Random Number Generation in C++0X: A Comprehensive Proposal, version 4

Document number:	WG21/N2111 = J16/06-0181
Date:	2006-10-19
Revises:	WG21/N2079 = J16/06-0149
Project:	Programming Language C++
Reference:	ISO/IEC IS 14882:2003(E)

Reply to:	Walter E. Brown <wb@fnal.gov>
	Mark Fischler <mf@fnal.gov>
	Jim Kowalkowski <jbk@fnal.gov>
	Marc Paterno <paterno@fnal.gov>
	CEPA Dept., Computing Division
	Fermi National Accelerator Laboratory
	Batavia, Illinois 60510-0500
	U.S.A.

This document revises N2079 = Brown, *et al.*: **Random Number Generation in C++0X: A Comprehensive Proposal, version 3**. It incorporates all known corrections to that paper's language and typography.

Each local change in wording from the previous version of this paper is indicated as either added or ~~deleted~~ text. Changes in the index are not specially marked.

We would like to acknowledge the Fermi National Accelerator Laboratory's Computing Division, sponsors of our participation in the C++ standards effort, for its support. Thanks also to Paolo Carlini, Charles Karney, Bradley Lucier, Jens Maurer, Makoto Matsumoto, and Stephan Tolksdorf for their respective helpful correspondence regarding several technical aspects of this and previous editions of the proposal.

Contents

List of Tables

25 Algorithms library [lib.algorithms]

25.2 Mutating sequence operations [lib.alg.modifying.operations]

25.2.11 Random shuffle [lib.alg.random.shuffle]

```
template<class RandomAccessIterator>
void random_shuffle(RandomAccessIterator first,
                    RandomAccessIterator last);

template<class RandomAccessIterator, class RandomNumberGenerator>
void random_shuffle(RandomAccessIterator first,
                    RandomAccessIterator last,
                    RandomNumberGenerator& rand);

template <class RandomAccessIterator, class UniformRandomNumberGenerator>
void random_shuffle(RandomAccessIterator first,
                    RandomAccessIterator last,
                    UniformRandomNumberGenerator& g);
```

1 *Effects:* Shuffles the elements in the range $[first, last)$ with uniform distribution.

2 *Requires:* The type of $*first$ shall satisfy the `Swappable` requirements [lib.swappable].

3 *Complexity:* Exactly $(last - first) - 1$ swaps.

4 *Remarks:* The underlying source of random numbers for the first form of the function is implementation-defined. An implementation may use the `rand` function from the standard C library.

The second form of the function takes a random number generating function object *rand* such that if `n` is an argument for *rand*, with a positive value, that has type `iterator_traits<RandomAccessIterator>::difference_type`, then *rand*`(n)` returns a randomly chosen value, which lies in the interval $[0, n)$, and which has a type that is convertible to `iterator_traits<RandomAccessIterator>::difference_type`.

The third form of the function takes an object meeting the requirements of uniform random number generator [26.4.1.2].

26 Numerics library [lib.numerics]

26.4 Random number generation [lib.random.numbers]

1 This subclause defines a facility for generating (pseudo-)random numbers.

2 In addition to a few utilities, four categories of entities are described: *uniform random number generators*, *random number engines*, *random number engine adaptors*, and *random number distributions*. These categorizations are applicable to types that satisfy the corresponding requirements, to objects instantiated from such types, and to templates producing such types when instantiated. [*Note:* These entities are specified in such a way as to permit the binding of any uniform random number generator object `e` as the argument to any random number distribution object `d`, thus producing a zero-argument function object such as given by `bind(d,e)`. — *end note*]

3 Each of the entities specified via this subclause has an associated arithmetic type [basic.fundamental] identified as `result_type`. With `T` as the `result_type` thus associated with such an entity, that entity is characterized

a) as *boolean* or equivalently as *boolean-valued*, if `T` is `bool`;

b) otherwise as *integral* or equivalently as *integer-valued*, if `numeric_limits<T>::is_integer` is `true`;

c) otherwise as *floating* or equivalently as *real-valued*.

If integer-valued, an entity may optionally be further characterized as *signed* or *unsigned*, according to `T`.

4 Unless otherwise specified, all descriptions of calculations in this subclause use mathematical real numbers.

5 Throughout this subclause, the operators bitand, bitor, and xor denote the respective conventional bitwise operations. Further,

a) the operator rshift denotes a bitwise right shift with zero-valued bits appearing in the high bits of the result, and

b) the operator lshift_w denotes a bitwise left shift with zero-valued bits appearing in the low bits of the result, and whose result is always taken modulo 2^w.

26.4.1 Requirements [lib.rand.req]

26.4.1.1 General requirements [lib.rand.req.genl]

1 Throughout this subclause 26.4, the effect of instantiating a template

a) that has a template type parameter named `UniformRandomNumberGenerator` is undefined unless the corresponding template argument is cv-unqualified and satisfies the requirements of uniform random number generator [26.4.1.2].

b) that has a template type parameter named `Engine` is undefined unless the corresponding template argument is cv-unqualified and satisfies the requirements of random number engine [26.4.1.3].

c) that has a template type parameter named `RealType` is undefined unless the corresponding template argument is cv-unqualified and is one of `float`, `double`, or `long double`.

d) that has a template type parameter named `IntType` is undefined unless the corresponding template argument is cv-unqualified and is one of `short`, `int`, `long`, `long long`, `unsigned short`, `unsigned int`, `unsigned long`, or `unsigned long long`.

e) that has a template type parameter named `UIntType` is undefined unless the corresponding template argument is cv-unqualified and is one of `unsigned short`, `unsigned int`, `unsigned long`, or `unsigned long long`.

2 All members declared `static const` in any of the following classes or class templates shall be defined in such a way that they are usable as integral constant expressions.

26.4.1.2 Uniform random number generator requirements [lib.rand.req.urng]

1 A class `X` satisfies the requirements of a *uniform random number generator* if the expressions shown in table 1 are valid and have the indicated semantics. In that table,

a) `T` is the type named by `X`'s associated `result_type`, and

b) `u` is a value of `X`.

Table 1: Uniform random number generator requirements

expression	return type	pre/post-condition	complexity
`X::result_type`	`T`	`T` is an unsigned integer type [basic.fundamental].	compile-time
`u()`	`T`	Returns a value in the closed interval [`X::min`, `X::max`].	amortized constant
`X::min`	`T`	Denotes the least value potentially returned by `operator()`.	compile-time
`X::max`	`T`	Denotes the greatest value potentially returned by `operator()`.	compile-time

26.4.1.3 Random number engine requirements [lib.rand.req.eng]

1 A class `X` that satisfies the requirements of a uniform random number generator [26.4.1.2] also satisfies the requirements of a *random number engine* if the expressions shown in table 2 are valid and have the indicated semantics, and if `X` also satisfies all other requirements of this section 26.4.1.3. In that table and throughout this section 26.4.1.3,

a) `T` is the type named by `X`'s associated `result_type`;

b) `u` is a value of `X`, `v` is an lvalue of `X`, `x` and `y` are (possibly `const`) values of `X`;

c) `s` is a value of arithmetic type [basic.fundamental];

d) `q` is an lvalue of type `seed_seq` [26.4.7.1];

e) `z` is a value of type ~~`size_t`~~`unsigned long long`;

f) `os` is an lvalue of the type of some class template specialization `basic_ostream<charT, traits>`; and

g) `is` is an lvalue of the type of some class template specialization `basic_istream<charT, traits>`;

where `charT` and `traits` are constrained according to [lib.strings] and [lib.input.output].

2 A random number engine object `x` has at any given time a state $\mathtt{x}_i$ for some integer $i \geq 0$. Upon construction, a random number engine `x` has an initial state $\mathtt{x}_0$. An engine's state may be established by invoking a constructor, `seed` member function, `operator=`, or a suitable `operator>>`.

3 The specification of each random number engine defines the size of its state in multiples of the size of its `result_type`, given as an integral constant expression. The specification of each random number engine also defines

a) the *transition algorithm* TA by which the engine's state $\mathtt{x}_i$ is advanced to its *successor state* $\mathtt{x}_{i+1}$, and

b) the *generation algorithm* GA by which an engine's state is mapped to a value of type `result_type`.

Table 2: Random number engine requirements

expression	return type	pre/post-condition	complexity
`X()`	—	Creates an engine with the same initial state as all other default-constructed engines of type `X`.	$\mathcal{O}$(size of state)
`X(x)`	—	Creates an engine that compares equal to `x`.	$\mathcal{O}$(size of state)
`X(s)`	—	Creates an engine with initial state determined by `static_cast<X::result_type>(s)`.	$\mathcal{O}$(size of state)
`X(q)` [1)]	—	With $n =$ `q.size()`, creates an engine `u` with initial state determined as follows: If n is 0, `u == X()`; otherwise, the initial state depends on a sequence produced by one call to `q.randomize`.	$\mathcal{O}$(max(n,size of state))
`u.seed()`	`void`	post: `u == X()`	same as `X()`
`u.seed(s)`	`void`	post: `u == X(s)`	same as `X(s)`
`u.seed(q)`	`void`	post: `u == X(q)`.	same as `X(q)`
`u()`	`T`	Sets the state to $\mathtt{u}_{i+1} = \mathsf{TA}(\mathtt{u}_i)$ and returns $\mathsf{GA}(\mathtt{u}_i)$.	amortized constant

[1)] This constructor (as well as the corresponding `seed()` function below) may be particularly useful to applications requiring a large number of independent random sequences.

expression	return type	pre/post-condition	complexity
`u.discard(z)` [2)]	`void`	post: The state of `u` is identical to that produced by `z` consecutive calls to `u()`.	no worse than the complexity of `z` consecutive calls to `u()`
`x == y`	`bool`	With S_x and S_y as the infinite sequences of values that would be generated by repeated future calls to `x()` and `y()`, respectively, returns `true` if $S_x = S_y$; returns `false` otherwise.	$\mathcal{O}$(size of state)
`x != y`	`bool`	`!(x == y)`	$\mathcal{O}$(size of state)
`os << x`	reference to the type of `os`	With `os.`*fmtflags* set to `ios_base::dec|ios_base::fixed|ios_base::left` and the fill character set to the space character, writes to `os` the textual representation of `x`'s current state. In the output, adjacent numbers are separated by one or more space characters. post: The `os.`*fmtflags* and fill character are unchanged.	$\mathcal{O}$(size of state)
`is >> v`	reference to the type of `is`	Sets `v`'s state as determined by reading its textual representation from `is`. If bad input is encountered, ensures that `v`'s state is unchanged by the operation and calls `is.setstate(ios::failbit)` (which may throw `ios::failure` [lib.iostate.flags]). pre: The textual representation was previously written using an `os` whose imbued locale and whose type's template specialization arguments `charT` and `traits` were the same as those of `is`. post: The `is.`*fmtflags* are unchanged.	$\mathcal{O}$(size of state)

4 `X` shall satisfy the requirements of uniform random number generator [26.4.1.2] as well as of `CopyConstructible` [lib.copyconstructible] and of `Assignable` [lib.container.requirements]. Copy construction and assignment shall each be of complexity $\mathcal{O}$(size of state).

