ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

Quantifying the Error in CLT for Accurate GRN Generation

Shaik Jeelan Basha[1], L. Rangaswamy[2]

M.Tech Student, Dept. of ECE, SVIT College, Affiliated to JNTUA, AP, India[1] .

Assistant Professor, Dept. of ECE, SVIT College, Affiliated to JNTUA, AP, India[2]

.

ABSTRACT*:* Gaussian random numbers (GRNs) generated by central limit theorem (CLT) suffer from errors due to deviation from ideal Gaussian behavior for any finite number of additions. In this paper, we will show that it is possible to compensate the error in CLT, thereby correcting the resultant probability density function, particularly in the tail regions. We will provide a detailed mathematical analysis to quantify the error in CLT. This provides a design space with more than four degrees of freedom to build a variety of GRN generators (GRNGs). A framework utilizes this design space to generate customized hardware architectures. We will demonstrate designs of five different architectures of GRNGs, which vary in terms of consumed memory, logic slices, and multipliers on field-programmable gate array. Similarly, depending upon application, these architectures exhibit statistical accuracy from low (4σ) to extremely high (12σ). A comparison with previously published designs clearly indicate advantages of this methodology in terms of both consumed hardware resources and accuracy. We will also provide synthesis results of same designs in application-specific integrated circuit using 65-nm standard cell library. Finally, we will highlight some shortcomings associated with such architectures followed by their remedies..

I. INTRODUCTION

In probability theory, the central limit theorem (CLT) establishes that, for the most commonly studied scenarios, when independent random variables are added, their sum tends toward a normal distribution (commonly known as a bell curve) even if the original variables themselves are not normally distributed. In more precise terms, given certain conditions, the arithmetic mean of a sufficiently large number of iterates of independent random variables, each with a well-defined (finite) expected value and finite variance, will be approximately normally distributed, regardless of the underlying distribution. The theorem is a key concept in probability theory because it implies that probabilistic and statistical methods that work for normal distributions can be applicable to many problems involving other types of distributions.

To illustrate the meaning of the theorem, suppose that a sample is obtained containing a large number of observations, each observation being randomly generated in a way that does not depend on the values of the other observations, and that the arithmetic average of the observed values is computed. If this procedure is performed many times, the central limit theorem says that the computed values of the average will be distributed according to the normal distribution (commonly known as a "bell curve"). A simple example of this is that if one flips a coin many times the probability of getting a given number of heads in a series of flips should follow a normal curve, with mean equal to half the total number of flips in each series.

The central limit theorem has a number of variants. In its common form, the random variables must be identically distributed. In variants, convergence of the mean to the normal distribution also occurs for non-identical distributions or for non-independent observations, given that they comply with certain conditions.

In more general usage, a central limit theorem is any of a set of weak-convergence theorems in probability theory. They all express the fact that a sum of many independent and identically distributed (i.i.d.) random variables, or alternatively, random variables with specific types of dependence, will tend to be distributed according to one of a small set of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

attractor distributions. When the variance of the i.i.d. variables is finite, the attractor distribution is the normal distribution. In contrast, the sum of a number of i.i.d. random variables with power law tail distributions decreasing as $|x|-\alpha-1$ where $0<\alpha<2$ (and therefore having infinite variance) will tend to an alpha-stable distribution with stability parameter (or index of stability) of α as the number of variables grows.
Hence, it is very important to have a flexibility in design space for GRN generators (GRNGs). This paper comprises generation of accurate GRNs by correcting errors in CLT.
As suggested by the title of this paper, CLT is generally not used for the generation of high quality GRNs.

