FICHE SYNOPTIQUE 2003

Sujet : Test et optimisation d'un générateur pseudo-aléatoire.

M'étant toujours demandé comment fonctionnait la fonction rand sur les calculatrices, j'ai cherché l'an dernier quelques informations sur ce sujet, et j'ai découvert plusieurs méthodes de génération de nombres vraiment aléatoires (par des processus physiques), et d'autres créant des listes pseudo-aléatoires (par des générateurs informatiques).

Notamment, les plus simples d'entre eux, les générateurs congruentiels linéaires, produisent des séquences plus ou moins aléatoires en fonction des paramètres. J'ai donc été amené à trouver comment contrôler ces paramètres et donc optimiser le caractère aléatoire de la suite pseudo-aléatoire produite. Ceci demandait de définir ce qui caractérise précisément le caractère aléatoire.

Pour réaliser l'optimisation des générateurs congruentiels linéaires, je les ai testés avec différents paramètres, afin de vérifier s'ils étaient acceptables. J'ai donc réalisé un programme dans ce but. Lors de sa construction, j'ai dû notamment reporgrammmer une fonction de multiplication modulo un entier, afin d'éviter le dépassement du plus grand entier géré.

I/ Le test de la période

Définition du générateur congruentiel linéaire
Théorème de la période maximale
Algorithme de Pollard pour le test de la période

II/ Le test d'uniformité

Méthode du test du chi carré
Applications

III/ Le test d'indépendance

Test du poker
Test des séquences corissantes et décroissantes

Annexe

Table de valeurs de variance
Démonstration du théorème de période maximale
Code du programme de test en Caml

Bibliographie

Philippe Dumas, Xavier Gourdon, *Maple, son bon usage en mathématiques*, Springer, p. 82, 1997.
Donald E. Knuth, *The art of computer programming, Volume 2 : Seminumerical algorithms,* Addison Wesley, p 1-55, 61-65, 1998.

Articles consultés

J.P. Delahaye, *Aléas du hasard informatique,* Pour la science n°247, p. 92 –97, Mars 1998.
Gérard Grancher, *Simulations pseudo-aléatoires : techniques et applications,* 2001.
Pierre L'Ecuyer, *Combined multiple recursive random number generators,* 1995.
Pierre L'Ecuyer, *Software for uniform random number generation: distinguishing the good and the bad.*
Richard Simard, Pierre L'Ecuyer, Stefan Wegenkittel, *Sparse serial tests of uniformity for random numbers generators,* 2001.
Bernard Vuilleumier, *Construire un générateur de nombres aléatoires*, 1999

Sites ou pages Web consultés

http://193.48.37.48/~douillet/preprint/simul/node1.html
http://6371.lcs.mit.edu/Fall96/reports/eng_tung_vonkoch/rsaalg.htm
http://crypto.mat.sbg.ac.at/results/karl/server/node1.html
http://dreamos.sourceforge.net/doc/System/Algorithmes/random.html
http://id-net.fr/~goudey/gnpa.html
http://michel.arboi.free.fr/cryptFAQ/scicryptFR8.html
http://noosphere.princeton.edu/terror.html
http://server.cs.panam.edu/~meng/Course/CS6337/Note/master/node42.html
http://www.iecn.u-nancy.fr/~pincon/scilab/Doc/node1.html
http://www.lavarnd.org/index.html
http://www.math-info.univ-paris5.fr/smel/cours/mp/node7.html
http://www.random.org/