IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 18, Issue 6 Ser. I (Nov. – Dec. 2022), PP 18-20
www.iosrjournals.org

Optimal Choice of Mechanism for Random Selection

Dr. Raj KumariBahl[1], Prof. Yash Paul Sabharwal[2]
[1](*Associate Professor, Department of Statistics, Ramjas College, University of Delhi, India)*
[2](*Consulting Actuary, 27 Jaina Building, Roshanara Road, Delhi-110007, India)*

Abstract:
Random numbers are extremely important in cryptography (both quantum and classical), Statistics, probabilistic computation (Monte Carlo methods), numerical simulations, industrial testing and labeling, hazard games, scientific research, gaming, gambling and other fields. Random assignment in randomized controlled trials enables scientists to test hypotheses, and random numbers or pseudo random numbers help e-banking operations by generating 'One Time Passwords' or OTPs. Random numbers are generated through random number generators (RNGs). Random number generation is a process which, with the help of a device, creates a string of numbers or symbols that cannot be possibly predicted better than by a random chance. Although in the modern times, we have witnessed many sophisticated methods of random number generation, in this paper we look at traditional methods. We suggest mechanical mechanism for Random Selection of an item from a given list of items. Two criteria based on probabilistic considerations are suggested for optimal choice of the mechanism. Also reported are numerical results for commonly employed mechanisms. A part of the research problem considered here was also proposed as a puzzle[1].

Key Word*: Random Numbers, Random Number Generators, Minimum Effort, Binary Digits, Decimal Digits.*

Date of Submission: 02-11-2022 Date of Acceptance: 14-11-2022

I. Introduction

In the present day world, amidst pandemic situation, cyber space is becoming the new real world. Cyber security is extremely important for all businesses that involve a high degree of risk. In order to reduce the chance of information being leaked or hacked, random numbers are being commonly employed by business providers. Random numbers are generated through random number generators (RNGs). Random number generation is a process which, with the help of a device, creates a string of numbers or symbols that cannot be possibly predicted better than by a random chance. Random number generators can be classified into truly random hardware random-number generators (HRNGS), which generate random numbers as a function of current value of some physical environment attribute that is constantly changing in a manner that is practically impossible to model, or pseudo-random number generators (PRNGS), which generate numbers that look random, but are actually deterministic, and can be reproduced if the state of the PRNG is known. These random numbers are therefore referred to as pseudo random numbers. True random numbers, or more precisely non-deterministic random number generators, seem to be of an ever increasing importance. Random numbers are essential in Monte Carlo calculations, numerical simulations, statistical research, randomized algorithms, lottery etc. In fact, true random numbers are indispensable for cryptography and its numerous applications to cyber-security such as: Smart Energy Grid, e-banking, internet trade, prepaid cards etc.

These applications of random numbers have led to the development of many methods for generating random data, of which some have existed since ancient times, among whose ranks are well-known "classic" examples, including the rolling of dice, coin flipping, the shuffling of playing cards, the use of yarrow stalks (for divination) in the I Ching, as well as countless other techniques. Because of the mechanical nature of these techniques, generating large quantities of sufficiently random numbers (important in statistics) required much work and time. Thus, results would sometimes be collected and distributed as random number tables. One of the most important and most ancient methods of generating an*D*-digit random number table is by tossing an appropriate number of coins or dice. This technique is the focus of the paper. Indeed it is a well-known fact how W.G.Gosset used coin tossing experiments to generate the well-known Student's *t*- distribution[2].

In this paper, it is proposed to randomly select an item from amongst *D* distinct items, ensuring probability $\frac{1}{D}$ for each item. The suggested mechanism is to toss / roll *N* identical and homogeneous F-faced entities. *F*=2, *F*=4 and *F*=6 refer to the commonly known Coin Tossing, Tetrahedron and Cube Rolling scenarios respectively. The tossing/rolling are performed under controlled conditions as otherwise all external factors such as force with which the coin/dice is thrown, friction, gravitational force, wind flow, shape, size and weight of the experimental device can influence the result.

II. Essential Requirements

1. For a given *D*, *F* and *N* must satisfy $F^N \geq D$.

2. Assuming availability of a mechanism for tossing/rolling *N*, *F*-faced entities, thus suggesting the count of tossing/rolling to be the basic unit of effort.

3. Alternatively, if the tossing/rolling ought to be of an individual *F*-faced entity, the basic unit of effort will be *N*.