II. RELATED WORK

"Non-uniform random number generation through piecewise linear approximations," A hardware architecture for non-uniform random number generation, which allows the generator's distribution to be modified at run-time without reconfiguration is presented. The architecture is based on a piecewise linear approximation, using just one table lookup, one comparison and one subtract operation to map from a uniform source to an arbitrary non-uniform distribution, resulting in very low area utilization and high speeds. Customisation of the distribution is fully automatic, requiring less than a second of CPU time to approximate a new distribution, and typically around 1000 cycles to switch distributions at run-time. Comparison with Gaussian-specific generators shows that the new architecture uses less than half the resources, provides a higher sample rate and retains statistical quality for up to 50 billion samples, but can also generate other distributions. When higher statistical quality is required and multiple samples are required per cycle, a two-level piecewise generator can be used, reducing the RAM required per generated sample while retaining the simplicity and speed of the basic technique.
"Automatic generation of non-uniform random variates for arbitrary point wise computable probability densities by tiling," We present a rejection method based on recursive covering of the probability density function with equal tiles. The concept works for any probability density function that is pointwise computable or representable by tabular data. By the implicit construction of piecewise constant majorizing and minorizing functions that are arbitrarily close to the density function the production of random variates is arbitrarily independent of the computation of the density function and extremely fast. The method works unattended for probability densities with discontinuities (jumps and poles). The setup time is short, marginally independent of the shape of the probability density and linear in table size. Recently formulated requirements to a general and automatic non-uniform random number generator are topped. We give benchmarks together with a similar rejection method and with a transformation method.

"A hardware Gaussian noise generator using the box-muller method and its error analysis," We present a hardware Gaussian noise generator based on the Box-Muller method that provides highly accurate noise samples. The noise generator can be used as a key component in a hardware-based simulation system, such as for exploring channel code behavior at very low bit error rates, as low as 10-12 to 10-13. The main novelties of this work are accurate analytical error analysis and bit-width optimization for the elementary functions involved in the Box-Muller method. Two 16-bit noise samples are generated every clock cycle and, due to the accurate error analysis, every sample is analytically guaranteed to be accurate to one unit in the last place. An implementation on a Xilinx Virtex-4 XC4VLX100-12 FPGA occupies 1,452 slices, three block RAMs, and 12 DSP slices, and is capable of generating 750 million samples per second at a clock speed of 375 MHz. The performance can be improved by exploiting concurrent execution: 37 parallel instances of the noise generator at 95 MHz on a Xilinx Virtex-II Pro XC2VP100-7 FPGA generate seven billion samples per second and can run over 200 times faster than the output produced by software running on an Intel Pentium-4 3 GHz PC. The noise generator is currently being used at the Jet Propulsion Laboratory, NASA to evaluate the performance of low-density parity-check codes for deep-space communications.

III. EXISTING SYSTEM

Required speed and accuracy of GRNs differ greatly for various applications. For example, a tail accuracy from 4σ to 6σ is good enough for simulation of a product failure; whereas evolution algorithms require a tail accuracy of more than 9σ. Similarly, a Rayleigh fading channel requires low tail accuracy 4σ at low rate (few million samples per

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

second). On the other hand, a real-time multiple-input and multiple-output channel emulator may require GRN generation at extremely high rate (of the order of billion samples per second) with relatively low tail accuracy of 4σ. Another implementation is provided a more efficient approach based on polynomial curve fitting techniques and a hybrid (combination of logarithmic and uniform) segmentation scheme to approximate the BM functions. This design guaranteed a tail accuracy of 6.6σ generating 496 million GRNs per second and utilizing only 534 logic slices on Xilinx Virtex-2 FPGA. The design was scalable and capable of providing higher tail accuracy at the cost of a more complex address generator. We proposed a more optimized approach for piecewise polynomial approximations and hybrid segmentation schemes to evaluate the BM functions that significantly minimized the resource utilization (40% less than the previous best implementation). A GRNG commercially provided by Xilinx as an IP core is based on the hardware implementation of BM method. Maximum tail accuracy is 4.2σ and throughput is 245 million samples per second. An ASIC chip implementation of BM Method, However, the guaranteed accuracy was limited to 4σ and also, the quality of Gaussian samples was poor.