[2)] This operation is common in user code, and can often be implemented in an engine-specific manner so as to provide significant performance improvements over an equivalent naive loop that makes `z` consecutive calls to `u()`.

5 If a textual representation written via `os << x` was subsequently read via `is >> v`, then `x == v` provided that there have been no intervening invocations of `x` or of `v`.

26.4.1.4 Random number engine adaptor requirements [lib.rand.req.adapt]

1 A *random number engine adaptor* is a random number engine that takes values produced by some other random number engine or engines, and applies an algorithm to those values in order to deliver a sequence of values with different randomness properties. Engines adapted in this way are termed *base engines* in this context. The terms *unary*, *binary*, and so on, may be used to characterize an adaptor depending on the number n of base engines that adaptor utilizes.

2 A class `X` satisfies the requirements of a random number engine adaptor if the expressions shown in table 3 are valid and have the indicated semantics, and if `X` and its associated types also satisfies all other requirements of this section 26.4.1.4. In that table and throughout this section,

a) $\mathtt{B}_i$ is the type of the i^{th} of `X`'s base engines, $1 \le i \le n$; and

b) $\mathtt{b}_i$ is a value of $\mathtt{B}_i$.

If `X` is unary, i is omitted and understood to be 1.

Table 3: Random number engine adaptor requirements

expression	return type	pre/post-condition	complexity
`X::base`i`_type`	$\mathtt{B}_i$	—	compile time
`X::base`i`()`	`const` $\mathtt{B}_i$`&`	Returns a reference to $\mathtt{b}_i$.	constant

3 `X` shall satisfy the requirements of random number engine [26.4.1.3], subject to the following:

a) The base engines of `X` are arranged in an arbitrary but fixed order, and that order is consistently used whenever functions are applied to those base engines in turn.

b) The complexity of each function is at most the sum of the complexities of the corresponding functions applied to each base engine.

c) The state of `X` includes the state of each of its base engines. The size of `X`'s state is no less than the sum of the base engine sizes. Copying `X`'s state (*e.g.*, during copy construction or copy assignment), includes copying, in turn, each base engine of `X`.

d) The textual representation of `X` includes, in turn, the textual representation of each of its base engines.

e) When `X::X` is invoked with no arguments, each of `X`'s base engines is constructed, in turn, as if by its respective default constructor. When `X::X` is invoked with an `X::result_type` value s, each of `X`'s base engines is constructed, in turn, with the next available value from the list $s+0, s+1, \ldots$. When `X::X` is invoked with an argument of type `seed_seq`, each of `X`'s base engines is constructed, in turn, with that object as argument.

4 `X` shall have one additional constructor with n or more parameters such that the type of parameter i, $1 \le i \le n$, is `const` $\mathtt{B}_i$`&` and such that all remaining parameters, if any, have default values. The constructor shall construct `X`, initializing each of its base engines, in turn, with a copy of the value of the corresponding argument.

26.4.1.5 Random number distribution requirements [lib.rand.req.dist]

1 A class `X` satisfies the requirements of a *random number distribution* if the expressions shown in table 4 are valid and have the indicated semantics, and if `X` and its associated types also satisfies all other requirements of this section 26.4.1.5. In that table and throughout this section,

a) `T` is the type named by `X`'s associated `result_type`;

b) `P` is the type named by `X`'s associated `param_type`;

c) `u` is a value of `X` and `x` is a (possibly const) value of `X`;

d) `glb` and `lub` are values of `T` respectively corresponding to the greatest lower bound and the least upper bound on the values potentially returned by `u`'s `operator()`, as determined by the current values of `u`'s parameters;

e) `p` is a value of `P`;

f) `e` is an lvalue of an arbitrary type that satisfies the requirements of a uniform random number generator [26.4.1.2];

g) `os` is an lvalue of the type of some class template specialization `basic_ostream<charT, traits>`; and

h) `is` is an lvalue of the type of some class template specialization `basic_istream<charT, traits>`;

where `charT` and `traits` are constrained according to [lib.strings] and [lib.input.output].

2 The specification of each random number distribution identifies an associated mathematical *probability density function* $p(z)$ or an associated *discrete probability function* $P(z_i)$. Such functions are typically expressed using certain externally-supplied quantities known as the *parameters of the distribution*. Such distribution parameters are identified in this context by writing, for example, $p(z\,|\,a,b)$ or $P(z_i\,|\,a,b)$, to name specific parameters, or by writing, for example, $p(z\,|\,\{\mathtt{p}\})$ or $P(z_i\,|\,\{\mathtt{p}\})$, to denote a distribution's parameters `p` taken as a whole.

Table 4: Random number distribution requirements

expression	return type	pre/post-condition	complexity
`X::result_type`	`T`	`T` is an arithmetic type.	compile-time
`X::param_type`	`P`	—	compile-time
`X(p)`	—	Creates a distribution whose behavior is indistinguishable from that of a distribution newly constructed directly from the values used to construct `p`.	same as `p`'s construction
`u.reset()`	`void`	Subsequent uses of `u` do not depend on values produced by `e` prior to invoking `reset`.	constant
`x.param()`	`P`	Returns a value `p` such that `X(p).param() == p`.	no worse than the complexity of `X(p)`
`u.param(p)`	`void`	post: `u.param() == p`.	no worse than the complexity of `X(p)`

expression	return type	pre/post-condition	complexity
`u(e)`	`T`	With `p` = `u.param()`, the sequence of numbers returned by successive invocations with the same object `e` is randomly distributed according to the associated $p(z \mid \{\texttt{p}\})$ or $P(z_i \mid \{\texttt{p}\})$ function.	amortized constant number of invocations of `e`
`u(e,p)`	`T`	The sequence of numbers returned by successive invocations with the same objects `e` and `p` is randomly distributed according to the associated $p(z \mid \{\texttt{p}\})$ or $P(z_i \mid \{\texttt{p}\})$ function.	—
`x.min()`	`T`	Returns `glb`.	constant
`x.max()`	`T`	Returns `lub`.	constant
`os << x`	reference to the type of `os`	Writes to `os` a textual representation for the parameters and the additional internal data of `x`. post: The `os`.*fmtflags* and fill character are unchanged.	—
`is >> u`	reference to the type of `is`	Restores from `is` the parameters and additional internal data of `u`. If bad input is encountered, ensures that `u` is unchanged by the operation and calls `is.setstate(ios::failbit)` (which may throw `ios::failure` [lib.iostate.flags]). pre: `is` provides a textual representation that was previously written using an `os` whose imbued locale and whose type's template specialization arguments `charT` and `traits` were the same as those of `is`. post: The `is`.*fmtflags* are unchanged.	—

3 `X` shall satisfy the requirements of `CopyConstructible` [lib.copyconstructible] and `Assignable` [lib.container.requirements].

4 The sequence of numbers produced by repeated invocations of `x(e)` shall be independent of any invocation of `os << x` or of any `const` member function of `X` between any of the invocations `x(e)`.

5 If a textual representation is written using `os << x` and that representation is restored into the same or a different object `y` of the same type using `is >> y`, repeated invocations of `y(e)` shall produce the same sequence of numbers as would repeated invocations of `x(e)`.

6 It is unspecified whether `X::param_type` is declared as a (nested) `class` or via a `typedef`. In this subclause 26.4, declarations of `X::param_type` are in the form of `typedef`s only for convenience of exposition.

7 `P` shall satisfy the requirements of `CopyConstructible`, `Assignable`, and `EqualityComparable` [lib.equalitycomparable].

8 For each of the constructors of `X` taking arguments corresponding to parameters of the distribution, `P` shall have a corresponding constructor subject to the same requirements and taking arguments identical in number, type, and default values. Moreover, for each of the member functions of `X` that return values corresponding to parameters of the distribution, `P` shall have a corresponding member function with the identical name, type, and semantics.

9 `P` shall have a declaration of the form

```
typedef X distribution_type;
```

26.4.2 Header `<random>` synopsis [lib.rand.synopsis]

```
namespace std {
  // [26.4.3.1] Class template linear_congruential_engine
  template <class UIntType, UIntType a, UIntType c, UIntType m>
    class linear_congruential_engine;

  // [26.4.3.2] Class template mersenne_twister_engine
  template <class UIntType, size_t w, size_t n, size_t m, size_t r,
            UIntType a, size_t u, size_t s,
            UIntType b, size_t t,
            UIntType c, size_t l>
    class mersenne_twister_engine;

  // [26.4.3.3] Class template subtract_with_carry_engine
  template <class UIntType, size_t w}, size_t s, size_t r>
    class subtract_with_carry_engine;

  // [26.4.4.1] Class template discard_block_engine
  template <class Engine, size_t p, size_t r>
    class discard_block_engine;

  // [26.4.4.2] Class template randomindependent_bits_engine
  template <class Engine, size_t w, class UIntType>
    class randomindependent_bits_engine;

  // [26.4.4.3] Class template shuffle_order_engine
  template <class Engine, size_t k>
    class shuffle_order_engine;

  // [26.4.4.4] Class template xor_combine_engine
  template <class Engine1, size_t s1, class Engine2, size_t s2=0u>
    class xor_combine_engine;

  // [26.4.5] Engines and engine adaptors with predefined parameters
  typedef see below minstd_rand0;
```

```
typedef see below minstd_rand;
typedef see below mt19937;
typedef see below ranlux24_base;
typedef see below ranlux48_base;
typedef see below ranlux24;
typedef see below ranlux48;
typedef see below knuth_b;

// [26.4.6] Class random_device
class random_device;

// [26.4.7.1] Class seed_seq
class seed_seq;

// [26.4.7.2] Function template generate_canonical
template<class ~~result_type~~RealType, class UniformRandomNumberGenerator, size_t bits>
  result_type generate_canonical(UniformRandomNumberGenerator& g);

// [26.4.8.1.1] Class template uniform_int_distribution
template <class IntType = int>
  class uniform_int_distribution;

// [26.4.8.1.2] Class template uniform_real_distribution
template <class RealType = double>
  class uniform_real_distribution;

// [26.4.8.2.1] Class bernoulli_distribution
class bernoulli_distribution;

// [26.4.8.2.2] Class template binomial_distribution
template <class IntType = int>
  class binomial_distribution;

// [26.4.8.2.3] Class template geometric_distribution
template <class IntType = int>
  class geometric_distribution;

// [26.4.8.2.4] Class template negative_binomial_distribution
template <class IntType = int>
  class negative_binomial_distribution;

// [26.4.8.3.1] Class template poisson_distribution
template <class IntType = int>
  class poisson_distribution;

// [26.4.8.3.2] Class template exponential_distribution
template <class RealType = double>
  class exponential_distribution;

// [26.4.8.3.3] Class template gamma_distribution
```

```
  template <class RealType = double>
    class gamma_distribution;

  // [26.4.8.3.4] Class template weibull_distribution
  template <class RealType = double>
    class weibull_distribution;

  // [26.4.8.3.5] Class template extreme_value_distribution
  template <class RealType = double>
    class extreme_value_distribution;

  // [26.4.8.4.1] Class template normal_distribution
  template <class RealType = double>
    class normal_distribution;

  // [26.4.8.4.2] Class template lognormal_distribution
  template <class RealType = double>
    class lognormal_distbution;

  // [26.4.8.4.3] Class template chi_squared_distribution
  template <class RealType = double>
    class chi_squared_distribution;

  // [26.4.8.4.4] Class template cauchy_distribution
  template <class RealType = double>
    class cauchy_distribution;

  // [26.4.8.4.5] Class template fisher_f_distribution
  template <class RealType = double>
    class fisher_f_distribution;

  // [26.4.8.4.6] Class template student_t_distribution
  template <class RealType = double>
    class student_t_distribution;

  // [26.4.8.5.1] Class template discrete_distribution
  template <class IntType = int>
    class discrete_distribution;

  // [26.4.8.5.2] Class template piecewise_constant_distribution
  template <class RealType = double>
    class piecewise_constant_distribution;

  // [26.4.8.5.3] Class template general_pdf_distribution
  template <class RealType = double>
    class general_pdf_distribution;
} // namespace std
```