III. Probabilistic Considerations

With$F^N > D$, we can associate $\left[\frac{F^N}{D}\right]$ of the F^N outcomes with each of the *D* entities, where $\left[\frac{F^N}{D}\right]$ stands for the greatest integer function of $\frac{F^N}{D}$. Assuming equal probability for each outcome, probability *P* of success and *Q* of failure at a tossing/rolling will be

$P = \frac{D\left[\frac{F^N}{D}\right]}{F^N}$(1)

and

$Q = 1 - P.$ (2)

Waiting time for the first success is known to follow Geometric Distribution with

Mean Waiting Time = $\sum_{k=1}^{\infty} kPQ^{k-1} = \frac{1}{P}$. (3)

As stated above, two plausible functions for optimal solution to the random selection from the given *D* entities will be:

$C_1 = \frac{1}{P} = \frac{F^N}{D\left[\frac{F^N}{D}\right]}$ (4)

and

$C_2 = \frac{N}{P} = \frac{NF^N}{D\left[\frac{F^N}{D}\right]}$ (5)

where the latter refers to the average effort required to select an item.

IV. Numerical Results

We carried out numerical experiments with *F*=2, *F*=4 and *F*=6 and noted certain very interesting exceptions. For the case when *F*=2, i.e. coin tossing experiments are considered, for *D*=5, *D*=9 and *D*=10, minimum effort is obtained for the next higher number of tossing. This means that although for these three cases, 3, 4 and 4 tossed coins respectively would suffice, optimal effort is obtained with respectively 4, 5 and 5 coins. For *D*=5, the effort with 3 coins is 4.8 while with 4 coins it is 2.66666667. For *D*=9, the effort with 4 coins is 7.11111111 while with 5 coins it is 5.92592593. Finally for coin tossing set up, for *D*=10, the effort with 4 coins is 6.4 while with 5 coins it is 5.3333333. In the case of a tetrahedron, i.e. *F*=4, with *D*=9, a similar pattern emerges, i.e. although two rolling were enough; minimum effort is obtained with three rolling. For *D*=9, the effort with 2 rolling of tetrahedron is 3.55555556 while with 3 rolling it is 3.04761905. Also it is noteworthy that for the tetrahedron case, for *D*=10, equal effort is obtained for two and three rolling. These results are portrayed in Table 1 below which provides optimal choices of*F*,*N* for selected values of *D*. We denote the minimum number of tosses under C_1 by MN_1 and minimum number of tosses under $C_2$by MN_2. The effort in the two cases is denoted respectively by $E_1$and E_2. While *D*=2, *D*=8 and *D*=10 refer to the well-known binary, octal and decimal systems, *D*=4 and *D*=6 are used to generate `One Time Passwords' (OTPs) for banks and e-commerce retailers. It is interesting to note that a 6-digit code is now more commonly used as an OTP in comparison to a 4-digit one since it provides more space to generate elaborate combinations totally unique when compared to each other, thus making it difficult to hack. Moreover it also hits the sweet spot when it comes to memorizing numbers at a glance. The following table thus provides a bird's eye view of the effort required in generating such *D*-digit combinations by flipping a coin or rolling a tetrahedron or a die.

Table 1: Optimal choices of *F* and *N* for given values of *D*.

D	*F*	MN_1	E_1	MN_2	E_2
2	2	1	1.00000000	1	1.00000000
2	4	1	1.00000000	1	1.00000000
2	6	1	1.00000000	1	1.00000000
3	2	2	1.00000000	2	1.00000000
3	4	1	2.66666667	1	2.66666667
3	6	1	1.33333333	1	1.33333333
4	2	2	2.00000000	2	2.00000000
4	4	1	1.00000000	1	1.00000000
4	6	1	1.50000000	1	1.50000000
5	2	4	4.26666667	4	4.26666667
5	4	2	2.13333333	2	2.13333333
5	6	1	1.20000000	1	1.20000000
6	2	3	4.00000000	3	4.00000000
6	4	2	1.00000000	2	1.00000000
6	6	1	1.00000000	1	1.00000000
7	2	3	3.42857143	3	3.42857143
7	4	2	2.28571429	2	2.28571429
7	6	2	2.05714286	2	2.05714286
8	2	3	3.00000000	3	3.00000000
8	4	2	2.00000000	2	2.00000000
8	6	2	2.25000000	2	2.25000000
9	2	5	5.92592593	5	5.92592593
9	4	3	3.04761905	3	3.04761905
9	6	2	2.00000000	2	2.00000000
10	2	5	5.33333333	5	5.33333333
10	4	2,3	3.20000000	2,3	3.20000000
10	6	2	2.40000000	2	2.40000000

References

[1]. Bahl, R.K. and Sabharwal, Y.P. Puzzle 257.The Actuary, March 2001, p.38, 2001.
[2]. Trkulja, V. and Hrabač, P..The Role of *t*-test in Beer Brewing. Croatian Medical Journal, 61(1), p.69, 2020

Dr. Raj KumariBahl. et. al. "Optimal Choice of Mechanism for Random Selection." *IOSR Journal of Mathematics (IOSR-JM)*, 18(6), (2022): pp. 18-20.