PEMBANGKIT BILANGAN ACAK (Random Number Generator)

Mata Kuliah Pemodelan & Simulasi

Riani Lubis
Program Studi Teknik Informatika
Universitas Komputer Indonesia

Random Number Generator (1)

- Cara memperoleh :
  - Melempar dadu
  - Mengocok kartu
  - Cakram putar
  - Tabel bilangan acak
  - Pseudo Random Number
- Random Number Generator (RNG) adalah algoritma yang digunakan untuk menghasilkan urut-urutan (sequence) dari angka sebagai hasil perhitungan dengan komputer yang diketahui distribusinya sehingga angka-angka tersebut muncul secara random dan digunakan terus-menerus.

Random Number Generator (2)

- Sequence yang dimaksud di sini adalah bahwa random number tersebut harus dapat dihasilkan secara urut dalam jumlah yang mengikuti algoritma tertentu dan sesuai dengan distribusi yang dikehendaki.

- Distribusi yang dimaksud adalah distribusi probabilitas yang digunakan untuk meninjau/terlibat langsung dalam penarikan random number tersebut.

- Pada umumnya probabilitas yang digunakan untuk hal ini adalah distribusi Uniform.

Random Number

- Kemunculannya tidak dapat diprediksi.
- Tidak ada komputasi yang benar-benar menghasilkan deret bilangan acak secara sempurna
- Bilangan acak yang dibangkitkan oleh komputer adalah bilangan acak semu (Pseudo Random Number), karena menggunakan rumus-rumus matematika
- Banyak algoritma atau metode yang dapat digunakan untuk membangkitkan bilangan acak
- Bilangan acak dapat dibangkitkan dengan pola tertentu yang dinamakan dengan distribusi mengikuti fungsi distribusi yang ditentukan
- Bilangan acak yang dibangkitkan tidak boleh berulang secara periodik.
- Deret bilangan acak yang baik adalah deret bilangan acak yang tidak mengandung pengulangan bilangan secara periodik, karena berarti kemunculannya dapat diprediksi.

Sifat-Sifat Pembangkit PRN

- **Independent** : tiap variablenya harus bebas dari ketentuan tersendiri, seperti :
  - Z_{i-1} : merupakan hasil akhir
  - Z_0 : merupakan angka pertama/seed (nilainya bebas)
  - a : merupakan konstanta (angka yang nilainya konstan & ditentukan bebas)
  - c : merupakan konstanta (angka yang nilainya bebas)
- **Uniform** : suatu distribusi yang umum (distribusi probabilitas) dan sama untuk semua besaran yang dikeluarkan/diambil. Hal ini berarti bahwa diusahakan probabilitasnya sama untuk setiap penarikan random number tersebut.

- **Dense** : Density Probabilitas Distribution harus mengikuti syarat probabilitas (antara 0 dan 1). Hal ini berarti dalam penarikan angka-angka yang dibutuhkan dari RNG cukup banyak dan dibuat sedemikian rupa sehingga $0 \leq R.N. \leq 1$

- **Efficient** : artinya dapat cukup sederhana dan dalam menggunakan cara ini harus terlebih dahulu memilih angka-angka untuk variable-variabelnya yang cocok. Hal ini berarti dalam penarikan random number tersebut harus dapat menentukan angka-angka untuk variabelnya yang sesuai sehingga dapat berjalan terus-menerus.

