrog method** With the leapfrog method the sequential generator's numbers r_i are alternated distributed over the different processors. For p processors we get the new sequences

$$
\begin{aligned}
t_{0,i} &= r_{pi} \\
t_{1,i} &= r_{pi+1} \\
&\dots \\
t_{p-1,i} &= r_{pi+(p-1)} \,.
\end{aligned}
$$

Figures 1 and 2 illustrate these different methods.

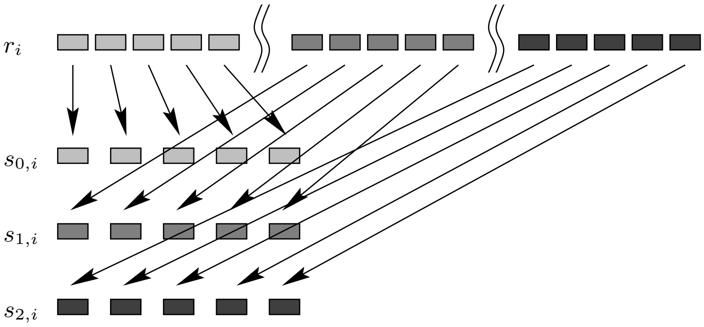


Figure 1: A sequential pseudo random number generator's parallelisation using sequence splitting.

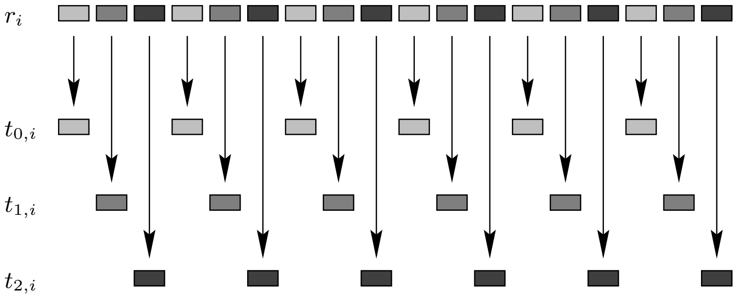


Figure 2: A sequential pseudo random number generator's parallelisation using leapfrog method.

A way to implement the leapfrog method could be to dedicate one processor to random number generation and spread these numbers via a network to the other processors. But this wold be a very inefficient way.

TRNG (Tina's Random Number Generators) is a library that gives you a powerfull tool for Monte Carlo simmulations on parallel computers. TRNG is a collection of random number generators specially designed for the needs of parallel Monte Carlo simmulations. With TRNG you can generate parallel streams of pseudo random numbers (with leapfrog or sequence splitting method) *without* any communication. Tina's Random Number Generators have a highly tuned implementation, have a long period and are empirically tested. Tina's Random Number Generators are easy to use and can be extendend by the user. It is a tool for your everyday work.

1.0.2 Software Distribution and Instalation

Tina's Random Number Generators are copyrighted by Heiko Bauke. You can contact the author of TRNG via electronic mail to `heiko.bauke@physik.uni-magdeburg.de` and get the software from `http://tina.nat.uni-magdeburg.de/TRNG`.

TRNG is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation. This program is distributed *without any* *warranty*; without even the implied warranty of *merchantability* or *fitness for a particular purpose*. See the GNU General Public License for more details.

Download the latest tar file from `http://tina.nat.uni-magdeburg.de/TRNG` and unpack and untar the file. Change into the directory `trng` and type `make`. After you have become root type `make install`. That's all!

If you don't have the GNU compiler but the SUN-Workshop compiler use the makefile `Makefile.SW` and type `make -f Makefile.SW` and `make -f Makefile.SW install`.

If you have installed TRNG successfully you can compile programs that use Tina's Random Number Generators, just include the header file `trng.h` and use the linker flag `-ltrng`.

TRNG comes with some example- and test-programs. You may compile these programs with `make examples` (or `make -f Makefile.SW examples`). The binaries are located in the directory `bin`. To compile the MPI-examples you need a MPI-Implementation with C^{++}-support like LAM (`http://www.lam-mpi.org`). Start these programs without commandline arguments to get a short description. The reader should investigate the following programs.

- `plausibility` This program does some tests for leapfrog and sequence splitting.
- `diehard_file` With this program you can generate files for applying the diehard test [9].
- `pi` This MPI program shows how to use TRNG. It computes π by a Monte Carlo method.
- `pi_advanced` This is a version of the program pi where the result is independent of the number processors.
- `exception` This is an example for exception handling in TRNG.
- `template_demo` TRNG is implemeted by using templates. This example shows how hande these templates.
- `copy_demo` is a demo programm that shows the difference between random number assigment and the copy function.

The author hopes that TRNG is a useful tool that fulfils your needs for parallel Monte Carlo simmulations. Please send feedback and bug reports to `heiko.bauke@physik.uni-magdeburg.de`.

1.0.3 An Example

In the following program we compute π by a Monte Carlo simmulation. The program uses MPI.

```
// ************************************************************
//
// Monte-Carlo-pi-Calulation
//
// ************************************************************


#include <cstdlib>
#include <cmath>
#include <iostream>
#include <trng.h>
#include <mpi.h>

using namespace TRNG;
using namespace std;

int main(int argc, char *argv[]) {

  // number of points in quare
  const long all_samples=10000001;

  // pseudo random number generator object
  LCG64 r;
  // MPI initialisation
  MPI::Init(argc, argv);

  // get rank and number of processes
  int size=MPI::COMM_WORLD.Get_size();
  int rank=MPI::COMM_WORLD.Get_rank();

  // split sequence of pseudo random numbers by leapfrog method
  r.split(size, rank);

  // no points in the quare
  long in=0l;

  // compute number of points per processor
  long num_samples=all_samples/size;
  // all_samples is not a multiple of size
  if (all_samples%size>rank)
    ++num_samples;

  for (long i=0l; i<num_samples; ++i) {
    double x=r.uniform();
    double y=r.uniform();
    // is point in square
    if (x*x+y*y<=1.0)
      // yes? increment in
      ++in;
  }

  // collect results and print pi
  long in_all;
  MPI::COMM_WORLD.Reduce(&in, &in_all, 1, MPI::LONG, MPI::SUM, 0);
  if (rank==0) {
    double pi=4.0*static_cast<double>(in_all)/static_cast<double>(all_samples);
    cout << "pi = " << pi << endl;
  }

  // quit MPI
  MPI::Finalize();

  return EXIT_SUCCESS;
}
```

The first version of our program gives *not* rusults independent of number of processors. The second version shows how to make the program independent of the number of used processors. The trick is to use different generators to calculate the x- and y-coordinates.

```
// ****************************************************************
//
// Monte-Carlo-pi-Calulation
//
// ****************************************************************


#include <cstdlib>
#include <cmath>
#include <iostream>
#include <trng.h>
#include <mpi.h>

using namespace TRNG;
using namespace std;

int main(int argc, char *argv[]) {

  // number of points in quare
  const long all_samples=1000000l;

  // pseudo random number generator object
  LCG64 rx;
  LCG64 ry;
  // jump 2^26 steps ahead; 2^26 >> all_samples
  ry.jump2(26);

  // MPI initialisation
  MPI::Init(argc, argv);

  // get rank and number of processes
  int size=MPI::COMM_WORLD.Get_size();
  int rank=MPI::COMM_WORLD.Get_rank();

  // split sequence of pseudo random numbers by leapfrog method
  rx.split(size, rank);
  ry.split(size, rank);

  // no points in the quare
  long in=0l;

  // compute number of points per processor
  long num_samples=all_samples/size;
  // all_samples is not a multiple of size
  if (all_samples%size>rank)
    ++num_samples;

  for (long i=0l; i<num_samples; ++i) {
    double x=rx.uniform();
    double y=ry.uniform();
    // is point in square
    if (x*x+y*y<=1.0)
      // yes? increment in
      ++in;
  }

  // collect results and print pi
  long in_all;
  MPI::COMM_WORLD.Reduce(&in, &in_all, 1, MPI::LONG, MPI::SUM, 0);
  if (rank==0) {
    double pi=4.0*static_cast<double>(in_all)/static_cast<double>(all_samples);
    cout << "pi = " << pi << endl;
  }

  // quit MPI
  MPI::Finalize();

  return EXIT_SUCCESS;
}
```

If a TRNG function is called with an invalid argument this function throws an exception **TRNG::error** (p. 51). The next example shows how to handle these exceptions.

```
#include <cstdlib>
#include <iostream>
#include <stdexcept>
#include <trng.h>

using namespace std;
using namespace TRNG;


int main(void) {
  ParkMiller R;

  cout << R.normal_dist() << endl;
  try {
    R.jump2(16l);
    cout << "jumped forward" << endl;
    // you can't jump backwards
    R.jump2(-16l);
    cout << "jumped backward" << endl;
  }
  catch (exception &e) {
    cerr << "oops!! " << e.what() << endl;
  }
  catch (...) {
    cerr << "something else went wrong" << endl;
  }
  return EXIT_SUCCESS;
}
```

Sometimes it is desired to use a random number generator object as a function argument. Tina's random number genrators are implemented by a template technique. The next program is an example with a function with a random number generator as an argument.

```
#include <cstdlib>
#include <iostream>
#include <trng.h>

using namespace std;
using namespace TRNG;

template<class RNG_type>
void foo(RNG_type &R) {
  cout << R.rand() << " is a random number from generator "
       << R.name() << endl;
}

int main(void) {
  ParkMiller R1;
  LCG64 R2;
  foo(R1);
  foo(R2);
  return EXIT_SUCCESS;
}
```

1.0.4 How to extent TRNG

Youd cant find your favourite Tina's Random Number Generators? No problem! Yust extend TRNG to your needs. In the following example we implement an exclusive or lagged fibonacci generator. This example shows only how TRNG could be extented in principle. Sequence splitting and leapfrog method are implemented in a very stupid way. Unused values are just thrown away. Don't uses this generator in your applications. Doun't use exclusive or lagged fibonacci generator at all, see [2].

```
// ---------------------------------------------------------------------
// Time-stamp: <Montag, 21.04.2003, 14:27:38; edited by bauke>
//
// Tina's random number generators TRNG
//
// lagged Fibonacci generator
//
// Copyright (C) 2001, 2002 Heiko Bauke
//
// heiko.bauke@physik.uni-magdeburg.de
//
// TRNG is free software; you can redistribute it and/or
// modify it under the terms of the GNU General Public License
// as published by the Free Software Foundation. This program
// is distributed WITHOUT ANY WARRANTY; without even the implied
// warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
// See the GNU General Public License for more details.
//
```

```
// --------------------------------------------------------------------

#ifndef FIBONACCI_H
#define FIBONACCI_H

#include <trng.h>
#include <strstream>


// This is an example for extending Tina's random number generators.
// We implement a exclusive or lagged Fibonacci generator.
//
//   r_i=r_(i-q) xor r_(i-p); p>q
//
// Sequence splitting and leapfrog method are implemented in a very stupid
// way. Unused values are just thrown away. Don't use this generator in
// your applications.

// the template parametr determine the lags
template<long p1, long q1>
class Fibonacci : public TRNG::RNG<Fibonacci<p1, q1> > {
private:
  std::vector<long> r;
  long p, q, pointer, steps;
  TRNG::ParkMiller R_init;
public:
  // TRNG::user1_t for a user implemeneted rng
  static const TRNG::RNG_type type=TRNG::user1_t;

  const char * name(void) {
    std::ostrstream o;
    o << "Fibonacci(" << q << "," << p << ")";
    return o.str();
  }

  void reset(void) {
    steps=1l;
    max_val=0x7fffffffl;
    max_val2=max_val/2l;
  }

  void seed(long s) {
    R_init.seed(s);
    for (int i=0; i<p; ++i)
      r[i]=R_init.rand();
    pointer=0;
  }

  // calculate the next random number
  long rand(void) {
    long t;
    ++pointer;
    if (pointer==p)
      pointer=0l;
    r[pointer]=r[pointer]^r[(pointer+q)<p ? (pointer+q) : (pointer+q-p)];
    t=r[pointer];
    for (long i=1l; i<steps; ++i) {
      ++pointer;
      if (pointer==p)
        pointer=0l;
      r[pointer]=r[pointer]^r[(pointer+q)<p ? (pointer+q) : (pointer+q-p)];
    }
    return t;
  }

  void split(long s, long n) {
    if (s<1l || n>s || n<0l)
      throw TRNG::error("invalid arguments for Fibonacci::split");
    if (s>1l) {
      for (long i=0l; i<n; ++i)
```

```
        rand();
      steps*=s;
    }
  }

  void jump2(long s) {
    if (s<0l || s>63l)
      throw TRNG::error("invalid argument for Fibonacci::split");
    unsigned long long to=1ull<<s;
    for (unsigned long long i=0ull; i<to; ++i)
      rand();
  }

  void save_status(std::vector<long> &s) {
    s.resize(p+5);
    s[0]=type;
    s[1]=q;
    s[2]=p;
    s[3]=pointer;
    s[4]=steps;
    for (int i=0; i<p; ++i)
      s[i+5]=r[i];
  }

  void load_status(const std::vector<long> &s) {
    if (s[0]!=type)
      throw TRNG::error("Fibonacci::load_status wrong parameter");
    q=s[1];
    p=s[2];
    pointer=s[3];
    steps=s[4];
    r.resize(p);
      for (int i=0; i<p; ++i)
        r[i]=s[i+5];
  }

  Fibonacci & Fibonacci::operator=(TRNG::RNG<Fibonacci> &other) {
    if (this!=&other) {
      std::vector<long> s;
      other.save_status(s);
      load_status(s);
    }
    return *this;
  }

  Fibonacci(long seed_=0l) : r() {
    if (p1<0l || q1<0l || p1==q1)
      throw TRNG::error("bad arguments for Fibonacci::Fibonacci");
    if (p1>q1) {
      p=p1;
      q=q1;
    } else {
      p=q1;
      q=p1;
    }
    r.resize(p);
    reset();
    seed(seed_);
  }

  virtual ~Fibonacci() {};
};


#endif
```

2 Tina's Random Number Generators Namespace Index

2.1 Tina's Random Number Generators Namespace List

Here is a list of all documented namespaces with brief descriptions:

3 Tina's Random Number Generators Hierarchical Index

3.1 Tina's Random Number Generators Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

4 Tina's Random Number Generators Compound Index

4.1 Tina's Random Number Generators Compound List

Here are the classes, structs, unions and interfaces with brief descriptions:

5 Tina's Random Number Generators Namespace Documentation

5.1 TRNG Namespace Reference

Tina's random number generators namespace.

Compounds

- struct **vector2d_struct**
  Two dimensional vector structure.
- struct **vector3d_struct**
  Three dimensional vector structure.
- struct **vector4d_struct**

Four dimensional vector structure.

- class **RNG**

  Pseudo random number generator template.

- class **generic_MLCG**

  Linear congruential generator.

- class **ParkMiller_param**

  Parameter set for linear congruential generators.

- class **ParkMiller**

  Linear congruential generator.

- class **LCG32_param**

  Parameter set for linear congruential generators.

- class **LCG32**

  Linear congruential generator.

- class **LCG64_param**

  Parameter set for linear congruential generators.

- class **LCG64**

  linear congruential generator.

- class **MRG2_param**

  Parameter set for multiple recursive generator.

- class **MRG2**

  multiple recursive generator.

- class **MRG3_param**

  Parameter set for multiple recursive generator.

- class **MRG3**

  multiple recursive generator.

- class **MRG4_param**

  Parameter set for multiple recursive generator.

- class **MRG4**

  multiple recursive generator.

- class **MRG5_param**

  Parameter set for multiple recursive generator.

- class **MRG5**

  multiple recursive generator.

- class **YARNLCG64_param**

  Parameter set for linear congruential generators.

- class **YARNLCG64**

  YARN – a modified linear recursive generator.

- class **YARN2_param**

  Parameter set for multiple recursive generator.