26.4.3 Random number engine class templates [lib.rand.eng]

1 Except where specified otherwise, the complexity of all functions specified in the following sections is constant.

2 Except as required by table 2, no function described in this section 26.4.3 throws an exception.

3 The class templates specified in this section 26.4.3 satisfy the requirements of random number engine [26.4.1.3]. Descriptions are provided here only for operations on the engines that are not described in those requirements or for operations where there is additional semantic information. Declarations for copy constructors, for copy assignment operators, ~~for the bits_of_randomness member,~~ and for equality and inequality operators are not shown in the synopses.

26.4.3.1 Class template linear_congruential_engine [lib.rand.eng.lcong]

1 A linear_congruential_engine random number engine produces unsigned integer random numbers. The state x_i of a linear_congruential_engine object x is of size 1 and consists of a single integer. The transition algorithm is a modular linear function of the form $\mathsf{TA}(x_i) = (a \cdot x_i + c) \bmod m$; the generation algorithm is $\mathsf{GA}(x_i) = x_{i+1}$.

```
template <class UIntType, UIntType a, UIntType c, UIntType m>
class linear_congruential_engine
{
public:
  // types
  typedef UIntType result_type;

  // engine characteristics
  static const result_type multiplier = a;
  static const result_type increment = c;
  static const result_type modulus = m;
  static const result_type min = c == 0u ? 1u: 0u;
  static const result_type max = m - 1u ;
  static const result_type default_seed = 1u;

  // constructors and seeding functions
  explicit linear_congruential_engine(result_type s = default_seed);
  explicit linear_congruential_engine(seed_seq& q);
  void seed(result_type s = default_seed);
  void seed(seed_seq& q);

  // generating functions
  result_type operator()();
  void discard(~~size_t~~unsigned long long z);
};
```

2 The template parameter UIntType shall denote an unsigned integral type large enough to store values as large as $m-1$. If the template parameterm is 0, the modulus m used throughout this section 26.4.3.1 is numeric_limits<result_type>::max() plus 1. [*Note:* The result need not be representable as a value of type result_type. — *end note*] Otherwise, the following relations shall hold: a < m and c < m.

3 The textual representation consists of the value of x_i.

```
explicit linear_congruential_engine(result_type s = default_seed);
```

4 *Effects:* Constructs a `linear_congruential_engine` object. If $c \bmod m$ is 0 and `s` mod m is 0, sets the engine's state to 1, otherwise sets the engine's state to `s` mod m.

```
explicit linear_congruential_engine(seed_seq& q);
```

5 *Effects:* Constructs a `linear_congruential_engine` object. With $k = \left\lceil \frac{\log_2 m}{32} \right\rceil$ and a an array (or equivalent) of length $k+3$, invokes `q.randomize(`$a+0$`, `$a+k+3$`)` and then computes $S = \left(\sum_{j=0}^{k-1} a_{j+3} \cdot 2^{32j} \right) \bmod m$. If $c \bmod m$ is 0 and S is 0, sets the engine's state to 1, else sets the engine's state to S.

26.4.3.2 Class template `mersenne_twister_engine` [lib.rand.eng.mers]

1 A `mersenne_twister_engine` random number engine[3] produces unsigned integer random numbers in the closed interval $[0, 2^w - 1]$. The state $\mathtt{x}_i$ of a `mersenne_twister_engine` object `x` is of size n and consists of a sequence X of n values of the type delivered by `x`; all subscripts applied to X are to be taken modulo n.

2 The transition algorithm employs a twisted generalized feedback shift register defined by shift values n and m, a twist value r, and a conditional xor-mask a. To improve the uniformity of the result, the bits of the raw shift register are additionally *tempered* (*i.e.*, scrambled) according to a bit-scrambling matrix defined by values u, s, b, t, c, and ℓ.

The state transition is performed as follows:

a) Concatenate the upper $w - r$ bits of X_{i-n} with the lower r bits of X_{i+1-n} to obtain an unsigned integer value Y.

b) With $\alpha = a \cdot (Y \mathbin{\mathsf{bitand}} 1)$, set X_i to $X_{i+m-n} \mathbin{\mathsf{xor}} (Y \mathbin{\mathsf{rshift}} 1) \mathbin{\mathsf{xor}} \alpha$.

3 The generation algorithm determines the unsigned integer values z_1, z_2, z_3, z_4 as follows, then delivers z_4 as its result:

a) Let $z_1 = X_i \mathbin{\mathsf{xor}} (X_i \mathbin{\mathsf{rshift}} u)$.

b) Let $z_2 = z_1 \mathbin{\mathsf{xor}} \big((z_1 \mathbin{\mathsf{lshift}}_w s) \mathbin{\mathsf{bitand}} b \big)$.

c) Let $z_3 = z_2 \mathbin{\mathsf{xor}} \big((z_2 \mathbin{\mathsf{lshift}}_w t) \mathbin{\mathsf{bitand}} c \big)$.

d) Let $z_4 = z_3 \mathbin{\mathsf{xor}} (z_3 \mathbin{\mathsf{rshift}} \ell)$.

```
  template <class UIntType, size_t w, size_t n, size_t m, size_t r,
            UIntType a, size_t u, size_t s,
            UIntType b, size_t t,
            UIntType c, size_t l>
class mersenne_twister_engine
{
public:
  // types
  typedef UIntType} result_type;

  // engine characteristics
  static const size_t word_size = w;
  static const size_t state_size = n;
  static const size_t shift_size = m;
```

[3] The name of this engine refers, in part, to a property of its period: For properly-selected values of the parameters, the period is closely related to a large Mersenne prime number.

```
    static const size_t mask_bits = r;
    static const UIntType xor_mask = a;
    static const size_t tempering_u = u;
    static const size_t tempering_s = s;
    static const UIntType tempering_b = b;
    static const size_t tempering_t = t;
    static const UIntType tempering_c = c;
    static const size_t tempering_l = l;
    static const result_type min = 0;
    static const result_type max = 2^w − 1;
    static const result_type default_seed = 5489u;

    // constructors and seeding functions
    explicit mersenne_twister_engine(result_type value = default_seed);
    explicit mersenne_twister_engine(seed_seq& q);
    void seed(result_type value = default_seed);
    void seed(seed_seq& q);

    // generating functions
    result_type operator()();
    void discard(size_tunsigned long long z);
  };
```

4 The following relations shall hold: $1 \leq$ `m` $\leq$ `n`; $0 \leq$ `r`,`u`,`s`,`t`,`l` $\leq$ `w` $\leq$ `numeric_limits<result_type>::digits`; $0 \leq$ `a`,`b`,`c` $\leq 2^{\mathtt{w}} - 1$.

5 The textual representation of $\mathtt{x}_i$ consists of the values of $X_{i-n}, \ldots, X_{i-1}$, in that order.

`explicit mersenne_twister_engine(result_type value = default_seed);`

6 *Effects:* Constructs a `mersenne_twister_engine` object. Sets X_{-n} to `value` mod 2^w. Then, iteratively for $i = 1-n, \ldots, -1$, sets X_i to

$$\left[1812433253 \cdot \left(X_{i-1} \,\mathsf{xor}\, (X_{i-1} \,\mathsf{rshift}\, (w-2))\right) + i \bmod n\right] \bmod 2^w \,.$$

7 *Complexity:* $\mathscr{O}(\mathrm{n})$.

`explicit mersenne_twister_engine(seed_seq& q);`

8 *Effects:* Constructs a `mersenne_twister_engine` object. With $k = \lceil w/32 \rceil$ and a an array (or equivalent) of length $n \cdot k$, invokes `q.randomize(`$a+0$`,` $a+n\cdot k$`)` and then, iteratively for $i = -n, \ldots, -1$, sets X_i to $\left(\sum_{j=0}^{k-1} a_{k(i+n)+j} \cdot 2^{32j}\right) \bmod 2^w$. Finally, if the most significant $w-r$ bits of X_{-n} are zero, and if each of the other resulting X_i is 0, changes X_{-n} to 2^{w-1}.

26.4.3.3 Class template `subtract_with_carry_engine` [lib.rand.eng.sub]

1 A `subtract_with_carry_engine` random number engine produces unsigned integer random numbers.

2 The state $\mathtt{x}_i$ of a `subtract_with_carry_engine` object `x` is of size $\mathscr{O}(\mathrm{r})$, and consists of a sequence X of r integer values $0 \le X_i < m = 2^w$; all subscripts applied to X are to be taken modulo r. The state $\mathtt{x}_i$ additionally consists of an integer c (known as the *carry*) whose value is either 0 or 1.

