Chapter 5

Random Number Generators

This chapter describes the C* interface for the CMSSL random number generators (RNGs). One section is devoted to each of the following topics:

- introduction
- state tables
- safety checkpointing
- alternate stream checkpointing
- references

Man pages for the RNG routines follow these sections.

5.1 Introduction

The CMSSL includes two RNGs:

- the Fast RNG
- the VP RNG

These operations use a lagged-Fibonacci algorithm. They provide more functionality and faster performance than the **`prand()`** function.

Copyright © 1993 Thinking Machines Corporation

5.1.1 The Fast RNG and the VP RNG Compared

To construct pseudo-random values, the CMSSL random number generators use *state tables*. The difference between the Fast RNG and the VP RNG lies in the allocation of their state tables, as follows:

- The Fast RNG operation stores one state table per processing element.
- The VP RNG operation stores one state table per position of the destination parallel variable.

The Fast RNG thus consumes substantially less processing element memory than the VP RNG. The VP RNG can produce identical results on CM partitions of different sizes. Also, the VP RNG is slightly faster than the Fast RNG, albeit at potentially high cost in memory.

The VP RNG, which mimics the Fast RNG, is generally used if access to a CM partition of a specific size is not guaranteed. For instance, if you are using a 16-processing-element partition while developing an application that will ultimately run on a 64-processing-element partition, use the VP RNG to produce the same results that the Fast RNG will produce when the application is finally run on the larger partition. The VP RNG produces the same result for each position of the destination parallel variable, regardless of the partition size or the shape of the parallel variable — provided that the same *total* number of positions is maintained and that the same seed is used.

5.1.2 The RNG Routines

Most applications that use the CMSSL RNG simply require you to call the Fast or VP RNG and then deallocate the state table. The following operations provide this functionality:

CMSSL_initialize_fast_rng
CMSSL_fast_rng
CMSSL_deallocate_fast_rng

CMSSL_initialize_vp_rng
CMSSL_vp_rng
CMSSL_deallocate_vp_rng

Version 3.2 Beta, December 1993
Copyright © 1993 Thinking Machines Corporation

Note that explicitly initializing these RNGs is only necessary if the default table parameters are not suitable for your application. Section 5.2 discusses the state table parameters.

To guard against the effects of forced interruption, or to use more than one stream of random values, some applications require *checkpointing*. Checkpointing is the process of recording state information at a specific point in the random number stream generation. Later, the stream generation can be continued from the checkpoint.

In *safety checkpointing*, you save the RNG state to a file in case of forced interruption — for instance, during long periods of application execution. If an interruption occurs, you can restore the state and continue processing. Safety checkpointing is not available in this beta release.

In *alternate stream checkpointing*, you save the RNG states associated with two distinct streams of random numbers in order to switch back and forth between the streams. Alternate stream checkpointing is accomplished with the following operations:

CMSSL_fast_rng_state_field
CMSSL_fast_rng_residue
CMSSL_reinitialize_fast_rng

CMSSL_vp_rng_state_field
CMSSL_vp_rng_residue
CMSSL_reinitialize_vp_rng

See Section 5.3 for a detailed description of alternate stream checkpointing.

5.1.3 Implementation

The lagged-Fibonacci algorithm used by both CMSSL random number generators is widely used to produce a uniform distribution of random values. This implementation has been subjected to a battery of statistical tests, both on the stream of values within each processing element and for cross-processing-element correlation. The only test that the CMSSL RNGs fail is the Birthday Spacings Test, as predicted in reference 2 listed in Section 5.4. Despite this failure, these lagged-Fibonacci RNGs are recommended for the most rigorous applications such as Monte Carlo simulations of lattice gases.

Copyright © 1993 Thinking Machines Corporation

5.2 State Tables

If you do not initialize the Fast RNG or VP RNG explicitly, the C* interface uses default parameters to initialize the RNG automatically the first time you call it. If you want to use non-default state table parameters, you must initialize the VP or Fast RNG explicitly.

5.2.1 Fast RNG State Tables

The **CMSSL_initialize_fast_rng** routine allocates the state tables for the Fast RNG and initializes them with values generated internally. To provide a non-default seed for the Fast RNG, you must call **CMSSL_seed_fast_rng** before calling **CMSSL_initialize_fast_rng**.

Figure 11 shows a Fast RNG state table. In the Fast RNG, one state table is associated with each processing element; from this table, random values are constructed for each subgrid position. (The *subgrid* associated with a processing element is the set of parallel variable positions residing in that processing element's memory. See the *C* Programming Guide* for details.) Thus, each time you call **CMSSL_fast_rng**, the number of pseudo-random values produced by each state table is equal to the subgrid size.