Penentuan Random Number

a. Tabel Random Number; tabel ini sudah banyak ditemukan mulai dari enam digit sampai dengan belasan digit.

b. Electronic Random Number; number ini banyak juga dipergunakan dalam percobaan penelitian.

c. Congruential Pseudo Random Number Generator :

1. Linear Congruential Generator (LCG)
2. Multiplicative Random Number Generator
3. Mixed Congruential Random Number Generator
4. Lainnya :
   a. Fibonacci Generator
   b. Composite Generator
   c. Feedback Shift Register Generator

Linear Congruential Generator (LCG)

- Metode ini digunakan untuk membangkitkan bilangan acak dengan distribusi uniform
- Pseudo RNG, berbentuk :

$$Z_i = (a \,.\, Z_{i-1} + c) \bmod m$$

Dimana :

Z_i = nilai bilangan ke-*i* dari deretnya (RN yang baru)

Z_{i-1} = nilai bilangan sebelumnya (RN yang lama/semula)

a = konstanta pengali

c = *increment* (angka konstan yang bersyarat)

m = modulus (modulo)

Kunci pembangkit adalah Z_0 yang disebut *seed*.

- Bilangan acak seragam (Distribusi Uniform) : $U_i = Z_i / m$

Beberapa Persyaratan Bagi LCG

- Konstanta a, c, dan m adalah bilangan bulat positif ($a < m$ dan $c < m$)
- Sebaiknya konstanta c berangka ganjil jika m bernilai tidak terbagikan, sehingga memudahkan dan memperlancar perhitungan-perhitungan di dalam komputer dapat berjalan dengan mudah & lancar.
- Z_0 yang pertama, merupakan angka integer, ganjil dan cukup besar.
- Jika komputer biner dengan ukuran satu huruf adalah b bit, maka yang biasa digunakan untuk nilai m adalah $m = 2^b$ (yaitu jumlah total bilangan bulat nonnegatif yang dapat dinyatakan dengan kapasitas satu huruf)

Contoh LCG (1)

Membangkitkan delapan bilangan acak dengan asumsi :

a = 2, c = 7, m = 10, dan Z_0= 2

i	Z_{i-1}	Z_i (Random Integer Number)	U_i (Uniform R. N)
1	2	Z_1 = (2 * 2 + 7) mod 10 = 1	U_1 = 1 / 10 = 0,100
2	1	Z_2 = (2 * 1 + 7) mod 10 = 9	U_2 = 9 / 10 = 0,900
3	9	Z_3 = (2 * 9 + 7) mod 10 = 5	U_3 = 5 / 10 = 0,500
4	5	Z_4 = (2 * ..... + 7) mod 10 = ...	U_4 = ... / 10 = ...
5	.....	Z_5 = (2 * ..... + 7) mod 10 = ...	U_5 = ... / 10 = ...
6	.....	Z_6 = (2 * ..... + 7) mod 10 = ...	U_6 = ... / 10 = ...
7	.....	Z_7 = (2 * ..... + 7) mod 10 = ...	U_7 = ... / 10 = ...
8	.....	Z_8 = (2 * ..... + 7) mod 10 = ...	U_8 = ... / 10 = ...

Berdasarkan hasil perhitungan sebelumnya, diperoleh ke-delapan bilangan acak yang dibangkitkan yaitu:

Bilangan Ke-	Bilangan Acak (Ui)
1	0,100
2	0,900
3	0,500
4	.....
5	.....
6	.....
7	.....
8	.....

- Apakah terjadi pengulangan secara periodik ?
- Jika terjadi pengulangan, pada periode ke berapakah pengulangan terjadi ?
- Jika membangkitkan bilangan acak dilanjutkan hingga bilangan ke-10, apakah terjadi pengulangan secara periodik ?

Contoh LCG (2)

Membangkitkan delapan bilangan acak dengan asumsi :

a = 5, c = 7, m = 8, dan Z_0= 4

i	Z_{i-1}	Z_i (Random Integer Number)	U_i (Uniform R. N)
1	4	Z_1 = (5 * 4 + 7) mod 8 = 3	U_1 = 3 / 8 = 0,375
2	3	Z_2 = (5 * 3 + 7) mod 8 = 6	U_2 = 6 / 8 = 0,750
3	6	Z_3 = (5 * 6 + 7) mod 8 = 5	U_3 = 5 / 8 = 0,625
4	5	Z_4 = (5 * ..... + 7) mod 8 = ...	U_4 = ... / 8 = ...
5	.....	Z_5 = (5 * ..... + 7) mod 8 = ...	U_5 = ... / 8 = ...
6	.....	Z_6 = (5 * ..... + 7) mod 8 = ...	U_6 = ... / 8 = ...
7	.....	Z_7 = (5 * ..... + 7) mod 8 = ...	U_7 = ... / 8 = ...
8	.....	Z_8 = (5 * ..... + 7) mod 8 = ...	U_8 = ... / 8 = ...

