

Corrections of

"Transform of various Random Noises in sequences of proved random numbers"
by René BLACHER

1 Corrections for reviewer 1

In phrase 1 of the summary I replace "In a previous paper, we have shown how to obtain sequences of numbers proved random." by "In a previous paper, we have shown how to obtain sequences of numbers proved random : these sequences can be regarded as a sample of IID sequences of random variables."

In phrase 1 of section 1.1 "To have IID random numbers" is replaced by "To have IID random or pseudo-random numbers"

At the end of section 6.1, I add in the footnote of "This is especially true for texts: a text is a noise randomly chosen : *footnote* : It is not surprising...."

"This is especially true for texts: a text is a noise randomly chosen : *footnote* : We mean that text can be regarded as a realization of some sequences of random variables. It is not surprising...."

In section 6.4, new pages 17-18, I add

" Indeed, a way in order to understand what we want to mean when we say "noises not too deterministic" is to compare with min -entropy : $H_\infty(X) = \min_x \log\left(\frac{1}{P\{X=x\}}\right)$. Indeed, by Shaltiel (2011), if $H_\infty(X) \leq qN$, T_q cannot be an 0-extractor : i.e. a necessary condition in order that $T_q(Y_n^\theta)$ is IID is that $P\{(Y_1^\theta, \dots, Y_N^\theta) = (\eta_1, \dots, \eta_N)\} \leq \frac{1}{2^{qN}}$ for all $m(\eta_1, \dots, \eta_N) \in \{0, 1, \dots, m-1\}^N$. If it is not case, we say "the noise y_n is too deterministic".

For example, assume $m = O(4 * 10^{36})$, $q = 33$ and $N_0 = 10^5$. Then, if y_n is not too deterministic, $P\{(Y_1^\theta, \dots, Y_N^\theta) = (\eta_1, \dots, \eta_N)\} = O(\beta)$ where $\beta = 1/m^N$. Then, if $H_\infty(X) \leq qN$, $\frac{m^N}{2^{qN}} = \left(\frac{m}{2^q}\right)^N \geq 5^{33N}$. Then, there exists $(\eta_1^0, \dots, \eta_N^0)$ such that $P\{(Y_1^\theta, \dots, Y_N^\theta) = (\eta_1^0, \dots, \eta_N^0)\} = O(5^{33N}\beta)$. Of course, in this case, there is a very big breakdown of randomness and one can say that Y_N^θ is very deterministic. "

We replace section 8.1

" 8.1 Description of the method

We are interested in the choice of parameters in the building of IID sequences. Then, we consider the case of sequences of noises $y'_n \in \{0, 1, \dots, m-1\}$, $n = 1, 2, \dots, N_0$. We set $y_n = \overline{y'_n + rand_0(n)}/m$ where $rand_0(n)$ is pseudo random generator. Then, by applying Remark 4.3, we shall impose that

$$\sqrt{\frac{N_0^3 q 2^q}{m}} \leq 1/N_0 .$$

Remark that this condition is less good than the condition used when one impose that the Lipschitz coefficients K_0 are small : $\frac{\gamma(m)K_0 N_0 2^q}{m} \leq 10^{-3}$. "

by

" 8.1 Choice of parameters

We are interested in the choice of parameters in the building of IID sequences. Then, we consider the case of sequences of noises $y'_n \in \{0, 1, \dots, m-1\}$, $n = 1, 2, \dots, N_0$. We set $y_n =$

$\overline{y'_n + rand_0(n)}/m$ where $rand_0(n)$ is pseudo random generator. Then, by applying Remark 4.3, we shall impose that

$$\sqrt{\frac{N_0^3 q 2^q}{m}} \leq 1/N_0 .$$

Remark that this condition is less good than the condition used when one impose that the Lipschitz coefficients K_0 are small : $\frac{\gamma(m)K_0 N_0 2^q}{m} \leq 10^{-3}$. "

2 Corrections for reviewer 2

Page 2 : I replace "Central Limit Theorem" by "Central Limit Theorem (CLT)" .

