# Performance Modeling of Computer Systems and Networks

Prof. Vittoria de Nitto Personè

**Discrete-Event Simulation** 

Università degli studi di Roma Tor Vergata

Department of Civil Engineering and Computer Science Engineering

Copyright © Vittoria de Nitto Personè, 2021 https://creativecommons.org/licenses/by-nc-nd/4.0/

1

Quanto ci mette un ordine ad arrivare, viene modellato con probabilità.

### Multi-Stream Lehmer RNGs

- · Typical DES models have many stochastic components
- · Want a unique source of randomness for each component
- · One (poor) option: multiple RNGs
- Better option: one RNG with multiple "streams" of random numbers

one stream per stochastic component



We will partition output from our Lehmer RNG into multiple streams

Prof. Vittoria de Nitto Personè

2

```
Case study ssq
                  Arrival and service processes
         two stochastic components: arrival and service
         allocate a different state variable to each
double GetService(void)
                                           double GetService(void)
     return Uniform(1.0, 2.0); -
                                                double s;
                                                static long x = 12345;
                                                                              solo la prima volta!
                                                PutSeed(x);
                                                s = Uniform(1.0, 2.0);
                                                GetSeed(&x);
                                                return (s);
        • x represents the current state of the service process
         lo stato è l'ultimo valore generato, in pratica quando richiamo la funzione
         questa riparte dall'ultimo valore estratto e 'procede'.
                          Prof. Vittoria de Nitto Personè
                                                                            3
```

3

```
Case study ssq
                       Arrival and service processes
              Arrival should have its own static variable, initialized
              differently
                                       double GetArrival(void)
double GetArrival(void)
                                           {
{
                                                 static double arrival = START;
     static double arrival = START;
                                                                                        solo la prima volta!
                                                 static long x = 54321; cambio seme
     arrival += Exponential(2.0);
                                                 PutSeed(x);
     return (arrival);
                                                 arrival += Exponential(2.0);
}
                                                 GetSeed(&x);
                                                 return (arrival);
                                           }
            • x represents the current state of arrival process
                             Prof. Vittoria de Nitto Personè
```

## The Modified Arrival and Service Processes

- As modified, arrival and service times are drawn from different streams of random numbers
- Provided the streams don't overlap → the processes are uncoupled
- · Execution time cost is negligible

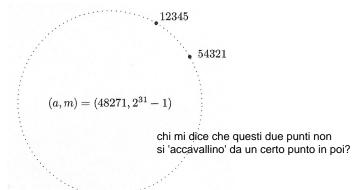
Prof. Vittoria de Nitto Personè

5

5

Pseudo-random generators Lehmer multi-stream

- Potential problem: assignment of initial seeds to produce disjoint streams
- If states are picked at whim, no guarantee of disjoint streams
- Some initial states may only be a few calls to Random apart!



Prof. Vittoria de Nitto Personè

6

## **Jump Multipliers**

· We will develop a multi-stream version of rng

**Theorem** 

Given  $g(x) = ax \mod m$  and integer j (1<j<m-1)

**jump function**:  $g^{j}(x) = (a^{j} \mod m)x \mod m$ 

jump multiplier: a j mod m

If  $g(\cdot)$  generates  $x_0, x_1, x_2,...$  then  $g^i(\cdot)$  generates  $x_0, x_j, x_{2j},...$  mi sposto su sequenze di lunghezza 'j'.

This theorem is the key to creating streams

Prof. Vittoria de Nitto Personè

7

/

Pseudo-random generators Lehmer multi-stream

#### Example 1

• If m = 31, a = 3 and j = 6, the jump multiplier is

$$a^{j} \mod m = 3^{6} \mod 31 = 16$$

- If  $x_0 = 1$ , then  $g(x) = 3x \mod 31$  generates:
- 1, 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1, . . .
- The jump function  $g^6(x) = 16x \mod 31$  generates:

e' come avere sei generatori disgiunti, anche se in realtà ne sto usando uno! Questa tecnica è migliore di usare 6 generatori di Lehmer.