Copyright © 1993 Thinking Machines Corporation

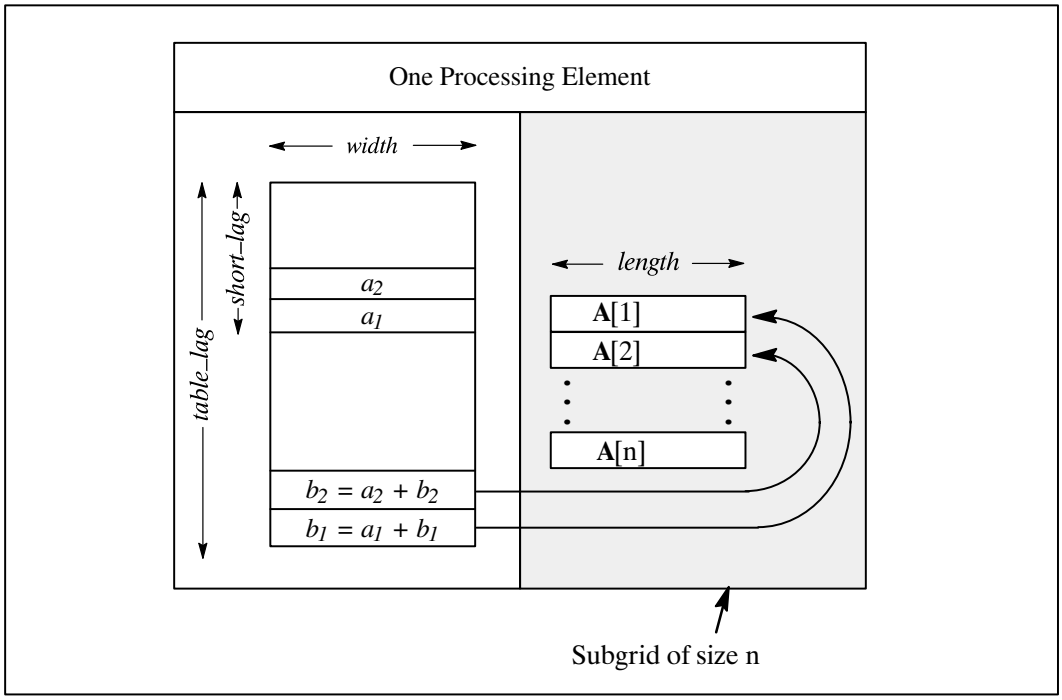

Figure 11. Fast RNG state table.

If you do not call **CMSSL_initialize_fast_rng** explicitly, or you do not call **CMSSL_seed_fast_rng**, **CMSSL_fast_rng** selects a dynamic seed value based on the system time. As a result, with default initialization, different results are obtained in different runs. Explicit initialization is required to obtain identical results.

5.2.2 VP RNG State Tables

The **CMSSL_initialize_vp_rng** routine allocates the state tables for the VP RNG and initializes them with values generated internally. The application provides a seed in the **CMSSL_initialize_vp_rng seed** argument. Figure 12, below, shows one VP RNG state table. In contrast to the Fast RNG state table, each subgrid position has its own state table. Each time you call **CMSSL_vp_rng**, each state table produces only one value.

Copyright © 1993 Thinking Machines Corporation

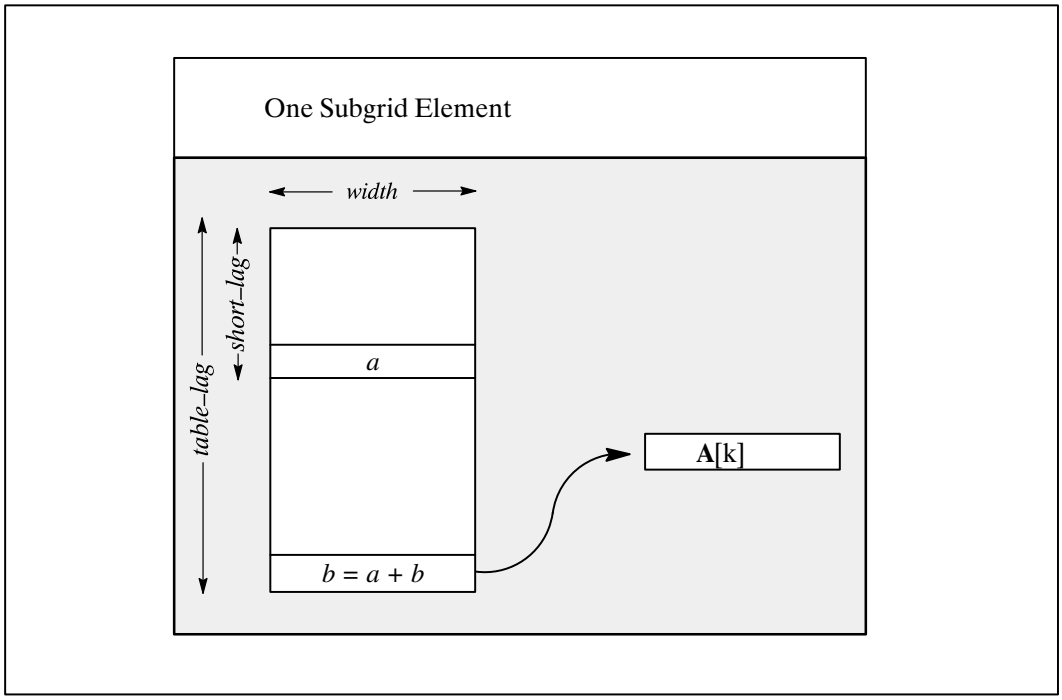

Figure 12. VP RNG state table.

If you do not call **CMSSL_initialize_vp_rng** explicitly, **CMSSL_vp_rng** selects a dynamic seed based on the system time. As a result, with default initialization, different results are obtained in different runs. Explicit initialization is required to obtain identical results.

5.2.3 State Table Parameters

For either CMSSL RNG, each state table has **`table_lag`** elements and width **`width`** bits. The state table is treated as a circular buffer. Internal variables are initialized so that they point into the table at offsets of **`short_lag`** and **`table_lag`** elements. The operation of generating a pseudo-random value (termed *stepping* the RNG) consists of adding the element at the **`short_lag`** marker to the element at the **`table_lag`** marker. This sum is shown as $b = a + b$ in the figures above, where the element shown as b is overwritten by the sum. All or a portion of the bits in element b are used to construct a pseudo-random value, which is then copied to the destination. The markers are then either decremented by one element or cycled around the buffer.

