ALGORITHMES PROBABILISTES

Introduction

Il existe quatre grands types d'algorithmes probabilistes :

1. Les algorithmes numériques. Par exemple, on utilise l'aléatoire pour découper un intervalle de calcul.
2. Les méthodes de Monte-Carlo. Il s'agit de calculer une valeur incorrecte en un temps déterministe avec une probabilité d'erreur mesurable et pouvant être rendue arbitrairement petite.
3. Les méthodes de Las Vegas. C'est un algorithme qui renvoie une valeur toujours correcte en un temps aléatoire (avec une probabilité souvent très faible, le programme peut ne jamais se terminer).
4. Les algorithmes de randomisation. On introduit de l'aléatoire dans les données en entrée pour faire baisser la complexité moyenne.

1. Générateurs de nombres pseudo-aléatoires

Les nombres pseudo-aléatoires ainsi générés sont utiles dans plusieurs domaines :

1. les algorithmes probabilistes ;
2. la cryptographie ;
3. les tests (paramètres d'entrées choisis aléatoirement).

Un générateur de nombres pseudo-aléatoires est une fonction qui renvoie $x \in [0, 1[$.
En python, il y a le module *random*. Un *import* random donne accès à :
— *random.uniform(a,b)* qui renvoie un réel $a \leq x < b$ (0 et 1 par défaut pour a et b) ;
— *random.randinit(a,b)* qui renvoie un entier $a \leq x \leq b$.
— *random.choice(seq)* qui renvoie un élément parmi *seq* ;
— *random.random()* qui renvoie $x \in [0, 1[$.

Il faut cependant initialiser toutes ces méthodes avec *random.seed(x)*. Par défaut c'est l'heure du système.

Définition 1.1
Un générateur est une suite de nombres réels qui vont se comporter statistiquement comme une suite de nombres aléatoires sur $[0, 1[$.

Exemple. — Soit $(x_n)_{n\in\mathbf{N}}$ une suite d'entiers. On pose x_0 la graine. On définit la relation de récurrence par

$$x_{n+1} = Ax_n \mod M$$

avec $A, M \in \mathbf{N}$. La valeur retournée est x_n/M.

Proposition 1.2
La suite $(x_n)_{n\in\mathbf{N}}$ est périodique de période $P < M$. Si M est premier, $P = M - 1$ si, et seulement si, A vérifie $A^{M-1} = 1 \mod M$ et $A^k \neq 1 \mod M$ pour tout $k < M$.

Exemple. — Avec $M = 2^{31} - 1$ et $A = 397\ 204\ 094$.
Pour faciliter les calculs, on utilise généralement un M sous la forme $M = 2^\beta$.

Proposition 1.3
Si M est de cette forme, alors la période maximale est $2^{\beta-2}$ et est réalisée si $A = \pm 3 \mod 8$ et $x_0 = \pm 1 \mod 8$.

2. Monte-Carlo

Définition 2.1
Une variable aléatoire Y est une fonction qui associe à chaque résultat d'une expérience aléatoire un entier k. La loi de Y est une suite $(p_k)_{k\in K} \in [0, 1]$ traduisant $\mathbf{P}[Y = y_k] = p_k$ avec $\sum p_k = 1$.

Exemple. — Pour les dés, $\{y_k\} = \{1, 2, \ldots, 6\}$ et $p_k = 1/6$.

Définition 2.2
L'espérance de Y, notée, $\mathbf{E}[Y]$, est la somme :

$$\mathbf{E}[Y] = \sum_{k\geq 0} y_k p_k$$

si cette série converge.
La variance de Y est

$$\mathrm{Var}(Y) = \sum_{k\geq 0} p_k y_k^2 = \mathbf{E}[Y]^2.$$

THÉORÈME 2.3 (Loi des grands nombres)
Soit (Y_i) une suite de variables aléatoires indépendantes et de même loi. Alors

$$m_n = \frac{1}{N} \sum_{i=1}^{N} Y_i \overset{N\to\infty}{\longrightarrow} \mathbf{E}[Y].$$