3 The state transition is performed as follows:

a) Let $Y = X_{i-s} - X_{i-r} - c$.

b) Set X_i to $y = Y \bmod m$. Set c to 1 if $Y < 0$, otherwise set c to 0.

[*Note:* This algorithm corresponds to a modular linear function of the form $\mathsf{TA}(\mathtt{x}_i) = (a \cdot \mathtt{x}_i) \bmod b$, where b is of the form $m^r - m^s + 1$ and $a = b - (b-1)/m$. *— end note*]

4 The generation algorithm is given by $\mathsf{GA}(\mathtt{x}_i) = y$, where y is the value produced as a result of advancing the engine's state as described above.

```
template <class UIntType, size_t w, size_t s, size_t r>
class subtract_with_carry_engine
{
public:
  // types
  typedef UIntType result_type;

  // engine characteristics
  static const size_t word_size = w;
  static const size_t short_lag = s;
  static const size_t long_lag = r;
  static const result_type min = 0;
  static const result_type max = m-1;
  static const result_type default_seed = 19780503u;

  // constructors and seeding functions
  explicit subtract_with_carry_engine(result_type value = default_seed);
  explicit subtract_with_carry_engine(seed_seq& q);
  void seed(result_type value = default_seed);
  void seed(seed_seq& q);

  // generating functions
  result_type operator()();
  void discard(~~size_t~~unsigned long long z);
};
```

5 The following relations shall hold: $0 <$ `s` $<$ `r`, and $0 <$ `w` $\le$ `numeric_limits<result_type>::digits`.

6 The textual representation consists of the values of $X_{i-r}, \ldots, X_{i-1}$, in that order, followed by c.

`explicit subtract_with_carry_engine(result_type value = default_seed);`

7 *Effects:* Constructs a `subtract_with_carry_engine` object. Sets the values of $X_{-r}, \ldots, X_{-1}$, in that order, as required below. If X_{-1} is then 0, sets c to 1; otherwise sets c to 0.

8 *Required behavior:* First construct `e`, a `linear_congruential_engine` object, as if by the following definition:

```
linear_congruential_engine<result_type
                           40014u,0u,2147483563u> e(value == 0u ? default_seed : value);
```

To set an X_k, use new values $z_0, \ldots, z_{n-1}$ obtained from n successive invocations of e taken modulo 2^{32}. Set X_k to $\left(\sum_{j=0}^{n-1} z_j \cdot 2^{32j}\right) \bmod m$. If X_{-1} is then 0, sets c to 1; otherwise sets c to 0.

9 *Complexity:* Exactly $n \cdot$ r invocations of e.

```
explicit subtract_with_carry_engine(seed_seq& q);
```

10 *Effects:* Constructs a `subtract_with_carry_engine` object. With $k = \lceil w/32 \rceil$ and a an array (or equivalent) of length $r \cdot k$, invokes `q.randomize(`$a+0$`, `$a+r \cdot k$`)` and then, iteratively for $i = -r, \ldots, -1$, sets X_i to $\left(\sum_{j=0}^{k-1} a_{k(i+r)+j} \cdot 2^{32j}\right) \bmod m$. If X_{-1} is then 0, sets c to 1; otherwise sets c to 0.

26.4.4 Random number engine adaptor class templates [lib.rand.adapt]

1 Except where specified otherwise, the complexity of all functions specified in the following sections is constant.

2 Except as required by table 2, no function described in this section 26.4.4 throws an exception.

3 The class templates specified in this section 26.4.4 satisfy the requirements of random number engine adaptor [26.4.1.4]. Descriptions are provided here only for operations on the engine adaptors that are not described in those requirements or for operations where there is additional semantic information. Declarations for copy constructors, for copy assignment operators, and for equality and inequality operators are not shown in the synopses.

26.4.4.1 Class template `discard_block_engine` [lib.rand.adapt.disc]

1 A `discard_block_engine` random number engine adaptor produces random numbers selected from those produced by some base engine e. The state $\mathtt{x}_i$ of a `discard_block_engine` engine adaptor object x consists of the state $\mathtt{e}_i$ of its base engine e and an additional integer n. The size of the state is the size of e's state plus 1.

2 The transition algorithm discards all but $r > 0$ values from each block of $p \geq r$ values delivered by e. The state transition is performed as follows: If $n \geq r$, advance the state of e from $\mathtt{e}_i$ to $\mathtt{e}_{i+p-r}$ and set n to 0. In any case, then increment n and advance e's then-current state $\mathtt{e}_j$ to $\mathtt{e}_{j+1}$.

3 The generation algorithm yields the value returned by the last invocation of `e()` while advancing e's state as described above.

```
template <class Engine, size_t p, size_t r>
class discard_block_engine
{
public:
  // types
  typedef Engine base_type;
  typedef typename base_type::result_type result_type;

  // engine characteristics
  static const size_t block_size = p;
  static const size_t used_block = r;
  static const result_type min = base_type::min;
```

```
    static const result_type max = base_type::max;

    // constructors and seeding functions
    discard_block_engine();
    explicit discard_block_engine(const base_type& urng);
    explicit discard_block_engine(result_type s);
    explicit discard_block_engine(seed_seq& q);
    void seed();
    void seed(result_type s);
    void seed(seed_seq& q);

    // generating functions
    result_type operator()();
    void discard(~~size_t~~unsigned long long z);

    // property functions
    const base_type& base() const;

  private:
    base_type e;    // exposition only
    int n;          // exposition only
  };
```

4 The following relations shall hold: $1 \leq$ `r` $\leq$ `p`.

5 The textual representation consists of the textual representation of `e` followed by the value of `n`.

6 In addition to its behavior pursuant to section 26.4.1.4, each constructor that is not a copy constructor sets `n` to 0.

26.4.4.2 Class template `independent_bits_engine` [lib.rand.adapt.ibits]

1 An ~~`random`~~`independent_bits_engine` random number engine adaptor combines random numbers that are produced by some base engine e, so as to produce random numbers with a specified number of bits w. The state x_i of an ~~`random`~~`independent_bits_engine` engine adaptor object `x` consists of the state e_i of its base engine `e`; the size of the state is the size of e's state.

2 ~~With~~The transition and generation algorithms are described in terms of the following integral constants:

a) Let $R =$ `e.max - e.min + 1` and $m = \lfloor \log_2 R \rfloor$~~,~~.

b) With n as determined below, let $w_0 = \lfloor w/n \rfloor$, $n_0 = n - w \bmod n$, $y_0 = 2^{w_0} \lfloor R/2^{w_0} \rfloor$, and $y_1 = 2^{w_0+1} \lfloor R/2^{w_0+1} \rfloor$.

c) Let $n = \lceil w/m \rceil$ if and only if the relation $R - y_0 \leq \lfloor y_0/n \rfloor$ holds as a result. Otherwise let $n = 1 + \lceil w/m \rceil$.

[*Note:* The relation $w = n_0 w_0 + (n - n_0)(w_0 + 1)$ always holds. — *end note*]

3 ~~t~~The transition algorithm is carried out by invoking `e()` as often as needed to obtain ~~$k = \lceil w/m \rceil$~~ n_0 values less than ~~2^m~~ y_0 + `e.min` and $n - n_0$ values less than $y_1 +$ `e.min`.

4 The generation algorithm uses the values produced while advancing the state as described above to yield a ~~`result_type`~~ quantity S obtained as if by the following algorithm:

```
  S = 0;
```

```
for (k = 0; k ≠ n_0; k += 1) {
  do u = e() - e.min; while (u ≥ y_0);
  S = 2^{w_0} · S + u mod 2^{w_0};
}
for (k = n_0; k ≠ n; k += 1) {
  do u = e() - e.min; while (u ≥ y_1);
  S = 2^{w_0+1} · S + u mod 2^{w_0+1};
}
```

```
template <class Engine, size_t w, class UIntType>
class ~~random~~independent_bits_engine
{
public:
  // types
  typedef Engine base_type;
  typedef UIntType result_type;

  // engine characteristics
  static const result_type min = 0;
  static const result_type max = 2^w - 1;

  // constructors and seeding functions
  ~~random~~independent_bits_engine();
  explicit ~~random~~independent_bits_engine(const base_type& urng);
  explicit ~~random~~independent_bits_engine(result_type s);
  explicit ~~random~~independent_bits_engine(seed_seq& q);
  void seed();
  void seed(result_type s);
  void seed(seed_seq& q);

  // generating functions
  result_type operator()();
  void discard(~~size_t~~unsigned long long z);

  // property functions
  const base_type& base() const;

private:
  base_type e;    // exposition only
};
```

5 The following relations shall hold: $0 < w \leq$ `numeric_limits<result_type>::digits`. ~~Additionally, `numeric_limits<base_type::result_type>::digits` ≤ `numeric_limits<result_type>::digits` shall hold.~~

6 The textual representation consists of the textual representation of `e`.

26.4.4.3 Class template `shuffle_order_engine` [lib.rand.adapt.shuf]

1 A `shuffle_order_engine` random number engine adaptor produces the same random numbers that are produced by some base engine e, but delivers them in a different sequence. The state $\mathtt{x}_i$ of a `shuffle_order_engine` engine adaptor object `x` consists of the state $\mathtt{e}_i$ of its base engine `e`, an additional value Y of the type delivered by `e`, and an additional sequence V of k values also of the type delivered by `e`. The size of the state is the size of e's state plus $k+1$.

2 The transition algorithm permutes the values produced by e. The state transition is performed as follows:

a) Calculate an integer j as $\left\lfloor \frac{k \cdot (Y - b_{\min})}{b_{\max} - b_{\min} + 1} \right\rfloor$~~, if e is integer-valued, or as $\lfloor k \cdot Y \rfloor$, if e is real-valued~~.

b) Set Y to V_j and then set V_j to `b()`.

3 The generation algorithm yields the last value of `Y` produced while advancing `e`'s state as described above.

```
template <class Engine, size_t k>
class shuffle_order_engine
{
public:
  // types
  typedef Engine base_type;
  typedef typename base_type::result_type result_type;

  // engine characteristics
  static const size_t table_size = k;
  static const result_type min = base_type::min;
  static const result_type max = base_type::max;

  // constructors and seeding functions
  shuffle_order_engine();
  explicit shuffle_order_engine(const base_type& urng);
  explicit shuffle_order_engine(result_type s);
  explicit shuffle_order_engine(seed_seq& q);
  void seed();
  void seed(result_type s);
  void seed(seed_seq& q);

  // generating functions
  result_type operator()();
  void discard(size_tunsigned long long z);

  // property functions
  const base_type& base() const;

private:
  base_type e;          // exposition only
  result_type Y;        // exposition only
  result_type V[k];     // exposition only
};
```

4 The following relation shall hold: $1 \leq \mathtt{k}$.

5 The textual representation consists of the textual representation of `e`, followed by the `k` values of V, followed by the value of Y.

