BoxMuller AWGN Signal Generator For FPGA

V1.0

Curve Technology

www.curvtech.com

info@curvtech.com

2018/8/26

Revision History

Date	Version	Revision
2018.08.26	V1.0	Initial release

Features

- Based on the Box-Muller algorithm with no central limit theorem required
- Piecewise polynomial based Chebyshev function approximation units with range reduction
- Period of generated noise sequence is 2^88 (about 10^25)
- 18-bit noise samples with 5 bits of integer and 13 bits of fraction, accurate to one unit in the last place (ulp) up to 8.1573σ, which models the true Gaussian PDF accurately for a simulation size of over 10^{15} samples
- Core can be reset to its initial state and work on clock enable signal
- Bit-true MATLAB and C mex programs included
- Maximum clock rate and output sample rate of 320MHz on Xilinx VCU108 Board

Box-Muller Algorithm

The **Box–Muller transform**, by George Edward Pelham Box and Mervin Edgar Muller [1], is a pseudo-random number sampling method for generating pairs of independent, standard, normally distributed (zero expectation, unit variance) random numbers, given a source of uniformly distributed random numbers.

The Box-Muller method starts with two independent uniform random variables, u_0 and u_1, over the interval [0, 1). The following mathematical operations are performed to generate two samples, x_0 and x_1, of a Gaussian distribution N(0,1).

$$x_0 = \sqrt{-2\ln(u_0)}\sin(2\pi u_1) \quad (1)$$

$$x_1 = \sqrt{-2\ln(u_0)}\cos(2\pi u_1) \quad (2)$$

Split the procedure into three steps for hardware implementation:

$$e = -2\ln(u_0) \quad (3)$$

$$f = \sqrt{e} \quad (4)$$

$$g0 = \sin(2\pi u_1), g1 = \cos(2\pi u_1) \quad (5)$$

Normal Distribution Performance Test

Test Environment

Taus_URNG, seeds are 2846420573 2846420573 2846420573
Taus_URNG, seeds are 912462866 912462866 912462866

Test Generated samples number for analysis: 1e7

Fixed point Accuracy Evaluation

Fixed point output is compared to float point model (with same URNG input):

	Floor truncation	Round
e max error value (abs)	6.3224e-08	3.4341e-08
f max error value (abs)	3.1588e-05	2.3977e-05
g0/g1 max error value (abs)	1.0174e-04 1.0174 e-04	1.1467e-04 1.1467 e-04
x0/x1 max error value (abs)	4.8891e-04 4.8123e-04	5.5051e-04 6.1058e-04
x0/x1 mean value	-5.6479e-04 8.4952e-05	-5.6477e-04 8.4947e-05
x0/x1 variance value	0.99978 1.0001	0.99982 1.0001

The results show that accuracy loss caused by truncation can be neglected. So truncation method is used in hardware.

Anderson-Darling test result

adtest result (vs. MATLAB *randn()* function):

	H	P	adsta	cv
This design	0	0.7810	0.2398	0.7519
MATLAB randn()	0	0.3270	0.4209	0.7519