- class **YARN2**

  YARN – a modified multiple recursive generator.

- class **YARN3_param**

  Parameter set for multiple recursive generator.

- class **YARN3**

  YARN – a modified multiple recursive generator.

- class **YARN4_param**

  Parameter set for multiple recursive generator.

- class **YARN4**

  YARN – a modified multiple recursive generator.

- class **YARN5_param**

  Parameter set for multiple recursive generator.

- class **YARN5**

  YARN – a modified multiple recursive generator.

- class **CLCG2_param**

  Parameter set for combined linear congruential generators.

- class **CLCG2**

  combined generator.

- class **CLCG3_param**

  Parameter set for combined linear congruential generators.

- class **CLCG3**

  combined generator.

- class **CLCG4_param**

  Parameter set for combined linear congruential generators.

- class **CLCG4**

  combined generator.

- class **EINV_param**

  Parameter set for explicit inversive congruential generator.

- class **EINV**

  explicit inversive congruential generator.

- class **EINVLCG64_param**

  Parameter set for combined generator.

- class **EINVLCG64**

  combined generator.

- class **trng_gsl**

  wrapper class for GSL random number generators.

- class **error**

  class for error handling.

- class **power**

  power (p. 65).

Typedefs

- typedef **vector2d_struct vector2d**

  Two dimensional vector.

- typedef **vector3d_struct vector3d**

  Three dimensional vector.

- typedef **vector4d_struct vector4d**

  Four dimensional vector.

Enumerations

- enum **RNG_type** { **RNG_t**, **generic_MLCG_t**, **ParkMiller_t**, **LCG32_t**, **LCG64_t**, **MRG2_t**, **MRG3_t**, **MRG4_t**, **MRG5_t**, **YARNLCG64_t**, **YARN2_t**, **YARN3_t**, **YARN4_t**, **YARN5_t**, **CLCG2_t**, **CLCG3_t**, **CLCG4_t**, **EINV_t**, **EINVLCG64_t**, **trng_gsl_t**, **user1_t** = 1001, **user2_t** = 1002, **user3_t** = 1003, **user4_t** = 1004, **user5_t** = 1005 }

  Pseudo random number generator types.

Functions

- const char ∗ **version** (void)

  TRNG version.

- long **modulo_invers** (long, long)

  modulo invers.

- void **gauss** (std::vector< long > &, std::vector< long > &, long)

  linear system solver in modular arithmetic.

- void **matrix_mult** (const std::vector< long > &, const std::vector< long > &, std::vector< long > &, long)

  matrix multiplication.

- void **matrix_vec_mult** (const std::vector< long > &, const std::vector< long > &, std::vector< long > &, long)

  matrix vector multiplication.

- double **Gamma** (double)

  Γ*-function.*

- double **ln_Gamma** (double)

  ln *of* Γ*-function.*

- double **Gamma_P** (double, double)

  incomplete Γ*-function.*

- double **Gamma_Q** (double, double)

  incomplete Γ*-function.*

- double **incomp_Gamma** (double, double)

  incomplete Γ*-function.*

- double **comp_incomp_Gamma** (double, double)

  incomplete Γ*-function.*

- double **Gamma_ser** (double, double)

  incomplete Γ*-function.*

- double **Gamma_cf** (double, double)

  incomplete Γ*-function.*

- double **ln_factorial** (long)

  logarithm of the factorial function.

- long **binomial_coeff** (long, long)

  binomial coefficient.

- double **errf** (double)

  error function.

- double **chi_square_test** (const std::vector< double > &, const std::vector< double > &)

  Chisquare test.

- double **chi_square_prob** (double, long)

  chisquare test.

- double **Stirling_num2** (long, long)

  Stirling number.

- double **Student_t** (double, long, bool=true)

  values for Student's t-distribution.

- long **find_interval** (const std::vector< double > &, double)

  find interval.

- double **uniform_pdf** (double)
  probalility density.
- double **uniform_pdf** (double, double, double)
  probalility density.
- double **uniformco_pdf** (double)
  probalility density.
- double **uniformco_pdf** (double, double, double)
  probalility density.
- double **uniformcc_pdf** (double)
  probalility density.
- double **uniformcc_pdf** (double, double, double)
  probalility density.
- double **uniformoc_pdf** (double)
  probalility density.
- double **uniformoc_pdf** (double, double, double)
  probalility density.
- double **uniformoo_pdf** (double)
  probalility density.
- double **uniformoo_pdf** (double, double, double)
  probalility density.
- double **normal_dist_pdf** (double, double, double)
  probalility density.
- double **exp_dist_pdf** (double, double)
  probalility density.
- double **laplace_dist_pdf** (double, double)
  probalility density.
- double **tent_dist_pdf** (double, double)
  probalility density.
- double **Gamma_dist_pdf** (double, double, double)
  probalility density.
- double **Beta_dist_pdf** (double, double, double)
  probalility density.
- double **chi_square_dist_pdf** (double, double)
  probalility density.

- double **Student_t_dist_pdf** (double, double)
  probalility density.
- double **binomial_dist_pdf** (long, long, double)
  probalility density.
- double **poisson_dist_pdf** (long, double)
  probalility density.
- double **geometric_dist_pdf** (long, double)
  probalility density.

5.1.1 Detailed Description

All function and classes are encapsulated by the namespace TRNG.

5.1.2 Typedef Documentation

5.1.2.1 typedef struct vector2d_struct TRNG::vector2d

This structure is for storing two dimensional vectors. The method **TRNG::RNG::spherical2d**(void) (p. 80) returns this structure.

Definition at line 85 of file trng.h.

5.1.2.2 typedef struct vector3d_struct TRNG::vector3d

This structure is for storing three dimensional vectors. The method **TRNG::RNG::spherical3d**(void) (p. 80) returns this structure.

Definition at line 102 of file trng.h.

5.1.2.3 typedef struct vector4d_struct TRNG::vector4d

This structure is for storing four dimensional vectors. The method **TRNG::RNG::spherical4d**(void) (p. 80) returns this structure.

Definition at line 121 of file trng.h.

5.1.3 Enumeration Type Documentation

5.1.3.1 enum TRNG::RNG_type

Every pseudo random number generator's type can be identified by a class member type which has anny value from this enumeration type.

Enumeration values:

RNG_t	not specialized random number generator.
generic_MLCG_t	generic multiplicative linear congruential random number generator.
ParkMiller_t	random number generator class **ParkMiller** (p. 64).
LCG32_t	random number generator class **LCG32** (p. 52).
LCG64_t	random number generator class **LCG64** (p. 54).
MRG2_t	random number generator class **MRG2** (p. 56).

MRG3_t	random number generator class **MRG3** (p. 58).
MRG4_t	random number generator class **MRG4** (p. 60).
MRG5_t	random number generator class **MRG5** (p. 62).
YARNLCG64_t	random number generator class **YARNLCG64** (p. 93).
YARN2_t	random number generator class **YARN2** (p. 85).
YARN3_t	random number generator class **YARN3** (p. 87).
YARN4_t	random number generator class **YARN4** (p. 89).
YARN5_t	random number generator class **YARN5** (p. 91).
CLCG2_t	random number generator class **CLCG2** (p. 40).
CLCG3_t	random number generator class **CLCG3** (p. 43).
CLCG4_t	random number generator class **CLCG4** (p. 45).
EINV_t	random number generator class **EINV** (p. 47).
EINVLCG64_t	random number generator class **EINVLCG64** (p. 49).
trng_gsl_t	random number generator class **trng_gsl** (p. 82).
user1_t	user defined random number generator class nr 1.
user2_t	user defined random number generator class nr 2.
user3_t	user defined random number generator class nr 3.
user4_t	user defined random number generator class nr 4.
user5_t	user defined random number generator class nr 5.

Definition at line 44 of file trng.h.

5.1.4 Function Documentation

5.1.4.1 const char * TRNG::version (void)

This function returns a pointer to a zero termiated string with the TRNG version.

Returns:
pointer to a zero termiated string

Definition at line 30 of file trnglib.cc.

5.1.4.2 long TRNG::modulo_invers (long *a*, long *m*)

Solves the equation $a \cdot x = 1 \mod m$.

Returns:
the inverse of a.

Parameters:

a	a positive integer.
m	a prime modulus.

Exceptions:
error (p. 51) if $a \leq 0$ or $m \leq 1$ or no inversive exists

See also:
TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 46 of file trnglib.cc.

Referenced by gauss().

5.1.4.3 void TRNG::gauss (std::vector< long > & *a*, std::vector< long > & *b*, long *m*)

Solves a system of linear equations

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \mod m$$

in modular arithmetic using Gau"s elimination.

Parameters:

- ***a*** reference to the coefficient matrix, content is destroyed after function call
- ***b*** reference to the inhomogenous right side, contains the solution $(x_1, x_2, \ldots, x_n)^T$ after function call
- ***m*** prime modulus m

Exceptions:

error (p. 51) if coefficient matrix is singular or the matrices have invalid sizes

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 94 of file trnglib.cc.

References modulo_invers().

5.1.4.4 void TRNG::matrix_mult (const std::vector< long > & *a*, const std::vector< long > & *b*, std::vector< long > & *c*, long *m*)

Multiply two equal sized quadratic matrices a and b in modular arithmetic, $c = a \cdot b \mod m$.

Parameters:

- ***a*** reference to matrix a
- ***b*** reference to matrix b
- ***c*** reference to matrix c
- ***m*** modulus m

Exceptions:

error (p. 51) if the matrices are different sized

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 183 of file trnglib.cc.

5.1.4.5 void TRNG::matrix_vec_mult (const std::vector< long > & *a*, const std::vector< long > & *b*, std::vector< long > & *c*, long *m*)

Multiply a quadratic matrix a and \$a\$ vector b in modular arithmetic, $c = a \cdot b \mod m$.

Parameters:

a reference to matrix a

b reference to vector b

c reference to vector c

m modulus m

Exceptions:

error (p. 51) if the matrices are different sized

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 217 of file trnglib.cc.

5.1.4.6 double TRNG::Gamma (double *x*)

Computes the Γ-function $\Gamma(x) = \int\limits_0^\infty t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$ for positive arguments.

Parameters:

x argument

Exceptions:

error (p. 51) if $x \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 291 of file trnglib.cc.

5.1.4.7 double TRNG::ln_Gamma (double *x*)

Computes the Γ-function's logarithm $\ln\Gamma(x) = \ln\int\limits_0^\infty t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$ for positive arguments. Method is discribed in [6].

Parameters:

x argument

Exceptions:

error (p. 51) if $x \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 254 of file trnglib.cc.

5.1.4.8 double TRNG::Gamma_P (double *a*, double *x*)

Computes the incomplete Γ-function $P(a,x)=\frac{1}{\Gamma(a)}\int\limits_0^x t^{a-1}\mathrm{e}^{-t}\,\mathrm{d}t$ for positive arguments.

Parameters:

a argument a

x argument x

Exceptions:

error (p. 51) if $x<0$ or $a\leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 353 of file trnglib.cc.

5.1.4.9 double TRNG::Gamma_Q (double *a*, double *x*)

Computes the incomplete Γ-function $Q(a,x)=\frac{1}{\Gamma(a)}\int\limits_x^\infty t^{a-1}\mathrm{e}^{-t}\,\mathrm{d}t$ for positive arguments.

Parameters:

a argument a

x argument x

Exceptions:

error (p. 51) if $x<0$ or $a\leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 377 of file trnglib.cc.

5.1.4.10 double TRNG::incomp_Gamma (double *a*, double *x*)

Computes the incomplete Γ-function $\gamma(a,x)=\int\limits_0^x t^{a-1}\mathrm{e}^{-t}\,\mathrm{d}t$ for positive arguments.

Parameters:

a argument a

x argument x

Exceptions:

error (p. 51) if $x < 0$ or $a \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 401 of file trnglib.cc.

5.1.4.11 double TRNG::comp_incomp_Gamma (double *a*, double *x*)

Computes the complementary incomplete Γ-function $\Gamma(a,x) = \int\limits_x^\infty t^{a-1}\mathrm{e}^{-t}\,\mathrm{d}t$ for positive arguments.

Parameters:

a argument a

x argument x

Exceptions:

error (p. 51) if $x < 0$ or $a \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 423 of file trnglib.cc.

5.1.4.12 double TRNG::Gamma_ser (double *a*, double *x*)

Computes incomplete Gamma function's ($P(a,x)$) **power** (p. 65) series representation for $x \leq a+1$.

Parameters:

a argument a

x argument x

Exceptions:

error (p. 51) if $x < 0$ or $a \leq 0$ or at convergence problems

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 444 of file trnglib.cc.

5.1.4.13 double TRNG::Gamma_cf (double *a*, double *x*)

Computes incomplete Gamma function's ($Q(a,x)$) continued fraction representation for $x \geq a+1$.

Parameters:

a argument a

x argument x

Exceptions:

error (p. 51) if $x < 0$ or $a \leq 0$ or at convergence problems

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 482 of file trnglib.cc.

5.1.4.14 double TRNG::ln_factorial (long *n*)

Returns:

$\ln(n!)$

Parameters:

n n

Exceptions:

error (p. 51) if $n < 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 529 of file trnglib.cc.

5.1.4.15 long TRNG::binomial_coeff (long *n*, long *k*)

Returns:

binomial coefficient $\binom{n}{k}$, if $n < 0$ or $k < 0$ or $k > n$ 0 is returned

Parameters:

n n

k k

Author:

Heiko Bauke

Definition at line 555 of file trnglib.cc.

5.1.4.16 double TRNG::errf (double *x*)

Computes the error function

$$errf(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} \mathrm{e}^{-\frac{t^2}{2}} \, \mathrm{d}t \,.$$

Returns:

$errf(x)$

Author:

Heiko Bauke

Definition at line 575 of file trnglib.cc.

5.1.4.17 double TRNG::chi_square_test (const std::vector< double > & *prob*, const std::vector< double > & *observ*)

Applies a χ^2-test.

Returns:

χ^2-value

Parameters:

prob reference to a vector with some probabilities

observ reference to a vector with numbers of actual observations

Exceptions:

error (p. 51) if arguments are not equal sized or number of observations is less then five

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 594 of file trnglib.cc.

5.1.4.18 double TRNG::chi_square_prob (double *chi2*, long *df*)

Computes the probability corresponding to a χ^2-value. See [4] page 41 for details.

Parameters:

chi2 χ^2-value

df degrees of freedom

Exceptions:

error (p. 51) if degrees of freedom less than one

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 626 of file trnglib.cc.

5.1.4.19 double TRNG::Stirling_num2 (long *n*, long *m*)

Computes the Stirling number of the 2nd kind $\left\{ n \atop m \right\}$, see also [5] pp. 65ff.

Returns:

Stirling number of the 2nd kind $\left\{ {n \atop m} \right\}$

Parameters:

n 1st parameter

m 2nd parameter

Author:

Heiko Bauke

Definition at line 651 of file trnglib.cc.

5.1.4.20 double TRNG::Student_t (double *p*, long *nu*, bool *symmetric* = true)

Computes $t_{p,\nu}$ of the t-distribution. $t_{p,\nu}$ is defined in the symmetric case as

$$p = \frac{\Gamma((\nu+1)/2)}{\sqrt{\pi\nu}\,\Gamma(\nu/2)} \int_{-t_{p,\nu}}^{t_{p,\nu}} (1+x^2/\nu)^{\frac{\nu+1}{2}}\,\mathrm{d}x$$

and in the asymmetric case as

$$p = \frac{\Gamma((\nu+1)/2)}{\sqrt{\pi\nu}\,\Gamma(\nu/2)} \int_{-\infty}^{t_{p,\nu}} (1+x^2/\nu)^{\frac{\nu+1}{2}}\,\mathrm{d}x\,.$$

Parameters:

p probability p

nu degrees of freedom ν

symmetric is true for the symmetric case

Exceptions:

error (p. 51) if less than one degree of freedom or probability out of range $0 < p < 1$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 691 of file trnglib.cc.