6 In addition to its behavior pursuant to section 26.4.1.4, each constructor that is not a copy constructor initializes `V[0]`, ..., `V[k-1]` and Y, in that order, with values returned by successive invocations of `e()`.

26.4.4.4 Class template `xor_combine_engine` [lib.rand.adapt.xor]

1 An `xor_combine_engine` random number engine adaptor produces random numbers from two integer-valued base engines `e1` and `e2` by merging their left-shifted random values via bitwise exclusive-or. The state $\mathtt{x}_i$ of an `xor_combine_engine` engine adaptor object `x` consists of the states $\mathtt{e1}_i$ and $\mathtt{e2}_i$ of its base engines. The size of the state is the size of the state of `e1` plus the size of the state of `e2`.

2 The transition algorithm advances, in turn, the state of each base engine.

3 The generation algorithm is $\mathsf{GA}(\mathtt{x}_i) = (v_1 \mathbin{\mathsf{lshift}_w} \mathtt{s1}) \mathbin{\mathsf{xor}} (v_2 \mathbin{\mathsf{lshift}_w} \mathtt{s2})$, where w denotes the value of `numeric_limits<result_type>::digits` and v_1 and v_2, respectively, denote the values of `(e1()-e1.min)` and `(e2()-e2.min)`.

```
template <class Engine1, size_t s1, class Engine2, size_t s2=0u>
class xor_combine_engine
{
public:
  // types
  typedef Engine1 base1_type;
  typedef Engine2 base2_type;
  typedef see below result_type;

  // engine characteristics
  static const size_t shift1 = s1;
  static const size_t shift2 = s2;
  static const result_type min = 0;
  static const result_type max = see below;

  // constructors and seed functions
  xor_combine_engine();
  xor_combine_engine(const base1_type & urng1, const base2_type & urng2);
  xor_combine_engine(result_type s);
  explicit xor_combine_engine(seed_seq& q);
  void seed();
  void seed(result_type s);
  void seed(seed_seq& q);

  // generating functions
  result_type operator()();
  void discard(~~size_t~~unsigned long long z);

  // property functions
  const base1_type& base1() const;
  const base2_type& base2() const;
```

```
  private:
    base1_type e1;    // exposition only
    base2_type e2;    // exposition only
  };
```

4 The following relations shall hold: $\texttt{s1} \geq \texttt{s2} \geq 0$.

5 [*Note:* An `xor_combine_engine` engine adaptor that fails to observe the following recommendations may have significantly worse uniformity properties than either of the base engines it is based on:

a) While two shift values (template parameters `s1` and `s2`) are provided for simplicity of interface, it is advisable that `s2` be zero. (If `s2` is non-zero then the low bits will always be 0.)

b) It is also advisable for `e2`'s `max` to be $2^n - 1 - \texttt{min}$ for some non-negative integer n, and for the shift value `s1` to be no greater than that n.

— *end note*]

6 Both `Engine1::result_type` and `Engine2::result_type` shall denote (possibly different) unsigned integral types. The member `result_type` shall denote either the type `Engine1::result_type` or the type `Engine2::result_type`, whichever provides the most storage according to clause [basic.fundamental].

7 With

a) $m_1 = min(\texttt{Engine1::max} - \texttt{Engine1::min}, 2^{w-\texttt{s1}} - 1)$,

b) $m_2 = min(\texttt{Engine2::max} - \texttt{Engine2::min}, 2^{w-\texttt{s2}} - 1)$, and

c) $s = \texttt{s1} - \texttt{s2}$,

the value of the member `max` is $M(m_1, m_2, s)$ lshift_w `s2`, where $M(a,b,d)$ is defined as follows:

If $a = 0$ or $b < 2^d$, define $M(a,b,d)$ as $a \cdot 2^d + b$.

Otherwise, let t and u denote the greater and the lesser, respectively, of $a \cdot 2^d$ and b. With $p = \lfloor \log_2 u \rfloor$, if $k = \lfloor t/2^p \rfloor$ is odd, define $M(a,b,d)$ as $(k+1) \cdot 2^p - 1$.

Otherwise, if $a \cdot 2^d \geq b$, define $M(a,b,d)$ as $(k+1) \cdot 2^p + M\left((t \bmod 2^p)/2^d, u \bmod 2^p, d\right)$.

Otherwise, define $M(a,b,d)$ as $(k+1) \cdot 2^p + M\left((u \bmod 2^p)/2^d, t \bmod 2^p, d\right)$.

8 The textual representation consists of the textual representation of `e1` followed by the textual representation of `e2`.

26.4.5 Engines and engine adaptors with predefined parameters [lib.rand.predef]

```
typedef linear_congruential_engine<uint_fast32_t, 16807, 0, 2147483647>
        minstd_rand0;
```

1 *Required behavior:* The 10000^{th} consecutive invocation of a default-constructed object of type `minstd_rand0` shall produce the value 1043618065.

```
typedef linear_congruential_engine<uint_fast32_t, 48271, 0, 2147483647>
        minstd_rand;
```

2 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `minstd_rand` shall produce the value 399268537.

```
typedef mersenne_twister_engine<uint_fast32_t,
                                32,624,397,31,0x9908b0df,11,7,0x9d2c5680,15,0xefc60000,18>
        mt19937;
```

3 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `mt19937` shall produce the value 4123659995.

```
typedef subtract_with_carry_01_engine<uint_fast32_t, 24, 10, 24>
        ranlux24_base;
```

4 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `ranlux24_base` shall produce the value 7937952.

```
typedef subtract_with_carry_01_engine<uint_fast64_t, 48, 5, 12>
        ranlux48_base;
```

5 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `ranlux48_base` shall produce the value 61839128582725.

```
typedef discard_block_engine<ranlux24_base, 223, 23>
        ranlux24;
```

6 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `ranlux24` shall produce the value 9901578.

```
typedef discard_block_engine<ranlux48_base, 389, 11>
        ranlux48
```

7 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `ranlux48` shall produce the value 249142670248501.

```
typedef shuffle_order_engine<minstd_rand0,256>
        knuth_b;
```

8 *Required behavior:* The 10000$^{\text{th}}$ consecutive invocation of a default-constructed object of type `knuth_b` shall produce the value 1112339016.

26.4.6 Class `random_device` [lib.rand.device]

1 A `random_device` uniform random number generator produces non-deterministic random numbers. It satisfies the requirements of uniform random number generator [26.4.1.2].

2 If implementation limitations prevent generating non-deterministic random numbers, the implementation may employ a random number engine.

```
class random_device
{
public:
  // types
```

```
    typedef unsigned int result_type;

    // generator characteristics
    static const result_type min = see below;
    static const result_type max = see below;

    // constructors
    explicit random_device(const string& token = implementation-defined);

    // generating functions
    result_type operator()();

    // property functions
    double entropy() const;

  private:
    random_device(const random_device& );
    void operator=(const random_device& );
  };
```

3 The values of the `min` and `max` members are identical to the values returned by `numeric_limits<result_type>::min()` and `numeric_limits<result_type>::max()`, respectively.

```
explicit random_device(const string& token = implementation-defined);
```

4 *Effects:* Constructs a `random_device` non-deterministic uniform random number generator object. The semantics and default value of the `token` parameter are implementation-defined.[4)]

5 *Throws:* A value of an implementation-defined type derived from `exception` if the `random_device` could not be initialized.

```
double entropy() const;
```

6 *Returns:* If the implementation employs a random number engine, returns 0.0. Otherwise, returns an entropy estimate[5)] for the random numbers returned by `operator()`, in the range $\texttt{min}\cancel{()}$ to $\log_2(\texttt{max}\cancel{()}+1)$.

7 *Throws:* Nothing.

```
result_type operator()();
```

8 *Returns:* A non-deterministic random value, uniformly distributed between `min` and `max`, inclusive. It is implementation-defined how these values are generated.

9 *Throws:* A value of an implementation-defined type derived from `exception` if a random number could not be obtained.

[4)] The parameter is intended to allow an implementation to differentiate between different sources of randomness.

[5)] If a device has n states whose respective probabilities are $P_0, \ldots, P_{n-1}$, the device entropy S is defined as $S = -\sum_{i=0}^{n-1} P_i \cdot \log P_i$.

26.4.7 Utilities [lib.rand.util]

26.4.7.1 Class seed_seq [lib.rand.util.seedseq]

1 An object of type seed_seq consumes a sequence of integer-valued data and produces a fixed number of unsigned integer values, $0 \le i < 2^{32}$, based on the consumed data. [*Note:* Such an object provides a mechanism to avoid replication of streams of random variates. This can be useful in applications requiring large numbers of random number engines. — *end note*]

2 In addition to the requirements set forth below, instances of seed_seq shall meet the requirements of CopyConstructible [lib.copyconstructible] and of Assignable [lib.container.requirements].

```
class seed_seq
{
public:
  // types
  typedef uint_least32_t result_type;

  // constructors and reset functions
  seed_seq();
  template<class InputIterator> seed_seq(InputIterator begin, InputIterator end);

  // generating functions
  template<class RandomAccessIterator>
    void randomize(RandomAccessIterator begin, RandomAccessIterator end) const;

  // property functions
  size_t size() const;
  template<class OutputIterator> void get_seeds(OutputIterator dest) const;

private:
  vector<result_type> v;   // exposition only
};
```

```
explicit seed_seq();
```

3 *Effects:* Constructs a seed_seq object as if by default-constructing its member v.

4 *Throws:* Nothing.

```
template<class InputIterator> seed_seq(InputIterator begin, InputIterator end);
```

5 *Requires:* InputIterator shall satisfy the requirements of an input iterator [lib.input.iterator] such that iterator_traits<InputIterator>::value_type shall denote an integral type.

6 *Effects:* Constructs a seed_seq object by rearranging the bits of the supplied sequence [begin,end) into 32-bit units, as if by first concatenating all the *n* bits that make up the supplied sequence to initialize a single (possibly very large) unsigned binary number, *b*, and then carrying out the following algorithm:

```
for( v.clear(); n > 0; n -= 32 )
  v.push_back(b mod 2^32), b /= 2^32;
```

```
template<class RandomAccessIterator>
void randomize(RandomAccessIterator begin, RandomAccessIterator end) const;
```

7 *Requires:* RandomAccessIterator shall meet the requirements of a random access iterator [lib.random.access.iterators] such that iterator_traits<RandomAccessIterator>::value_type shall denote an unsigned integral type capable of accommodating 32-bit quantities.