Page 3, line 7 : I replace "defined on a probability space $(\Omega, \mathcal{A}, P)$ and let be $y_n = Y_n(\omega).....$ " by " defined on a probability space $(\Omega, \mathcal{A}, P)$. Let....." .

In page 5, theorem 2, I replace $P_{X_n}(Bo)$ by $P_{X_n^\theta}(Bo)$

In Remark 1.1 : I replace e by f.

Page 7, line 11, I replace IID by IID.

In Example 3.1, I replace "Let $\mathcal{T}_1$ be a test in order to know if a sequence y_n admits a random sequence Y_n , $n = 1, 2, ..., n_I$ as model." by "Let $\mathcal{T}_1$ be a test in order to test the hypothesis $<<$ the sequence y_n^1 , $n = 1, 2, ..., n_I$, is a realization of the sequence of random variables Y_n^1 , $n = 1, 2, ..., n_I$, $>>$."

6.1 line 9 We replace $P_e(Y_n \in E)$ by $P_e(y_n \in E)$

Page 13, Proof of theorem 2 : We write "the previous results hold for various b. Then, we can choose....."

Lemma 4-1 : I add : "it is enough to use the CLT".

Moreover, a list of Symbols is added : section 1.6

3 Corrections for reviewer 3

At the end of section 1.1, I write "Now we can also show that the technique used is valid in many other cases than distributions with Lipschitz coefficients not too large: it is the aim of this paper".

At the begining of section 1.4, I add " Then, we shall now see that functions T_q transforms the vast majority of noises in IID sequences."

In section 4.1, I write " **This method can be applied as soon as $\sum_{\gamma_s \in \mathcal{G}_k} P\{Y_n^\theta = \gamma_s | Y_{n-s}^\theta = y'_s, s = 1, ..., p\}$ behaves as sums randomly chosen (cf section 5). It will be shown below that it is generally the case for the vast majority of models. To prove this, we need a measure on all models Y_n^θ which takes account of this fact. "**

At the end of section 1.4, I add **As a matter of fact, we understand in this paper that functions T_q transforms noises which are not too deterministic in IID sequences.**

At the end of section 4.4, I add

" Then, theorem 2 show that, for the vast majority of models Y_n^θ of a sequence y_n , $n=1,\dots,N$, $T_q(Y_n^\theta)$ is ϵ -equivalent to the IID model, i.e. $T_q(y_n)$ admits the IID models for correct model if m and q are well chosen. As a matter of fact we shall see below that it is the case for the models Y_n^θ which are not too deterministic."

In section 6.4, I write **" In conclusion, the measure defined in notations 4.5 adapts well to the results obtained and it is quite selected."**

At the end of section 9, I add "As a matter of fact it is enough that y_n is a noise not too deterministic. For example, one can choose the following noises

- 1) Texts or transformed texts (cf Blacher (2011))
- 2) Files systems of the computers
- 3) Music (e.g. Rap music as Marsaglia (1995))
- 4) Elapsed time between emission of particles during radioactive decay
- 5) Thermal noise from a semiconductor diode or resistor
- 6) The frequency instability of a free running oscillator
- 7) Quantum phenomena

4 Answer for reviewer 2 and 3

I agree with comments of reviewer 2 and 3.

5 Answer for reviewer 1

For reviewer 1, here is my comment

I corrected the paper according remarks 1,2,3,4. Now, some comments are not true : Thus, a comment is " A fundamental problem with the authors' approach is that they substitute the (non existing) definition of randomness by requirement that a sequence obeys some distribution which is a very weak criterion of randomness. Just an example imagine a sequence of 8-bit binary sequential numbers 0,,255. this sequence is perfectly uniformly distributed and yet it is not random." He has not understood that I do not use unidimensional distribution, but multidimensional distribution : the example does not hold in dimension N.

Other example "there are many technical imperfections that are uncorrectable by the reader, such as in the beginning of Sect 1.2 where a-prime and b-prime are never defined!" : I use a very classical notation which is very known.