5.1.4.21 long TRNG::find_interval (const std::vector< double > & *borders*, double *x*)

This function searches for the interval which contains x using an $O(\ln n)$ algorithm. The intervals are

$$I_0 = (-\infty, b_0]\,, \quad I_1 = (-b_0, b_1]\,, \quad I_2 = (-b_1, b_2]\,, \quad \ldots \quad I_{n-1} = (-b_{n-2}, \infty)$$

if b is a sorted vector with elements b_i with $0 \le i \le n-2$.

Returns:

interval number

Parameters:

borders reference to a sorted vector b_i with interval edges

x value that determs the interval

Author:

Heiko Bauke

Definition at line 762 of file trnglib.cc.

Referenced by TRNG::RNG< LCG32 >::binomial_dist_tab().

5.1.4.22 double TRNG::uniform_pdf (double *x*)

Calculates the probalility density function for in $[0, 1)$ equidistributed random variate.

Returns:

1 if $x \in [0, 1)$ else 0

Author:

Heiko Bauke

Definition at line 789 of file trnglib.cc.

References uniformco_pdf().

5.1.4.23 double TRNG::uniform_pdf (double *x*, double *a*, double *b*)

Calculates the probalility density function for in $[a, b)$ equidistributed random variate.

Returns:

$\frac{1}{b-a}$ if $x \in [a, b)$ else 0

Author:

Heiko Bauke

Definition at line 800 of file trnglib.cc.

References uniformco_pdf().

5.1.4.24 double TRNG::uniformco_pdf (double *x*)

Calculates the probalility density function for in $[0, 1)$ equidistributed random variate.

Returns:

1 if $x \in [0, 1)$ else 0

Author:

Heiko Bauke

Definition at line 813 of file trnglib.cc.

Referenced by uniform_pdf().

5.1.4.25 double TRNG::uniformco_pdf (double *x*, double *a*, double *b*)

Calculates the probalility density function for in $[a, b)$ equidistributed random variate.

Returns:
$\frac{1}{b-a}$ if $x \in [a, b)$ else 0

Author:
Heiko Bauke

Definition at line 827 of file trnglib.cc.

5.1.4.26 double TRNG::uniformcc_pdf (double *x*)

Calculates the probalility density function for in $[0, 1]$ equidistributed random variate.

Returns:
1 if $x \in [0, 1]$ else 0

Author:
Heiko Bauke

Definition at line 843 of file trnglib.cc.

5.1.4.27 double TRNG::uniformcc_pdf (double *x*, double *a*, double *b*)

Calculates the probalility density function for in $[a, b]$ equidistributed random variate.

Returns:
$\frac{1}{b-a}$ if $x \in [a, b]$ else 0

Author:
Heiko Bauke

Definition at line 858 of file trnglib.cc.

5.1.4.28 double TRNG::uniformoc_pdf (double *x*)

Calculates the probalility density function for in $(0, 1]$ equidistributed random variate.

Returns:
1 if $x \in (0, 1]$ else 0

Author:
Heiko Bauke

Definition at line 874 of file trnglib.cc.

5.1.4.29 double TRNG::uniformoc_pdf (double *x*, double *a*, double *b*)

Calculates the probalility density function for in $(a, b]$ equidistributed random variate.

Returns:
$\frac{1}{b-a}$ if $x \in (a, b]$ else 0

Author:
Heiko Bauke

Definition at line 888 of file trnglib.cc.

5.1.4.30 double TRNG::uniformoo_pdf (double *x*)

Calculates the probalility density function for in $(0, 1)$ equidistributed random variate.

Returns:

1 if $x \in (0, 1)$ else 0

Author:

Heiko Bauke

Definition at line 904 of file trnglib.cc.

5.1.4.31 double TRNG::uniformoo_pdf (double *x*, double *a*, double *b*)

Calculates the probalility density function for in (a, b) equidistributed random variate.

Returns:

$\frac{1}{b-a}$ if $x \in (a, b)$ else 0

Author:

Heiko Bauke

Definition at line 918 of file trnglib.cc.

5.1.4.32 double TRNG::normal_dist_pdf (double *x*, double *sigma* = 1.0, double *mu* = 0.0)

This function calculates the probalility density for a random variate with normal distribution. This distribution is defined as

$$p(x) = \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

with mean μ and variance σ.

Returns:

$p(x)$

Parameters:

x x

sigma variance σ

mu mean μ

Exceptions:

error (p. 51) if $\sigma \le 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 943 of file trnglib.cc.

5.1.4.33 double TRNG::exp_dist_pdf (double *x*, double *mu* = 1.0)

This function calculates the probalility density for a random variate with exponential distribution. This distribution is defined as

$$p(x) = \begin{cases} \frac{1}{\mu}\mathrm{e}^{-\frac{x}{\mu}} & x \geq 0 \\ 0 & \text{else} \end{cases}$$

with $\mu > 0$.

Returns:

$p(x)$

Parameters:

x x

mu mean μ, $\mu > 0$

Exceptions:

error (p. 51) if $\mu \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 971 of file trnglib.cc.

5.1.4.34 double TRNG::laplace_dist_pdf (double *x*, double *a* = 1.0)

This function calculates the probalility density for a random variate with Laplace distribution. This distribution is defined as

$$p(x) = \frac{1}{2a}\mathrm{e}^{-|x|/a}$$

with $a > 0$.

Returns:

$p(x)$

Parameters:

x x

a parameter a, $a > 0$

Exceptions:

error (p. 51) if $a \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 997 of file trnglib.cc.

5.1.4.35 double TRNG::tent_dist_pdf (double *x*, double *a* = 1.0)

The tent shaped probability distribution is defined as

$$p(x) = \begin{cases} \frac{x+a}{a^2} & -a \leq x \leq 0 \\ \frac{a-x}{a^2} & 0 \leq x \leq a \\ 0 & \text{else} \end{cases}$$

with $a > 0$.

Returns:

$p(x)$

Parameters:

x x

a parameter a

Exceptions:

error (p. 51) if $a \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 1024 of file trnglib.cc.

5.1.4.36 double TRNG::Gamma_dist_pdf (double *x*, double *a*, double *b*)

This function calculates the probalility density for a random variate with Γ-distribution. This distribution is defined as

$$p(x) = \begin{cases} \frac{1}{\Gamma(a)b^a} x^{a-1} \mathrm{e}^{-\frac{x}{b}} & x > 0 \\ 0 & \text{else} \end{cases}.$$

Returns:

$p(x)$

Parameters:

x x

a parameter a, $a > 0$

b parameter b, $b > 0$

Exceptions:

error (p. 51) if $a \leq 0$ or $b \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 1055 of file trnglib.cc.

5.1.4.37 double TRNG::Beta_dist_pdf (double *x*, double *a*, double *b*)

This function calculates the probalility density for a random variate with B-distribution. This distribution is defined as

$$p(x) = \begin{cases} \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1} & 0 \leq x \leq 1 \\ 0 & \text{else} \end{cases} .$$

Returns:

$p(x)$

Parameters:

x x

a parameter a, $a > 0$

b parameter b, $b > 0$

Exceptions:

error (p. 51) if $a \leq 0$ or $b \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 1092 of file trnglib.cc.

5.1.4.38 double TRNG::chi_square_dist_pdf (double *x*, double *nu*)

This function calculates the probalility density for a random variate with χ^2-distribution. This distribution is defined as

$$p(x) = \begin{cases} \frac{\left(\frac{x}{2}\right)^{\frac{\nu}{2}-1}}{2\Gamma(\frac{\nu}{2})} \mathrm{e}^{-\frac{x}{2}} & x \geq 0 \\ 0 & \text{else} \end{cases} .$$

Returns:

$p(x)$

Parameters:

x x

nu parameter ν, $\nu \geq 1$

Exceptions:

error (p. 51) if $\nu < 1$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 1124 of file trnglib.cc.

5.1.4.39 double TRNG::Student_t_dist_pdf (double *x*, double *nu*)

This function calculates the probalility density for a random variate with Student's t distribution. This distribution is defined as

$$p(x) = \frac{\Gamma\left(\frac{\nu-1}{2}\right)}{\sqrt{\nu\pi}\Gamma\left(\frac{\nu}{2}\right)}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} .$$

Returns:
$p(x)$

Parameters:

x x

nu parameter ν, $\nu \geq 1$

Exceptions:
error (p. 51) if $\nu \leq 0$

See also:
TRNG::error (p. 51)

Author:
Heiko Bauke

Definition at line 1151 of file trnglib.cc.

5.1.4.40 double TRNG::binomial_dist_pdf (long *k*, long *n*, double *p* = 0.5)

This function calculates the probalility density for a random variate with binomial distribution. This distribution is defined as

$$p(k) = \frac{n!}{k!(n-k)!}p^k(1-p)^{n-k} , \qquad 0 \leq k \leq n .$$

Returns:
$p(k)$

Parameters:

k parameter k

n number of trails n

p probability p in each trail

Exceptions:
error (p. 51) if $p \leq 0$ or $p > 1$ or $n \leq 0$

See also:
TRNG::error (p. 51)

Author:
Heiko Bauke

Definition at line 1177 of file trnglib.cc.

5.1.4.41 double TRNG::poisson_dist_pdf (long *k*, double *mu*)

This function calculates the probalility density for a random variate with poisson distribution. This distribution is defined as

$$p(k) = \begin{cases} \dfrac{\mu^k}{k!}\mathrm{e}^{-\mu} & k \geq 0 \\ 0 & \text{else} \end{cases}$$

with mean $\mu \geq 0$.

Returns:

$p(k)$

Parameters:

k parameter k

mu mean μ

Author:

Heiko Bauke

Definition at line 1208 of file trnglib.cc.

5.1.4.42 double TRNG::geometric_dist_pdf (long *k*, double *q*)

This function calculates the probalility density for a random variate with geometric distribution. This distribution is defined as

$$p(k) = q(1-q)^{k-1}\,, \qquad k \geq 1\,.$$

Returns:

$p(k)$

Parameters:

q probability q

k parameter k

Exceptions:

error (p. 51) if $p \leq 0$ or $p > 1$ or $n \leq 0$

See also:

TRNG::error (p. 51)

Author:

Heiko Bauke

Definition at line 1231 of file trnglib.cc.

5.2 TRNG::CLCG2_param_sets Namespace Reference

Different parameter sets for random number generators of **CLCG2** (p. 40) type.

Variables

- const **CLCG2_param TRNG** = **CLCG2_param**(376555083l, 2147482951l, 1028879659l, 2147482949l)

  TRNG default.

5.3 TRNG::CLCG3_param_sets Namespace Reference

Different parameter sets for random number generators of **CLCG3** (p. 43) type.

Variables

- const **CLCG3_param TRNG** = **CLCG3_param**(376555083l, 2147482951l,1028879659l, 2147482949l, 225802979l, 2147482943l)

  TRNG default.

5.4 TRNG::CLCG4_param_sets Namespace Reference

Different parameter sets for random number generators of **CLCG4** (p. 45) type.

Variables

- const **CLCG4_param TRNG** = **CLCG4_param**(376555083l, 2147482951l, 1028879659l, 2147482949l, 225802979l, 2147482943l,2028073966l, 2147482859l)

  TRNG default.

5.5 TRNG::EINV_param_sets Namespace Reference

Different parameter sets for random number generators of **EINV** (p. 47) type.

Variables

- const **EINV_param TRNG** = **EINV_param**(1073741831l, 0l, 1342177283l)

  TRNG default.

5.6 TRNG::EINVLCG64_param_sets Namespace Reference

Different parameter sets for random number generators of **EINV** (p. 47) type.

Variables

- const **EINVLCG64_param TRNG** = **EINVLCG64_param**(1073741831l, 0l, 1342177283l, 18145460002477866997ull, 1ull)

  TRNG default.

5.7 TRNG::LCG32_param_sets Namespace Reference

Different parameter sets for random number generators of **LCG32** (p. 52) type.

Variables

- const **LCG32_param VAX** = **LCG32_param**(69069ul, 1ul)
  random number generator used by VAX.

- const **LCG32_param SuperDuper** = **LCG32_param**(69069ul, 0ul)
  Marsaglia's Super-Duper.

- const **LCG32_param Derive** = **LCG32_param**(3141592653ul, 1ul)
  random number generator used in Derive.

- const **LCG32_param LEcuyer1** = **LCG32_param**(2891336453ul, 1ul)
  random number generator proposed by L'Ecuyer [8].

- const **LCG32_param LEcuyer2** = **LCG32_param**(29943829ul, 1ul)
  random number generator proposed by L'Ecuyer [8].

- const **LCG32_param LEcuyer3** = **LCG32_param**(32310901ul, 1ul)
  random number generator proposed by L'Ecuyer [8].

5.8 TRNG::LCG64_param_sets Namespace Reference

Different parameter sets for random number generators of **LCG64** (p. 54) type.

Variables

- const **LCG64_param TRNG** = **LCG64_param**(18145460002477866997ull, 1ull)
  TRNG default.

- const **LCG64_param LEcuyer1** = **LCG64_param**(2862933555777941757ull, 1ull)
  random number generator proposed by L'Ecuyer [8].

- const **LCG64_param LEcuyer2** = **LCG64_param**(3202034522624059733ull, 1ull)
  random number generator proposed by L'Ecuyer [8].

- const **LCG64_param LEcuyer3** = **LCG64_param**(3935559000370003845ull, 1ull)
  random number generator proposed by L'Ecuyer [8].

5.9 TRNG::MRG2_param_sets Namespace Reference

Different parameter sets for random number generators of **MRG2** (p. 56) type.

Variables

- const **MRG2_param LEcuyer1** = **MRG2_param**(1498809829l, 1160990996l, 2147483647l)
  random number generator proposed by L'Ecuyer [11].

- const **MRG2_param LEcuyer2** = **MRG2_param**(46325l, 1084587l, 2147483647l)
  random number generator proposed by L'Ecuyer [11].

5.10 TRNG::MRG3_param_sets Namespace Reference

Different parameter sets for random number generators of **MRG3** (p. 58) type.

Variables

- const **MRG3_param LEcuyer1** = **MRG3_param**(2021422057l, 1826992351l, 1977753457l, 2147483647l)

  random number generator proposed by L'Ecuyer [11].

- const **MRG3_param LEcuyer2** = **MRG3_param**(1476728729l, 0l, 1155643113l, 2147483647l)

  random number generator proposed by L'Ecuyer [11].

- const **MRG3_param LEcuyer3** = **MRG3_param**(65338l, 0l, 64636l, 2147483647l)

  random number generator proposed by L'Ecuyer [11].

5.11 TRNG::MRG4_param_sets Namespace Reference

Different parameter sets for random number generators of **MRG4** (p. 60) type.

Variables

- const **MRG4_param LEcuyer1** = **MRG4_param**(2001982722l, 1412284257l, 1155380217l, 1668339922l, 2147483647l)

  random number generator proposed by L'Ecuyer [11].

- const **MRG4_param LEcuyer2** = **MRG4_param**(64886l, 0l, 0l, 64322l, 2147483647l)

  random number generator proposed by L'Ecuyer [11].

5.12 TRNG::MRG5_param_sets Namespace Reference

Different parameter sets for random number generators of **MRG5** (p. 62) type.

Variables

- const **MRG5_param LEcuyer1** = **MRG5_param**(177786l, 0l, 0l, 0l, 64654l, 2147483647l)

  random number generator proposed by L'Ecuyer [11].

5.13 TRNG::ParkMiller_param_sets Namespace Reference

Different parameter sets for random number generators of **ParkMiller** (p. 64) type.

Variables

- const **ParkMiller_param mindstd** = **ParkMiller_param**(16807l, 2147483647l)

  random number generator by Park and Miller [10].