8 *Effects:* With $s = \texttt{v.size()}$ and $n = \texttt{end} - \texttt{begin}$, fills the supplied range $[\texttt{begin}, \texttt{end})$ according to the following algorithm[6] in which each operation is to be carried out modulo 2^{32}, each indexing operator applied to begin is to be taken modulo n, each indexing operator applied to v is to be taken modulo s, and $T(x)$ is defined as $x\,\mathsf{xor}\,(x\,\mathsf{rshift}\,30)$:

a) Set begin[0] to $5489 + s$. Then, iteratively for $k = 1, \ldots, n-1$, set begin[k] to

$$1812433253 \cdot T(\texttt{begin[k-1]}) + k\,.$$

b) With m as the larger of s and n, transform each element of the range (possibly more than once): iteratively for $k = 0, \ldots, m-1$, set begin[k] to

$$(\texttt{begin[k]}\ \mathsf{xor}\ (1664525 \cdot T(\texttt{begin[k-1]}))) + \texttt{v[k]} + (k \bmod s)\ .$$

c) Transform each element of the range one last time, beginning where the previous step ended: iteratively for $k = m \bmod n, \ldots, n-1, 0, \ldots, (m-1) \bmod n$, set begin[k] to

$$(\texttt{begin[k]}\ \mathsf{xor}\ (1566083941 \cdot T(\texttt{begin[k-1]}))) - k\,.$$

9 *Throws:* Nothing.

```
size_t size() const;
```

10 *Returns:* The number of 32-bit units the object can deliver, as if by returning the result of v.size().

```
template<class OutputIterator> void get_seeds(OutputIterator dest) const;
```

11 *Requires:* OutputIterator shall satisfy the requirements of an output iterator [lib.output.iterator] such that iterator_traits<OutputIterator>::value_type shall be assignable from result_type.

12 *Effects:* Copies the sequence of prepared 32-bit units to the given destination, as if by executing the following statement:

```
copy(v.begin(), v.end(), dest);
```

26.4.7.2 Function template generate_canonical [lib.rand.util.canonical]

1 Each function instantiated from the template described in this section 26.4.7.2 maps the result of one or more invocations of a supplied uniform random number generator g to one member of the specified ~~result_type~~RealType such that, if the values g_i produced by g are uniformly distributed, the instantiation's results t_j, $0 \leq t_j < 1$, are distributed as uniformly as possible as specified below.

[6] ~~This algorithm is due to Dr. Makoto Matsumoto, with an improvement (approved by Dr. Matsumoto) suggested by Dr. Charles Karney.~~

2 [*Note:* Obtaining a value in this way can be a useful step in the process of transforming a value generated by a uniform random number generator into a value that can be delivered by a random number distribution. — *end note*]

3 ~~With ε as the value of `numeric_limits<result_type>::epsilon()`,~~

a) ~~If `result_type` is a floating-point type [basic.fundamental], $\varepsilon \leq t_j \leq 1-\varepsilon$.~~

b) ~~If `result_type` is a signed or unsigned integral type [basic.fundamental], `numeric_limits<result_type>::min()` $\leq t_j \leq$ `numeric_limits<result_type>::max()`.~~

```
template<class result_typeRealType, class UniformRandomNumberGenerator, size_t bits=1u>
result_typeRealType generate_canonical(UniformRandomNumberGenerator& g);
```

4 *Complexity:* Exactly $k = \max(1, \lceil b/\log_2 R \rceil)$ invocations of `g`, where b[7] is the lesser of `numeric_limits<~~result_type~~RealType>::digits` and `bits` ~~(but not less than one)~~, and R is the value of `g.max - g.min + 1`.

5 *Required behavior:* Invokes `g()` k times to obtain values $g_0, \ldots, g_{k-1}$, respectively. Calculates a quantity

$$S = \sum_{i=0}^{k-1} (g_i - \texttt{g.min}) \cdot R^i$$

using arithmetic of type ~~`result_type`~~`RealType`~~, if floating-point, otherwise using exact arithmetic~~.

6 *Returns:* ~~With ε as above, and with M as the value of $1+$ `numeric_limits<result_type>::max()`, either [...], if `result_type` is real-valued, or [...], otherwise~~ S/R^k.

7 *Throws:* What and when `g` throws.

26.4.8 Random number distribution class templates [lib.rand.dist]

1 The classes and class templates specified in this section 26.4.8 satisfy all the requirements of random number distribution [26.4.1.5]. Descriptions are provided here only for operations on the distributions that are not described in those requirements or for operations where there is additional semantic information. Declarations for copy constructors, for copy assignment operators, and for equality and inequality operators are not shown in the synopses.

2 The algorithms for producing each of the specified distributions are implementation-defined.

3 The value of each probability density function $p(z)$ and of each discrete probability function $P(z_i)$ specified in this section is 0 everywhere outside its stated domain.

26.4.8.1 Uniform distributions [lib.rand.dist.uni]

26.4.8.1.1 Class template `uniform_int_distribution` [lib.rand.dist.uni.int]

1 A `uniform_int_distribution` random number distribution produces random integers i, $a \leq i \leq b$, distributed according to the constant discrete probability function

$$P(i \mid a, b) = 1/(b-a+1) .$$

[7] b is introduced to avoid any attempt to produce more bits of randomness than can be held in ~~the `result_type`~~`RealType`.

```
template <class IntType = int>
class uniform_int_distribution
{
public:
  // types
  typedef IntType result_type;
  typedef unspecified param_type;

  // constructors and reset functions
  explicit uniform_int_distribution(IntType a = 0, IntType b = numeric_limits<IntType>::max());
  explicit uniform_int_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  result_type a() const;
  result_type b() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

`explicit uniform_int_distribution(IntType a = 0, IntType b = numeric_limits<IntType>::max());`

2 *Requires:* `a` $\leq$ `b`.

3 *Effects:* Constructs a `uniform_int_distribution` object; `a` and `b` correspond to the respective parameters of the distribution.

`result_type a() const;`

4 *Returns:* The value of the `a` parameter with which the object was constructed.

`result_type b() const;`

5 *Returns:* The value of the `b` parameter with which the object was constructed.

26.4.8.1.2 Class template `uniform_real_distribution` [lib.rand.dist.uni.real]

1 A `uniform_real_distribution` random number distribution produces random numbers x, $a \cancel{<}\leq x < b$, distributed according to the constant probability density function

$$p(x\,|\,a,b) = 1/(b-a)\ .$$

```
template <class RealType = double>
class uniform_real_distribution
{
public:
  // types
  typedef RealType result_type;
  typedef unspecified param_type;

  // constructors and reset functions
  explicit uniform_real_distribution(RealType a = 0.0, RealType b = 1.0);
  explicit uniform_real_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  result_type a() const;
  result_type b() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

`explicit uniform_real_distribution(RealType a = 0.0, RealType b = 1.0);`

2 *Requires:* $\mathtt{a} \leq \mathtt{b}$ and $\mathtt{b} - \mathtt{a} \leq$ `numeric_limits<RealType>::max()`.

3 *Effects:* Constructs a `uniform_real_distribution` object; `a` and `b` correspond to the respective parameters of the distribution.

`result_type a() const;`

4 *Returns:* The value of the `a` parameter with which the object was constructed.

`result_type b() const;`

5 *Returns:* The value of the `b` parameter with which the object was constructed.

26.4.8.2 Bernoulli distributions [lib.rand.dist.bern]

26.4.8.2.1 Class `bernoulli_distribution` [lib.rand.dist.bern.bernoulli]

1 A `bernoulli_distribution` random number distribution produces `bool` values b distributed according to the discrete probability function

$$P(b\,|\,p) = \begin{cases} p & \text{if} \quad b = \mathtt{true} \\ 1-p & \text{if} \quad b = \mathtt{false} \end{cases} .$$

```
class bernoulli_distribution
{
public:
  // types
  typedef bool result_type;
  typedef unspecified param_type;

  // constructors and reset functions
  explicit bernoulli_distribution(double p = 0.5);
  explicit bernoulli_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  double p() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

`explicit bernoulli_distribution(double p = 0.5);`

2 *Requires:* $0 \leq \texttt{p} \leq 1$.

3 *Effects:* Constructs a `bernoulli_distribution` object; `p` corresponds to the parameter of the distribution.

`double p() const;`

4 *Returns:* The value of the `p` parameter with which the object was constructed.

26.4.8.2.2 Class template `binomial_distribution` [lib.rand.dist.bern.bin]

1 A `binomial_distribution` random number distribution produces integer values $i \geq 0$ distributed according to the discrete probability function

$$P(i\,|\,t,p) = \binom{t}{i} \cdot p^i \cdot (1-p)^{t-i}\,.$$

```
template <class IntType = int>
class binomial_distribution
{
public:
  // types
  typedef IntType result_type;
  typedef unspecified param_type;
```

```
  // constructors and reset functions
  explicit binomial_distribution(IntType t = 1, double p = 0.5);
  explicit binomial_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  IntType t() const;
  double p() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

`explicit binomial_distribution(IntType t = 1, double p = 0.5);`

2 *Requires:* $0 \leq \texttt{p} \leq 1$ and $0 \leq \texttt{t}$.

3 *Effects:* Constructs a `binomial_distribution` object; `t` and `p` correspond to the respective parameters of the distribution.

`IntType t() const;`

4 *Returns:* The value of the `t` parameter with which the object was constructed.

`double p() const;`

5 *Returns:* The value of the `p` parameter with which the object was constructed.

26.4.8.2.3 Class template `geometric_distribution` [lib.rand.dist.bern.geo]

1 A `geometric_distribution` random number distribution produces integer values $i \geq 0$ distributed according to the discrete probability function

$$P(i\,|\,p) = p \cdot (1-p)^i \,.$$

```
template <class IntType = int>
class geometric_distribution
{
public:
  // types
  typedef IntType result_type;
  typedef unspecified param_type;
```

```
  // constructors and reset functions
  explicit geometric_distribution(double p = 0.5);
  explicit geometric_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  double p() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
  };
```

`explicit geometric_distribution(double p = 0.5);`

2 *Requires:* $0 < \mathtt{p} < 1$.

3 *Effects:* Constructs a `geometric_distribution` object; `p` corresponds to the parameter of the distribution.

`double p() const;`

4 *Returns:* The value of the `p` parameter with which the object was constructed.