Copyright © 1993 Thinking Machines Corporation

The state table parameters are critical to proper CMSSL RNG operation. The defaults used for automatic initialization are (17, 5) for **table_lag** and **short_lag**. For information about the defaults for **width**, refer to the man page for Fast RNG or VP RNG. Also, refer to the man pages for specific requirements and recommendations regarding **table_lag**, **short_lag**, and **width**.

The *period* of a random number generator is the number of discrete pseudo-random values it can generate before repeating the original stream. For applications that call a CMSSL RNG many times, it is important to make sure the period is long enough. The period should be greater than the total number of values produced by any one state table during all calls to the RNG. Otherwise, it may be possible to detect correlations within the stream produced by one processing element or between streams in different processing elements. See the man page for Fast RNG or VP RNG, later in this chapter, for information on calculating an RNG period from different table parameters.

5.2.4 Need for Deallocation

Both the Fast RNG and the VP RNG allocate state tables as heap memory in the processing elements; until explicitly deallocated, the tables occupy processing element memory. The operations **CMSSL_deallocate_fast_rng** and **CMSSL_deallocate_vp_rng** deallocate the memory allocated for the state tables. It is important that you use the deallocation routines, especially for the VP RNG, in which the state tables can occupy a significant amount of processing element storage space. (In the Fast RNG, the state table size is only on the order of **table_lag**.)

5.2.5 Parameters Saved During Checkpointing

Figure 13 shows how a CMSSL RNG state table is stepped. Cycling through the circular buffer requires **table_lag** steps. During one cycle, each element is used once as the a value and once as the b value in the computation $b = a + b$; thus, all element values are modified. Then the cycle repeats using the new values. The **residue** is the number of steps taken so far in a cycle. At any point, if you save the residue and the values in the state table, you can resume stream generation with the next step.

Copyright © 1993 Thinking Machines Corporation

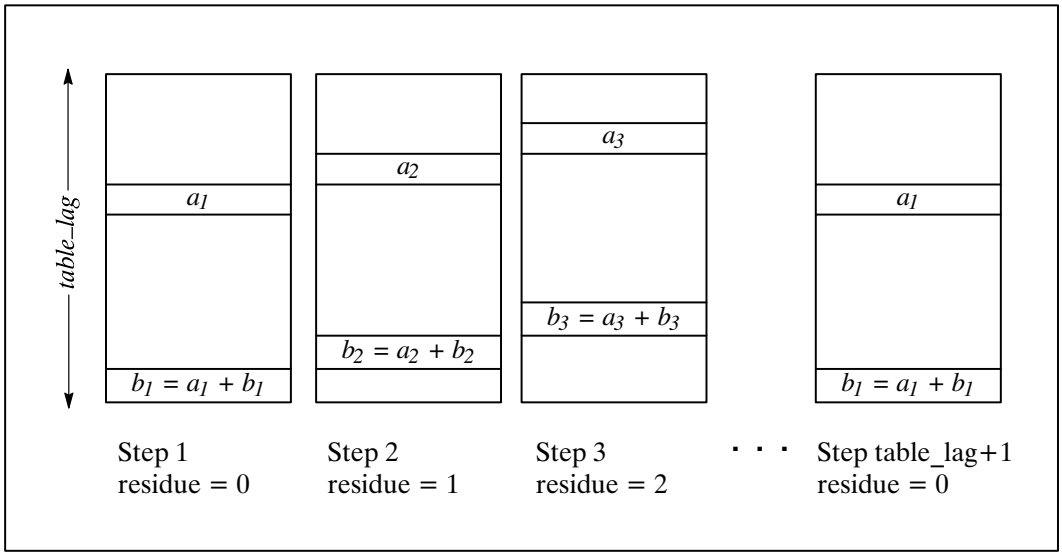

Figure 13. Stepping the state table.

The following routines save or return information for checkpointing:

- The **CMSSL_fast_rng_state_field** and **CMSSL_vp_rng_state_field** routines return internal information about the state table.
- The **CMSSL_fast_rng_residue** and **CMSSL_vp_rng_residue** routines return the residue value.

As explained in Section 5.3, for alternate-stream checkpointing, you save the information returned by the **CMSSL_fast_rng_state_field** and **CMSSL_fast_rng_residue** (or **CMSSL_vp_rng_state_field** and **CMSSL_vp_rng_residue**) routines, but not the actual contents of the state table, and external storage is not required.

5.3 Alternate-Stream Checkpointing

It is possible to switch back and forth between two or more Fast or VP RNG streams by saving the state and reinitializing one RNG after the other. For instance, you can use this strategy to make separate random picks from two databases that need to be merged or compared in some way. You can also

Copyright © 1993 Thinking Machines Corporation

use it to increase efficiency when one stream of random numbers requires a wide state table and another can use a narrower state table.

If two or more VP RNG calls use destination parallel variables with different shapes, you *must* use alternate-stream checkpointing.

Figure 14 is a flowchart for alternate-stream checkpointing using two random number streams. The first RNG is initialized and its state is saved. Then the second RNG is initialized and its state is saved. To alternate between streams, first one and then the other RNG loops through the reinitialization, use, and state-saving phases.

The state-saving phase of alternate-stream checkpointing does not require saving a copy of the state table contents. Two state tables are allocated during initialization; their internal states are used repeatedly during reinitialization; and finally both are deallocated.