- const **ParkMiller_param Fishman1** = **ParkMiller_param**(742938285l, 2147483647l)
  random number generator by Fishman [3].
- const **ParkMiller_param Fishman2** = **ParkMiller_param**(950706376l, 2147483647l)
  random number generator by Fishman [3].
- const **ParkMiller_param Fishman3** = **ParkMiller_param**(1226874159l, 2147483647l)
  random number generator by Fishman [3].
- const **ParkMiller_param Fishman4** = **ParkMiller_param**(62089911l, 2147483647l)
  random number generator by Fishman [3].
- const **ParkMiller_param Fishman5** = **ParkMiller_param**(1343714438l, 2147483647l)
  random number generator by Fishman [3].

5.14 TRNG::YARN2_param_sets Namespace Reference

Different parameter sets for random number generators of **YARN2** (p. 85) type.

Variables

- const **YARN2_param LEcuyer1** = **YARN2_param**(1498809829l, 1160990996l, 2147483647l, 123567893l)
  random number generator proposed by L'Ecuyer [11].
- const **YARN2_param LEcuyer2** = **YARN2_param**(46325l, 1084587l, 2147483647l, 123567893l)
  random number generator proposed by L'Ecuyer [11].

5.15 TRNG::YARN3_param_sets Namespace Reference

Different parameter sets for random number generators of **YARN3** (p. 87) type.

Variables

- const **YARN3_param LEcuyer1** = **YARN3_param**(2021422057l, 1826992351l, 1977753457l, 2147483647l, 123567893l)
  random number generator proposed by L'Ecuyer [11].
- const **YARN3_param LEcuyer2** = **YARN3_param**(1476728729l, 0l, 1155643113l, 2147483647l, 123567893l)
  random number generator proposed by L'Ecuyer [11].
- const **YARN3_param LEcuyer3** = **YARN3_param**(65338l, 0l, 64636l, 2147483647l, 123567893l)
  random number generator proposed by L'Ecuyer [11].

5.16 TRNG::YARN4_param_sets Namespace Reference

Different parameter sets for random number generators of **YARN4** (p. 89) type.

Variables

- const **YARN4_param LEcuyer1** = **YARN4_param**(2001982722l, 1412284257l, 1155380217l, 1668339922l, 2147483647l, 123567893l)

  random number generator proposed by L'Ecuyer [11].

- const **YARN4_param LEcuyer2** = **YARN4_param**(64886l, 0l, 0l, 64322l, 2147483647l, 123567893l)

  random number generator proposed by L'Ecuyer [11].

5.17 TRNG::YARN5_param_sets Namespace Reference

Different parameter sets for random number generators of **YARN5** (p. 91) type.

Variables

- const **YARN5_param LEcuyer1** = **YARN5_param**(177786l, 0l, 0l, 0l, 64654l, 2147483647l, 123567893l)

  random number generator proposed by L'Ecuyer [11].

5.18 TRNG::YARNLCG64_param_sets Namespace Reference

Different parameter sets for random number generators of **YARNLCG64** (p. 93) type.

Variables

- const **YARNLCG64_param TRNG** = **YARNLCG64_param**(18145460002477866997ull, 1ull, 123567893l)

  TRNG default.

- const **YARNLCG64_param LEcuyer1** = **YARNLCG64_param**(2862933555777941757ull, 1ull, 123567893l)

  random number generator proposed by L'Ecuyer [8].

- const **YARNLCG64_param LEcuyer2** = **YARNLCG64_param**(3202034522624059733ull, 1ull, 123567893l)

  random number generator proposed by L'Ecuyer [8].

- const **YARNLCG64_param LEcuyer3** = **YARNLCG64_param**(3935559000370003845ull, 1ull, 123567893l)

  random number generator proposed by L'Ecuyer [8].

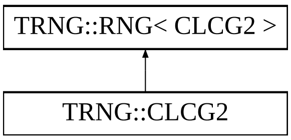
6 Tina's Random Number Generators Class Documentation

6.1 TRNG::CLCG2 Class Reference

combined generator.

`#include <trng.h>`

Inheritance diagram for TRNG::CLCG2::



Public Methods

- **CLCG2** (**CLCG2_param** param=**CLCG2_param_sets::TRNG**, long seed_=0l)
  constructor.

6.1.1 Detailed Description

This is a combined linear congruential random number generator with two generators.

$$\begin{aligned} q_{1,i} &= a_1 \cdot q_{1,i-1} \mod m_1 \\ q_{2,i} &= a_2 \cdot q_{2,i-1} \mod m_2 \\ r_i &= q_{1,i} + q_{2,i} \mod m_1 - 1 \end{aligned}$$

See also [7].

Author:
Heiko Bauke

Definition at line 2286 of file trng.h.

6.1.2 Constructor & Destructor Documentation

6.1.2.1 TRNG::CLCG2::CLCG2 (CLCG2_param *param* = CLCG2_param_sets::TRNG, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with

$$\begin{aligned} q_{1,i} &= 376\,555\,083 \cdot q_{1,i-1} \mod 2\,147\,482\,951 \\ q_{2,i} &= 1\,028\,879\,659 \cdot q_{2,i-1} \mod 2\,147\,482\,949 \\ r_i &= q_{1,i} + q_{2,i} \mod 2\,147\,482\,950\,. \end{aligned}$$

This generator has a period of $\frac{(2\,147\,482\,951-1)(2\,147\,482\,949-1)}{2} \approx 2^{61} \approx 2.31 \cdot 10^{18}$. The multipliers were found by an exhausive search applying the spectral test in up to eight dimensions.

Parameters:
param parameter set
seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.2 TRNG::CLCG2_param Class Reference

Parameter set for combined linear congruential generators.

`#include <trng.h>`

Public Methods

- **CLCG2_param** (long a1_, long modulus1_, long a2_, long modulus2_)

Public Attributes

- const long **a1**

  multiplier of 1st generator.

- const long **modulus1**

  prime modulus of 1st generator.

- const long **a2**

  multiplier of 2nd generator.

- const long **modulus2**

  prime modulus of 2nd generator.

6.2.1 Detailed Description

This class implements the parameter set for combined linear congruential generators with prime moduli and is used by class **CLCG2** (p. 40). See also **CLCG2_param_sets** (p. 35).

Definition at line 2247 of file trng.h.

6.2.2 Constructor & Destructor Documentation

6.2.2.1 TRNG::CLCG2_param::CLCG2_param (long *a1_*, long *modulus1_*, long *a2_*, long *modulus2_*) `[inline]`

The parameter of the constructor specify the multipliers and the prime moduli.

Parameters:

a1_ multiplier of 1st generator

modulus1_ prime modulus of 1st generator

a2_ multiplier of 2nd generator

modulus2_ prime modulus of 2nd generator

Definition at line 2261 of file trng.h.

References a1, a2, modulus1, and modulus2.

The documentation for this class was generated from the following file:

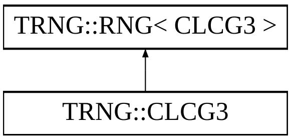
- **trng.h**

6.3 TRNG::CLCG3 Class Reference

combined generator.

`#include <trng.h>`

Inheritance diagram for TRNG::CLCG3::



Public Methods

- **CLCG3** (**CLCG3_param** param=**CLCG3_param_sets::TRNG**, long seed_=0l)
  constructor.

6.3.1 Detailed Description

This is a combined linear congruential random number generator with three generators.

$$\begin{aligned} q_{1,i} &= a_1 \cdot q_{1,i-1} \mod m_1 \\ q_{2,i} &= a_2 \cdot q_{2,i-1} \mod m_2 \\ q_{3,i} &= a_3 \cdot q_{3,i-1} \mod m_3 \\ r_i &= q_{1,i} + q_{2,i} + q_{3,i} \mod m_1 - 1 \end{aligned}$$

See also [7].

Author:
Heiko Bauke

Definition at line 2383 of file trng.h.

6.3.2 Constructor & Destructor Documentation

6.3.2.1 TRNG::CLCG3::CLCG3 (CLCG3_param *param* = CLCG3_param_sets::TRNG, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with

$$\begin{aligned} q_{1,i} &= 376\,555\,083 \cdot q_{1,i-1} \mod 2\,147\,482\,951 \\ q_{2,i} &= 1\,028\,879\,659 \cdot q_{2,i-1} \mod 2\,147\,482\,949 \\ q_{3,i} &= 225\,802\,979 \cdot q_{3,i-1} \mod 2\,147\,482\,943 \\ r_i &= q_{1,i} + q_{2,i} + q_{3,i} \mod 2\,147\,482\,950\,. \end{aligned}$$

This generator has a period of $\frac{(2\,147\,482\,951-1)(2\,147\,482\,949-1)(2\,147\,482\,943-1)}{4} \approx 2^{91} \approx 2.48 \cdot 10^{27}$. The multipliers were found by an exhausive search applying the spectral test in up to eight dimensions.

Parameters:
param parameter set
seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.4 TRNG::CLCG3_param Class Reference

Parameter set for combined linear congruential generators.

`#include <trng.h>`

Public Methods

- **CLCG3_param** (long a1_, long modulus1_, long a2_, long modulus2_, long a3_, long modulus3_)

Public Attributes

- const long **a1**
  multiplier of 1st generator.
- const long **modulus1**
  prime modulus of 1st generator.
- const long **a2**
  multiplier of 2nd generator.
- const long **modulus2**
  prime modulus of 2nd generator.
- const long **a3**
  multiplier of 3rd generator.
- const long **modulus3**
  prime modulus of 3rd generator.

6.4.1 Detailed Description

This class implements the parameter set for combined linear congruential generators with prime moduli and is used by class **CLCG3** (p. 43). See also **CLCG3_param_sets** (p. 36).

Definition at line 2338 of file trng.h.

6.4.2 Constructor & Destructor Documentation

6.4.2.1 TRNG::CLCG3_param::CLCG3_param (long *a1_*, long *modulus1_*, long *a2_*, long *modulus2_*, long *a3_*, long *modulus3_*) `[inline]`

The parameter of the constructor specify the multipliers and the prime moduli.

Parameters:

a1_ multiplier of 1st generator

modulus1_ prime modulus of 1st generator

a2_ multiplier of 2nd generator

modulus2_ prime modulus of 2nd generator

a3_ multiplier of 3rd generator

modulus3_ prime modulus of 3rd generator

Definition at line 2356 of file trng.h.

References a1, a2, a3, modulus1, modulus2, and modulus3.

The documentation for this class was generated from the following file:

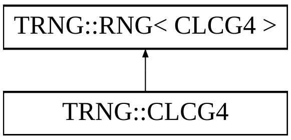
- **trng.h**

6.5 TRNG::CLCG4 Class Reference

combined generator.

`#include <trng.h>`

Inheritance diagram for TRNG::CLCG4::



Public Methods

- **CLCG4** (**CLCG4_param** param=**CLCG4_param_sets::TRNG**, long seed_=0l)
  constructor.

6.5.1 Detailed Description

This is a combined linear congruential random number generator with four generators.

$$\begin{aligned} q_{1,i} &= a_1 \cdot q_{1,i-1} \mod m_1 \\ q_{2,i} &= a_2 \cdot q_{2,i-1} \mod m_2 \\ q_{3,i} &= a_3 \cdot q_{3,i-1} \mod m_3 \\ q_{4,i} &= a_3 \cdot q_{4,i-1} \mod m_4 \\ r_i &= q_{1,i} + q_{2,i} + q_{3,i} + q_{4,i} \mod m_1 - 1 \end{aligned}$$

See also [7].

Author:
Heiko Bauke

Definition at line 2492 of file trng.h.

6.5.2 Constructor & Destructor Documentation

6.5.2.1 TRNG::CLCG4::CLCG4 (CLCG4_param *param* = CLCG4_param_sets::TRNG, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with

$$
\begin{aligned}
q_{1,i} &= 376\,555\,083 \cdot q_{1,i-1} \mod 2\,147\,482\,951 \\
q_{2,i} &= 1\,028\,879\,659 \cdot q_{2,i-1} \mod 2\,147\,482\,949 \\
q_{3,i} &= 225\,802\,979 \cdot q_{3,i-1} \mod 2\,147\,482\,943 \\
q_{4,i} &= 2\,028\,073\,966 \cdot q_{3,i-1} \mod 2\,147\,482\,859 \\
r_i &= q_{1,i} + q_{2,i} + q_{3,i} + q_{4,i} \mod 2\,147\,482\,950\,.
\end{aligned}
$$

This generator has a period of $\frac{(2\,147\,482\,951-1)(2\,147\,482\,949-1)(2\,147\,482\,943-1)(2\,147\,482\,859-1)}{8} \approx 2^{121} \approx 2.66 \cdot 10^{36}$. The multipliers were found by an exhausive search applying the spectral test in up to eight dimensions.

Parameters:

param parameter set

*seed_* default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.6 TRNG::CLCG4_param Class Reference

Parameter set for combined linear congruential generators.

`#include <trng.h>`

Public Methods

- **CLCG4_param** (long a1_, long modulus1_, long a2_, long modulus2_, long a3_, long modulus3_, long a4_, long modulus4_)

Public Attributes

- const long **a1**

  multiplier of 1st generator.

- const long **modulus1**

  prime modulus of 1st generator.

- const long **a2**

  multiplier of 2nd generator.

- const long **modulus2**

  prime modulus of 2nd generator.

- const long **a3**

  multiplier of 3rd generator.

- const long **modulus3**

  prime modulus of 3rd generator.

- const long **a4**

  multiplier of 4th generator.

- const long **modulus4**

  prime modulus of 4th generator.

6.6.1 Detailed Description

This class implements the parameter set for combined linear congruential generators with prime moduli and is used by class **CLCG4** (p. 45). See also **CLCG4_param_sets** (p. 36).

Definition at line 2441 of file trng.h.

6.6.2 Constructor & Destructor Documentation

6.6.2.1 TRNG::CLCG4_param::CLCG4_param (long *a1_*, long *modulus1_*, long *a2_*, long *modulus2_*, long *a3_*, long *modulus3_*, long *a4_*, long *modulus4_*) `[inline]`

The parameter of the constructor specify the multipliers and the prime moduli.

Parameters:

a1_ multiplier of 1st generator

modulus1_ prime modulus of 1st generator

a2_ multiplier of 2nd generator

modulus2_ prime modulus of 2nd generator

a3_ multiplier of 3rd generator

modulus3_ prime modulus of 3rd generator

a4_ multiplier of 4rd generator

modulus4_ prime modulus of 4rd generator

Definition at line 2463 of file trng.h.

The documentation for this class was generated from the following file:

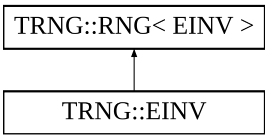
- **trng.h**

6.7 TRNG::EINV Class Reference

explicit inversive congruential generator.

`#include <trng.h>`

Inheritance diagram for TRNG::EINV::



Public Methods

- **EINV** (**EINV_param** param=**EINV_param_sets::TRNG**, long seed_=0l)
  constructor.

6.7.1 Detailed Description

This is an explicit inversive congruential generator with prime modulus.

$$r_i = \overline{a \cdot i + b} \mod m$$

This generator has a period of m. This generator type has excelent statistical properties but its period is too short for large applications. You may combine this genrator with another one. See also [1].

Author:
Heiko Bauke

Definition at line 2594 of file trng.h.

6.7.2 Constructor & Destructor Documentation

6.7.2.1 TRNG::EINV::EINV (EINV_param *param* = EINV_param_sets::TRNG, long *seed_* = 0l)

The default multiplier is $a = 1\,073\,741\,831$, additive constant $b = 0$ and modulus $m = 1\,342\,177\,283$.

Parameters:
param parameter set
seed_ seed

The documentation for this class was generated from the following file:

- **trng.h**

6.8 TRNG::EINV_param Class Reference

Parameter set for explicit inversive congruential generator.

`#include <trng.h>`

Public Methods

- **EINV_param** (long a_, long b_, long modulus_)

Public Attributes

- const long **a**
  multiplier.
- const long **b**
  additive constant.
- const long **modulus**
  prime modulus.

