Université Paris 7
IUP 2
Analyse de Performance et Simulation
Année 2003-2004

Résumé de Cours pour le TD no 2
Générer des nombres aléatoires, MSN et Méthode congruentielle linéaire

1 Introduction

- Référence : Knuth *The Art of Computer Programming* Vol 2.
- Pourquoi chercher des nombres aléatoires ?
  - Simulation d'un phénomène naturel exple : physique nucléaire (collisions aléatoires de particules) recherche opérationnelle (arrivée à un intervalle aléatoire)
  - Echantillonage (quand c'est impossible d'etudier tous les cas : on recherche plutôt un comportement typique.)
  - Programmation
    - tester l'efficacité des programmes
    - algorithmes probabilistes qui sont souvent plus efficace que leurs homologues probabilistes.
  - Jeux : dés, cartes, loto...
  - Et aussi Analyse numérique, Prise de décision...
- Que veut dire aléatoire ?

  Pas de discussion philosophique ici.
  On préfère parler de suite de nombres aléatoires indépendants suivants une distribution donnée.
  (Dans le cas uniforme : indépendance, même probabilité pour chaque élément d'être à un indice quelconque.)
- Historique
  - Construction de table par tirage à la main dans une urne. (Table de 40 000 chiffres aléatoires.)
  - Utilisation de moyens mécaniques : résistances...
    Exple : ERNIE pour le loto brittanique...

2 Des Méthodes de génération

- Pourquoi veut-on des méthodes de génération de nombres aléatoires par ordinateur ?

  - Ne pas avoir à adjoindre à tous les ordinateurs un outil méchanique qui génèrerait des nombres aléatoires.
  - Difficiles de vérifier ces générateurs.
  - Nécessité dans beuacoup de cas de reproduire les calculs pour les tester.
  - Simplicité pour la programmation et possibilité d'un tirage d'un très grand nombre de nombres aléatoires en peu de temps.

  → Donc intérêt pour la production de nombres aléatoires en utilisant les opérations arithmétiques usuelles d'un ordinateur.

- MSN Middle Square Method (Von Neumann 1946)
  - Prendre un nombre à 10 chiffres.
  - L'élever au carré.
  - Garder les 10 chiffres du milieu.

- Notion de suite pseudo ou quasi-aléatoire.

  La suite n'est pas à proprement parler aléatoire puisque un élément est entièrement déterminé par son prédécesseur, mais elle semble l'être.

- Algorithme super-aléatoire :

  Paradoxe des anniversaires : si 23 personnes ou plus sont dans une salle, on a plus d'une chance sur deux que deux d'entre elles aient leur anniversaire le même jour.

  Donc une suite sur un ensemble avec n éléments va avoir en moyenne une boucle avec $\sqrt{n}$ éléments. Par exemple pour un ensemble à 10 000 éléments, on ne pourra générer avec un telle fonction une suite d'au plus 100 nombres aléatoires.

  La morale de cette histoire est que les nombres aléatoires ne doivent pas être générés selon une méthode choisie au hasard.

  Il ne sert à rien d'essayer de créer des suites de nombres aléatoires en utilisant des algorithmes très compliqués que l'on ne peut analyser mathématiquement.

- La Méthode congruentielle linéaire.

  Générer selon une distribution uniforme.

  C'est la méthode qui sert de base à la plupart des générateurs.

  La suite de nombres aléatoires $\{X_n\}$ est donnée par :

$$X_{n+1} = (aX_n + c) \bmod m, n \geq 0$$

  avec m, le modulo a, le multiplicateur c, l'incrément X_0 la valeur de départ.

  Exemple, la suite obtenue qund $m = 10$, $X_0 = a = c = 7$ est

$$7, 6, 9, 0, 7, 6, 9, 0, ...$$