Générateur pseudo-aléatoire

F. Kany. ISEN-Brest & La Croix-Rouge

Position du problème

Une méthode classique pour générer une suite aléatoire $\{r_1, r_2, \ldots, r_k\}$ avec $r_i \in [0, M-1]$ consiste à utiliser la relation de récurrence suivante : $r_i = \text{reste}\left(\frac{a.r_{i-1}+c}{M}\right)$ où a et c sont des constantes. On initialise cette suite en choisissant r_1 et on obtient une séquence périodique (de $n \leq M$ termes) qui se répète à l'infini. On a donc intérêt à choisir a et M grands (par exemple $2^{31} \simeq 2.10^9$ pour une machine 32-bits) pour éviter les répétitions. (Si un programme nécessite, au total, plus de M tirages au sort, il faudra réinitialiser la suite au cours du calcul).

On peut tester le caractère aléatoire de la suite en traçant, sur un graphique à deux dimensions, les points de coordoonées $(x_i, y_i) = (r_{2.i-1}, r_{2.i})$. Le cortex étant particulièrement doué pour reconnaître les formes (à la différence de l'ordinateur), il est facile de **voir** si la suite est aléatoire.

1. Écrire un programme générant la suite (r_i) avec : $a = 57$, $c = 1$, $M = 256$ et $r_1 = 10$.
2. Déterminer la période de la séquence. Visualiser l'ensemble des points tels que $(x_i, y_i) = (r_{2.i-1}, r_{2.i})$ pour voir si la suite est aléatoire.
3. Reprendre les mêmes questions avec $M = 2^{48}$, $c = 11$, $a = 25\,214\,903\,917$.