6.8.1 Detailed Description

This class implements the parameter set for explicit inversive congruential with prime modulus and is used by class **EINV** (p. 47). See also **EINV_param_sets** (p. 36).

$$r_i = \overline{a \cdot i + b} \quad \mathrm{mod}\ m$$

Definition at line 2559 of file trng.h.

6.8.2 Constructor & Destructor Documentation

6.8.2.1 TRNG::EINV_param::EINV_param (long *a_*, long *b_*, long *modulus_*) `[inline]`

The parameters of the constructor specify the multiplier and the prime modulus.

Parameters:

a_ multiplier a

b_ additive constant b

modulus_ prime modulus$m$

Definition at line 2571 of file trng.h.

References a, b, and modulus.

The documentation for this class was generated from the following file:

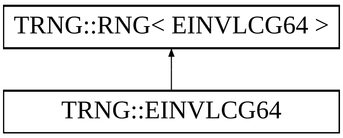
- **trng.h**

6.9 TRNG::EINVLCG64 Class Reference

combined generator.

`#include <trng.h>`

Inheritance diagram for TRNG::EINVLCG64::



Public Methods

- **EINVLCG64** (**EINVLCG64_param** param=**EINVLCG64_param_sets::TRNG**, long seed_=0l)

  constructor.

6.9.1 Detailed Description

This is a combined generator.

$$\begin{aligned} q_{1,i} &= \overline{a \cdot i + b} \quad \mathrm{mod}\ m \\ q_{2,i} &= c \cdot q_{2,i-1} + d \quad \mathrm{mod}\ 2^{64} \\ r_i &= q_{1,i} + \lfloor q_{2,i}/2^{33} \rfloor \quad \mathrm{mod}\ 2^{31} \end{aligned}$$

Author:
Heiko Bauke

Definition at line 2697 of file trng.h.

6.9.2 Constructor & Destructor Documentation

6.9.2.1 TRNG::EINVLCG64::EINVLCG64 (EINVLCG64_param *param* = EINVLCG64_param_sets::TRNG, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with

$$\begin{aligned} q_{1,i} &= \overline{1073741831 \cdot i} \mod (2^{30}+2^{28}+3) \\ q_{2,i} &= 18\,145\,460\,002\,477\,866\,997 \cdot q_{2,i-1} + 1 \mod 2^{64}\,. \\ r_i &= q_{1,i} + \lfloor q_{2,i}/2^{33} \rfloor \mod 2^{31} \end{aligned}$$

Parameters:

param	param set
seed_	seed

The documentation for this class was generated from the following file:

- **trng.h**

6.10 TRNG::EINVLCG64_param Class Reference

Parameter set for combined generator.

`#include <trng.h>`

Public Methods

- **EINVLCG64_param** (long a_, long b_, long modulus_, unsigned long long c_, unsigned long long d_)

  multiplier for linear congruential generator.

Public Attributes

- const long **a**

  multiplier for explicit inversive congruential generator.

- const long **b**

  additive constant for explicit inversive congruential generator.

- const long **modulus**

  prime modulus for explicit inversive congruential generator.

- const unsigned long long **d**

  multiplier for linear congruential generator.

6.10.1 Detailed Description

This class implements the parameter set for conbined generator and is used by class **EINVLCG64** (p. 49). See also **EINVLCG64_param_sets** (p. 36).

$$\begin{aligned} q_{1,i} &= \overline{a \cdot i + b} \mod m \\ q_{2,i} &= c \cdot q_{2,i-1} + d \mod 2^{64} \\ r_i &= q_{1,i} + \lfloor q_{2,i}/2^{33} \rfloor \mod 2^{31} \end{aligned}$$

Definition at line 2656 of file trng.h.

6.10.2 Constructor & Destructor Documentation

6.10.2.1 TRNG::EINVLCG64_param::EINVLCG64_param (long *a_*, long *b_*, long *modulus_*, unsigned long long *c_*, unsigned long long *d_*) `[inline]`

The parameters of the constructor specify the multiplier, the additive constant and the prime modulus for the explicit inversive generator and the multiplier and the additive constant for the linear congruential generator.

Parameters:

a_ multiplier a

b_ additive constant b

modulus_ prime modulus$m$

c_ multiplier c

d_ additive constant d

Definition at line 2675 of file trng.h.

The documentation for this class was generated from the following file:

- **trng.h**

6.11 TRNG::error Class Reference

class for error handling.

`#include <trnglib.h>`

6.11.1 Detailed Description

This class is thrown, if an error occurs. It is public public inherited by std::exception.

Definition at line 36 of file trnglib.h.

The documentation for this class was generated from the following file:

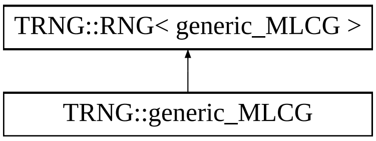
- **trnglib.h**

6.12 TRNG::generic_MLCG Class Reference

Linear congruential generator.

`#include <trng.h>`

Inheritance diagram for TRNG::generic_MLCG::



6.12.1 Detailed Description

This class implements a simple linear congruential pseudo random number generator with a prime modulus. The pseudo random numberr_i is calculated by

$$r_i = a \cdot r_{i-1} \mod m\,.$$

The modulus m has to be a prime smaller than 2^{31} and a a generating element of the multiplicative group modulo m to generate a maxmal length period $m-1$. The behaviour of method **rand**() (p. 70) is different from other generators, it never returns 0. For this reason this generator is for internal use only.

Author:
Heiko Bauke

Definition at line 1044 of file trng.h.

The documentation for this class was generated from the following file:

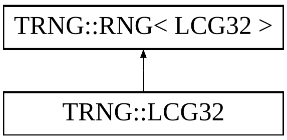
- **trng.h**

6.13 TRNG::LCG32 Class Reference

Linear congruential generator.

`#include <trng.h>`

Inheritance diagram for TRNG::LCG32::



Public Methods

- **LCG32** (**LCG32_param** param=**LCG32_param_sets::VAX**, long seed_=0l)
  constructor.

6.13.1 Detailed Description

This class implements a simple linear congruential pseudo random number generator with a power of two modulus in the form

$$\begin{aligned} q_i &= a \cdot q_{i-1} + b \mod 2^{32} \\ r_i &= \lfloor q_i/2 \rfloor\,. \end{aligned}$$

r_i is the actual pseudo random number. To get a full period of 2^{32} a and b have to be choosen that $a \equiv 1 \mod 4$ and b is odd. If $b = 0$ the maximal period is 2^{30}. A generator with $b = 0$ has a full period if $\pm 3 = a \mod 8$.

Author:

Heiko Bauke

Definition at line 1227 of file trng.h.

6.13.2 Constructor & Destructor Documentation

6.13.2.1 TRNG::LCG32::LCG32 (LCG32_param *param* = LCG32_param_sets::VAX, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator used on VAX. This generator has a period of $2^{32} \approx 4.29 \cdot 10^9$. This generator is just a toy. Its period is too short. See also **LCG32_param_sets** (p. 36).

Parameters:

param parameter set

*seed_* default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.14 TRNG::LCG32_param Class Reference

Parameter set for linear congruential generators.

`#include <trng.h>`

Public Methods

- **LCG32_param** (unsigned long a_, unsigned long b_)

Public Attributes

- const unsigned long **a**

  multiplier.

- const unsigned long **b**

  additive constant.

6.14.1 Detailed Description

This class implements the parameter set for linear congruential generators with modulus 2^{32} and is used by class **LCG32** (p. 52). See also **LCG32_param_sets** (p. 36).

$$r_i = a \cdot r_{i-1} + b \mod 2^{32}$$

Definition at line 1180 of file trng.h.

6.14.2 Constructor & Destructor Documentation

6.14.2.1 TRNG::LCG32_param::LCG32_param (unsigned long *a_*, unsigned long *b_*) `[inline]`

The parameter of the constructor specify the multiplier and the additive constant.

Parameters:

a_ multiplier a

b_ additive constant b

Definition at line 1190 of file trng.h.

References a, and b.

The documentation for this class was generated from the following file:

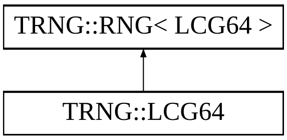
- **trng.h**

6.15 TRNG::LCG64 Class Reference

linear congruential generator.

`#include <trng.h>`

Inheritance diagram for TRNG::LCG64::



Public Methods

- **LCG64** (**LCG64_param** param=**LCG64_param_sets::TRNG**, long seed_=0l)
  constructor.

6.15.1 Detailed Description

This class implements a simple linear congruential pseudo random number generator with a power of two modulus in the form

$$q_i = a \cdot q_{i-1} + b \mod 2^{64}$$
$$r_i = \lfloor q_i / 2^{33} \rfloor .$$

r_i is the actual pseudo random number. To get a full period of 2^{64} a and b have to be choosen that $a \equiv 1 \mod 4$ and b is odd.

Author:

Heiko Bauke

Definition at line 1317 of file trng.h.

6.15.2 Constructor & Destructor Documentation

6.15.2.1 TRNG::LCG64::LCG64 (LCG64_param *param* = LCG64_param_sets::TRNG, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a = 18\,145\,460\,002\,477\,866\,997$ and $b = 1$. This generator has a period of $2^{64} \approx 1.84 \cdot 10^{19}$. **LCG64** (p. 54) is the quick and dirty generator in **TRNG** (p. 13).

Parameters:

param parameter set

seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.16 TRNG::LCG64_param Class Reference

Parameter set for linear congruential generators.

`#include <trng.h>`

Public Methods

- **LCG64_param** (unsigned long long a_, unsigned long long b_)

Public Attributes

- const unsigned long long **a**
  multiplier.
- const unsigned long long **b**
  additive constant.

6.16.1 Detailed Description

This class implements the parameter set for linear congruential generators with modulus 2^{64} and is used by class **LCG64** (p. 54). See also **LCG64_param_sets** (p. 37).

$$r_i = a \cdot r_{i-1} + b \mod 2^{64}$$

Definition at line 1276 of file trng.h.

6.16.2 Constructor & Destructor Documentation

6.16.2.1 TRNG::LCG64_param::LCG64_param (unsigned long long *a_*, unsigned long long *b_*) `[inline]`

The parameter of the constructor specify the multiplier and the additive constant.

Parameters:

a_ multiplier a

b_ additive constant b

Definition at line 1286 of file trng.h.

References a, and b.

The documentation for this class was generated from the following file:

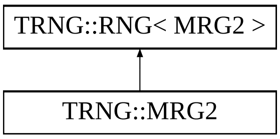
- **trng.h**

6.17 TRNG::MRG2 Class Reference

multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::MRG2::



Public Methods

- **MRG2** (**MRG2_param** param=**MRG2_param_sets::LEcuyer1**, long seed_=0l)
  constructor.

6.17.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order two with a prime modulus.

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} \mod m$$

Author:
Heiko Bauke

Definition at line 1395 of file trng.h.

6.17.2 Constructor & Destructor Documentation

6.17.2.1 TRNG::MRG2::MRG2 (MRG2_param *param* = MRG2_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 1\,498\,809\,829$, $a_2 = 1\,160\,990\,996$ and $m = 2^{31} - 1$ as proposed in [11]. This generator has a period of $2^{31} - 1^{2} - 1 \approx 2^{62} \approx 4.61 \cdot 10^{18}$.

Parameters:

param parameter set

seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.18 TRNG::MRG2_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **MRG2_param** (long a1_, long a2_, long modulus_)

Public Attributes

- const long **a1**
  multiplier a_1*.*
- const long **a2**
  multiplier a_2*.*
- const long **modulus**
  modulus m*.*

6.18.1 Detailed Description

This class implements the parameter set for multiple recursive generators with two coefficients and prime modulus and is used by class **MRG2** (p. 56). See also **MRG2_param_sets** (p. 37).

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} \mod m$$

Definition at line 1362 of file trng.h.

6.18.2 Constructor & Destructor Documentation

6.18.2.1 TRNG::MRG2_param::MRG2_param (long *a1_*, long *a2_*, long *modulus_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1

a2_ multiplier a_2

modulus_ modulus m

Definition at line 1374 of file trng.h.

References a1, a2, and modulus.

The documentation for this class was generated from the following file:

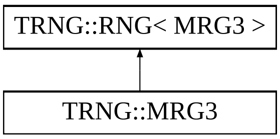
- **trng.h**

6.19 TRNG::MRG3 Class Reference

multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::MRG3::



Public Methods

- **MRG3** (**MRG3_param** param=**MRG3_param_sets::LEcuyer1**, long seed_=0l)
  constructor.

6.19.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order three with a prime modulus.

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} + a_3 \cdot r_{i-3} \mod m$$

Author:
Heiko Bauke

Definition at line 1490 of file trng.h.

6.19.2 Constructor & Destructor Documentation

6.19.2.1 TRNG::MRG3::MRG3 (MRG3_param *param* = MRG3_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 2\,021\,422\,057$, $a_2 = 1\,826\,992\,351$, $a_3 = 1\,977\,753\,457$ and $m = 2^{31} - 1$ as proposed in [11]. This generator has a period of $2^{31} - 1^3 - 1 \approx 2^{93} \approx 9.90 \cdot 10^{27}$.

Parameters:
param parameter set
seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.20 TRNG::MRG3_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **MRG3_param** (long a1_, long a2_, long a3_, long modulus_)

Public Attributes

- const long **a1**
  multiplier a_1*.*
- const long **a2**
  multiplier a_2*.*
- const long **a3**
  multiplier a_3*.*
- const long **modulus**
  modulus m*.*

6.20.1 Detailed Description

This class implements the parameter set for multiple recursive generators with three coefficients and prime modulus and is used by class **MRG3** (p. 58). See also **MRG3_param_sets** (p. 38).

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} + a_3 \cdot r_{i-3} \mod m$$

Definition at line 1453 of file trng.h.

6.20.2 Constructor & Destructor Documentation

6.20.2.1 TRNG::MRG3_param::MRG3_param (long *a1_*, long *a2_*, long *a3_*, long *modulus_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1
a2_ multiplier a_2
a3_ multiplier a_3
modulus_ modulus m

Definition at line 1467 of file trng.h.

References a1, a2, a3, and modulus.

The documentation for this class was generated from the following file:

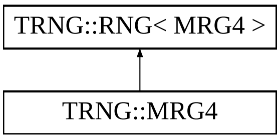
- **trng.h**

6.21 TRNG::MRG4 Class Reference

multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::MRG4::



Public Methods

- **MRG4** (**MRG4_param** param=**MRG4_param_sets::LEcuyer1**, long seed_=0l)
  constructor.

6.21.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order four with a prime modulus.

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} + a_3 \cdot r_{i-3} + a_4 \cdot r_{i-4} \mod m$$

Author:
Heiko Bauke

Definition at line 1587 of file trng.h.

6.21.2 Constructor & Destructor Documentation

6.21.2.1 TRNG::MRG4::MRG4 (MRG4_param *param* = MRG4_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 2\,001\,982\,722$, $a_2 = 1\,412\,284\,257$, $a_3 = 1\,155\,380\,217$, $a_4 = 1\,668\,339\,922$ and $m = 2^{31} - 1$ as proposed by [11]. This generator has a period of $2^{31} - 1^{4} - 1 \approx 2^{124} \approx 2.13 \cdot 10^{37}$.

Parameters:
param parameter set
*seed_* default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.22 TRNG::MRG4_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **MRG4_param** (long a1_, long a2_, long a3_, long a4_, long modulus_)

Public Attributes

- const long **a1**
  multiplier a_1*.*
- const long **a2**
  multiplier a_2*.*
- const long **a3**
  multiplier a_3*.*
- const long **a4**
  multiplier a_4*.*
- const long **modulus**
  modulus m*.*

6.22.1 Detailed Description

This class implements the parameter set for multiple recursive generators with four coefficients and prime modulus and is used by class **MRG4** (p. 60). See also **MRG4_param_sets** (p. 38).

