Corpuscular Random Number Generator

Harsh Bhasin, *Member, IACSIT*

***Abstract*—If a sample of blood is taken it will have different cells having different hemoglobin content and volumes. No two samples of blood will have exactly same number of cells having same amount of hemoglobin or volume .If the above principle can be used to make a random number generator, then it will have the blend of nature along with the surety of the sample being truly random. The work proposes using the content of hemoglobin as the starting point of making a random number generator. The concept is exciting but during the research it was found that the behavior has been mathematically analyzed in 2010 [1].The problem therefore gave rise to another problem, that of converting the values generated by a mathematical function into a sample having very low coefficient of auto correlation and satisfying most of the properties of random numbers.**

***Index Terms*—Random number, corpuscular theory, RBC, pseudo random number generators.**

I. Introduction

The belief that two samples of blood will never contain the same number of cells having same hemoglobin content and volume and rigorous mathematical analysis is the basis of the work proposed. The random number generator will be called Corpuscle Random Number Generator (CRNG) here forth. The CRNG does not use the Pseudo Random Number Generator of the language in which it has been implemented. The algorithm has complexity of O (n^2) and does not require excessive computing powers as in Genetic Algorithms.

II. Random Number

Random number generation is the art of producing pure gibberish as quickly as possible. According to Eric Hoffer "creativity is the ability to introduce order into the randomness of nature". So in order to be creative also we need random numbers. It has been shown that most of the random number generators cannot be regarded as a 'true' random number generator. Since its output is predictable. The physical method of producing random number may include atomic or subatomic physical phenomenon .The need to generate random number as early as possible for cryptographic systems led to the creation of random bit generator Working at 300 gigabit per second at the bar LLAN University in Israel .In a random number generator even the slightest pattern cannot be tolerated. To detect such bias, we have a wide variety of tests. Test results are usually reported as a chi^2 measure. A chi^2 measure of ± 2 is probably random noise, ± 3 probably means the generator is biased, and ± 4 almost certainly means the generator is biased. In our case the chi square measure is approximately -2, which is considered as a good random sample. Moreover the above method opens window of AI to a new process of generation of Random numbers.

Manuscript received January 4, 2012; revised February 28, 2012.

Harsh Bhasin is working at Computergrad.com, India (e-mail: i_harsh_bhasin@yahoo.com).

III. Red Blood Cells

In healthy human adults, ~2.5×10^{11} new red blood cells (RBCs) are released from the bone marrow into the peripheral circulation per day, and about the same number are cleared. The cells composing the circulating population are thus continuously changing, but in healthy individuals the characteristics of the population are very stable. Recently, it has become possible to identify and characterize very young circulating RBCs (reticulocytes) [2]. RBCs undergo a rapid reduction in volume and hemoglobin in the few days after release from the bone marrow [3]. This rapid phase is followed by a much longer period of slower reduction; that is 4-7 days; during which volume and hemoglobin are co regulated .The variation in hemoglobin concentration is lower than that for volume and hemoglobin content . It has been shown in recent studies [1] that the variation of above two factors can be mathematically expressed as $f(\Delta) = 1/(1+e^{\Delta})$ where Δ is a factor proportional to the hemoglobin content and volume [1].

IV. Proposed Work

Step Number 1: Initial population generation

The value of $f(\Delta)$ of 3 samples of blood was analyzed the first being a very young sample called reticulocytes, second being middle aged blood cells about 50-60 days old and third being those cells which are old of about 80-90 days.

Since the value of the function decrease rapidly in the first few days therefore instead of taking a gap of 1unit, span of 0.01 unit has been taken till the value of Δ becomes 4.After that a span of 0.1 unit has been taken till the value of Δ becomes 7 after which a gap of 1 unit has been taken till Δ becomes 10.

The first set of values generates a smooth predictable graph shown in the Fig. 1.

The values generated are multiplied by 1000 and converted into integers giving a set of numbers ranging from about 500 to 0.The same procedure was applied to the other two samples but to make the values generated by the 3 sets comparable the values were multiplied by 10 to the power of α where α is two more than the highest power obtained in the

respective series. This step will be called moderation here forth.