Copyright © 1993 Thinking Machines Corporation

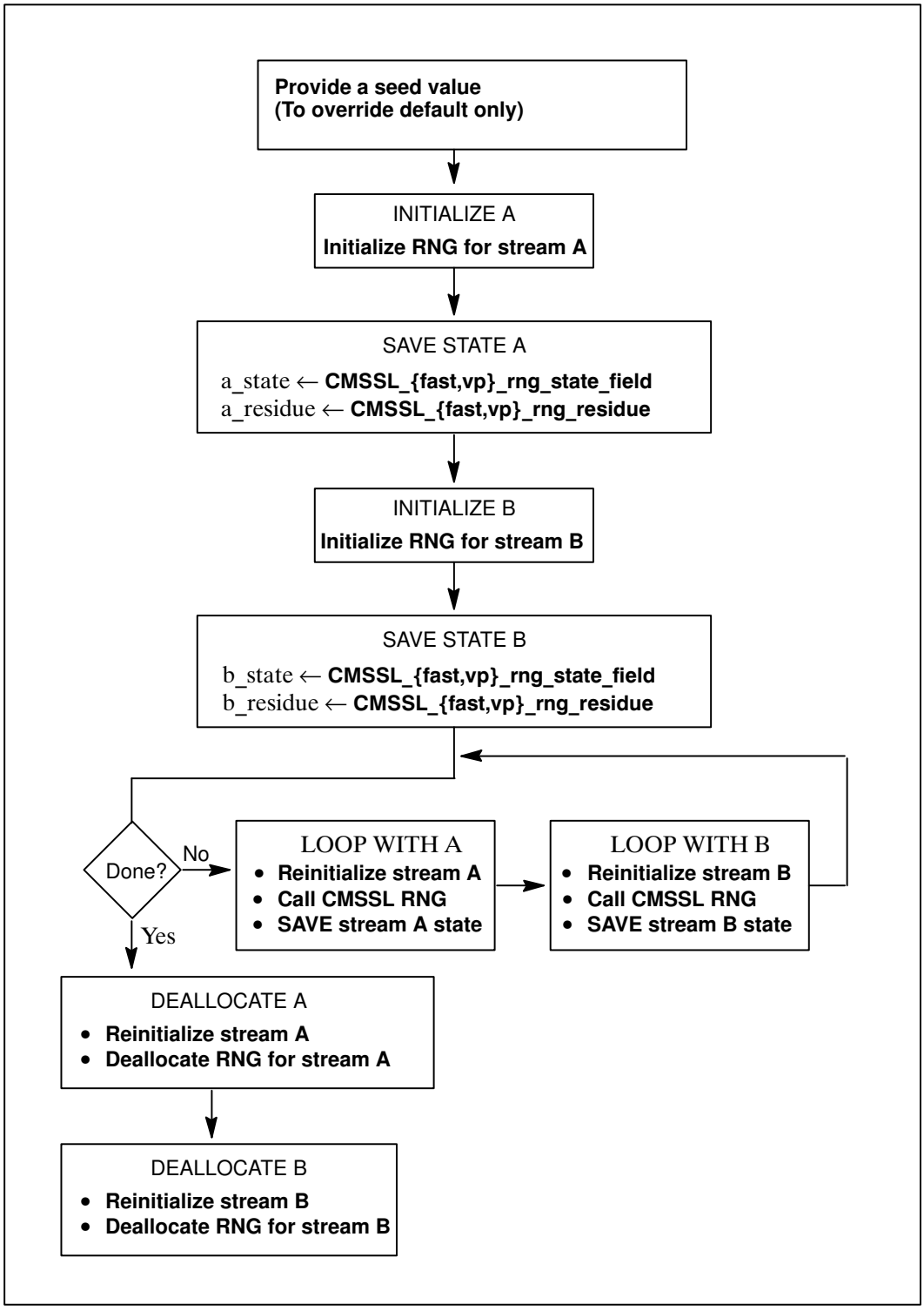

Figure 14. Alternate-stream checkpointing.

Copyright © 1993 Thinking Machines Corporation

5.4 References

For an analysis of the lagged-Fibonacci algorithm and a discussion of optimal lag parameter choices, see:

1. Knuth, D. *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*. Reading, Mass.: Addison-Wesley, 1973. Pp. 26−28.

For a discussion of the vulnerability of lagged-Fibonacci generators to the Birthday Spacings Test, see:

2. Marsaglia, G. A Current View of Random Number Generators. In *Computer Science and Statistics*, 16th Symposium on the Interface, Atlanta, March 1985.

Copyright © 1993 Thinking Machines Corporation

Fast RNG

The CMSSL Fast RNG routines use a lagged-Fibonacci algorithm to generate pseudo-random numbers and store them in a parallel variable. Results may be integer values subject to a limit, or real values between 0.0 and 1.0.

SYNTAX

```
#include <cm/cmssl.h>

void CMSSL_seed_fast_rng(
    int seed);

int CMSSL_initialize_fast_rng(
    int table_lag, int short_lag, int width);

int CMSSL_fast_rng(
    ifd:void *A, ifd limit);

int CMSSL_fast_rng_state_field(
    int *state_table);

int CMSSL_fast_rng_residue(
    int *residue);

int CMSSL_reinitialize_fast_rng(
    int table_lag, int short_lag, int width, int state_table,
    int residue);

int CMSSL_deallocate_fast_rng(
    void);
```

OVERLOADED DATA TYPES

Abbreviation	Meaning
ifd	**int**, **float**, or **double**

ARGUMENTS

seed Seed with which **CMSSL_initialize_fast_rng** will be initialized. If you do not call **CMSSL_seed_fast_rng**, the Fast RNG selects a dynamic seed value based on the system time.

