Math Appl

http://wwwedu.ge.ch/cptic/clubs/mathappl/

Centre pédagogique des technologies de l'information et de la communication (CPTIC)
Rue Théodore-de-Bèze 2
Case Postale 3144
1211 GENÈVE 3
Tél: (022) 318.05.30
Fax: (022) 318.05.35
Directeur: Raymond Morel

Lettre nº 144

L'existence de nombres aléatoires peut être prouvée …

Mais ce résultat ne nous dit pas comment les obtenir

Les premiers nombres aléatoires ont été obtenus par des processus physiques

Aujourd'hui, ils sont calculés sur ordinateur à partir de fonctions mathématiques

Lundi 6 septembre 1999 à 17 h

Nombres aléatoires

Bernard Vuilleumier

La plupart des méthodes et des algorithmes utilisés dans les simulations stochastiques produisent du «hasard» à partir d'une suite infinie de «nombres aléatoires». De nombreux utilisateurs ignorent comment de tels nombres peuvent être obtenus et se contentent d'utiliser des fonctions standards pour les produire. Une telle attitude peut provoquer des surprises aux utilisateurs de simulations car les nombres aléatoires sont les fondations des simulations stochastiques, et de nombreux générateurs de nombres aléatoires présentent de sérieux défauts.

Il n'y a pas de problème mathématique fondamental avec les nombres aléatoires: leur existence peut être prouvée. Mais ce résultat ne nous donne pas pour autant le moyen de les produire. Nous devons donc trouver un processus observable dont les mathématiques sont un modèle «raisonnable». Et tout le problème se cache derrière ce mot «raisonnable». Comment pouvons-nous décider, à partir d'une suite finie de nombres, si le modèle qui permet de les obtenir est «raisonnable»? C'est là le problème de l'inférence statistique.

Les premiers utilisateurs de simulations stochastiques utilisaient des processus physiques considérés comme aléatoires: lancers de pièces de monnaies ou de dés par exemple. L'expérience de Buffon (voir TP) pour estimer le nombre π est une variante plus sophistiquée de ce type de processus. Aujourd'hui, les moyens mécaniques sont largement utilisés dans les jeux d'argent pour obtenir des nombres aléatoires: roulette des casinos, système d'extraction de boules pour les loteries à numéros, etc. Des tables de nombres aléatoires ont également été produites à partir de moyens électroniques. Toutes ces méthodes physiques ont longtemps semblé parfaitement capables de générer des nombres aléatoires. Pourtant, certaines séquences obtenues par ces méthodes se sont par la suite révélées biaisées: dans le cas de la table RAND (1955) produite par bruit électronique par exemple, le système d'enregistrement présentait un défaut mécanique. Donc même les procédés physiques réputés les plus sûrs doivent être testés!

Aujourd'hui, les nombres nécessaires aux simulations stochastiques sont des nombres calculés sur ordinateur. Ils miment les propriétés d'une séquence de variables aléatoires uniformément distribuées, bien qu'ils soient obtenus par des règles purement déterministes. Leur caractéristique essentielle est d'être imprévisibles pour ceux qui ne connaissent par leur «générateur». La suite de nombres ci-dessous est générée par une règle toute simple:

13, 8, 1, 2, 11, 14, 7, 12, 13, 12, 17, 2, 11, 10, 3, …

Mais pour quelqu'un qui ne connaît pas cette règle, trouver le nombre suivant n'est pas aisé! Les algorithmes utilisés pour la production de nombres aléatoires sont du même type que la règle qui a produit les nombres ci-dessus. Une analyse mathématique fouillée a bien sûr été nécessaire pour trouver, parmi tous les algorithmes possibles, ceux qui miment correctement une suite de nombres aléatoires. En conclusion, disons qu'un bon générateur de nombres aléatoires utilise un algorithme simple et rapide (prenant beaucoup moins de temps que l'évaluation d'un logarithme par exemple). Il est périodique et possède une longue période (2^{30} ou 10^9 au moins) et prend des valeurs également distribuées dans l'intervalle (0, 1). Il a des k-uples distribués aussi uniformément que possible dans l'intervalle $(0, 1)^k$ pour $k \leq 10$.

Prochaine réunion: lundi 4 octobre 1999 à 17h.

Travaux pratiques

Mots clefs
Aléatoire, Buffon, générateur, hasard, nombre, règle, simulation.

Pour réaliser une simulation stochastique

Exercice 1
a) Dans le volume VII du *Supplément à son Histoire naturelle*, Buffon aborde de nombreux problèmes de calcul des probabilités et de statistique. L'un des plus célèbres est celui de l'aiguille, dont l'énoncé est le suivant: sur un plan sont tracées des droites parallèles distantes de h. On jette «au hasard» sur ce plan une aiguille de longueur l, avec $l = h$; quelle est la probabilité pour que cette aiguille rencontre l'une des droites?
b) Réalisez une simulation stochastique de l'expérience de Buffon.

Pour découvrir un des premiers générateurs

Exercice 2
Dans les années 40, von Neumann conçut un des premiers générateurs de nombres aléatoires. Il utilisait la méthode suivante pour obtenir une suite de nombres à quatre chiffres : partant d'un nombre initial, il l'élevait au carré et extrayait les quatre chiffres du milieu. En partant de 8653 par exemple et en réitérant le procédé, nous obtenons 8653, 8744, 4575, 9306, 6016, 1922, 6940, …
a) Complétez la suite ci-dessus. Quels problèmes cet algorithme fait-il apparaître?
b) Examinez le comportement du générateur lorsque vous partez de la valeur initiale 2100.

Pour présenter l'ancêtre d'une famille de générateurs largement utilisés aujourd'hui

Générateur de Lehmer
En 1951, Lehmer proposa le générateur suivant:

$$U_i = aU_{i-1} \bmod 1$$

Ce générateur a donné naissance à la famille des générateurs congruentiels abondamment utilisés aujourd'hui et définis par:

$$X_i = (aX_{i-1} + c) \bmod M$$

où a, c et M sont entiers. Lorsque $c = 0$, on parle de générateur multiplicatif.

Théorème utile pour construire un bon générateur

Théorème
Un générateur multiplicatif possède une période $M - 1$ seulement si M est premier. La période divise alors $M - 1$ et est égale à $M - 1$ seulement et seulement si $a \neq 0$ et si $a^{(M-1)/p} \not\equiv 1$ modulo M, pour chaque facteur premier p de $M - 1$.

Nous verrons dans une prochaine lettre comment utiliser ce théorème et *Mathematica* pour construire un bon générateur de nombres aléatoires.

Sources et bibliographie

- Daniel DUGUE, «Probabilités» 18-1018b, *CD Universalis* v 4.0, 1998.
- Brian D. RIPLEY, *Stochastic Simulation*, Wiley, New-York 1987.