Random Number Generator

by Chengwu Shen

Outline

- Background
- Pseudo-Random Number Generator (PRNG)
- True Random Number Generator (TRNG)
- Lottery Activity (with prize)
- Discussion
- References

Background

- Long long ago
  - Dice, coins and other devices

- 2000 years ago in Roman Empire

Background

- Tippett (1927)
  - A table of 41,600 random digits taken from a 1925 census report
- Fisher and Yates (1928)
  - A table with digits picked from a table of logarithms
- Kermark and Kendrick (1937)
  - Table of digits taken from a telephone directory
  - Proposed run test and gap test
- Kendall and Babington-Smith (1938)
  - First “machine”
  - Cardboard disk into 10 sectors, rotating 250 turns per minute.
  - Light beam flashed at random time, at **about 2 seconds**
  - Flashed sector number was **recorded by a human.**

First Page of table From Kendall and Babington-smith

Appendix

Random Sampling Numbers Produced by the Machine

1st Thousand

23157	54859	01837	25993	76249	70886	95230	36744
05545	55043	10537	43508	90611	83744	10962	21343
14871	60350	32404	36223	50051	00322	11543	80834
38976	74951	94051	75853	78805	90194	32428	71695
97312	61718	99755	30870	94251	25841	54882	10513
11742	69381	44339	30872	32797	33118	22647	06850
43361	28859	11016	45623	93009	00499	43640	74036
93806	20478	38268	04491	55751	18932	58475	52571
49540	13181	08429	84187	69538	29661	77738	09527
36768	72633	37948	21569	41959	68670	45274	83880
07092	52392	24627	12067	06558	45344	67338	45320
43310	01081	44863	80307	52555	16148	89742	94647
61570	06360	06173	63775	63148	95123	35017	46993
31352	83799	10779	18941	31579	76448	62584	86919
57048	86526	27795	93692	90529	56546	35065	32254
09243	44200	68721	07137	30729	75756	09298	27650
97957	35018	40894	88329	52230	82521	22532	61587
93732	59570	43781	98885	56671	66826	95996	44569
72621	11225	00922	68264	35666	59434	71687	58167
61020	74418	45371	20794	95917	37866	99536	19378
97839	85474	33055	91718	45473	54144	22034	23000
89160	97192	22232	90637	35055	45489	88438	16361
25966	88220	62871	79265	02823	52862	84919	54883
81443	31719	05049	54806	74690	07567	65017	16543
11322	54931	42362	34386	08624	97687	46245	23245

2nd Thousand

64755	83885	84122	25920	17696	15655	95045	95947
10302	52289	77436	34430	38112	49067	07348	23328
71017	98495	51308	50374	66591	02887	53765	69149
60012	55605	88410	34879	79655	90169	78800	03666
37330	94656	49161	42802	48274	54755	44553	65090
47869	87001	31591	12273	60626	12822	34691	61212
38040	42737	64167	89578	39323	49324	88434	38706
73508	30908	83054	80078	86669	30295	56460	45336
32623	46474	84061	04324	20628	37319	32356	43969
97591	99549	36630	35106	62069	92975	95320	57734

Pseudo-Random Number Generator

- generate random numbers by using mathematical formulae or precalculated lists
- 3 important characteristics
  - Efficient
    - Produce many numbers in a short time
  - Deterministic
    - A given sequence of numbers can be reproduced at a later date
  - Periodic
    - A sequence will eventually repeat itself

Pseudo-Random Number Generator

- Suitable for applications which require many numbers and need to replay same sequence easily
  - Simulation, modeling applications
- Not suitable for applications which require high unpredictability
  - Data encryption, gambling, lottery, random sampling
- Quality differs for different OS
  - GNU/linux
  - Windows
  - MacOS

Linear Congruential Generator

$$X_{n+1} = (aX_n + c) \mod m$$

where X(1...k) is a sequence of pseudorandom values;

m, the “modulus”, 0 < m;

a, the “multiplier”, 0 < a < m;

c, the “increment”, 0 <= c < m;

X_0, the “seed” or “start value”, 0 <= X_0 < m;

Linear Congruential Generator

m=9, a=2, c=0, seed=3

Result for one cycle (x1 to xk, k successive numbers): 6,3

m=9, a=2, c=0, seed=1

Result for one cycle (x1 to xk, k successive numbers): 2,4,8,7,5,1

True Random Number Generator

- Extract randomness from physical phenomena
  - Mouse movements,
  - time delay between keystrokes
  - Radioactive source decay
  - Atmosphere noise
- Essence: Identifying little and unpredictable changes in certain data
- Characteristics:
  - Inefficient
  - Nondeterministic
  - No period

Let's go Lottery

https://www.random.org/lists/

Discussion

- Quantum phenomenon or chaotic systems?
- View 1:
  - Quantum is nondeterministic, chaos is deterministic
  - TRNG used chaotic systems so deterministic
- View 2:
  - Quantum is nondeterministic, chaos indeterministic
  - TRNG used quantum phenomenon so nondeterministic
- View 3:
  - Quantum deterministic, chaos is deterministic
  - TRNG is deterministic
- Randomness: cannot be predicted by humans
  - Unpredictable enough for human application purposes

References

- https://www.iro.umontreal.ca/~lecuyer/myftp/slides/wsc17rng-history-talk.pdf
- https://en.wikipedia.org/wiki/Linear_congruential_generator
- https://www.random.org/randomness/