FEE
www.fee.bzh

White paper For Engineer Eyes

WP-003Af – Dec. 2021
Auteur: J. Pontois

Générateurs de bruit pseudo-aléatoires

SOMMAIRE

1. OBJET

Ce document caractérise divers générateurs de bruit pseudo-aléatoires (numériques).

Note : document interne 010-NT-013A de Novembre 2013, passage en « White Paper » en décembre 2021.

2. GENERATEUR DE BRUIT BLANC

2.1. BRUIT BLANC UNIFORME

2.1.1. GENERATEUR PN

(clés : maximal length sequence, *m*-sequence, primitive polynomial)

Ce générateur est constitué d'un registre à décalage dont la sortie est dirigée vers l'entrée et vers des additionneurs modulo 2 (OU-exclusif) placés judicieusement entre certaines bascules du registre.
On peut générer un bruit blanc uniforme dans]0..1[à partir d'un générateur PN de n bits, en divisant à chaque itération le contenu de tout ou partie du registre à décalage (entier 1..2^n-1) par 2^n.
Il faut éviter la correspondance directe entre les bascules du registre à décalage et les n bits de sortie (utiliser par exemple une permutation non triviale) pour éviter les effets de rampe dus au principe de génération.

Principe :
Le registre à décalage représente un polynôme *P* de degré *N*-1 à coefficients dans le corps de Galois GF_2 (les éléments sont 0 et 1, l'addition est équivalente à la soustraction et au OU-exclusif, la multiplication est équivalente au ET logique).
Soit *G* le polynôme générateur : c'est un polynôme primitif de degré *N* (=> minimal => générateur => irréductible). Il existe au moins un polynôme primitif pour tout *N*.

On a les relations :

$$P(k) = \sum_{m=0}^{N-1} p_m(k).x^m$$

$$G = x^N + \sum_{m=1}^{N-1} g_m.x^m + 1$$

$P(k+1) = x.P(k) \bmod G = x^{k+1}.P(0) \bmod G$, soit :

$$p_{N-1}(k+1) = p_{N-2}(k) + p_{N-1}(k).g_{N-1}$$
$$p_{N-2}(k+1) = p_{N-3}(k) + p_{N-1}(k).g_{N-2}$$
....
$$p_1(k+1) = p_0(k) + p_{N-1}(k).g_1$$
$$p_0(k+1) = p_{N-1}(k)$$

si *P*(0) <> 0, la suite { *P*(*k*) } décrit l'ensemble des polynômes non nuls de degré inférieur ou égal à *N*-1 (séquence de longueur maximale 2^N-1 car *G* primitif).

Exemples de polynômes primitifs :

N	*G*	*N*	*G*	*N*	*G*
2	x^2+x+1	3	x^3+x+1	4	x^4+x+1
5	x^5+x^2+1	6	x^6+x+1	7	x^7+x+1

8	$x^8+x^4+x^3+x^2+1$	9	x^9+x^4+1	10	$x^{10}+x^3+1$
11	$x^{11}+x^2+1$	12	$x^{12}+x^6+x^4+x+1$	13	$x^{13}+x^4+x^3+x+1$
14	$x^{14}+x^5+x^3+x+1$	15	$x^{15}+x+1$	16	$x^{16}+x^5+x^3+x^2+1$
17	$x^{17}+x^3+1$	18	$x^{18}+x^7+1$	19	$x^{19}+x^5+x^2+x+1$
20	$x^{20}+x^3+1$	21	$x^{21}+x^2+1$	22	$x^{22}+x+1$
23	$x^{23}+x^5+1$	24	$x^{24}+x^4+x^3+x+1$	25	$x^{25}+x^3+1$
26	$x^{26}+x^6+x^2+x+1$	27	$x^{27}+x^5+x^2+x+1$	28	$x^{28}+x^3+1$
29	$x^{29}+x^2+1$	30	$x^{30}+x^6+x^4+x+1$	31	$x^{31}+x^3+1$
32	$x^{32}+x^7+x^6+x^2+1$	33	$x^{33}+x^{13}+1$	34	$x^{34}+x^8+x^4+x^3+1$
35	$x^{35}+x^2+1$	36	$x^{36}+x^{11}+1$	37	$x^{37}+x^6+x^4+x+1$
38	$x^{38}+x^6+x^5+x+1$	39	$x^{39}+x^4+1$	40	$x^{40}+x^5+x^4+x^3+1$
41	$x^{41}+x^3+1$	42	$x^{42}+x^7+x^4+x^3+1$	43	$x^{43}+x^6+x^4+x^3+1$
44	$x^{44}+x^6+x^5+x^2+1$	45	$x^{45}+x^4+x^3+x+1$	46	$x^{46}+x^8+x^7+x^6+1$
47	$x^{47}+x^5+1$	48	$x^{48}+x^9+x^7+x^4+1$	49	$x^{49}+x^9+1$
50	$x^{50}+x^4+x^3+x^2+1$	51	$x^{51}+x^6+x^3+x+1$	52	$x^{52}+x^3+1$
53	$x^{53}+x^6+x^2+x+1$	54	$x^{54}+x^8+x^6+x^3+1$	55	$x^{55}+x^{24}+1$
56	$x^{56}+x^7+x^4+x^2+1$	57	$x^{57}+x^7+1$	58	$x^{58}+x^{19}+1$
59	$x^{59}+x^7+x^4+x^2+1$	60	$x^{60}+x+1$	61	$x^{61}+x^5+x^2+x+1$
62	$x^{62}+x^6+x^5+x^3+1$	63	$x^{63}+x+1$	64	$x^{64}+x^4+x^3+x+1$

