Title : Tests robustes d'aléatoire.

Co-Encadrants :
Andrei ROMASHCHENKO, andrei.romashchenko@lirmm.fr,
Alexander SHEN, alexander.shen@lirmm.fr

Keywords : pseudo-random generators ; randomness

Prérequis : culture mathématique générale ; probabilité élémentaire ; anglais technique (lire et discuter de la documentation en anglais) ; programmation en C ; bonne capacité d'apprentissage et du bon sens :-)

Résumé : L'objet de ce T.E.R. est d'étudier la notion d'aléatoire et des tests pour les générateurs de nombres aléatoires. Nous proposons une approche générique pour construire des tests robustes pour les sources de bits aléatoires, et suggérons de développer une bibliothèque de logicielle qui pourrait améliorer les tests existants d'aléatoire.

Les tests d'aléatoire sont utilisés pour détecter des anomalies dans les générateurs aléatoires physiques. Les tests existants (voir NIST, Diehard, Dieharder et autres) ne sont typiquement pas fiables : même un bon générateur peut parfois échouer un test.

Au LIRMM nous avons développé une méthodologie qui permet de construire des tests plus fiables. Nous avons programmé certaines instances de tests dans ce format robuste, et on aimerait convertir de nombreux autres tests sous cette forme robuste.

Il existe des dizaines de tests documentés d'aléatoire. Chaque test typique est présenté dans la documentation par sa description mathématique et par un code de programme de référence (malheureusement, pas toujours correctement implémenté). Un tel programme peut comprendre plusieurs centaines de lignes. Notre objectif est de trouver pour chaque de ces algorithmes une version robuste et d'implémenter les nouveaux algorithme en C.

Une autre branche possible de ce projet : utiliser des extracteurs d'aléatoire pour améliorer la qualité des générateurs aléatoires pratiques.

Bibliographie :

[1] Alexander Shen. Making randomness tests more robust. (2018)
https://hal.archives-ouvertes.fr/hal-01707610/document

[2] Andrei Romashchenko, Alexander Shen. Randomness tests : theory and practice. (2021)
https://hal-lirmm.ccsd.cnrs.fr/lirmm-03371151/document

[3] R.G. Brown, Dieharder : A Random Number Test Suite. Version 3.31.1. (2021)
https://webhome.phy.duke.edu/∼rgb/General/dieharder.php