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} + a_3 \cdot r_{i-3} + a_4 \cdot r_{i-4} \mod m$$

Definition at line 1549 of file trng.h.

6.22.2 Constructor & Destructor Documentation

6.22.2.1 TRNG::MRG4_param::MRG4_param (long *a1_*, long *a2_*, long *a3_*, long *a4_*, long *modulus_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1

a2_ multiplier a_2

a3_ multiplier a_3

a4_ multiplier a_4

modulus_ modulus m

Definition at line 1565 of file trng.h.

References a1, a2, a3, a4, and modulus.

The documentation for this class was generated from the following file:

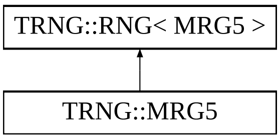
- **trng.h**

6.23 TRNG::MRG5 Class Reference

multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::MRG5::



Public Methods

- **MRG5** (**MRG5_param** param=**MRG5_param_sets::LEcuyer1**, long seed_=0l)
  constructor.

6.23.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order four with a prime modulus.

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} + a_3 \cdot r_{i-3} + a_4 \cdot r_{i-4} + a_5 \cdot r_{i-5} \mod m$$

Author:
Heiko Bauke

Definition at line 1689 of file trng.h.

6.23.2 Constructor & Destructor Documentation

6.23.2.1 TRNG::MRG5::MRG5 (MRG5_param *param* = MRG5_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 107\,374\,182$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 104\,480$ and $m = 2^{31} - 1$ as proposed by [11]. This generator has a period of $2^{31} - 1^5 - 1 \approx 2^{155} \approx 4.57 \cdot 10^{46}$.

Parameters:
param parameter set
seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.24 TRNG::MRG5_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **MRG5_param** (long a1_, long a2_, long a3_, long a4_, long a5_, long modulus_)

Public Attributes

- const long **a1**
  multiplier a_1.
- const long **a2**
  multiplier a_2.
- const long **a3**
  multiplier a_3.
- const long **a4**
  multiplier a_4.
- const long **a5**
  multiplier a_5.
- const long **modulus**
  modulus m.

6.24.1 Detailed Description

This class implements the parameter set for multiple recursive generators with five coefficients and prime modulus and is used by class **MRG5** (p. 62). See also **MRG5_param_sets** (p. 38).

$$r_i = a_1 \cdot r_{i-1} + a_2 \cdot r_{i-2} + a_3 \cdot r_{i-3} + a_4 \cdot r_{i-4} + a_5 \cdot r_{i-5} \mod m$$

Definition at line 1651 of file trng.h.

6.24.2 Constructor & Destructor Documentation

6.24.2.1 TRNG::MRG5_param::MRG5_param (long *a1_*, long *a2_*, long *a3_*, long *a4_*, long *a5_*, long *modulus_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1
a2_ multiplier a_2
a3_ multiplier a_3
a4_ multiplier a_4
a5_ multiplier a_5
modulus_ modulus m

Definition at line 1669 of file trng.h.

References a1, a2, a3, a4, a5, and modulus.

The documentation for this class was generated from the following file:

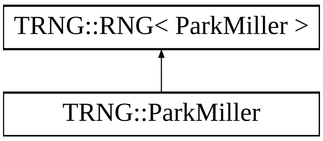
- **trng.h**

6.25 TRNG::ParkMiller Class Reference

Linear congruential generator.

`#include <trng.h>`

Inheritance diagram for TRNG::ParkMiller::



Public Methods

- **ParkMiller** (**ParkMiller_param** param=**ParkMiller_param_sets::mindstd**, long seed_=0l)
  constructor.

6.25.1 Detailed Description

This class implements a simple multiplicative linear congruential pseudo random number generator with a prime modulus in the form

$$\begin{aligned} q_i &= a \cdot q_{i-1} \mod m \\ r_i &= q_i - 1\,. \end{aligned}$$

r_i is the actual pseudo random number. The modulus m has to be a prime smaller than 2^{31} and a a generating element of the multiplicative group modulo m to generate a maxmal length period.

Author:
Heiko Bauke

Definition at line 1137 of file trng.h.

6.25.2 Constructor & Destructor Documentation

6.25.2.1 TRNG::ParkMiller::ParkMiller (ParkMiller_param *param* = ParkMiller_param_sets::mindstd, long *seed_* = 0l)

The default values of the constructor implement a modified random number generator proposed by Park and Miller. This generator has a period of $2^{31} - 2 \approx 2^{31} \approx 2.15 \cdot 10^9$. See also [10].

Parameters:
param parameter set
seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.26 TRNG::ParkMiller_param Class Reference

Parameter set for linear congruential generators.

`#include <trng.h>`

Public Methods

- **ParkMiller_param** (long a_, long modulus_)

Public Attributes

- const long **a**
  multiplier.
- const long **modulus**
  prime modulus.

6.26.1 Detailed Description

This class implements the parameter set for linear congruential generators with prime modulus and is used by class **ParkMiller** (p. 64). See also **ParkMiller_param_sets** (p. 38).

$$r_i = a \cdot r_{i-1} \mod m$$

Definition at line 1091 of file trng.h.

6.26.2 Constructor & Destructor Documentation

6.26.2.1 TRNG::ParkMiller_param::ParkMiller_param (long *a_*, long *modulus_*) `[inline]`

The parameter of the constructor specify the multiplier and the prime modulus.

Parameters:

a_ multiplier a

modulus_ prime modulus$m$

Definition at line 1101 of file trng.h.

References a, and modulus.

The documentation for this class was generated from the following file:

- **trng.h**

6.27 TRNG::power Class Reference

power (p. 65).

`#include <trnglib.h>`

6.27.1 Detailed Description

This data structure is used in the YARN random number generator family. It allows the fast calculation of all powers of a given base b modulo m.

Definition at line 55 of file trnglib.h.

The documentation for this class was generated from the following file:

- **trnglib.h**

6.28 TRNG::RNG< RNG_type > Class Template Reference

Pseudo random number generator template.

`#include <trng.h>`

Public Methods

- const char ∗ **name** (void)

  Name of Pseudo random number generator.

- void **reset** (void)

  Reset the pseudo random number generator.

- void **seed** (long s=0l)

  Seed the pseudo random number generator.

- long **rand** (void)

  Next pseudo random number.

- long **max** (void)

  Maximal pseudo random number.

- bool **boolean** (void)

  Pseudo random boolean.

- bool **boolean** (const double p)

  Pseudo random boolean.

- double **uniform** (void)

  Pseudo random number.

- double **uniform** (const double a, const double b)

  Pseudo random number.

- double **uniformco** (void)

  Pseudo random number.

- double **uniformco** (const double a, const double b)

  Pseudo random number.

- double **uniformcc** (void)

Pseudo random number.

- double **uniformcc** (const double a, const double b)

  Pseudo random number.

- double **uniformoc** (void)

  Pseudo random number.

- double **uniformoc** (const double a, const double b)

  Pseudo random number.

- double **uniformoo** (void)

  Pseudo random number.

- double **uniformoo** (const double a, const double b)

  Pseudo random number.

- long **uniforml** (const long b)

  Pseudo random number.

- long **uniforml** (const long a, const long b)

  Pseudo random number.

- double **normal_dist** (const double sigma=1.0, const double mu=0.0)

  Pseudo random number.

- double **exp_dist** (const double mu=1.0)

  Pseudo random number.

- double **laplace_dist** (const double a=1.0)

  Pseudo random number.

- double **tent_dist** (const double a=1.0)

  Pseudo random number.

- double **Gamma_dist** (const double a, const double b)

  Pseudo random number.

- double **Beta_dist** (const double a, const double b)

  Pseudo random number.

- double **chi_square_dist** (const double nu)

  pseudo random number.

- long **binomial_dist** (long n, double p=0.5)

  Pseudo random number.

- long **binomial_dist_tab** (long n, double p=0.5)

  Pseudo random number.

- double **Student_t_dist** (const double nu)

  Pseudo random number.

- long **poisson_dist** (double mu=1.0)

  Pseudo random number.

- long **geometric_dist** (double q)

  Pseudo random number.

- template<class t_function> double **rejection** (t_function p, double a1, double a2, double p_max)

  Pseudo random number.

- long **discrete_dist** (const std::vector< double > p)

  Pseudo random number.

- **vector2d spherical2d** (void)

  Pseudo random vector.

- **vector3d spherical3d** (void)

  Pseudo random vector.

- **vector4d spherical4d** (void)

  Pseudo random vector.

- void **split** (long s, long n)

  Sequence splitting.

- void **jump** (long long s)

  Sequence splitting.

- void **jump** (long long s, long n)

  Sequence splitting.

- void **jump2** (long s)

  Sequence splitting.

- void **jump2** (long s, long n)

  Sequence splitting.

- void **save_status** (std::vector< long > &s)

  Status saving.

- void **load_status** (const std::vector< long > &s)

  Status restoring.

Static Public Attributes

- const **TRNG::RNG_type type** = RNG_t

  Pseudo random number generator type.

Protected Attributes

- long **max_val**

  Maximum value that the random number gernerator's method **rand**() (p. 70) *can return.*

- long **max_val2**

  Half of the maximum value that method **rand**() (p. 70) *of the random number gernerator can return.*

6.28.1 Detailed Description

template<class RNG_type> class TRNG::RNG< RNG_type >

All the pseudo random number generators are derived form this base class. Routines for generation of uniform and nonuniform variartes are implemented in this base class. Generator specific tasks like sequence splitting or leapfrog method are implementetd by the derived classes. The method **rand**() (p. 70), the generator's core method, has of course also to be reimplemented for every new generator.

Author:

Heiko Bauke

Definition at line 135 of file trng.h.

6.28.2 Member Function Documentation

6.28.2.1 template<class RNG_type> const char* TRNG::RNG< RNG_type >::name (void) `[inline]`

Returns a pointer to a zero terminated string containing the name of pseudo random number generator.

Returns:

pointer to a zero termiated string

Definition at line 159 of file trng.h.

6.28.2.2 template<class RNG_type> void TRNG::RNG< RNG_type >::reset (void) `[inline]`

The parameters of the pseudo random number generator are set to some default values.

Definition at line 168 of file trng.h.

6.28.2.3 template<class RNG_type> void TRNG::RNG< RNG_type >::seed (long s = 0l) `[inline]`

The state of the pseudo random number generator is set. Calling **reset**() (p. 69) and **seed**() (p. 69) with the seed value used by the initialisation will set the generator in the same state as after initialisation.

Parameters:

s new seed

Exceptions:

error (p. 51) if $s < 0$

See also:
TRNG::error (p. 51)

Definition at line 181 of file trng.h.

6.28.2.4 template<class RNG_type> long TRNG::RNG< RNG_type >::rand (void) `[inline]`

This is core method of the generator. It calculates the next pseudo random number. It is an integer number r with $0 \leq r \leq$ max. You can determine the upper bound max by calling the method **max**() (p. 70).

Returns:
next integer pseudo random number

Definition at line 193 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::boolean(), TRNG::RNG< LCG32 >::uniformcc(), TRNG::RNG< LCG32 >::uniformco(), TRNG::RNG< LCG32 >::uniformoc(), and TRNG::RNG< LCG32 >::uniformoo().

6.28.2.5 template<class RNG_type> long TRNG::RNG< RNG_type >::max (void) `[inline]`

Returns:
maximal pseudo random number returned by **rand**() (p. 70)

Definition at line 201 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::boolean(), TRNG::RNG< LCG32 >::uniformcc(), TRNG::RNG< LCG32 >::uniformco(), TRNG::RNG< LCG32 >::uniformoc(), and TRNG::RNG< LCG32 >::uniformoo().

6.28.2.6 template<class RNG_type> bool TRNG::RNG< RNG_type >::boolean (void) `[inline]`

Returns:
pseudo random boolean with probability $\frac{1}{2}$ for return value true

Definition at line 210 of file trng.h.

6.28.2.7 template<class RNG_type> bool TRNG::RNG< RNG_type >::boolean (const double *p*) `[inline]`

Returns:
pseudo random boolean with probability p for return value true

Definition at line 219 of file trng.h.

6.28.2.8 template<class RNG_type> double TRNG::RNG< RNG_type >::uniform (void) `[inline]`

Returns:
a in $[0, 1)$ uniform distributed random number

Definition at line 227 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::uniforml().

6.28.2.9 template<class RNG_type> double TRNG::RNG< RNG_type >::uniform (const double *a*, const double *b*) `[inline]`

Returns:
a in $[a, b)$ uniform distributed random number

Parameters:
a lower bound

b upper bound

Definition at line 237 of file trng.h.

6.28.2.10 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformco (void) `[inline]`

Returns:
a in $[0, 1)$ uniform distributed random number

Definition at line 245 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::binomial_dist(), TRNG::RNG< LCG32 >::binomial_dist_tab(), TRNG::RNG< LCG32 >::discrete_dist(), TRNG::RNG< LCG32 >::Gamma_dist(), TRNG::RNG< LCG32 >::poisson_dist(), TRNG::RNG< LCG32 >::rejection(), TRNG::RNG< LCG32 >::spherical2d(), TRNG::RNG< LCG32 >::spherical3d(), TRNG::RNG< LCG32 >::spherical4d(), and TRNG::RNG< LCG32 >::uniform().

6.28.2.11 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformco (const double *a*, const double *b*) `[inline]`

Returns:
a in $[a, b)$ uniform distributed random number

Parameters:
a lower bound

b upper bound

Definition at line 256 of file trng.h.

6.28.2.12 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformcc (void) `[inline]`

Returns:
a in $[0, 1]$ uniform distributed random number

Definition at line 265 of file trng.h.

6.28.2.13 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformcc (const double *a*, const double *b*) `[inline]`

Returns:
a in $[a, b]$ uniform distributed random number

Parameters:
a lower bound

b upper bound

Definition at line 276 of file trng.h.

6.28.2.14 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformoc (void) `[inline]`

Returns:
a in $(0, 1]$ uniform distributed random number

Definition at line 285 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::exp_dist().

6.28.2.15 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformoc (const double *a*, const double *b*) `[inline]`

Returns:
a in $(a, b]$ uniform distributed random number

Parameters:
a lower bound

b upper bound

Definition at line 296 of file trng.h.

6.28.2.16 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformoo (void) `[inline]`

Returns:
a in $(0, 1)$ uniform distributed random number

Definition at line 305 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::Gamma_dist(), TRNG::RNG< LCG32 >::geometric_dist(), TRNG::RNG< LCG32 >::laplace_dist(), TRNG::RNG< LCG32 >::normal_dist(), and TRNG::RNG< LCG32 >::tent_dist().

6.28.2.17 template<class RNG_type> double TRNG::RNG< RNG_type >::uniformoo (const double *a*, const double *b*) `[inline]`

Returns:
a in (a, b) uniform distributed random number

Parameters:

- ***a*** lower bound
- ***b*** upper bound

Definition at line 316 of file trng.h.

6.28.2.18 template<class RNG_type> long TRNG::RNG< RNG_type >::uniforml (const long *b*) `[inline]`

Returns:

If $b > 0$ a in $[0, b)$ uniform distributed natural random number is returned, if $b < 0$ return value is in $(b, 0]$.

Parameters:

- ***b*** upper bound

Definition at line 326 of file trng.h.

6.28.2.19 template<class RNG_type> long TRNG::RNG< RNG_type >::uniforml (const long *a*, const long *b*) `[inline]`

Returns:

a in $[a, b)$ uniform distributed natural random number

Parameters:

- ***a*** lower bound
- ***b*** upper bound

Definition at line 336 of file trng.h.

6.28.2.20 template<class RNG_type> double TRNG::RNG< RNG_type >::normal_dist (const double *sigma* = 1.0, const double *mu* = 0.0) `[inline]`

A normal distributed random variate has a probability density

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{x^2}{2\sigma^2}} \,.$$

This method uses the polar (Box-Mueller) method, see [4] for details.