Copyright © 1993 Thinking Machines Corporation

table_lag Length of the state table. The default value for automatic initialization is 17. When you call **CMSSL_reinitialize_fast_rng**, supply the same value that was used in the original **CMSSL_initialize_fast_rng** call.

short_lag Offset into the state table. Must be less than **table_lag**. The default value for automatic initialization is 5. When you call **CMSSL_reinitialize_fast_rng**, supply the same value that was used in the original **CMSSL_initialize_fast_rng** call.

width Width of the state table in bits. Regardless of the value you supply, the RNG is *always* initialized with the following **width** values:

- 32, if **A** is a pointer to a parallel **int** and **limit** is 0.
- 64, if **A** is a pointer to a parallel **int** and **limit** is not 0.
- 32, if **A** is a pointer to a parallel **float** (unless you explicitly specify a **width** of 64, in which case the RNG is initialized with a **width** of 64).
- 64, if **A** is a pointer to a parallel **double**.

A Pointer to a parallel variable. Upon successful completion of **CMSSL_fast_rng**, this variable is overwritten with the RNG results.

limit Ignored unless **A** is a pointer to a parallel **int**. If **A** is a pointer to a parallel **int**, **limit** must be ≥ 0, and is the exclusive, positive upper bound on the pseudo-random values generated. A **limit** value of 0 is interpreted as allowing any 32-bit pattern, so that the full range of positive and negative integers is permitted.

state_table When you call **CMSSL_fast_rng_state_field**, supply a pointer to the variable that will contain internal information about the current state of the state table on return. When you call **CMSSL_reinitialize_fast_rng**, supply the value returned by a previous call to **CMSSL_fast_rng_state_field**.

Copyright © 1993 Thinking Machines Corporation

residue When you call **CMSSL_fast_rng_residue**, supply a pointer to the variable that will contain the checkpointed value of the state table residue on return. This value indicates how many times the state has been stepped, modulo the **table_lag**. When you call **CMSSL_reinitialize_fast_rng**, supply the value returned by a previous call to **CMSSL_fast_rng_residue**.

RETURNED VALUE

Each routine returns an integer. These return codes have the following meanings:

- **CMSSL_initialize_fast_rng** returns −1 if this initialization overwrote a previous initialization, or 0 if it did not.
- **CMSSL_fast_rng** returns −2 if default initialization was used, or 0 if default initialization was not used.
- **CMSSL_fast_rng_state_field** returns −2 if default initialization was used, or 0 if default initialization was not used.
- **CMSSL_fast_rng_residue** returns 0 if the routine succeeded.
- **CMSSL_reinitialize_fast_rng** returns−1 if this initialization overwrote a previous initialization, or 0 if it did not.
- **CMSSL_deallocate_fast_rng** returns 0 if the routine succeeded or −1 if there is no previous state to deallocate.

DESCRIPTION

The Fast RNG uses far less processing element memory than the VP RNG.

Usage. Follow these steps to use the Fast RNG:

1. Optionally, call **CMSSL_seed_fast_rng** to provide a seed for **CMSSL_initialize_fast_rng**.
2. Optionally, call **CMSSL_initialize_fast_rng**. This step is required only if the default initialization parameters are not suitable for your application.
3. Call **CMSSL_fast_rng** to generate the pseudo-random numbers. You may repeat this step as many times as you wish, but the state table parameters with which the RNG was initialized (explicitly or by default) must be appropriate for each call. If a **CMSSL_fast_rng** call requires different state table parameters, you must initiate a new state table by calling **CMSSL_initialize_fast_rng** with the new parameter values.

Copyright © 1993 Thinking Machines Corporation

4. After all **CMSSL_fast_rng** calls associated with one set of state table parameters have finished, call **CMSSL_deallocate_fast_rng** to deallocate the state table.

To perform alternate stream checkpointing, use the **CMSSL_fast_rng_state_field**, **CMSSL_fast_rng_residue**, and **CMSSL_reinitialize_fast_rng** routines.

Initialization. The **CMSSL_initialize_fast_rng** routine allocates one Fast RNG state table as heap memory in each processing element. The state table is initialized with values generated internally. The initialization routine also initializes internal state, including the state table information referenced by **CMSSL_fast_rng_state_field** and the residue referenced by **CMSSL_fast_rng_residue**.

Separate state tables are allocated in each processing element. The size of the state table in bits per processing element is the product of the **`table_lag`** and **`width`** parameters. For example, given a **`width`** of 32 and the recommended **`table_lag`** of 17, the state table occupies 544 bits per processing element.

If your application requires a state table configured differently from the default, you must call **CMSSL_seed_fast_rng** to initialize **CMSSL_initialize_fast_rng** with a seed, and then call **CMSSL_initialize_fast_rng**, before using **CMSSL_fast_rng**.

If you do not explicitly call **CMSSL_seed_fast_rng** and **CMSSL_initialize_fast_rng**, initialization occurs automatically when you first call **CMSSL_fast_rng**. The Fast RNG selects a dynamic seed value based on the system time. The other defaults used for automatic initialization are 17 for **`table_lag`** and 5 for **`short_lag`**; for **`width`** defaults, see the Arguments section above.

For reproducible results, use the same seed and the same Fast RNG parameters each time. If you need reproducible results on different partition sizes, use the VP RNG.

The state table parameters have an enormous effect on the results obtained by calls to **CMSSL_fast_rng**. Use the following guidelines for proper state table initialization:

- The *period* of a random number generator is the number of random values it produces before repeating the original stream. To avoid correlation, the period should be greater than the total number of random values produced by any processing element; that is,

  $$desired\text{-}period > \text{subgrid size} \times invocations$$

  where *invocations* is the number of times the program calls **CMSSL_fast_rng**.

Copyright © 1993 Thinking Machines Corporation

- The period is very sensitive to the choice of **table_lag** and **short_lag** values. The default pair of values, (17, 5), has been carefully chosen to produce the maximum period for the minimum storage. Other suggested values are (55, 24) and (71, 35). When the lag pairs are properly chosen, the period of the Fast RNG depends exponentially on the state table length (**table_lag**) and on the state table width (**width**), such that:

  $$period = (2^{\texttt{table_lag}} - 1) \times 2^{\texttt{width}}$$

  For a discussion on choosing proper lag value pairs, see the paper by Knuth referenced in Section 5.4.