Disadvantages

• Power consumption is high
• Area coverage is high

IV. PROPOSED METHOD

1) A detailed mathematical analysis to quantify the difference between ideal Gaussian probability density function (pdf) and the one that results from the addition of *n* numbers. This provides a flexible design space with more than four degrees of freedom that can be utilized to built a variety of efficient GRNGs ranging from low cost/accuracy to the ones with very high tail accuracy.

2) A framework that utilizes above mentioned design space and allows a designer to build efficient GRNGs tailored specifically for a given application. The framework also enables verification of statistical accuracy of the GRNG before actual hardware implementation; thereby, saving significant verification time.

3) Hardware implementation of five GRNGs using above framework. These provide tail accuracies varying from 4*σ* to 12*σ*, whereas consuming fewer hardware resources than any of the previously published designs.

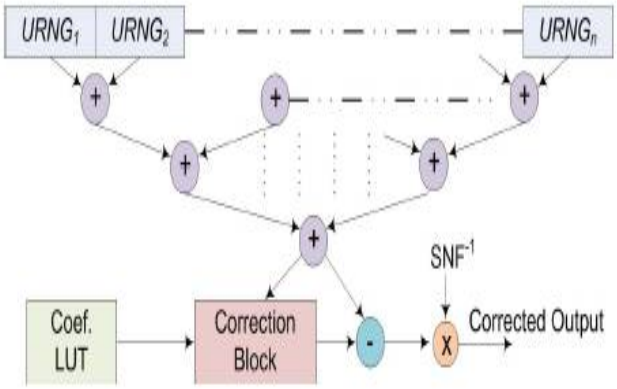

Fig 1 Generic CLT-based hardware GRNG.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