Distribution Figure

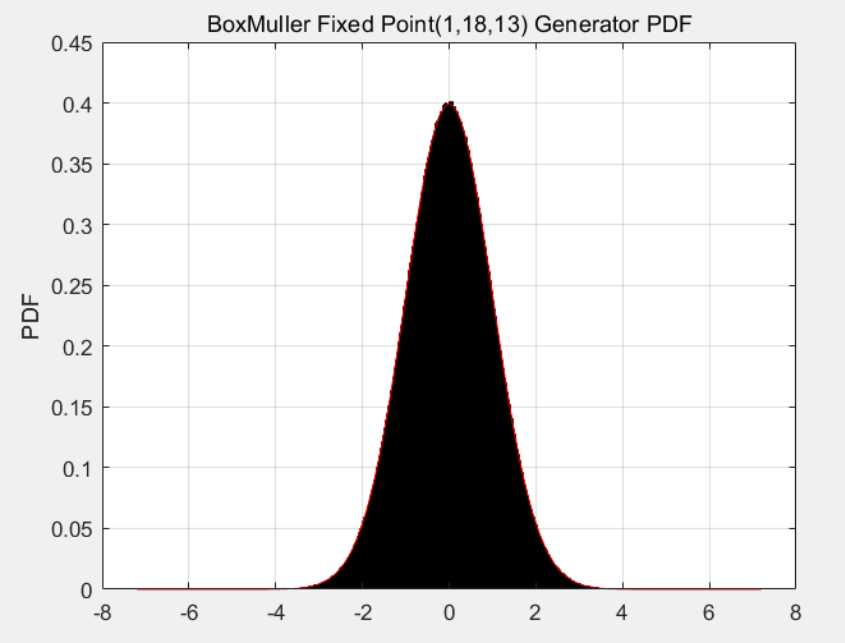

Figure 3. PDF Distribution of generated 1e7 samples

Resource Utilization and Throughput

Xilinx VCU108 FPGA Evaluation Board

Fmax : 330MHz (can be improved further more)

Latency : 16 cycles

Utilization Post-Synthesis | **Post-Implementation**

Graph | **Table**

Resource	Utilization	Available	Utilization %
LUT	1767	537600	0.33
LUTRAM	127	76800	0.17
FF	915	1075200	0.09
BRAM	2.50	1728	0.14
DSP	8	768	1.04
IO	23	832	2.76
BUFG	1	960	0.10

Figure 4. Resource Utilization

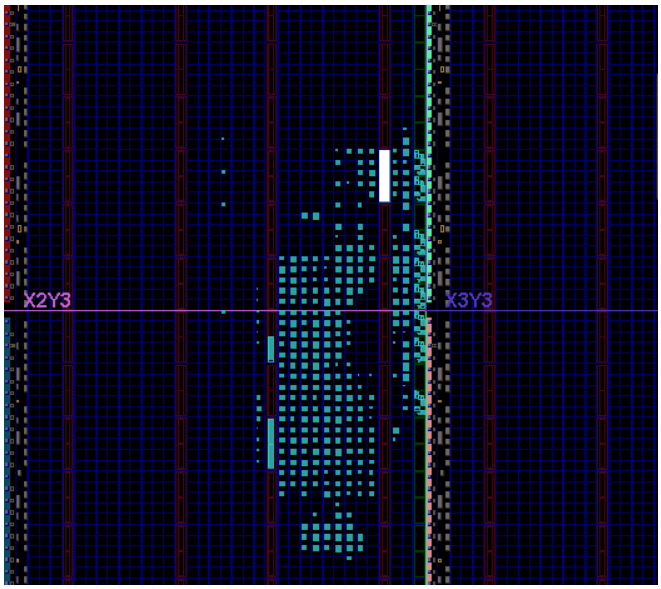

Figure 5. After Place and Route Photograph on Xilinx FPGA

Reference

[1] G. E. P. Box and Mervin E. Muller, *A Note on the Generation of Random Normal Deviates*, The Annals of Mathematical Statistics (1958), Vol. 29, No. 2 pp. 610–611 doi:10.1214/aoms/1177706645, JSTOR 2237361

[2] Box-Muller Transform wiki page https://en.wikipedia.org/wiki/Box%E2%80%93Muller_transform#cite_note-1

[3] R.C. Tausworthe, "Random Numbers Generated by Linear Recurrence Modulo Two," Math. and Computation, vol. 19, pp. 201-209, 1965.

[4] P. L'Ecuyer, "Maximally Equidistributed Combined Tausworthe Generators," Math. Computation, vol. 65, no. 213, pp. 203-213, 1996.

[5] M. J. Schulte and E. E. Swartzlander, "Hardware designs for exactly rounded elementary functions," IEEE Transactions on Computers, vol. 43, no. 8, pp. 964–973,Aug 1994.

[6] D. U. Lee, J. D. Villasenor, W. Luk, and P. H. W. Leong, "A hardware Gaussian noise generator using the box-muller method and its error analysis," IEEE Transactions on Computers, vol. 55, no. 6, pp. 659–671, June 2006.

[7] Lincoln Glauser, "The Design of a 24-bit Hardware Gaussian Noise Generator via the Box-Muller Method and its Error Analysis", (2017). Tesis. Rochester Institute of Technology.