Les générateurs de nombres aléatoires

Il n'existe pas de méthode numérique pour tirer des nombres aléatoires selon une distribution uniforme.

On peut en revanche tirer des nombres à partir de suites pseudo-aléatoires ; ces suites doivent, en théorie, vérifier une infinité de critères : la moyenne, la variance et tous les moments de la distribution doivent également être ceux d'une distribution uniforme.

Les nombres étant représentés par un nombre fini de bits, les générateurs pseudo-aléatoires sont forcément périodiques. Il est nécessaire (mais pas suffisant) que cette période soit très grande (en tous cas très supérieure au nombre de tirages nécessaires pour effectuer une simulation de type Monte-Carlo).

Il faut également que les séquences de nombres ne soient pas corrélées entre elles.

Il existe deux types d'algorithme pour générer des suites pseudo-aléatoires : ceux basés sur la congruence linéaire et ceux basés sur le déplacement de registre.

Congruence linéaire

On initialise une suite par x_0 et on calcule $x_{n+1} = (a.x_n + c) \bmod m$. On obtient des nombres entre 0 et $m-1$ avec une période m ; il faut donc que m soit très grand.

On peut augmenter la période en mixant des suites (ex : générateur rng cmrg) : $z_n = (x_n - y_n) \bmod m_1$ avec $\begin{cases} x_n = (a_1.x_{n-1} + a_2.x_{n-2} + a_3.x_{n-3} \bmod m_1 \\ y_n = (b_1.y_{n-1} + b_2.y_{n-2} + b_3.y_{n-3} \bmod m_2 \end{cases}$ (P. Lecuyer).

Déplacement de registre

On initialise une suite avec 250 termes (de x_1 à x_{250}) et on calcule $x_n = x_{n-103} \oplus x_{n-250}$ où $\oplus$ est l'opération XOR (Kirkpatrick et Stoll).