:

2.1.2. GENERATEUR A CONGRUENCE

Principe :

$$x_n = (a.x_{n-1} + b) \bmod c$$

Un générateur de bruit blanc dans [0 ;1[est obtenu par $\frac{x_n}{c}$.

Exemples :

a=0x41A7, *b*=0, *c*=2^{31}-1 : période 2^{31}-1, avec la contrainte $x_0 \neq 0$
a=0x41C64E6D, *b*=0x12345, *c*=2^{32}

Un exemple d'un générateur rapide est :

x_n = 0x10003 x_{n-1} mod 2^{32}

La sortie du générateur est 2^{-32} x_n, avec la contrainte x_0 impair
La période de ce générateur est 2^{30}. En fonction de x_0, il génère l'une ou l'autre de deux sous-suites opposées (en considérant des entiers signés 32 bits) et impaires.

2.1.3. GENERATEUR DE TYPE LAGGED-FIBONACCI

A partir d'un tableau de *N* mots de k bits représentant les N dernières sorties xn, on définit la sortie x_{n+1} par $x_{n+1} = x_{n-r}\ op\ x_{n-s}$ pour le générateur $F(r,s,op)$, avec *op* = '+', '-', '*', 'ou exclusif', …
Les meilleurs générateurs sont obtenus pour '*', les plus mauvais par 'ou exclusif'.
Pour '*', les valeurs x_n sont limitées aux entiers impairs

Exemples de 'bonnes' valeurs pour *r* et *s* :
(17, 5), (31,13), (55, 24), (68, 33), (97, 33), (607,273), (1279, 418)

La période maximale de ces générateurs est :
$(2^r-1)\ 2^{k-1}$ pour '+' et '-' (condition initiale : au moins un des x_n doit être impair)
$(2^r-1)\ 2^{k-3}$ pour '*' (entiers impairs)
(2^r-1) pour 'ou exclusif' (équivalent à *r* générateurs PN en parallèle)

2.2. BRUIT BLANC GAUSSIEN

2.2.1. UTILISATION DU THEOREME DE LA LIMITE CENTRALE

On génère un bruit blanc quasi-gaussien à partir d'un bruit blanc uniforme.
On effectue pour cela *n* tirages successifs dans l'intervalle [-0.5..0.5] que l'on somme.
Soit $u(t)$ bruit blanc uniforme dans [-0.5 ;+0.5]
on a $< u(t) > = 0$ et $< u^2(t) > = 1/12$.

Soit $g(t) = u_1(t) + u_2(t) + u_3(t) + ... + u_n(t)$ somme de *n* bruits blancs uniformes, indépendants.

On a $< g(t) > = 0$ et $< g^2(t) > = n / 12$

D'après le théorème de la limite centrale, $g(t)$ tend vers un bruit gaussien d'écart-type $\sqrt{\frac{n}{12}}$.

En limitant *n*, on obtient un bruit blanc quasi gaussien.

Pratique :
Pour obtenir un bruit blanc gaussien $g(t)$ centré d'écart-type σ à partir de générateurs $u_i(t)$ de bruit blanc uniforme dans [0 ;1], on a :

n=8 : $g(t) = \sigma\sqrt{\frac{2}{3}}\left(u_1(t)+...+u_8(t) - 4\right)$

n=12 : $g(t) = \sigma\left(u_1(t)+...+u_{12}(t) - 6\right)$

La sommation peut être obtenue indirectement en injectant le bruit blanc uniforme (centré) dans un filtre passe-bas de fréquence de coupure f_c. En choisissant une fréquence d'échantillonnage f_e telle que $f_e > 25\ f_c$, on obtient un bruit blanc quasi gaussien dont la puissance est inférieure à la puissance du bruit uniforme d'origine dans un rapport $2\frac{f_c}{f_e}$.

