Effective and fast generation of independent true random numbers and the central limit theorem

Rolf Freitag, University of Ulm

(April 15, 2001)

Abstract

Based on the central limit theorem, we present a new way to produce independent true random numbers out of n true random numbers which will work for $n = 2$ too. The key idea is to generate a random number by adding n true random numbers modulo m. The mathematical proof of this method is a numeric calculation for small $n > 0$ and the central limit theorem for large n. Because the n primary numbers can have low Markow entropies, this method is easy to implement in hardware and can also be used in processors.
Keywords: true random numbers, true random bits, central limit theorem, exclusive-or, exclusive-nor, exor, exnor

1 Introduction

In practice it's not simple to produce true random numbers, because real processes generally are not completely random. The radioactive decay for example is known to decrease with increasing time and radioactive detectors suffer from artefacts like a finite deadtime and depend on parameters like temperature and magnetic field. They do also show several aging effects.
Because of this, random numbers from hardware random number generators normally need an after-treatment although their low speed (less than 20 kilobyte per second) disqualifies them for supercomputing applications like monte carlo simulations and real time high speed applications like crosscorrelation measurements.
The main problem of most true random number generators is that they are prohabilistic, they do only 'something random' which can't be calculated or theoretically described.

The new true random number generation method avoides these disadvantages in order to be applied in digital ICs e. g. CPUs. This is important because a computer equipped with a generator of this type can avoid the effort of computing pseudorandom numbers.

It is known from the central limit theorem that the sum of many true random numbers is normally distributed if the Lindeberg criterion is fulfilled, which e. g. is the case for true random bits. That means e. g. that it is possible to produce a normally distributed random number by producing many true random bits even with low Markow entropies and adding them with a adder.
For simplicity we focus attention on the sum of m random bits modulo $k = 2$ because $k < 2$ is trivial, $k > 2$ is similar and the inverse (exnor) is also similar. The sum modulo

$k = 2$ can be implemented easily, fast, and cheap because the sum modulo 2 can be calculated with a simple parity generator; if $m = 2$ the parity generator is simply one exor gate. Because the m random bits can be taken from m bit random numbers and a l bit random number is simply a sequence of l random bits, it's not necessary to focus on more than random bits.

2 Exoring of two random Bit Sequences

Using the entropy [1] of a random bit sequence

$$E_1 = -p(0) \cdot log_2(p(0) - p(1)) \cdot log_2(p(1)) \tag{1}$$

it is easy to calculate the entropy of the sequence which is the *exor* of two similar and statistical independent random bit sequences minus the entropy of one pimary sequence:

$$\begin{aligned} E_2 - E_1 = -(x^2 + (1-x)^2) \cdot log_2(x^2 + (1-x)^2) \quad & -2 \cdot x \cdot (1-x) \cdot log_2(2 \cdot x \cdot (1-x)) \\ +x \cdot log_2(x) + (1-x) \cdot log_2(1-x) & \end{aligned} \tag{2}$$

with $x = p(0)$ and $1 - x = p(1)$.

For not perfect random sequences, i. e. $0 < x < 1, \quad x \neq 0.5$, this difference is positive, which can be shown numerically and graphically (Fig. 1)

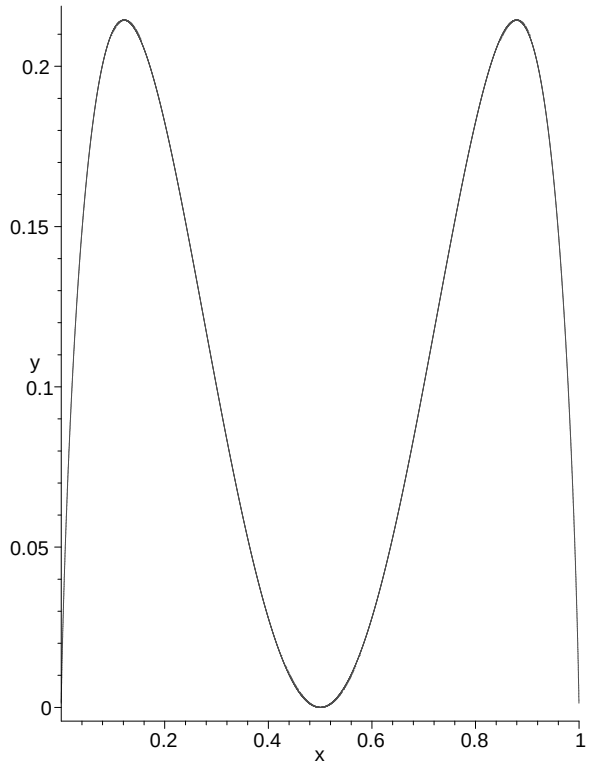

Figure 1: $y = E_2 - E_1$

Therefore the exoring of 2^n $(n > 0)$ is similar and independent random bit sequences generates a secondary random bit sequence with a greater entropy.
Because equation (2) is independent of the previous bits, the same is true for the Markov entropies.