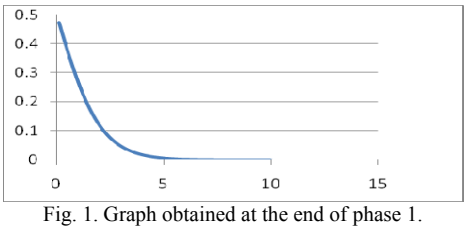

Fig. 1. Graph obtained at the end of phase 1.

The shape of the graph of the second and the third sample is similar to the first graph .The shape we obtain is predictable.

The task is now to apply a procedure which converts the graph into an unpredictable shape thus making it near impossible to predict the next vale of the random number generator.

Step number 2: Redundant value removal

The three set of values obtained in the previous step act as an input to the next module which removes the redundant values .The step is necessary to render backtracking to the original set of values difficult.

The results obtained by applying the step to the data obtained gives graph as shown in the Fig. 2.

The operation has converted the shape of the graph to almost linear. Three graphs were obtained of same nature were obtained in the step thus the set of values generates a n×3 matrix.

Step number 3 and 4: Transposition and redundant value removal

The matrix obtained in the previous step is transposed and is read column wise thus getting a large set of values .The repeated values are removed .To keep the things understandable only n values have been taken. The graph obtained in this step will be as shown in the Fig. 3.

Step Number 5: Conversion to Binary Numbers and inversion of each row

The numbers obtained in the previous step are converted into binary numbers thus giving us a new matrix

Step number 6: Cross Transposition

The first element of the first row is swapped with the last element of the last row. The second element of the first row is swapped with the second last element of the last row .The process swaps half the rows as shown in Fig. 4.

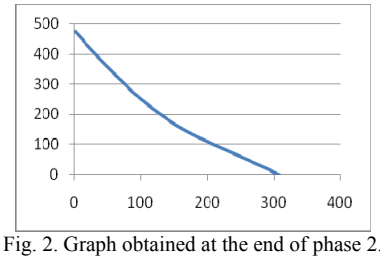

Fig. 2. Graph obtained at the end of phase 2.

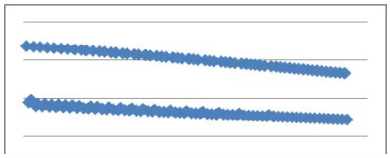

Fig. 3. Graph obtained at the end of phase 4.

1	1	0	0	1	1
1	0	0	0	1	1
1	1	1	1	0	0
1	0	1	1	1	0
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
1	1	1	0	0	0
0	1	0	1	0	1
1	1	1	0	1	0

Fig. 4. Example of cross transposition. The elements having same color are swapped.

1	1	0	0	1	1
1	0	0	0	1	1
1	1	1	1	0	0
1	0	1	1	1	0
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
1	1	1	0	0	0
0	1	0	1	0	1
1	1	1	0	1	0

Fig. 5. Only half the rows are swapped by the above process.

Step Number 7: Inversion of each row

Each row of the matrix so obtained is inverted.

Step Number 8: Removal of redundant values

The redundant values are removed thus generating a set of values which has coefficient of autocorelelation as -0.061. The graph obtained is shown in the Fig. 6.

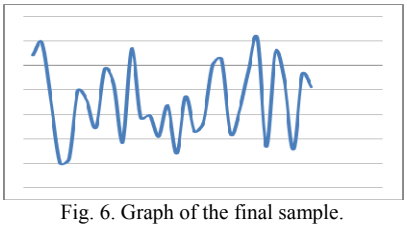

Fig. 6. Graph of the final sample.

The process can be summarized as shown in fig. 7.

V. Results

The above theory was tested by taking 20 set of values, that is 4000 values in total .A program in C was developed which takes the initial data as input and apply the above steps to generate the final set of values .The graphs were plotted in

excel and the graphs finally obtained showed no recognizable pattern.