V. SIMULATION RESULTS

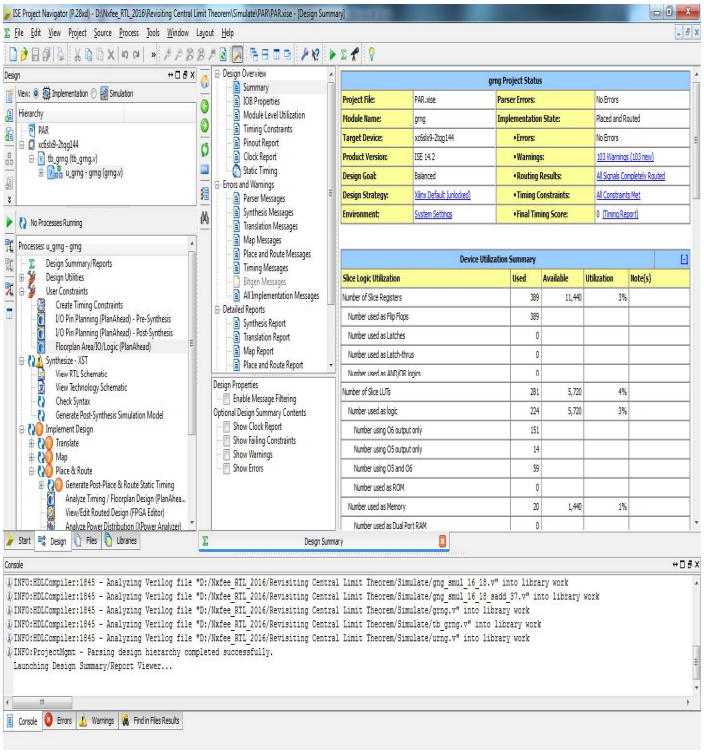

Fig 2: Synthesis report

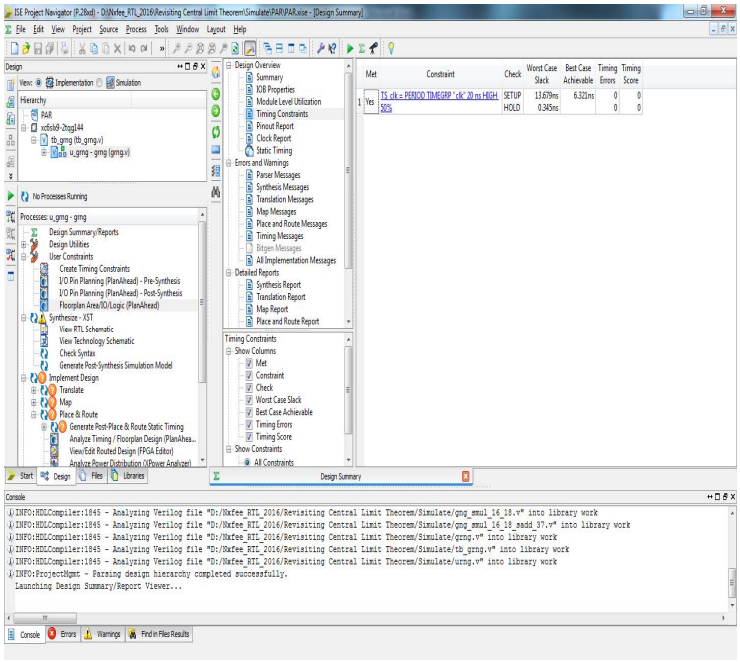

Fig 3: Timing report

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

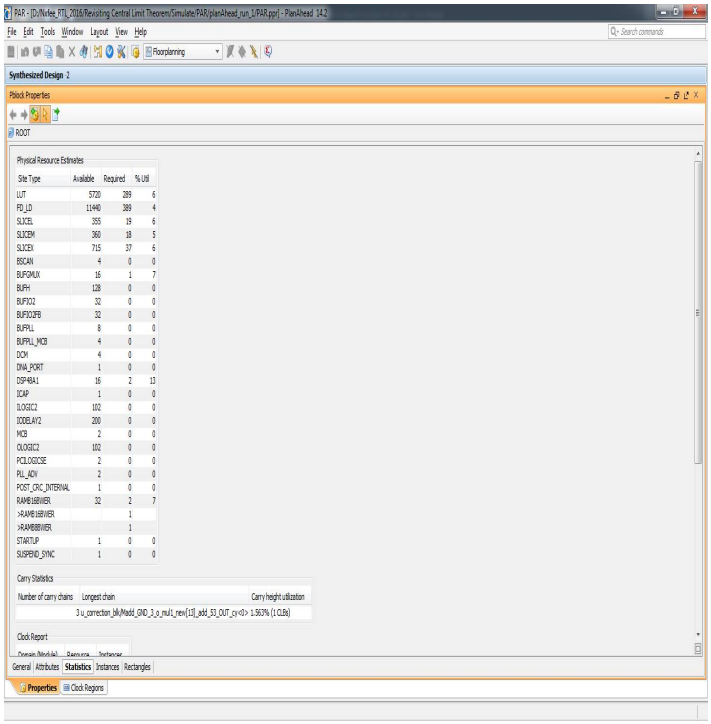

Fig 4: Area report

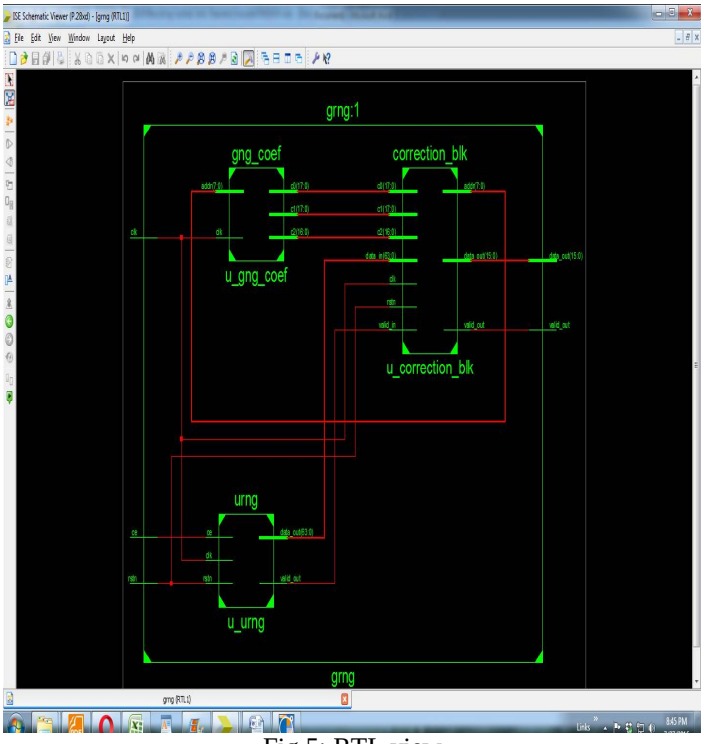

Fig 5: RTL view

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

VI. CONCLUSION

In this paper, we described how effectively the CLT can be used to produce statistically accurate GRNs at low cost using a novel framework. We demonstrated the framework by providing implementation of five different architectures that use same underlying methodology, exhibit different accuracies, and consume varying hardware resources. We illustrated

GRNGs providing tail accuracy as high as 12σ as well as ones which provide 1.75 giga samples per second. To further complement this paper, fully automated algorithms can be explored to find optimal GRNGs in the available design space suitable for specific applications. Similarly nonlinear segmentation algorithms could be explored to achieve GRNs with lower memory requirements and better accuracy.

REFERENCES

1. J. S. Malik, J. N. Malik, A. Hemani, and N. D. Gohar, "An efficient hardware implementation of high quality AWGN generator using BoxMuller method," in Proc. 11th ISCIT, Oct. 2011, pp. 449–454.
2. Additive White Gaussian Noise (AWGN) Core, v: 1.0, Xilinx Inc, San Jose, CA, USA, 2002.
3. E. Fung, K. Leung, N. Parimi, M. Purnaprajna, and V. C. Gaudet, "ASIC implementation of a high speed WGNG for communication channel emulation [white Gaussian noise generator]," in Proc. IEEE Workshop SIPS, Oct. 2004, pp. 304–309.