Prof. Vittoria de Nitto Personè

#### Example 1

• If m = 31, a = 3 and j = 6, the jump multiplier is

$$a^{j} \mod m = 3^{6} \mod 31 = 16$$

• If  $x_0 = 1$ , then  $g(x) = 3x \mod 31$  generates:

```
1, 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1, . . .
```

• The jump function  $g^6(x) = 16x \mod 31$  generates:

• I.e., the first sequence is  $x_0, x_1, x_2,...$ ; the second is  $x_0, x_6, x_{12},...$ 

Prof. Vittoria de Nitto Personè

9

9

Pseudo-random generators Lehmer multi-stream

#### Example 1

$$m = 31$$
,  $a = 3$ ,  $x_0 = 1$ 

<u>1</u>, 3, 9, 27, 19, 26, <u>16</u>, 17, 20, 29, 25, 13, <u>8</u>, 24, 10, 30, 28, 22, <u>4</u>, 12, 5, 15, 14, 11, <u>2</u>, 6, 18, 23, 7, 21, <u>1</u>, . . .

 $x_0 = \underline{1}$ , 3, 9, 27, 19, 26,

 $x_6 = \frac{1}{16}$ , 17, 20, 29, 25, 13,

 $x_{12} = 8, 24, 10, 30, 28, 22,$ 

 $x_{18} = 4$ , 12, 5, 15, 14, 11,

 $x_{24} = 2, 6, 18, 23, 7, 21,$ 

Devono però bastarmi questi numeri!

• The jump function  $g^6(x) = 16x \mod 31$  generates:

1, 16, 8, 4, 2, 1, . . .

Prof. Vittoria de Nitto Personè

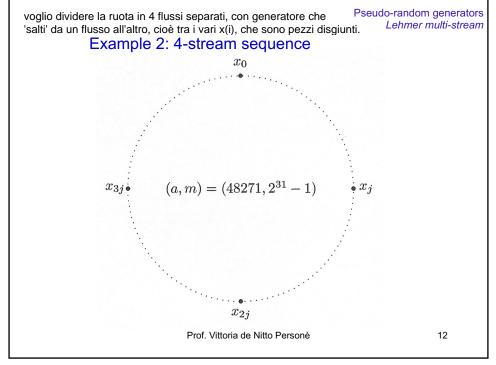
## Using the jump function

- First, compute the jump multiplier  $a^{j} \mod m$  (one time cost)
- Then,  $g^j(\cdot)$  allows jumping from  $x_0$  to  $x_i$  to  $x_{2i}$  to ...
- The user supplies ONE initial seed uso un seed e poi applico la funzione salto.
- If j is chosen well,  $g^{j}(\cdot)$  can "plant" additional initial seeds
- · Each planted seed corresponds to a different stream
- Each planted seed is separated by j calls to Random ogni seed dista 'j' dall'altro.

Prof. Vittoria de Nitto Personè

11

11



## An appropriate jump multiplier

- Consider 256 = 28 different streams of random numbers
- Partition the RNG output sequence into 256 disjoint subsequences of equal length
- Find the largest  $j < 2^{31}/2^8 = 2^{23}$  such that the jump multiplier is modulus-compatible
- $g^{j}(x) = (48271^{j} \mod m) x \mod m$  can be implemented via algorithm 1 (2.2.1 in the book)
- Then  $g^{j}(x)$  can be used to plant the other 255 initial seeds
- Possibility of stream overlap is minimized (though not eliminated!)

#### Algorithm 1

```
 \begin{array}{ll} t = a * (x \% q) - r * (x / q); & /* t = \gamma(x) * / \\ & \text{if (t > 0)} & \\ & \text{return (t);} & /* \delta(x) = 0 * / \\ & \text{else} & \\ & \text{return (t + m);} & /* \delta(x) = 1 * / \end{array}
```

Prof. Vittoria de Nitto Personè

13

13

Pseudo-random generators Lehmer multi-stream

## Maximal Modulus-Compatible Jump Multipliers

$$a = 48271$$
  $m = 2^{31} - 1$ 

## Example 2 (cont.)

# of streams	lunghezza sottosequenza	intero più grande ma minore di m/s jump size j	jump multiplier <i>a<sup>j</sup></i> mod <i>m</i>
1024	2097151	2082675	97070
512	4194303	4170283	44857
standard 256	8388607	8367782	22925
128	16777215	16775552	40509

Prof. Vittoria de Nitto Personè

## Library rngs

- · Upward-compatible multi-stream replacement for rng
- Provides 256 streams, indexed 0 to 255 (0 is the default)
- Only one stream is active at any time
- 6 available functions:
  - Random(void): to use the standard Lehmer generator
  - PutSeed(long x): to set the state of the active stream
  - GetSeed(long \*x): to obtain the state of the active stream
  - TestRandom(void): to test the implementation correctness
  - SelectStream(int s): to define the active stream da dove 'partire'.
  - PlantSeeds(long x): "plants" one seed per stream

a partire dal primo seme pianta tutti gli altri

Prof. Vittoria de Nitto Personè

15