2.2.2. INVERSION DE LA DENSITE DE PROBABILITE CUMULEE

On génère un bruit blanc gaussien à partir d'un bruit blanc uniforme.
On utilise pour cela deux variables aléatoires indépendantes *u* et *v* dans l'intervalle [0..1[. Le bruit gaussien *g* est défini par :

$$g = \sin(2\pi u) \cdot \sqrt{-2\log(1-v)}$$

3. GENERATION DE BRUIT IMPULSIONNEL DE TYPE ALPHA-STABLE

3.1. GENERATEUR POUR $\alpha \in]0;2]$

$u \in \left]-\frac{\pi}{2};+\frac{\pi}{2}\right[$, tirage aléatoire uniforme

$v \in]0;1]$, tirage aléatoire uniforme

3.1.1. FORMULE GENERALE

le bruit *y* est :

$$y = \frac{\sin(\alpha.u)}{\cos(u)^{\frac{1}{\alpha}}} \cdot \left[\frac{-\ln(v)}{\cos[(1-\alpha).u]}\right]^{1-\frac{1}{\alpha}}$$

avec $\langle y^2 \rangle = \infty$ pour $0 < \alpha < 2$

3.1.2. GENERATEUR POUR α=1

$$y = \tan(u)$$

3.1.3. GENERATEUR POUR α=2

$$y = 2\sin(u)\sqrt{-\ln(v)}$$

3.2. BRUIT IMPULSIONNEL BORNE AVEC α = 1

caractérisation : facteur de forme : $\beta \in]0;+\infty[$

$x \in [-1;+1]$, tirage aléatoire uniforme

soit $g(\beta) = \sqrt{\dfrac{\beta}{\arctan(\beta)} - 1}$

le bruit *y* est :

$$y = \sigma \frac{\tan\left(x.\arctan(\beta)\right)}{g(\beta)} \xrightarrow[\beta \longrightarrow 0]{} \sigma.x.\sqrt{3}$$

on a :

$\left\langle y^2 \right\rangle = \sigma^2$

$$|y|_{\max} = \sigma \frac{\beta}{g(\beta)} = \sigma \frac{\sqrt{\beta}}{\sqrt{\dfrac{1}{\arctan(\beta)} - \dfrac{1}{\beta}}} \xrightarrow[\beta \longrightarrow \infty]{} \sigma\sqrt{\frac{\beta\pi}{2}}$$

Densité de probabilité de la distribution α:

$pdf_\alpha(x) = \dfrac{\beta}{\gamma} e^{-\delta\left|\frac{x}{\gamma}\right|^\alpha}$, γ est l'écart-type

γ est défini si on limite de plus le bruit à $\pm x_m$ ($pdf_\alpha(x) = 0$ pour $x < -x_m$ ou $x > x_m$).

On a :

$$\begin{cases} A = \int_0^{x_m} e^{-x^\alpha} dx \\ B = \int_0^{x_m} x^2 e^{-x^\alpha} dx \end{cases} \text{ et } \begin{cases} \beta = \dfrac{1}{2}\sqrt{\dfrac{B}{A^3}} \\ \delta = \left(\dfrac{B}{A}\right)^{\frac{\alpha}{2}} \end{cases}$$

4. GENERATION DE BRUIT SUIVANT UNE DISTRIBUTION GAMMA

Densité de probabilité de la distribution en puissance :

$pdf_m(\gamma) = \left(\frac{m}{\bar{\gamma}}\right)^m \frac{\gamma^{m-1}}{\Gamma(m)} e^{-m\frac{\gamma}{\bar{\gamma}}}$, *m*>0 paramètre de la distribution, $\bar{\gamma}$ puissance moyenne

avec $\Gamma(m) = \int_0^\infty t^{m-1} e^{-t} dt$

Densité de probabilité cumulée de la distribution en puissance :

$cdf_m(\gamma) = \int_0^\infty pdf_m(t)dt = P\left(m, m\frac{\gamma}{\bar{\gamma}}\right)$, *P* fonction gamma incomplète : $P(m,x) = \frac{1}{\Gamma(m)} \int_0^x t^{m-1} e^{-t} dt$

soit *Q*(*m*,*x*) telle que $P\left(m, m.Q(m,x)\right) = x$, avec $x \in [0;1]$

Le générateur de bruit complexe γ-distribué est défini par :

$z = e^{2j\pi v}\sqrt{\bar{\gamma}.Q(m,u)}$, avec $u \in [0;1]$ et $v \in [0;1]$, *u* et *v* uniformément distribués