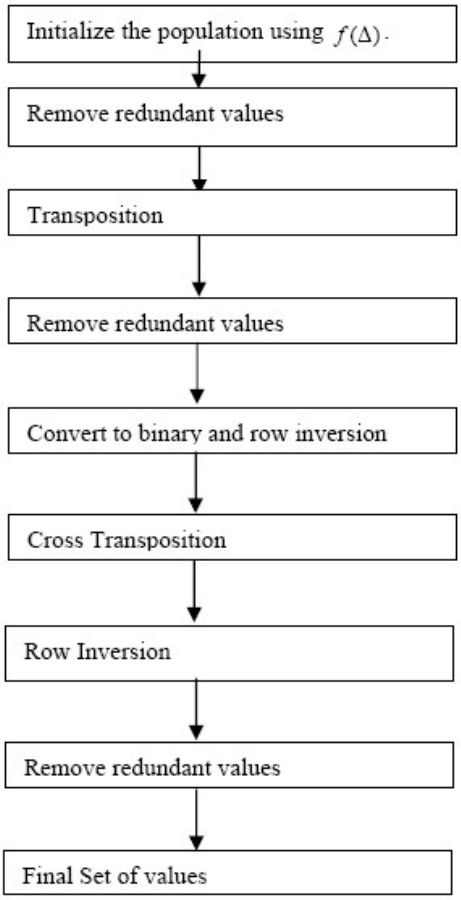

Fig. 7. Flow diagram of corpuscular random number generator.

The data obtained has a suitable coefficient of autocorrelation. The frequency test and gap test were applied to the data and the results were favorable. The following points are worth noting in the generator

- The above Random number generator does not use the pseudo random number generator of the language used.
- It works on the algorithm which has complexity of O (n^2).
- It does not require excessive resources.
- The idea came from a natural process that is the flow of blood.
- It gives a path to start with purely mathematical predictable function and generating values from the above but converting them into good random sample.

.

VI. Future Scope

The random number generator proposed above can generate a desired set of values by the process of modulation .In the experiment 3 set of values have been taken reticulocytes, middle aged blood cells and old blood cells .In the enhanced version of the CRNG 8 samples can be taken the very young blood cells, those having life 10-20 days, 20-30 days and so on.

The span between the values can be reduced to produce a large set of values. Moreover it has been found that the sample of blood contains 0.5 to 2 percent of the reticulocyes; we can incorporate the percentage composition to the software also. The importance of random numbers cannot be undermined they are used in cryptography for key generation. Their use in Artificial creativity is also explored .At the same time we must not forget that the present pseudo random number generators do not satisfy all the tests of randomness .There is a need , therefore to have a generator like CRNG which not only satisfy the tests of randomness but should also have low complexity and use minimal resources. The above theory needs to be implemented and tested for large set of values. Moreover it needs to be seen how better it is as compared to Random number generators based on cellular automata. The above theory is sure to give a way to produce good set of random numbers in spite of not using any Pseudo Random Number Generator.

References

[1] G. J. M. Higgins and L. Mahadevan. (November 2010). Physiological and pathological population dynamics of circulating human red blood cells. *PANS* [Online]. Available: http://www.pnas.org/content/early/2010/11/03/1012747107.abstract
[2] C. Plumb. (November 1994). Truly Random Numbers. *Dr.Dobbs Journal*, pp. 113.
[3] P. Zimmermann, *PGP Source Code and Internals*: MIT Press, 1995.
[4] J. Callas. (June 1996). Using and Creating Cryptographic-Quality Random Numbers, [Online]. Available: http://www.merrymeet.com/jon/usingrandom.html, 3 June 1996.
[5] T. Matthews, "Suggestions for random number generation in software," *RSA Data Security Engineering Report*, 15 December 1995, reprinted in RSA Laboratories' Bulletin no.1, 22 January 1996.
[6] B. Schneier, *Applied Cryptography (Second Edition), Bruce Schneier*: John Wiley and Sons, ch 4, 5, 1996.

Harsh Bhasin is a B. Tech (CSE), M. Tech (C. E), researcher. Many papers have been published\presented in IEEE conferences, International conferences, IJCA online, IJCSIT, IJCST, JCNWC and some national conferences and journals as yet. The topics that have been explored by him in the above papers are Genetic Algorithms, Cellular Automata, Natural Language processing, Corpuscular theory, Artificial Creativity.