26.4.8.2.4 Class template `negative_binomial_distribution` [lib.rand.dist.bern.negbin]

1 A `negative_binomial_distribution` random number distribution produces random integers $i \geq 0$ distributed according to the discrete probability function

$$P(i\,|\,k,p) = \binom{k+i-1}{i} \cdot p^k \cdot (1-p)^i \,.$$

```
template <class IntType = int>
class negative_binomial_distribution
{
public:
  // types
  typedef IntType  result_type;
  typedef unspecified param_type;

  // constructor and reset functions
  explicit negative_binomial_distribution(IntType k = 1, double p = 0.5);
  explicit negative_binomial_distribution(const param_type& parm);
  void reset();
```

```
    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    IntType k() const;
    double p() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

`explicit negative_binomial_distribution(IntType k = 1, double p = 0.5);`

2 *Requires:* $0 < \mathtt{p} \leq 1$ and $0 < \mathtt{k}$.

3 *Effects:* Constructs a `negative_binomial_distribution` object; `k` and `p` correspond to the respective parameters of the distribution.

`IntType k() const;`

4 *Returns:* The value of the `k` parameter with which the object was constructed.

`double p() const;`

5 *Returns:* The value of the `p` parameter with which the object was constructed.

26.4.8.3 Poisson distributions [lib.rand.dist.pois]

26.4.8.3.1 Class template `poisson_distribution` [lib.rand.dist.pois.poisson]

1 A `poisson_distribution` random number distribution produces integer values $i \geq 0$ distributed according to the discrete probability function

$$P(i\,|\,\mu) = \frac{e^{-\mu}\mu^i}{i\,!} \ .$$

The distribution parameter μ is also known as this distribution's *mean*.

```
  template <class IntType = int>
  class poisson_distribution
  {
  public:
    // types
    typedef IntType result_type;
    typedef unspecified param_type;

    // constructors and reset functions
```

```
    explicit poisson_distribution(double mean = 1.0);
    explicit poisson_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    double mean() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit poisson_distribution(double mean = 1.0);
```

2 *Requires:* $0 <$ `mean`.

3 *Effects:* Constructs a `poisson_distribution` object; `mean` corresponds to the parameter of the distribution.

```
double mean() const;
```

4 *Returns:* The value of the `mean` parameter with which the object was constructed.

26.4.8.3.2 Class template `exponential_distribution` [lib.rand.dist.pois.exp]

1 An `exponential_distribution` random number distribution produces random numbers $x > 0$ distributed according to the probability density function

$$p(x \,|\, \lambda) = \lambda e^{-\lambda x} .$$

```
  template <class RealType = double>
  class exponential_distribution
  {
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructors and reset functions
    explicit exponential_distribution(RealType lambda = 1.0);
    explicit exponential_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
```

```
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    RealType lambda() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit exponential_distribution(RealType lambda = 1.0);
```

2 *Requires:* $0 <$ `lambda`.

3 *Effects:* Constructs a `exponential_distribution` object; `lambda` corresponds to the parameter of the distribution.

```
RealType lambda() const;
```

4 *Returns:* The value of the `lambda` parameter with which the object was constructed.

26.4.8.3.3 Class template `gamma_distribution` [lib.rand.dist.pois.gamma]

1 A `gamma_distribution` random number distribution produces random numbers $x > 0$ distributed according to the probability density function

$$p(x\,|\,\alpha,\beta) = \frac{e^{-x/\beta}}{\beta^{\alpha}\cdot\Gamma(\alpha)}\cdot x^{\alpha-1}\,.$$

```
  template <class RealType = double>
  class gamma_distribution
  {
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructors and reset functions
    explicit gamma_distribution(RealType alpha = 1.0, RealType beta = 1.0);
    explicit gamma_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
```

```
    RealType alpha() const;
    RealType beta() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit gamma_distribution(RealType alpha = 1.0, RealType beta = 1.0);
```

2 *Requires:* $0 <$ `alpha` and $0 <$ `beta`.

3 *Effects:* Constructs a `gamma_distribution` object; `alpha` and `beta` correspond to the parameters of the distribution.

```
RealType alpha() const;
```

4 *Returns:* The value of the `alpha` parameter with which the object was constructed.

```
RealType beta() const;
```

5 *Returns:* The value of the `beta` parameter with which the object was constructed.

26.4.8.3.4 Class template `weibull_distribution` [lib.rand.dist.pois.weibull]

1 A `weibull_distribution` random number distribution produces random numbers $x \geq 0$ distributed according to the probability density function

$$p(x\,|\,a,b) = \frac{a}{b} \cdot \left(\frac{x}{b}\right)^{a-1} \cdot \exp\left(-\left(\frac{x}{b}\right)^{a}\right) .$$

```
  template <class RealType = double>
  class weibull_distribution
  {
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructor and reset functions
    explicit weibull_distribution(RealType a = 1.0, RealType b = 1.0)
    explicit weibull_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
```

```
    RealType a() const;
    RealType b() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit weibull_distribution(RealType a = 1.0, RealType b = 1.0);
```

2 *Requires:* $0 <$ a and $0 <$ b.

3 *Effects:* Constructs a `weibull_distribution` object; `a` and `b` correspond to the respective parameters of the distribution.

```
RealType a() const;
```

4 *Returns:* The value of the `a` parameter with which the object was constructed.

```
RealType b() const;
```

5 *Returns:* The value of the `b` parameter with which the object was constructed.

26.4.8.3.5 Class template `extreme_value_distribution` [lib.rand.dist.pois.extreme]

1 An `extreme_value_distribution` random number distribution produces random numbers x distributed according to the probability density function[8)]

$$p(x\,|\,a,b) = \frac{1}{b} \cdot \exp\left(\frac{a-x}{b} - \exp\left(\frac{a-x}{b}\right)\right) .$$

```
  template <class RealType = double>
  class extreme_value_distribution
  {
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructor and reset functions
    explicit extreme_value_distribution(RealType a = 0.0, RealType b = 1.0);
    explicit extreme_value_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
```

8) The distribution corresponding to this probability density function is also known (with a possible change of variable) as the Gumbel Type I, the log-Weibull, or the Fisher-Tippett Type I distribution.

```
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  RealType a() const;
  RealType b() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

```
explicit extreme_value_distribution(RealType a = 0.0, RealType b = 1.0);
```

2 *Requires:* $0 < \mathtt{b}$.

3 *Effects:* Constructs an `extreme_value_distribution` object; `a` and `b` correspond to the respective parameters of the distribution.

```
RealType a() const;
```

4 *Returns:* The value of the `a` parameter with which the object was constructed.

```
RealType b() const;
```

5 *Returns:* The value of the `b` parameter with which the object was constructed.

26.4.8.4 Normal distributions [lib.rand.dist.norm]

26.4.8.4.1 Class template `normal_distribution` [lib.rand.dist.norm.normal]

1 A `normal_distribution` random number distribution produces random numbers x distributed according to the probability density function

$$p(x\,|\,\mu,\sigma)p(x) = \frac{1}{\sigma\sqrt{2\pi}} \cdot \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right).$$

The distribution parameters μ and σ are also known as this distribution's *mean* and *standard deviation*.

```
template <class RealType = double>
class normal_distribution
{
public:
  // types
  typedef RealType result_type;
  typedef unspecified param_type;

  // constructors and reset functions
  explicit normal_distribution(RealType mean = 0.0, RealType stddev = 1.0);
  explicit normal_distribution(const param_type& parm);
  void reset();
```

```
    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    RealType mean() const;
    RealType stddev() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit normal_distribution(RealType mean = 0.0, RealType stddev = 1.0);
```

2 *Requires:* $0 <$ `stddev`.

3 *Effects:* Constructs a `normal_distribution` object; `mean` and `stddev` correspond to the respective parameters of the distribution.

```
RealType mean() const;
```

4 *Returns:* The value of the `mean` parameter with which the object was constructed.

```
RealType stddev() const;
```

5 *Returns:* The value of the `stddev` parameter with which the object was constructed.

26.4.8.4.2 Class template `lognormal_distribution` [lib.rand.dist.norm.lognormal]

1 A `lognormal_distribution` random number distribution produces random numbers $x > 0$ distributed according to the probability density function

$$p(x\,|\,m,s) = \frac{1}{sx\sqrt{2\pi}} \cdot \exp\left(-\frac{(\ln x - m)^2}{2s^2}\right) .$$

```
  template <class RealType = double>
  class lognormal_distribution
  {
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructor and reset functions
    explicit lognormal_distribution(RealType m = 0.0, RealType s = 1.0);
    explicit lognormal_distribution(const param_type& parm);
    void reset();
```

```
    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    RealType m() const;
    RealType s() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit lognormal_distribution(RealType m = 0.0, RealType s = 1.0);
```

2 *Requires:* $0 <$ `s`.

3 *Effects:* Constructs a `lognormal_distribution` object; `m` and `s` correspond to the respective parameters of the distribution.

```
RealType m() const;
```

4 *Returns:* The value of the `m` parameter with which the object was constructed.

```
RealType s() const;
```

5 *Returns:* The value of the `s` parameter with which the object was constructed.

26.4.8.4.3 Class template `chi_squared_distribution` [lib.rand.dist.norm.chisq]

1 A `chi_squared_distribution` random number distribution produces random numbers $x > 0$ distributed according to the probability density function

$$p(x\,|\,n) = \frac{x^{(n/2)-1} \cdot e^{-x/2}}{\Gamma(n/2) \cdot 2^{n/2}} ,$$

where n is a positive integer.

```
  template <class RealType = double>
  class chi_squared_distribution
  {
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructor and reset functions
    explicit chi_squared_distribution(int n = 1);
    explicit chi_squared_distribution(const param_type& parm);
    void reset();
```

```
  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  int n() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

```
explicit chi_squared_distribution(int n = 1);
```

2 *Requires:* $0 < \texttt{n}$.

3 *Effects:* Constructs a `chi_squared_distribution` object; `n` corresponds to the parameter of the distribution.

```
int n() const;
```

4 *Returns:* The value of the `n` parameter with which the object was constructed.

26.4.8.4.4 Class template `cauchy_distribution` [lib.rand.dist.norm.cauchy]

1 A `cauchy_distribution` random number distribution produces random numbers x distributed according to the probability density function

$$p(x\,|\,a,b) = \left(\pi b \left(1 + \left(\frac{x-a}{b}\right)^2\right)\right)^{-1}.$$

```
template <class RealType = double>
class cauchy_distribution
{
public:
  // types
  typedef RealType result_type;
  typedef unspecified param_type;

  // constructor and reset functions
  explicit cauchy_distribution(RealType a = 0.0, RealType b = 1.0);
  explicit cauchy_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
```

```
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  RealType a() const;
  RealType b() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

```
explicit cauchy_distribution(RealType a = 0.0, RealType b = 1.0);
```

2 *Requires:* $0 <$ b.