Returns:

a normal distributed random number with mean μ and variance σ

Parameters:

- ***sigma*** variance σ
- ***mu*** mean μ

Exceptions:

error (p. 51) if $\sigma \leq 0$

See also:

TRNG::error (p. 51)

Definition at line 356 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::Student_t_dist().

6.28.2.21 template<class RNG_type> double TRNG::RNG< RNG_type >::exp_dist (const double *mu* = 1.0) `[inline]`

A exponential distributed random variate has a probability density

$$p(x) = \begin{cases} \frac{1}{\mu}\mathrm{e}^{-\frac{x}{\mu}} & x \geq 0\,, \qquad \mu > 0 \\ 0 & \text{else} \end{cases} .$$

The transformation method is discribed in [4]. One random number is used to get one random number with exponential distribution.

Returns:
a exponential distributed random number with mean μ

Parameters:
mu mean μ

Exceptions:
error (p. 51) if $\mu \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 389 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::Student_t_dist().

6.28.2.22 template<class RNG_type> double TRNG::RNG< RNG_type >::laplace_dist (const double *a* = 1.0) `[inline]`

The two-sided exponential probability distribution is

$$p(x) = \frac{1}{2a}\mathrm{e}^{-|x|/a}\,, \qquad a > 0\,.$$

It is also known as the Laplace distribution. The is implementation adopted from the GNU scientific library and uses a simple transformation method. One random number is used to get one random number with Laplace distribution.

Returns:
a pseudo random number with probability density $p(x)$

Parameters:
a parameter a, $a > 0$

Exceptions:
error (p. 51) if $a \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 411 of file trng.h.

6.28.2.23 template<class RNG_type> double TRNG::RNG< RNG_type >::tent_dist (const double *a* = 1.0) `[inline]`

This method generates a pseudo randeom number with a tent shaped probability distribution.

$$p(x) = \begin{cases} \dfrac{x+a}{a^2} & -a \leq x \leq 0 \\ \dfrac{a-x}{a^2} & 0 \leq x \leq a \\ 0 & \text{else} \end{cases}, \qquad \text{with } a > 0$$

The implementation uses a simple transformation method. One random number is used to get one random number with a tent shaped distribution.

Returns:
a pseudo random number with probability density $p(x)$

Parameters:
a parameter a, $a > 0$

Exceptions:
error (p. 51) if $a \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 442 of file trng.h.

6.28.2.24 template<class RNG_type> double TRNG::RNG< RNG_type >::Gamma_dist (const double *a*, const double *b*) `[inline]`

A gamma distributed random number has a probability density

$$p(x) = \begin{cases} \dfrac{1}{\Gamma(a) b^a} x^{a-1} \mathrm{e}^{-\frac{x}{b}} & x > 0 \\ 0 & \text{else} \end{cases}.$$

The is implemetation adopted from the GNU scientific library. See also [4].

Returns:
a gamma distributed random number

Parameters:
a parameter a

b parameter b

Exceptions:
error (p. 51) if $a \leq 0$ or $b \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 472 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::Beta_dist(), TRNG::RNG< LCG32 >::chi_square_dist(), TRNG::RNG< LCG32 >::Gamma_dist(), and TRNG::RNG< LCG32 >::poisson_dist().

6.28.2.25 template<class RNG_type> double TRNG::RNG< RNG_type >::Beta_dist (const double *a*, const double *b*) `[inline]`

A Beta distributed random number has a probability density

$$p(x) = \begin{cases} \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1} & 0 \leq x \leq 1 \\ 0 & \text{else} \end{cases}$$

The method is discribed in [4] pp. 129-130.

Returns:
a Beta distributed random number

Parameters:
- ***a*** parameter a, $a > 0$
- ***b*** parameter b, $b > 0$

Exceptions:
error (p. 51) if $a \leq 0$ or $b \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 550 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::binomial_dist().

6.28.2.26 template<class RNG_type> double TRNG::RNG< RNG_type >::chi_square_dist (const double *nu*) `[inline]`

The χ^2-distribution is just a special case of the Γ-distribution with $a = \nu/2$ and $b = 1$.

$$p(x) = \frac{\left(\frac{x}{2}\right)^{\frac{\nu}{2}-1}}{2\Gamma\left(\frac{\nu}{2}\right)} \mathrm{e}^{-\frac{x}{2}}, \qquad x \leq 0$$

The method is discribed in [4] p. 130.

Returns:
a chi square distributed random number

Parameters:
- ***nu*** degrees of freedom ν

Exceptions:
error (p. 51) if $\nu < 1$

See also:
TRNG::error (p. 51)

Definition at line 575 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::Student_t_dist().

6.28.2.27 template<class RNG_type> long TRNG::RNG< RNG_type >::binomial_dist (long *n*, double *p* = 0.5) `[inline]`

The binomial distribution is a discrete distribution with

$$p(k) = \frac{n!}{k!(n-k)!}p^k(1-p)^{n-k}\,, \qquad 0 \le k \le n\,.$$

The method is discribed in [4] p. 131. The implemetation is adopted from the GNU scientific library.

Returns:
a binomial distributed pseudo random number

Parameters:
- ***n*** number of trails n
- ***p*** probability p in each trail

Exceptions:
error (p. 51) if $p \le 0$ or $p > 1$ or $n \le 0$

See also:
TRNG::error (p. 51)

Definition at line 597 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::poisson_dist().

6.28.2.28 template<class RNG_type> long TRNG::RNG< RNG_type >::binomial_dist_tab (long *n*, double *p* = 0.5) `[inline]`

The binomial distribution is a discrete distribution with

$$p(k) = \frac{n!}{k!(n-k)!}p^k(1-p)^{n-k}\,, \qquad 0 \le k \le n\,.$$

This method's implementation uses a lookup table and is very fast if this method is called often with the same parameter set.

Returns:
a binomial distributed pseudo random number

Parameters:
- ***n*** number of trails n
- ***p*** probability p in each trail

Exceptions:
error (p. 51) if $p \le 0$ or $p > 1$ or $n \le 0$

See also:
TRNG::error (p. 51)

Definition at line 637 of file trng.h.

6.28.2.29 template<class RNG_type> double TRNG::RNG< RNG_type >::Student_t_dist (const double *nu*) `[inline]`

Student's t-distribution with ν degrees of freedom is defined as

$$p(x) = \frac{\Gamma\left(\frac{\nu-1}{2}\right)}{\sqrt{\nu\pi}\Gamma\left(\frac{\nu}{2}\right)}\left(1+\frac{x^2}{\nu}\right)^{-\frac{\nu+1}{2}} .$$

This method's implementation is adopted from the GNU scientific library, see also [4].

Returns:
a random number with Student's-t distribution with ν degrees of freedom

Parameters:
nu degrees of freedom, $\nu > 0$

Exceptions:
error (p. 51) if $\nu \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 683 of file trng.h.

6.28.2.30 template<class RNG_type> long TRNG::RNG< RNG_type >::poisson_dist (double *mu* = 1.0) `[inline]`

The probability distribution for Poisson variates is

$$p(k) = \frac{\mu^k}{k!}\mathrm{e}^{-\mu} , \qquad k \geq 0 .$$

This method's implementation is adopted from the GNU scientific library, see also [4].

Returns:
a poisson distributed pseudo random number

Parameters:
mu mean μ

Exceptions:
error (p. 51) if $\mu \leq 0$

See also:
TRNG::error (p. 51)

Definition at line 715 of file trng.h.

6.28.2.31 template<class RNG_type> long TRNG::RNG< RNG_type >::geometric_dist (double *q*) `[inline]`

The geometric probability distribution is

$$p(k) = q(1-q)^{k-1} , \qquad k \geq 1 .$$

This method's implementation is adopted from the GNU scientific library, see also [4].

Returns:
a geometric distributed pseudo random number

Parameters:
q probability q

Exceptions:
error (p. 51) if $q \leq 0$ or $q > 1$

See also:
TRNG::error (p. 51)

Definition at line 753 of file trng.h.

6.28.2.32 template<class RNG_type> template<class t_function> double TRNG::RNG< RNG_type >::rejection (t_function *p*, double *a1*, double *a2*, double *p_max*) `[inline]`

Returns a random number calculated by the rejection method. Assume your desired probability distribution is $p(x) = \frac{3}{4}(1 - x^2)$ for $x \in [-1, 1]$. Write a class that calculates this probability distribution

```
class p {
public:
  double operator()(double x) {
    return 0.75*(1.0-x*x);
  }
};
```

and use

```
my_rng.rejection(p(), -1.0, 1.0, 0.75)
```

to generate a pseudo random number with probability distribution $p(x)$.

Returns:
random number

Parameters:
p function object, a function describing the probability density in the range between a_1 and a_2

a1 lower bound a_1

a2 upper bound a_2

p_max maximum of the probability function $p(x)$ for $x \in [a_1, a_2]$

Definition at line 790 of file trng.h.

6.28.2.33 template<class RNG_type> long TRNG::RNG< RNG_type >::discrete_dist (const std::vector< double > *p*) `[inline]`

This method can be used to generate discrete random variates with an arbitrary probability distribution. The algorithm is $O(\ln n)$. If you need a faster algorithm see [12].

Returns:
random number k, $0 \leq k \leq n - 1$

Parameters:
p n dimensional commulative probability vector p_0, $p_1, \ldots p_{n-1}$, with $p_i < p_{i+1}$ and $p_{n-1} = 1$

Exceptions:

error (p. 51) if vector empty

See also:

TRNG::error (p. 51)

Definition at line 812 of file trng.h.

6.28.2.34 template<class RNG_type> vector2d TRNG::RNG< RNG_type >::spherical2d (void) `[inline]`

This method calculates a unit vector with a uniform distributed direction in two dimensions. For a vector uniform distributed inside the unit citcle multiply the vector with $\sqrt{u}$ where u is uniforum distributed in $[0, 1)$. The vector is stored in a structure **vector2d** (p. 19).

Returns:

a two dimensional unit vector

Definition at line 839 of file trng.h.

6.28.2.35 template<class RNG_type> vector3d TRNG::RNG< RNG_type >::spherical3d (void) `[inline]`

This method calculates a unit vector with a uniform distributed direction in three dimensions. For a vector uniform distributed inside the unit shere multiply the vector with $\sqrt[3]{u}$ where u is uniforum distributed in $[0, 1)$. The vector is stored in a structure **vector3d** (p. 19).

Returns:

a three dimensional unit vector

Definition at line 863 of file trng.h.

6.28.2.36 template<class RNG_type> vector4d TRNG::RNG< RNG_type >::spherical4d (void) `[inline]`

This method calculates a unit vector with a uniform distributed direction in four dimensions. For a vector uniform distributed inside the unit hyper-shere multiply the vector with $\sqrt[4]{u}$ where u is uniforum distributed in $[0, 1)$. The vector is stored in a structure **vector4d** (p. 19).

Returns:

a four dimensional unit vector

Definition at line 887 of file trng.h.

6.28.2.37 template<class RNG_type> void TRNG::RNG< RNG_type >::split (long *s*, long *n*) `[inline]`

The pseudo random number generator's sequence is splitted into s sequences using the leapfrog method. Sequence number n is selected. $0 \leq n < s$

Parameters:

s number of sequences

n selected sequence

Exceptions:

error (p. 51) if $s < 1$ or $n \geq s$ or $n < 0$

See also:

TRNG::error (p. 51)

Definition at line 918 of file trng.h.

6.28.2.38 template<class RNG_type> void TRNG::RNG< RNG_type >::jump (long long *s*) `[inline]`

The pseudo random number generator jumps s steps ahead.

Parameters:

s determines the jump size

Exceptions:

error (p. 51) if $s < 0$

See also:

TRNG::error (p. 51)

Definition at line 929 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::jump().

6.28.2.39 template<class RNG_type> void TRNG::RNG< RNG_type >::jump (long long *s*, long *n*) `[inline]`

The pseudo random number generator jumps $n \cdot s$ steps ahead.

Parameters:

s determines the jump size

Exceptions:

error (p. 51) if $s < 0$ or $n < 0$

Parameters:

s paremeter s

n paremeter n

See also:

TRNG::error (p. 51)

Definition at line 950 of file trng.h.

6.28.2.40 template<class RNG_type> void TRNG::RNG< RNG_type >::jump2 (long *s*) `[inline]`

The pseudo random number generator jumps 2^s steps ahead.

Parameters:

s determines the jump size

Exceptions:

error (p. 51) if $s < 0$

See also:

TRNG::error (p. 51)

Definition at line 966 of file trng.h.

Referenced by TRNG::RNG< LCG32 >::jump(), and TRNG::RNG< LCG32 >::jump2().

6.28.2.41 template<class RNG_type> void TRNG::RNG< RNG_type >::jump2 (long *s*, long *n*) `[inline]`

The pseudo random number generator jumps $n \cdot 2^s$ steps ahead.

Parameters:

s determines the jump size

n determines the jump size

Exceptions:

if $s < 0$ or $n < 0$

See also:

TRNG::error (p. 51)

Definition at line 978 of file trng.h.

6.28.2.42 template<class RNG_type> void TRNG::RNG< RNG_type >::save_status (std::vector< long > & *s*) `[inline]`

The status of the pseudo random number generator is saved into a vector.

Parameters:

s reference to a vector of long

Definition at line 995 of file trng.h.

6.28.2.43 template<class RNG_type> void TRNG::RNG< RNG_type >::load_status (const std::vector< long > & *s*) `[inline]`

The status of the pseudo random number generator is restored from a vector.

Parameters:

s reference to a vector of long

Definition at line 1005 of file trng.h.

6.28.3 Member Data Documentation

6.28.3.1 template<class RNG_type> const TRNG::RNG_type TRNG::RNG< RNG_type >::type = RNG_t `[static]`

This numerical value determins the random number generator type.

Definition at line 151 of file trng.h.

The documentation for this class was generated from the following file:

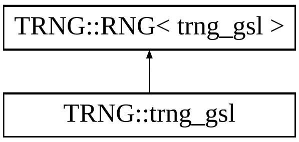
- **trng.h**

6.29 TRNG::trng_gsl Class Reference

wrapper class for GSL random number generators.

`#include <trng_gsl.h>`

Inheritance diagram for TRNG::trng_gsl::



Public Methods

- **trng_gsl** (const gsl_rng_type *T_=gsl_rng_mt19937, long seed_=0l)
  constructor.

6.29.1 Detailed Description

This class implements a simple wrapper for the random number generators in the GNU Scientific Library. Don't use tese generators in parallel applications. Leapfrog and jumping ahead are implemented by throwing some numbers away.

See also:
`http://sources.redhat.com/gsl/ref/gsl-ref_toc.html`

Author:
Heiko Bauke

Definition at line 38 of file trng_gsl.h.

6.29.2 Constructor & Destructor Documentation

6.29.2.1 TRNG::trng_gsl::trng_gsl (const gsl_rng_type * *T_* = gsl_rng_mt19937, long *seed_* = 0l) `[inline]`

The constructor takes two agruments.

Parameters:
T_ random number generator type, see also GNU Scientific Library Reference Manual.
seed_ default seed

See also:
`http://sources.redhat.com/gsl/ref/gsl-ref_17.html`

Definition at line 161 of file trng_gsl.h.

The documentation for this class was generated from the following file:

- **trng_gsl.h**

6.30 TRNG::vector2d_struct Struct Reference

Two dimensional vector structure.

`#include <trng.h>`

Public Attributes

- double **x1**

  1st element.

- double **x2**

  2nd element.

The documentation for this struct was generated from the following file:

- **trng.h**

6.31 TRNG::vector3d_struct Struct Reference

Three dimensional vector structure.

`#include <trng.h>`

Public Attributes

- double **x1**

  1st element.

- double **x2**

  2nd element.

- double **x3**

  3rd element.

The documentation for this struct was generated from the following file:

- **trng.h**

6.32 TRNG::vector4d_struct Struct Reference

Four dimensional vector structure.

`#include <trng.h>`

Public Attributes

- double **x1**

  1st element.

