Générateurs de nombres aléatoires

Algorithmes et Structures de Données II, GymInf

Juan-Carlos Barros, Yves Dethurens, Daniel Kessler et Jean-Francis Ravoux

5 juillet 2021

Table des matières

1 Introduction

1.1 Que veut-on simuler et pourquoi ?

— distributions aléatoires (bla)
— utilité directe (ex : jeus) et indirecte (ex : algos aléatoires)

1.2 TRNG vs PRNG

...

2 Générateurs de suites pseudo-aléatoires

2.1 Historique

von Neumann[**VonNeumann**] (bla)

2.2 Caractéristiques communes

— période (bla)
— seed (bla)

2.3 Générateurs linéaires congruents (LCG)

...

2.4 Mersenne Twister et les LFSR

...

3 Générateurs de "vraies" suites aléatoires

3.1 Généralités - Processeur incapable

— Processeur arrive plutôt bien à propager de l'aléatoire
— Voir algorithmes présentés précédemment
— Mais il lui faut un coup de pouce au départ
— Besoin d'une graine pour démarrer
— Pourquoi hasard inaccessible au processeur ?
— Car le processeur est profondément déterministe

3.2 Généralités - Le Monde réel oui

— Aléatoire inévitable et dérangeant dans le monde réel !
  — Incertitudes fondamentales des mesures
  — Impossibilité de contrôler une valeur physique
— Monde réel est donc LA source d'inspiration

3.3 Collection d'entropie

— Principales sources de hasard :
  — phénomènes physiques stochastiques :
    — bruit thermique (Johnson et Nyquist)

    - autres phénomènes statistiques (vagues, etc.)
  - phénomènes quantiques intrinsèquement aléatoires
    - effet photoélectrique
    - n'importe quelle autre mesure quantique

3.4 Algorithmes d'aggrégation et expansion d'entropie

- Algorithme pour grossir le flux de TRNG (pas assez rapide)
- HAVEGE (utilisé pas le noyau Linux)
- HArdware Volatile Entropy Gathering and Expansion
- https ://www.irisa.fr/caps/projects/hipsor/misc.php

3.5 Le futur est-il quantique ?

- Sources quantiques :
  - source de radioactivité détectée par un compteur Geiger
  - photons traversant un miroir semi-réfléchissant
  - C'est le choix de la compagnie Genevoise ID Quantique

3.6 Exemple genevois : ID Quantique

- Principe de la source ID Quantique :
  - photons traversant un miroir semi-réfléchissant
  - événements mutuellement exclusifs (réflexion / transmission)
  - Détection associée respectivement à des valeurs de bit 0 ou 1

4 Que fait le module "random" de Python ?

bla sur les PRNG et TRNG utilisés (indirectement) par Python et résumé de résultats de petits tests

5 Conclusion

bla bla