- The RNG is *always* initialized with the **width** values shown in the Arguments section.

Random Number Generation. The **CMSSL_fast_rng** routine copies a pseudo-random value, chosen from a uniform distribution, into each position of **A**. The distribution range in the **float** or **double** case is from 0.0 (inclusive) to 1.0 (exclusive). The distribution range in the integer case with a positive limit is from 0 (inclusive) to the specified **limit** (exclusive). The distribution range in the integer case with a 0 **limit** is all integer values from -2^{31} to $2^{31} - 1$ (in other words, any 32-bit pattern).

The State Field, Residue, and Reinitialization Routines. The **CMSSL_fast_rng_state_field**, **CMSSL_fast_rng_residue**, and **CMSSL_reinitialize_fast_rng** routines provide a method for alternate-stream checkpointing, in which the application switches back and forth between two or more Fast RNG streams by saving the state and reinitializing one RNG after the other.

To perform checkpointing using these routines, follow these steps:

1. After the Fast RNG has been initialized either implicitly or explicitly by **CMSSL_initialize_fast_rng**, and after **CMSSL_fast_rng** has been called zero or more times, call **CMSSL_fast_rng_state_field** and **CMSSL_fast_rng_residue**.

2. Save the values of **state_table** and **residue**.

3. To restart a previously checkpointed Fast RNG number stream, call **CMSSL_reinitialize_fast_rng** with the previously saved **state_table** and **residue** values.

The **CMSSL_fast_rng_state_field** routine returns internal information about the Fast RNG state table; this information was generated previously by an implicit or ex-

Copyright © 1993 Thinking Machines Corporation

plicit call to **CMSSL_initialize_fast_rng**. The state table resides in the processing elements; its size is the product of **table_lag** and **width**.

The **CMSSL_fast_rng_residue** routine returns the residue: a count of the number of times that the Fast RNG state has been stepped, modulo the **table_lag**. The residue is the product of the subgrid size and the number of calls to **CMSSL_fast_rng** that have occurred since the last call to **CMSSL_initialize_fast_rng** or **CMSSL_reinitialize_fast_rng**.

The **CMSSL_reinitialize_fast_rng** routine reinitializes the Fast RNG from a previously checkpointed state so that an interrupted computation can be resumed.

Deallocation. The **CMSSL_deallocate_fast_rng** routine deallocates the heap field that has been used to store the state table for the Fast RNG. Call this routine when you are finished with the Fast RNG.

NOTES

Numerical Performance. The lagged-Fibonacci algorithm implemented by this RNG is widely used to produce a uniform distribution of random values.

For a **width** of 32 bits and using the default **table_lag** and **short_lag** values (17, 5), the period of the fast RNG is $(2^{17}-1)2^{32} \approx 5.6\text{e}15$ bits.

Running time for the Fast RNG increases with the state table width and the number of bits used. For best results, reduce the table width to the number of bits required and use a **limit** value of 0.

Applications. The Fast RNG should be used in applications such as Monte Carlo simulations where speed is a priority and there is enough room for the state table.

Reproducible Results. To obtain reproducible results from the Fast RNG, call **CMSSL_seed_fast_rng** with the same seed each time, and call **CMSSL_initialize_fast_rng** explicitly.

In contrast, checkpointing and reinitializing an RNG is used to *continue* random value stream generation from a previous or alternate state.

No Error Checking on Reinitialization. The **CMSSL_reinitialize_fast_rng** routine does not perform error checking on the input parameters. Unpredictible results or halted execution are likely under the following conditions:

- The size of **state_table** is less than (**table_lag** × **width**).

Copyright © 1993 Thinking Machines Corporation

- **`residue`** is negative or **`residue`** ≥ **`table_lag`**.

EXAMPLES

Sample C* code that uses the Fast RNG routines can be found on-line in the subdirectory

`random/cstar/`

of a CMSSL examples directory whose location is site-specific.

Copyright © 1993 Thinking Machines Corporation

VP RNG

The CMSSL VP RNG routines use a lagged-Fibonacci algorithm to generate pseudo-random numbers and store them in a parallel variable. Results may be integer values subject to a limit, or real values between 0.0 and 1.0.

SYNTAX

```
#include <cm/cmssl.h>

int CMSSL_initialize_vp_rng(
    ifd:void *A_template, int table_lag, int short_lag,
    int width, int seed);

int CMSSL_vp_rng(
    ifd:void *A, ifd limit);

int CMSSL_vp_rng_state_field(
    ifd:void *A_template, int *state_table);

int CMSSL_vp_rng_residue(
    ifd:void *A_template, int *residue);

int CMSSL_reinitialize_vp_rng(
    int table_lag, int short_lag, int width, int state_table,
    int residue);

int CMSSL_deallocate_vp_rng(
    ifd:void *A_template);
```

OVERLOADED DATA TYPES

Abbreviation	Meaning
ifd	**int**, **float**, or **double**

ARGUMENTS

A_template Pointer to a parallel variable of the same shape as the **A** argument supplied to any **CMSSL_vp_rng** call for this RNG stream. Information about shape is taken from this argument.