- double **x2**

  2nd element.

- double **x3**

  3rd element.

- double **x4**

  4th element.

The documentation for this struct was generated from the following file:

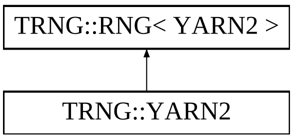
- **trng.h**

6.33 TRNG::YARN2 Class Reference

YARN – a modified multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::YARN2::



Public Methods

- **YARN2** (**YARN2_param** param=**YARN2_param_sets::LEcuyer1**, long seed_=0l)

  constructor.

6.33.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order two with a prime modulus.

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} \mod m$$

Linear structures are destroyed by the nonlinear bijective mapping

$$r_i = \begin{cases} g^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}.$$

The parameter g has to be a generating element of the multiplicative group modulo m.

Author:

Heiko Bauke

Definition at line 1901 of file trng.h.

6.33.2 Constructor & Destructor Documentation

6.33.2.1 TRNG::YARN2::YARN2 (YARN2_param *param* = YARN2_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 1\,498\,809\,829$, $a_2 = 1\,160\,990\,996$ and $m = 2^{31} - 1$ as proposed in [11]. This generator has a period of $(2^{31}-1)^2 - 1 \approx 2^{62} \approx 4.61 \cdot 10^{18}$. The parameter g is chosen to be $123\,567\,893$.

Parameters:

param parameter set

seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.34 TRNG::YARN2_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **YARN2_param** (long a1_, long a2_, long modulus_, long g_)

Public Attributes

- const long **a1**

  multiplier a_1*.*

- const long **a2**

  multiplier a_2*.*

- const long **modulus**

  modulus m*.*

- const long **g**

  generating element g *modulo* m*.*

6.34.1 Detailed Description

This class implements the parameter set for modified multiple recursive generators with two coefficients and prime modulus and is used by class **YARN2** (p. 85). See also **YARN2_param_sets** (p. 39).

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} \mod m$$

$$r_i = \begin{cases} g^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}$$

Definition at line 1857 of file trng.h.

6.34.2 Constructor & Destructor Documentation

6.34.2.1 TRNG::YARN2_param::YARN2_param (long *a1_*, long *a2_*, long *modulus_*, long *g_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1

a2_ multiplier a_2

modulus_ modulus m

g_ generating element g modulo m

Definition at line 1871 of file trng.h.

References a1, a2, g, and modulus.

The documentation for this class was generated from the following file:

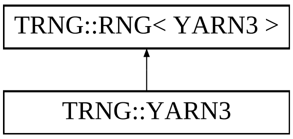
- **trng.h**

6.35 TRNG::YARN3 Class Reference

YARN – a modified multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::YARN3::



Public Methods

- **YARN3** (**YARN3_param** param=**YARN3_param_sets::LEcuyer1**, long seed_=0l)
  constructor.

6.35.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order three with a prime modulus.

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} + a_3 \cdot q_{i-3} \mod m$$

Linear structures are destroyed by the nonlinear bijective mapping $r_i = \begin{cases} b^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}$. The parameter b has to be a generating element of the multiplicative group modulo m.

Author:
Heiko Bauke

Definition at line 1998 of file trng.h.

6.35.2 Constructor & Destructor Documentation

6.35.2.1 TRNG::YARN3::YARN3 (YARN3_param *param* = YARN3_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 2\,021\,422\,057$, $a_2 = 1\,826\,992\,351$, $a_3 = 1\,977\,753\,457$ and $m = 2^{31} - 1$ as proposed in [11]. This generator has a period of $(2^{31} - 1)^3 - 1 \approx 2^{93} \approx 9.90 \cdot 10^{27}$. The parameter g is chosen to be $123\,567\,893$.

Parameters:

param parameter set

seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.36 TRNG::YARN3_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **YARN3_param** (long a1_, long a2_, long a3_, long modulus_, long g_)

Public Attributes

- const long **a1**

  multiplier a_1*.*

- const long **a2**

  multiplier a_2*.*

- const long **a3**

  multiplier a_3*.*

- const long **modulus**

  modulus m*.*

- const long **g**

  generating element g *modulo* m*.*

6.36.1 Detailed Description

This class implements the parameter set for modified multiple recursive generators with three coefficients and prime modulus and is used by class **YARN3** (p. 87). See also **YARN3_param_sets** (p. 39).

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} + a_3 \cdot q_{i-3} \mod m$$

$$r_i = \begin{cases} g^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}$$

Definition at line 1955 of file trng.h.

6.36.2 Constructor & Destructor Documentation

6.36.2.1 TRNG::YARN3_param::YARN3_param (long *a1_*, long *a2_*, long *a3_*, long *modulus_*, long *g_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1

a2_ multiplier a_2

a3_ multiplier a_3

modulus_ modulus m

g_ generating element g modulo m

Definition at line 1971 of file trng.h.

References a1, a2, a3, g, and modulus.

The documentation for this class was generated from the following file:

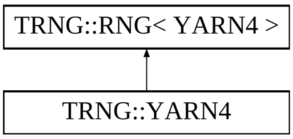
- **trng.h**

6.37 TRNG::YARN4 Class Reference

YARN – a modified multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::YARN4::



Public Methods

- **YARN4** (**YARN4_param** param=**YARN4_param_sets::LEcuyer1**, long seed_=0l)
  constructor.

6.37.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order four with a prime modulus.

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} + a_3 \cdot q_{i-3} + a_4 \cdot q_{i-4} \mod m$$

Linear structures are destroyed by the nonlinear bijective mapping $r_i = \begin{cases} b^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}$. The parameter b has to be a generating element of the multiplicative group modulo m.

Author:

Heiko Bauke

Definition at line 2097 of file trng.h.

6.37.2 Constructor & Destructor Documentation

6.37.2.1 TRNG::YARN4::YARN4 (YARN4_param *param* = YARN4_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 2\,001\,982\,722$, $a_2 = 1\,412\,284\,257$, $a_3 = 1\,155\,380\,217$, $a_4 = 1\,668\,339\,922$ and $m = 2^{31} - 1$ as proposed by [11]. This generator has a period of $(2^{31}-1)^4-1 \approx 2^{124} \approx 2.13{\cdot}10^{37}$. The parameter g is chosen to be 123 567 893.

Parameters:

param parameter set

seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.38 TRNG::YARN4_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **YARN4_param** (long a1_, long a2_, long a3_, long a4_, long modulus_, long g_)

Public Attributes

- const long **a1**

  multiplier a_1*.*

- const long **a2**

  multiplier a_2*.*

- const long **a3**

  multiplier a_3*.*

- const long **a4**

  multiplier a_4*.*

- const long **modulus**

  modulus m*.*

- const long **g**

  generating element g *modulo* m*.*

6.38.1 Detailed Description

This class implements the parameter set for modified multiple recursive generators with four coefficients and prime modulus and is used by class **YARN4** (p. 89). See also **YARN4_param_sets** (p. 39).

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} + a_3 \cdot q_{i-3} + a_4 \cdot q_{i-4} \mod m$$
$$r_i = \begin{cases} g^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}$$

Definition at line 2053 of file trng.h.

6.38.2 Constructor & Destructor Documentation

6.38.2.1 TRNG::YARN4_param::YARN4_param (long *a1_*, long *a2_*, long *a3_*, long *a4_*, long *modulus_*, long *g_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1

a2_ multiplier a_2

a3_ multiplier a_3

a4_ multiplier a_4

modulus_ modulus m

g_ generating element g modulo m

Definition at line 2071 of file trng.h.

The documentation for this class was generated from the following file:

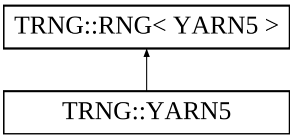
- **trng.h**

6.39 TRNG::YARN5 Class Reference

YARN – a modified multiple recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::YARN5::



Public Methods

- **YARN5** (**YARN5_param** param=**YARN5_param_sets::LEcuyer1**, long seed_=0l)

  constructor.

6.39.1 Detailed Description

This multiple recursive generator uses a linear recurrence of order five with a prime modulus.

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} + a_3 \cdot q_{i-3} + a_4 \cdot q_{i-4} + a_5 \cdot q_{i-5} \mod m$$

Linear structures are destroyed by the nonlinear bijective mapping \f]r_{i} = \begin{cases} b^{q_{i}}\mod m & \text{if }q_{i}\ne 0 \ 0 & \text{if }q_{i} =0 \ \end{cases}\,. \f] The parameter b has to be a generating element of the multiplicative group modulo m.

Author:
Heiko Bauke

Definition at line 2202 of file trng.h.

6.39.2 Constructor & Destructor Documentation

6.39.2.1 TRNG::YARN5::YARN5 (YARN5_param *param* = YARN5_param_sets::LEcuyer1, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a_1 = 107\,374\,182$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 65\,322$ and $m = 2^{31} - 1$ as proposed by [11]. This generator has a period of $(2^{31} - 1)^5 - 1 \approx 2^{155} \approx 4.57 \cdot 10^{46}$. The parameter g is chosen to be $123\,567\,893$.

Parameters:
param parameter set
seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.40 TRNG::YARN5_param Class Reference

Parameter set for multiple recursive generator.

`#include <trng.h>`

Public Methods

- **YARN5_param** (long a1_, long a2_, long a3_, long a4_, long a5_, long modulus_, long g_)

Public Attributes

- const long **a1**
  multiplier a_1.
- const long **a2**
  multiplier a_2.
- const long **a3**
  multiplier a_3.
- const long **a4**

multiplier a_4*.*

- const long **a5**

  multiplier a_5*.*

- const long **modulus**

  modulus m*.*

- const long **g**

  generating element g *modulo* m*.*

6.40.1 Detailed Description

This class implements the parameter set for modified multiple recursive generators with five coefficients and prime modulus and is used by class **YARN5** (p. 91). See also **YARN5_param_sets** (p. 40).

$$q_i = a_1 \cdot q_{i-1} + a_2 \cdot q_{i-2} + a_3 \cdot q_{i-3} + a_4 \cdot q_{i-4} + a_5 \cdot q_{i-5} \mod m$$
$$r_i = \begin{cases} g^{q_i} \mod m & \text{if } q_i \neq 0 \\ 0 & \text{if } q_i = 0 \end{cases}$$

Definition at line 2153 of file trng.h.

6.40.2 Constructor & Destructor Documentation

6.40.2.1 TRNG::YARN5_param::YARN5_param (long *a1_*, long *a2_*, long *a3_*, long *a4_*, long *a5_*, long *modulus_*, long *g_*) `[inline]`

The parameter of the constructor specify the multipliers and the modulus.

Parameters:

a1_ multiplier a_1

a2_ multiplier a_2

a3_ multiplier a_3

a4_ multiplier a_4

a5_ multiplier a_5

modulus_ modulus m

g_ generating element g modulo m

Definition at line 2173 of file trng.h.

The documentation for this class was generated from the following file:

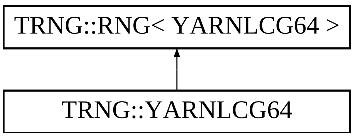
- **trng.h**

6.41 TRNG::YARNLCG64 Class Reference

YARN – a modified linear recursive generator.

`#include <trng.h>`

Inheritance diagram for TRNG::YARNLCG64::



Public Methods

- **YARNLCG64** (**YARNLCG64_param** param=**YARNLCG64_param_sets::TRNG**, long seed_=0l)

  constructor.

6.41.1 Detailed Description

This class implements a modified linear congruential pseudo random number generator with a power of two modulus of the form

$$\begin{aligned} s_i &= a \cdot s_{i-1} + b \mod 2^{64} \\ q_i &= \lfloor s_i / 2^{33} \rfloor \,. \end{aligned}$$

To get a full period of 2^{64} a and b have to be choosen that $a \equiv 1 \mod 4$ and b is odd. Linear structures are destroyed by the nonlinear bijective mapping

$$r_i = \begin{cases} g^{q_i} \mod 2^{31}-1 & \text{if } q_i \neq 0 \land q_i \neq 2^{31}-1 \\ q_i & \text{else} \end{cases} .$$

The parameter g has to be a generating element of the multiplicative group modulo $2^{31} - 1$.

Author:

Heiko Bauke

Definition at line 1806 of file trng.h.

6.41.2 Constructor & Destructor Documentation

6.41.2.1 TRNG::YARNLCG64::YARNLCG64 (YARNLCG64_param *param* = YARNLCG64_param_sets::TRNG, long *seed_* = 0l)

The constructor's default values implement a pseudo random number generator with $a = 18\,145\,460\,002\,477\,866\,997$, $b = 1$ and $g = 123\,567\,893$. This generator has a period of $2^{64} \approx 1.84 \cdot 10^{19}$.

Parameters:

param parameter set

seed_ default seed

The documentation for this class was generated from the following file:

- **trng.h**

6.42 TRNG::YARNLCG64_param Class Reference

Parameter set for linear congruential generators.

`#include <trng.h>`

Public Methods

- **YARNLCG64_param** (unsigned long long a_, unsigned long long b_, long g_)

Public Attributes

- const unsigned long long **a**

  multiplier.

- const unsigned long long **b**

  additive constant.

- const long **g**

  generating element modulo $2^{31}-1$.

6.42.1 Detailed Description

This class implements the parameter set for linear congruential generators with modulus 2^{64} and is used by class **YARNLCG64** (p. 93). See also **YARNLCG64_param_sets** (p. 40).

$$r_i = a \cdot r_{i-1} + b \mod 2^{64}$$

Definition at line 1754 of file trng.h.

6.42.2 Constructor & Destructor Documentation

6.42.2.1 TRNG::YARNLCG64_param::YARNLCG64_param (unsigned long long *a_*, unsigned long long *b_*, long *g_*) `[inline]`

The parameter of the constructor specify the multiplier, the additive constant and the generating element modulo $2^{31}-1$.

Parameters:

a_ multiplier a

b_ additive constant b

g_ generating element g modulo $2^{31}-1$

Definition at line 1766 of file trng.h.

References a, b, and g.

The documentation for this class was generated from the following file:

- **trng.h**

References

[1] J. Eichenauer-Hermann. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Mathematics of Computation*, 60:375–384, 1993.

[2] Alan M. Ferrenberg and D. P. Landau. Monte carlo simulations: Hidden errors from “good” random number generators. *Physical Review Letters*, 69(23):3382–3384, 1992.

[3] George. S. Fishman and Louis S. Moore III. An exhausive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. *SIAM. J. Sci. Stat. Comp.*, 7(1):24–45, 1986.

[4] Donald E. Knuth. *The art of computer programming*, volume 2. Addison-Wesley, Reading, Messachusetts, 2nd edition, 1981.

[5] Donald E. Knuth. *The art of computer programming*, volume 1. Addison-Wesley, Reading, Messachusetts, 2nd edition, 1981.

[6] C. Lanczos. *SIAM Journal on Numerical Analysis, ser. B*, 1:86–96, 1964.

[7] Pierre L’Ecuyer. Efficient and protable random number generators. *Communications of the ACM*, 31(6):742–749, 774, Juni 1988.

[8] Pierre L’Ecuyer. Tables of linear congruential generators of different sizes and good lattice structure. *Mathematics of Computation*, 68:249–260, 1999.

[9] George Marsaglia. `http://stat.fsu.edu/pub/diehard/cdrom/`; `http://stat.fsu.edu/~geo/`, 1995.

[10] Stephen K. Park and Keith W. Miller. Random number generators: good ones are hard to find. *Communications of the ACM*, 31(10):1192–1201, Oktober 1988.

[11] Raymond Couture Pierre L’Ecuyer, François Blouin. A search for good multiple recursive random number generators. *ACM Transactions on Modeling and Computer Simulation*, 3(2):87–98, April 1993.

[12] Alastair J. Walker. An efficient method for generating discrete random variables with general distributions,. *ACM Trans on Mathematical Software*, 3:253–256, 1977.

Index