Université de Montréal

Pierre L'Ecuyer
Professeur titulaire

Département d'informatique et de
recherche opérationnelle
Pavillon Aisenstadt
Université de Montréal
C.P. 6128, succursale centre-ville
Montréal (Québec), CANADA, H3C 3J7

Tél.: (514) 343 - 2143
e-mail: lecuyer@iro.umontreal.ca
web: http://www.iro.umontreal.ca/~lecuyer

Le 2 septembre 2019

Proposition de projet de maitrise:
Conception et implantation de batteries de tests statistiques dans TestU01

Ceci est une proposition de sujet de recherche de maitrise au laboratoire d'optimisation et simulation au DIRO, à l'Université de Montréal. Le projet est présentement disponible à compter de septembre 2019 ou janvier 2020.

La librairie TestU01, développée au DIRO sur une période d'environ 20 ans, fournit une grande collection de tests statistiques pour tester l'indépendance et l'uniformité des générateurs pseudoaléatoires, et implante aussi de nombreux générateurs proposés dans la littérature ou retrouvés dans les logiciels. Voir [1] et `http://simul.iro.umontreal.ca/testu01/tu01.html`. TestU01 contient aussi des batteries de tests prédéfinies qui sont devenues le standard de facto dans le monde pour tester les générateurs pseudoaléatoires autant pour la simulation que pour la cryptographie. Les batteries de tests de cette librairie ont été conçues au départ pour des générateurs produisant des nombres ayant (au moins) 32 bits de précision et testent uniquement les 32 bits les plus significatifs.

Durant l'été 2018, deux étudiants stagiaires ont fait des améliorations substantielles à TestU01. Ils ont amélioré l'efficacité de l'implantation de certains tests, amélioré l'approximation de la loi de probabilité de la statistique de test (pour calculer la p-valeur) pour certains tests, et modifié l'implantation des tests pour pouvoir tester des générateurs produisant plus de 32 bits de précision en output (par exemple 53 bits ou 64 bits).

Le projet consiste à ajouter à la librairie quelques nouveaux tests, à généraliser certains tests actuellement dispinibles, à ajouter quelques nouveaux types de générateurs originaux ou proposés récemment, à définir et implanter des batteries de tests pour des générateurs produisant des nombres ayant un nombre arbitraire de bits de précision (par exemple 53 bits ou 64 bits), et à construire des implantations pouvant exécuter des tests en parallèle sur des systèmes multiprocesseurs. On veut construire en particulier des batteries de tests séquentielles (ou multiniveaux) automatisées dans lesquelles on commence par des tests simples et peu coûteux, et si le générateur passe bien les tests à un niveau donné, on passe au niveau suivant où les tests

sont plus exigeants. De plus, lorsque des p-valeurs un peu suspectes sont observées pour un test donné, on voudra que le logiciel applique automatiquement des versions additionnelles plus poussées du même test. Finalement, le tout devra être mis en libre accès sur GitHub avec une documentation claire et détaillée.

Ce projet sera effectué en collaboration avec d'autres chercheurs (du Japon et d'Italie) et probablement en collaboration avec Google en 2020.

L'étudiant(e) sélectionné(e) recevra une bourse pendant la durée de son projet de recherche de maitrise.

Si vous êtes déjà admis(e) à la maitrise au DIRO et si ce projet vous intéresse, envoyez-moi par courriel un CV (en .pdf) et une copie de vos bulletins de notes de niveau universitaire.

REFERENCES

1. P. L'Ecuyer and R. Simard. TestU01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software*, 33(4):Article 22, August 2007.