3 *Effects:* Constructs a `cauchy_distribution` object; `a` and `b` correspond to the respective parameters of the distribution.

```
RealType a() const;
```

4 *Returns:* The value of the `a` parameter with which the object was constructed.

```
RealType b() const;
```

5 *Returns:* The value of the `b` parameter with which the object was constructed.

26.4.8.4.5 Class template `fisher_f_distribution` [lib.rand.dist.norm.f]

1 A `fisher_f_distribution` random number distribution produces random numbers $x \geq 0$ distributed according to the probability density function

$$p(x\,|\,m,n) = \frac{\Gamma\big((m+n)/2\big)}{\Gamma(m/2)\,\Gamma(n/2)} \cdot \left(\frac{m}{n}\right)^{m/2} \cdot x^{(m/2)-1} \cdot \left(1+\frac{mx}{n}\right)^{-(m+n)/2},$$

where m and n are positive integers.

```
template <class RealType = double>
class fisher_f_distribution
{
public:
  // types
  typedef RealType result_type;
  typedef unspecified param_type;

  // constructor and reset functions
  explicit fisher_f_distribution(int m = 1, int n = 1);
  explicit fisher_f_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
```

```
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  int m() const;
  int n() const;
  param_type param() const;
  void param(const param_type& parm);
  result_type min() const;
  result_type max() const;
};
```

```
explicit fisher_f_distribution(int m = 1, int n = 1);
```

2 *Requires:* $0 < \mathtt{m}$ and $0 < \mathtt{n}$.

3 *Effects:* Constructs a `fisher_f_distribution` object; `m` and `n` correspond to the respective parameters of the distribution.

```
int m() const;
```

4 *Returns:* The value of the `m` parameter with which the object was constructed.

```
int n() const;
```

5 *Returns:* The value of the `n` parameter with which the object was constructed.

26.4.8.4.6 Class template `student_t_distribution` [lib.rand.dist.norm.t]

1 A `student_t_distribution` random number distribution produces random numbers x distributed according to the probability density function

$$p(x\,|\,n) = \frac{1}{\sqrt{n\pi}} \cdot \frac{\Gamma\big((n+1)/2\big)}{\Gamma(n/2)} \cdot \left(1+\frac{x^2}{n}\right)^{-(n+1)/2} ,$$

where n is a positive integer.

```
template <class RealType = double>
class student_t_distribution
{
public:
  // types
  typedef RealType result_type;
  typedef unspecified param_type;

  // constructor and reset functions
  explicit student_t_distribution(int n = 1);
  explicit student_t_distribution(const param_type& parm);
  void reset();

  // generating functions
```

```
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    int n() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
explicit student_t_distribution(int n = 1);
```

2 *Requires:* $0 < \text{n}$.

3 *Effects:* Constructs a `student_t_distribution` object; `n` and `n` correspond to the respective parameters of the distribution.

```
int n() const;
```

4 *Returns:* The value of the `n` parameter with which the object was constructed.

26.4.8.5 Sampling distributions [lib.rand.dist.samp]

26.4.8.5.1 Class template `discrete_distribution` [lib.rand.dist.samp.discrete]

1 A `discrete_distribution` random number distribution produces random integers i, $0 \leq i < n$, distributed according to the discrete probability function

$$P(i \,|\, p_0, \ldots, p_{n-1}) = p_i \,.$$

```
  template <class IntType = int>
  class discrete_distribution
  {
  public:
    // types
    typedef IntType result_type;
    typedef unspecified param_type;

    // constructor and reset functions
    discrete_distribution();
    template <class InputIterator>
      discrete_distribution(InputIterator firstW, InputIterator lastW);
    explicit discrete_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
```

```
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    vector<double> probabilities() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
discrete_distribution();
```

2 *Effects:* Constructs a `discrete_distribution` object with $n = 1$ and $p_0 = 1$. [*Note:* Such an object will always deliver the value 0. — *end note*]

```
template <class InputIterator>
discrete_distribution(InputIterator firstW, InputIterator lastW);
```

3 *Requires:*

a) `InputIterator` shall satisfy the requirements of an input iterator [lib.input.iterator].

b) If `firstW == lastW`, let the sequence w have length $n = 1$ and consist of the single value $w_0 = 1$. Otherwise, `[firstW,lastW)` shall form a sequence w of length $n > 0$ and `*firstW` shall yield a value w_0 convertible to `double`. [*Note:* The values w_k are commonly known as the *weights*. — *end note*]

c) The following relations shall hold: $w_k \geq 0$ for $k = 0, \ldots, n-1$, and $0 < S = w_0 + \cdots + w_{n-1}$.

4 *Effects:* Constructs a `discrete_distribution` object with probabilities

$$p_k = \frac{w_k}{S} \text{ for } k = 0, \ldots, n-1.$$

```
vector<double> probabilities() const;
```

5 *Returns:* A `vector<double>` whose `size` member returns n and whose `operator[]` member returns p_k when invoked with argument k for $k = 0, \ldots, n-1$.

26.4.8.5.2 Class template `piecewise_constant_distribution` [lib.rand.dist.samp.pconst]

1 A `piecewise_constant_distribution` random number distribution produces random numbers x, $b_0 \leq x < b_n$, uniformly distributed over each subinterval $[b_i, b_{i+1})$ according to the probability density function

$$p(x \mid b_0, \ldots, b_n, \ \rho_0, \ldots, \rho_{n-1}) = \rho_i \text{ , for } b_i \leq x < b_{i+1} \text{ .}$$

The $n+1$ distribution parameters b_i are also known as this distribution's *interval boundaries*.

```
  template <class RealType = double>
  class piecewise_constant_distribution
  {
```

```
  public:
    // types
    typedef RealType result_type;
    typedef unspecified param_type;

    // constructor and reset functions
    piecewise_constant_distribution();
    template <class InputIteratorB, class InputIteratorW>
      piecewise_constant_distribution(InputIteratorB firstB, InputIteratorB lastB,
                                      InputIteratorW firstW);
    explicit piecewise_constant_distribution(const param_type& parm);
    void reset();

    // generating functions
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng);
    template <class UniformRandomNumberGenerator>
      result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

    // property functions
    vector<RealType> intervals() const;
    vector<double> densities() const;
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
piecewise_constant_distribution();
```

2 *Effects:* Constructs a `piecewise_constant_distribution` object with $n = 1$, $\rho_0 = 1$, $b_0 = 0$, and $b_1 = 1$.

```
template <class InputIteratorB, class InputIteratorW>
piecewise_constant_distribution(InputIteratorB firstB, InputIteratorB lastB, InputIteratorW firstW);
```

3 *Requires:*

a) `InputIteratorB` shall satisfy the requirements of an input iterator [lib.input.iterator], as shall `InputIteratorW`.

b) If `firstB == lastB`,

   (a) let the sequence w have length $n = 1$ and consist of the single value $w_0 = 1$, and

   (b) let the sequence b have length $n+1$ with $b_0 = 0$ and $b_1 = 1$.

   Otherwise,

   (c) `[firstB, lastB)` shall form a sequence b of length $n+1$ whose leading element b_0 shall be convertible to `result_type`, and

   (d) the length of the sequence w starting from `firstW` shall be at least n, `*firstW` shall return a value w_0 that is convertible to `double`, and any w_k for $k \geq n$ shall be ignored by the distribution.

[*Note:* The values w_k are commonly known as the *weights*. — *end note*]

c) The following relations shall hold for $k = 0, \ldots, n-1$: $b_k < b_{k+1}$ and $0 \leq w_k$. Also, $0 < S = w_0 + \cdots + w_{n-1}$.

4 *Effects:* Constructs a `piecewise_constant_distribution` object with probability densities

$$\rho_k = \frac{w_k}{S \cdot (b_{k+1} - b_k)} \quad \text{for } k = 0, \ldots, n-1.$$

```
vector<result_type> intervals() const;
```

5 *Returns:* A `vector<result_type>` whose `size` member returns $n+1$ and whose `operator[]` member returns b_k when invoked with argument k for $k = 0, \ldots, n$.

```
vector<double> densities() const;
```

6 *Returns:* A `vector<result_type>` whose `size` member returns n and whose `operator[]` member returns ρ_k when invoked with argument k for $k = 0, \ldots, n-1$.

26.4.8.5.3 Class template `general_pdf_distribution` [lib.rand.dist.samp.genpdf]

1 A `general_pdf_distribution` random number distribution produces random numbers x, $x_{\min} \leq x < x_{\max}$, distributed according to the probability density function

$$p(x \,|\, x_{\min}, x_{\max}, \rho) = \rho(x) \text{ , for } x_{\min} \leq x < x_{\min} \text{ .}$$

```
template <class RealType = double>
class general_pdf_distribution
{
public:
  // types
  typedef RealType result_type;
  typedef unspecified param_type;

  // constructor and reset functions
  general_pdf_distribution();
  template <class Func>
    general_pdf_distribution(result_type xmin, result_type xmax, Func pdf);
  explicit general_pdf_distribution(const param_type& parm);
  void reset();

  // generating functions
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng);
  template <class UniformRandomNumberGenerator>
    result_type operator()(UniformRandomNumberGenerator& urng, const param_type& parm);

  // property functions
  result_type xmin() const;
  result_type xmax() const;
```

```
    param_type param() const;
    void param(const param_type& parm);
    result_type min() const;
    result_type max() const;
  };
```

```
general_pdf_distribution();
```

2 *Effects:* Constructs a `general_pdf_distribution` object with $x_{min} = 0$ and $x_{max} = 1$ such that $p(x) = 1$ for all $x_{min} \le x < x_{max}$.

```
template <class Func>
general_pdf_distribution(result_type xmin, result_type xmax, Func pdf);
```

3 *Requires:*

a) `pdf` shall be callable with one argument of type `result_type`, and shall return values of a type convertible to `double`;

b) $x_{\min} < x_{\max}$, and for all $x_{\min} \le x < x_{\max}$, `pdf`$(x)$ shall return a value that is non-negative, non-NaN, and non-infinity; and

c) the following relations shall hold:

$$0 < z = \int_{x_{\min}}^{x_{\max}} f(x)\,dx < \infty\,,$$

where f is the mathematical function corresponding to the supplied `pdf`. [*Note:* This implies that the user-supplied `pdf` need not be normalized. —*end note*]

4 *Effects:* Constructs a `general_pdf_distribution` object; `xmin` and `xmax` correspond to the respective parameters of the distribution and the corresponding probability density function is given by $\rho(x) = f(x)/z$.

```
result_type xmin() const;
```

5 *Returns:* The value of the `xmin` parameter with which the object was constructed.

```
result_type xmax() const;
```

6 *Returns:* The value of the `xmax` parameter with which the object was constructed.

Index