PAGE NO.
DATE :

RANDOM NUMBER

(i) MID-SQUARE METHOD

→ Take 4 digit no. Z_0
→ Square it and make it 8 digit by adding 0 on left
→ Take mid 4 digits
→ Continue the process n times

eg

i	Z_i	Random No	Z_i^2
0	7182	-	51581124
1	5811	0.5811	33767721
2	7677	0.7677	58936329
:			

DISADVANTAGE:

(i) if Z_i = 1009, process stops for such no's.
if Z_i = 3600, process stops with repetation of same Random no
(ii) numbers are not random. If we know any one no, we can find entire sequence.

→ Numbers generated by Arithmetic methods are PSEUDO-RANDOM. MID-SQUARE is also an arithmetic method.

(ii) CONDITIONS OF RANDOM-NO.

(a) Must be uniformly distributed b/w [0, 1]

Scanned by CamScanner

(b) Must generate random no.'s quickly
(c) Must require less storage
(d) 2 - random no. should not be correlated to each other
(e) Stream of random no.'s must be reproducible for 2 reasons
(i) we may want to use same series of random no.'s for different simulation
(ii) eases debugging and verification

(iii) LINEAR-CONGRUENTIAL GENERATOR (LCG)

$$Z_i = (aZ_{i-1} + c) \bmod m$$

Z_0, a, c, m is given
$0 < a < c < m$ and $Z_0 < m$

* The random no's start repeating after some random no. Z_i. So length of this cycle is called PERIOD of generator. The maximum period can be m. This type of generator is called FULL-LENGTH LCG.

* CONDITIONS FOR FULL-LENGTH LCG
(a) m and c are co-prime
(b) if q is a prime no. that divides m, then q should divide a-1
(c) If 4 divides m, then 4 divides a-1

Scanned by CamScanner

PAGE NO. _____
DATE : | | |

(iv) MIXED GENERATOR

In some computers, division was slow. Also, we wanted full cycle length. So, we choose

(i) $m = 2^b$, where b = no. of bits in a word.

EXPLICIT DIVISION CAN BE REPLACED BY SHIFT OPERATION

For 32-bit compiler, we choose $b = 31$ as last bit is for sign bit.

(ii) c is odd

(iii) $a - 1$ is divisible by 4

(iv) Z_0 = any number b/w $[0, m-1]$

(v) MULTIPLICATIVE GENERATOR

(i) $c = 0$

(ii) If we use $m = 2^b$, then we can not produce of cycle of $> 2^{b-2}$ i.e one-fourth of full length cycle. But we can produce cycle of $m-1$ by a correct choice of m.

(iii) m = largest prime $< 2^b$ and a is primitive element of m i.e $a^l - 1$ is divisible by m for smallest $l = m - 1$.

→ Period = $m - 1$. All no. b/w 1 to $m-1$ are produced once.

→ Called PRIME MODULUS MULTIPLICATIVE LCG.

Scanned by CamScanner

PAGE NO. _____
DATE : | | |

ISSUES

(i) as $m \neq 2^b$, we have to do explicit division

(ii) how to find primitive element of m

(v) TESTING OF RANDOM NO's

→ TEST FOR UNIFORMITY OF RANDOM NO's

(i) Kolmogorov Smirnov Test

(ii) Chi-squared test. (←)

KOLMOGORAV SMINOV TEST

(i) Rank no's in ascending order and label them as $i = 1, 2, \ldots N$

(ii) $D^+ = \max\left[\frac{i}{N} - R_i\right] \quad \forall\ i \in [1, N]$

$D^- = \max\left[R_i - \left(\frac{i-1}{N}\right)\right] \quad \forall\ i \in [1, N]$

$D = \max(D_i^+, D^-)$

(iii) $D < D_\alpha \rightarrow$ ACCEPTED UNIFORMITY

$D > D_\alpha \rightarrow$ NOT UNIFORM

(1) Random NO's = 0.44, 0.81, 0.14, 0.05, 0.93

$D_\alpha = 0.565 \ (\alpha = 0.05)$

Test for Uniformity

Scanned by CamScanner

Ans.

i	1	2	3	4	5
R_i	0.05	0.14	0.33	0.74	0.81
i/N	0.2	0.4	0.6	0.8	I.O.
D^+	0.15	0.26	0.27	0.36	
R_i	0.05	0.14	0.44	0.81	0.93
i/N	0.2	0.4	0.6	0.8	1.0
D^+	0.15	0.26	0.16	—	0.07
D^-	0.05	—	0.04	0.21	0.13

$D^+ = 0.26$ $\quad D^- = 0.21$

$D = 0.26$

$D < D_\alpha$ ∴ Accepted uniformity

SIMULATION

* Simulation is the process of designing a model of a real system and conducting experiments with the ~~syst~~ model for the purpose of understanding the behaviour for the operation of system
* we design a duplicate model of system and check its performance before building the actual system