3 Exoring of n random Bit Sequences

Due to the central limit theorem [2] the density function of the sum k of $n \gg 1$ random bits is (nearly) the normal distribution, because this sum complies with the Lindeberg condition.

If the peak value p_v of the density function is exactly $m+0.5$ ($m \in \mathbb{N}$) the amplitude of the density function at $m-l-1$ ($l \in \mathbb{N}$) is the same as at $m+l$ and hence the sum modulo 2 has an exact 50% probability to be 0 or 1. This is the best case, because it means that a sequence of these secondary bits has an entropy of exact 1.0 bit/bit.

In the worst case, $p_v = m$ ($m \in \mathbb{N}$), the absolute value of the difference of the probability that the sum modulo 2 is 0 and the probability that the sum modulo 2 is 1 is

$$\mid p(0) - p(1) \mid_{worst\ case} = \frac{1}{\sigma \cdot \sqrt{2 \cdot \pi}} \left(1 - 2 \cdot \sum_{k=1}^{\infty} \left(e^{-\frac{(2 \cdot k-1)^2}{2 \cdot \sigma^2}} - e^{-\frac{(2 \cdot k)^2}{2 \cdot \sigma^2}} \right) \right) \quad . \tag{3}$$

Due to the Ars conjectandi [3] the standard variance is proportional $\sqrt{n}$, i. e. $\sigma = c \cdot \sqrt{n}$, and therefore

$$\mid p(0) - p(1) \mid_{worst\ case} = \frac{\sqrt{2}}{c \cdot \sqrt{n \cdot \pi}} \left(\sum_{k=1}^{\infty} \left(e^{-\frac{(2 \cdot k-1)^2}{2 \cdot c^2 \cdot n}} - e^{-\frac{(2 \cdot k)^2}{2 \cdot c^2 \cdot n}} \right) \right) \quad . \tag{4}$$

The limit value of this expression for $n \to \infty$ is simply zero and it is monotonic decreasing with increasing n (Fig. 2)

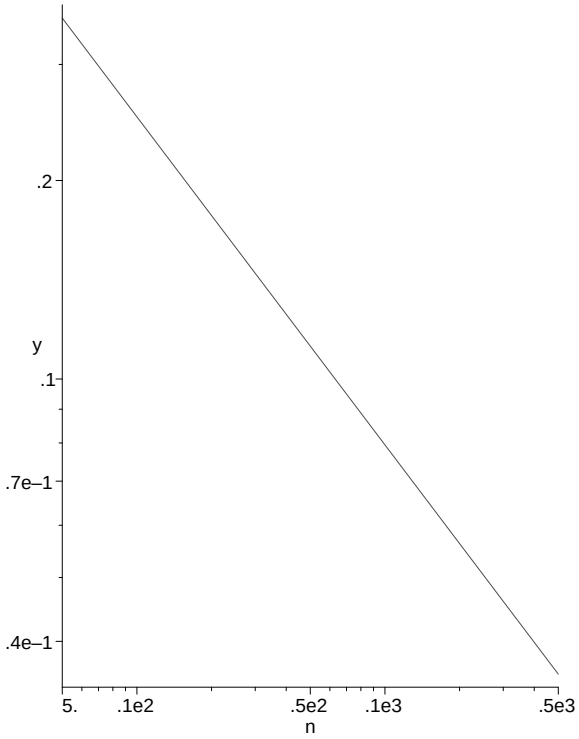

Figure 2: $y = \mid p(0) - p(1) \mid_{worst\ case}$, $c = 0.5$

So even in the worst case the generation of a high entropy random bit sequence by exoring n low entropy random bit sequences is no problem because the primary random

bit sequences don't have to be statistical independent.
Because equation (4) is independent of the previous bits, the same is true for the Markov entropies.

Acknowledgments

I wish to thank M. Haupt and M. Schulz for their comments.

References

[1] Völz, Holz: *Grundlagen der Information*, Berlin, 1991, page 25

[2] Bronstein, Il'ja N.: *Taschenbuch der Mathematik*, 24. ed., 1989, page 667

[3] Brenig, Wilhelm: *Statistische Theorie der Wärme, Volume 1: Gleichgewichtsphänomene*, Berlin, New York, 3. ed., 1992, page 22