4. D.-U. Lee, W. Luk, J. D. Villasenor, G. Zhang, and P. H. W. Leong, "A hardware Gaussian noise generator using the Wallace method," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 13, no. 8, pp. 911–920, Aug. 2005.
5. D. B. Thomas and W. Luk, "Non-uniform random number generation through piecewise linear approximations," IET Comput. Digit. Techn., vol. 1, no. 4, pp. 312–321, 2007.
6. D. B. Thomas, L Howes, and W. Luk, "A comparison of CPUs, GPUs, FPGAs, and massively parallel processor arrays for random number generation," in Proc. ACM/SIGDA Symp. FPGA, 2009.
7. J. S. Malik, J. N. Malik, A. Hemani, and N. D. Gohar, "Generating high tail accuracy Gaussian random numbers in hardware using central limit theorem," in Proc. 19th Int. Conf. VLSI-SoC, 2011, pp. 60–65.
8. P. Kabal, "Generating Gaussian pseudo-random deviates," Dept. Elect. Comput. Eng., McGill Univ., Tech. Rep., 2000.
9. R. J. Andraka and R. M. Phelps, "An FPGA based processor yields a real time high fidelity radar environment simulator," MAPLD, Greenbelt, MD, USA, 1998.
10. D. B. Thomas and W. Luk, "The LUT-SR family of uniform random number generators for FPGA architectures," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 4, pp. 761–770, Apr. 2013.
11. D. B. Thomas and W. Luk, "FPGA-optimized uniform random number generators using LUTs and shift registers," in Proc. Int. Conf. FPL, Aug./Sep. 2010, pp. 77–82.
12. D. B. Thomas and W. Luk, "High quality uniform random number generation through LUT optimized linear recurrences," in Proc. IEEE Field-Programmable Technol., Dec. 2005, pp. 61–68.