Copyright © 1993 Thinking Machines Corporation

table_lag Length of the state table. The default value for automatic initialization is 17. When you call **CMSSL_reinitialize_vp_rng**, supply the same value that was used in the original **CMSSL_initialize_vp_rng** call.

short_lag Offset into the state table. Must be less than **table_lag**. The default value for automatic initialization is 5. When you call **CMSSL_reinitialize_vp_rng**, supply the same value that was used in the original **CMSSL_initialize_vp_rng** call.

width Width of the state table in bits. Regardless of the value you supply, the RNG is *always* initialized with the following **width** values:

- 32, if **A** is a pointer to a parallel **int** and **limit** is 0.
- 64, if **A** is a pointer to a parallel **int** and **limit** is not 0.
- 32, if **A** is a pointer to a parallel **float** (unless you explicitly specify a **width** of 64, in which case the RNG is initialized with a **width** of 64).
- 64, if **A** is a pointer to a parallel **double**.

seed Seed used to initialize the VP RNG for reproducible results. If you do not explicitly initialize the VP RNG, the VP RNG selects a dynamic seed value based on the system time.

A Pointer to a parallel variable. Upon successful completion of **CMSSL_vp_rng**, this variable is overwritten with the RNG results.

limit Ignored unless **A** is a pointer to a parallel **int**. If **A** is a pointer to a parallel **int**, **limit** must be ≥ 0, and is the exclusive, positive upper bound on the pseudo-random values generated. A **limit** value of 0 is interpreted as allowing any 32-bit pattern, so that the full range of positive and negative integers is permitted.

state_table When you call **CMSSL_vp_rng_state_field**, supply a pointer to the variable that will contain internal information about the current state of the state table on return. When you call **CMSSL_reinitialize_vp_rng**, supply the value returned by a previous call to **CMSSL_vp_rng_state_field**.

Copyright © 1993 Thinking Machines Corporation

`residue` When you call **CMSSL_vp_rng_residue**, supply a pointer to the variable that will contain the checkpointed value of the state table residue on return. This value indicates how many times the state has been stepped, modulo the **`table_lag`**. When you call **CMSSL_reinitialize_vp_rng**, supply the value returned by a previous call to **CMSSL_vp_rng_residue**.

RETURNED VALUE

Each routine returns an integer. These return codes have the following meanings:

- **CMSSL_initialize_vp_rng** returns −1 if this initialization overwrote a previous initialization, or 0 if it did not.
- **CMSSL_vp_rng** returns −2 if default initialization was used, or 0 if default initialization was not used.
- **CMSSL_vp_rng_state_field** returns −2 if default initialization was used, or 0 if default initialization was not used.
- **CMSSL_vp_rng_residue** returns 0 if the routine succeeded.
- **CMSSL_reinitialize_vp_rng** returns−1 if this initialization overwrote a previous initialization, or 0 if it did not.
- **CMSSL_deallocate_vp_rng** returns 0 if the routine succeeded or −1 if there is no previous state to deallocate.

DESCRIPTION

The VP RNG is useful for producing identical streams of random numbers on partitions of different sizes, as long as the number of positions in **`A`** is constant. The VP RNG is slightly faster than the Fast RNG; however, it uses far more processing element memory than either.

Usage. Follow these steps to use the VP RNG:

1. Call **CMSSL_initialize_vp_rng** (optional). This step is required only if the default initialization parameters are not suitable for your application.
2. Call **CMSSL_vp_rng** to generate the pseudo-random numbers. You may repeat this step as many times as you wish, but the state table parameters with which the RNG was initialized (explicitly or by default) must be appropriate for each call. If a **CMSSL_vp_rng** call requires different state table parame-

Copyright © 1993 Thinking Machines Corporation

ters, you must initiate a new state table by calling **CMSSL_initialize_vp_rng** with the new parameter values.

3. After all **CMSSL_vp_rng** calls associated with one set of state table parameters have finished, call **CMSSL_deallocate_vp_rng** to deallocate the state table.

To perform alternate stream checkpointing, use the **CMSSL_vp_rng_state_field**, **CMSSL_vp_rng_residue**, and **CMSSL_reinitialize_vp_rng** routines.

Initialization. The **CMSSL_initialize_vp_rng** routine allocates a VP RNG state table as heap memory in the processing elements. The state table is initialized with values generated internally. The initialization routine also initializes internal state, including the state table information referenced by **CMSSL_vp_rng_state_field** and the residue referenced by **CMSSL_vp_rng_residue**.

The VP RNG is designed to produce identical results on partitions of different sizes. To get identical results, be sure the following conditions are true:

- The shape associated with **A_template** does not change between runs; this ensures that the same total number of positions are used each time.
- The same **seed** is used each time. If you do not call **CMSSL_initialize_vp_rng** explicitly, **CMSSL_vp_rng** selects a dynamic seed value based on the system time. As a result, with default initialization, different results are obtained in different runs. Explicit initialization is required to obtain identical results.

The **A_template** parameter is used to determine the shape in which random values are used. A separate state table is allocated for each position of **A**. The size of the state table in bits per position of **A** is the product of the **table_lag** and **width** parameters. For example, given a **width** of 32 and the recommended **table_lag** of 17, the state table occupies 544 bits per position of **A**.

If your application requires a state table configured differently from the default, you must call **CMSSL_initialize_vp_rng** (supplying a seed in the **seed** argument) before using **CMSSL_vp_rng**.

To produce the same results as the Fast RNG would produce, you must ensure that the total number of **A** positions used by the VP RNG equals the total number of processing elements used by the Fast RNG. Also, the **seed** you use to initialize the VP RNG state table must be the same as the seed you use when you call **CMSSL_seed_fast_rng** before calling **CMSSL_initialize_fast_rng**.