Berdasarkan hasil perhitungan sebelumnya, diperoleh ke-delapan bilangan acak yang dibangkitkan yaitu:

Bilangan Ke-	Bilangan Acak
1	0,375
2	0,750
3	0,625
4	.....
5	.....
6	.....
7	.....
8	.....

- Apakah terjadi pengulangan secara periodik ?
- Jika membangkitkan bilangan acak dilanjutkan hingga bilangan ke-13, apakah terjadi pengulangan secara periodik ?

Contoh LCG (3)

Membangkitkan 20 bilangan acak dengan asumsi:

a = 21, c = 3, m = 16, dan Z_0= 13

Maka :

$$Z_1 = (21 * Z_0 + 3) \bmod 16$$
$$= (21 * 13+3) \bmod 16$$
$$= 276 \bmod (16)$$
$$= 4$$

Dan,

$$U_i = Z_i/16$$
$$= 4/16$$
$$= 0,2500$$

i	$21Z_{i-1}+3$	Z_i	$U_i = Z_i/16$
0		13	
1	276	4	0.2500
2	87	7	0.4375
3	150	6	0.3750
4	129	1	0.0625
5	24	8	0.5000
6	171	11	0.6875
7	234	10	0.6250
8	213	5	0.3125
9	108	12	0.7500
10	255	15	0.9375
11	318	14	0.8750
12	297	9	0.5625
13	192	0	0.0000
14	3	3	0.1875
15	66	2	0.1250
16	45	13	0.8125
17	276	4	0.2500
18	87	7	0.4375
19	150	6	0.3750
20	129	1	0.0625

Apakah ini berarti terjadi pengulangan secara periodik

Multiplicative Random Number Generator

$$Z_i = (a \cdot Z_{i-1}) \bmod m$$

- Agar Zi berprilaku acak yang dapat dipertanggungjawabkan :
  - Modulo m dipilih sebesar mungkin untuk memperbesar periode
  - a dipilih agar korelasi antar Z_i minimum
  - Benih Z_o: bilangan Bulat positif ganjil, $Z_o<m$
  - Bilangan acak : $U_i = Z_i/m$

Contoh

Membangkitkan lima bilangan acak dengan ketentuan :

a = 5, m = 8, dan Z_0= 4

i	Z_{i-1}	Z_i (Random Integer Number)	U_i (Uniform R. N)
1	3	Z_1 = (5 * 4) mod 8 = ...	U_1 = ... / 8 = ...
2	.....	Z_2 = (5 * .....) mod 8 = ...	U_2 = ... / 8 = ...
3	.....	Z_3 = (5 * .....) mod 8 = ...	U_3 = ... / 8 = ...
4	.....	Z_4 = (5 * .....) mod 8 = ...	U_4 = ... / 8 = ...
5	.....	Z_5 = (5 * .....) mod 8 = ...	U_5 = ... / 8 = ...

- Apakah terjadi pengulangan secara periodik ?

Mixed Congruential Random Number Generator

- Pseudo Random Number ini dapat dirumuskan dengan :

$$\mathbf{Z_i = \left[(a^n Z_{i-1}) + \left(\frac{a^n - 1}{a - 1} \right) C \right] mod\ \ m}$$

- Syarat utama n harus sejumlah bilangan integer dan lebih besar dari nol, rumus ini dikenal juga dengan nama 'Linier Congruential RNG'
- Namun apabila nilai C = 0 maka akan diperoleh rumus yang dikenal 'Multiplicative Congruent RNG'.