If you do not explicitly initialize the VP RNG, initialization occurs automatically when you first call **CMSSL_vp_rng**. The VP RNG selects a dynamic **seed** value

Copyright © 1993 Thinking Machines Corporation

based on the system time. The other defaults used for automatic initialization are 17 for **table_lag** and 5 for **short_lag**; for **width** defaults, see the Arguments section above. The **A** supplied in the first invocation of **CMSSL_vp_rng** is used as the default **A_template**.

The state table parameters have an enormous effect on the results obtained by calls to **CMSSL_vp_rng**. Use the following guidelines for proper state table initialization:

- The *period* of a random number generator is the number of random values it produces before repeating the original stream. To avoid correlation, the period should be greater than the total number of random values produced for any subgrid position; that is,

  $$desired - period > invocations$$

  where *invocations* is the number of times the program calls **CMSSL_vp_rng**.

- The period is very sensitive to the choice of **table_lag** and **short_lag** values. The default pair of values, (17, 5), has been carefully chosen to produce the maximum period for the minimum storage. Other suggested values are (55, 24) and (71, 35). When the lag pairs are properly chosen, the period of the VP RNG depends exponentially on the state table length (**table_lag**) and on the state table width (**width**), such that:

  $$period = (2^{\texttt{table_lag}} - 1) \times 2^{\texttt{width}}$$

  For a discussion on choosing proper lag value pairs, see the paper by Knuth referenced in Section 5.4.

- The RNG is *always* initialized with the **width** values shown in the Arguments section, above.

If the subgrid size times the number of processing elements is *N*, the state table in each subgrid position is initialized as though it were a Fast RNG state table in a partition with *N* processing elements.

Random Number Generation. The **CMSSL_vp_rng** routine copies a pseudo-random value, chosen from a uniform distribution, into each position of **A**. The distribution range in the **float** or **double** case is from 0.0 (inclusive) to 1.0 (exclusive). The distribution range in the integer case with a positive limit is from 0 (inclusive) to the specified **limit** (exclusive). The distribution range in the integer case with a 0 **limit** is all integer values from -2^{31} to $2^{31} - 1$ (in other words, any 32-bit pattern).

Copyright © 1993 Thinking Machines Corporation

Each time the VP RNG is called, it generates one random value per subgrid position, and places the random values in **A**. For any one stream of random values, all **A** arguments must have the same shape, size, and axis orderings. To generate random values for parallel variables that differ in these attributes, use alternate-stream checkpointing (described below).

The State Field, Residue, and Reinitialization Routines. The **CMSSL_vp_rng_state_field**, **CMSSL_vp_rng_residue**, and **CMSSL_reinitialize_vp_rng** routines provide a method for alternate-stream checkpointing, in which the application switches back and forth between two or more VP RNG streams by saving the state and reinitializing one RNG after the other.

To perform checkpointing using these routines, follow these steps:

1. After the VP RNG has been initialized either implicitly or explicitly by **CMSSL_initialize_vp_rng**, and after **CMSSL_vp_rng** has been called zero or more times, call **CMSSL_vp_rng_state_field** and **CMSSL_vp_rng_residue**.
2. Save the values of **state_table** and **residue**.
3. To restart a previously checkpointed VP RNG number stream, call **CMSSL_reinitialize_vp_rng** with the previously saved **state_table** and **residue** values.

The **CMSSL_vp_rng_state_field** routine returns internal information about the VP RNG state table; this information was generated previously by an implicit or explicit call to **CMSSL_initialize_vp_rng**. The state table resides in the processing elements; its size is the product of **table_lag** and **width**.

The **CMSSL_vp_rng_residue** routine returns the residue: a count of the number of times that the VP RNG state has been stepped, modulo the **table_lag**. The residue is the product of the subgrid size and the number of calls to **CMSSL_vp_rng** that have occurred since the last call to **CMSSL_initialize_vp_rng** (implicit or explicit) or **CMSSL_reinitialize_vp_rng**.

The **CMSSL_reinitialize_vp_rng** routine reinitializes the VP RNG from a previously checkpointed state so that an interrupted computation can be resumed.

Deallocation. The **CMSSL_deallocate_vp_rng** routine deallocates the heap field that has been used to store the state table for the VP RNG. Call this routine when you are finished with the VP RNG. Using **CMSSL_deallocate_vp_rng** is important because the VP RNG state table field can use a significant amount of processing element memory.

Copyright © 1993 Thinking Machines Corporation

NOTES

Numerical Performance. The lagged-Fibonacci algorithm implemented by this RNG is widely used to produce a uniform distribution of random values.

For a **`width`** of 32 bits and using the default **`table_lag`** and **`short_lag`** values (17, 5), the period of the VP RNG is $(2^{17}-1)2^{32} \approx 5.6e15$ bits.

Running time for the VP RNG increases with the state table width and the number of bits used. For best results, reduce the table width to the number of bits required and use a **`limit`** value of 0.

Applications. The VP RNG mimics the Fast RNG. It should be used in applications such as Monte Carlo simulations where reproducible results across different partition sizes must be verified.

Reproducible Results. To obtain reproducible results from the VP RNG, call **CMSSL_initialize_vp_rng** using the same **`seed`** value each time.

In contrast, checkpointing and reinitializing an RNG is used to *continue* random value stream generation from a previous or alternate state.

No Error Checking on Reinitialization. The **CMSSL_reinitialize_vp_rng** routine does not perform error checking on the input parameters. Unpredictible results or halted execution are likely under the following conditions:

- The size of **`state_table`** is less than (**`table_lag`** $\times$ **`width`**).
- **`residue`** is negative or **`residue`** $\geq$ **`table_lag`**.

EXAMPLES

Sample C* code that uses the VP RNG routines can be found on-line in the subdirectory **`random/cstar/`** of a CMSSL examples directory whose location is site-specific.

Copyright © 1993 Thinking Machines Corporation