Weiterbildung "Bayes-Statistik und Simulation", Juni 2012

Erzeugung von Zufallszahlen

Praktisch alle Simulationen verwenden "Zufallszahlen", die nicht wirklich zufällig sind, sondern von einem deterministischen Algorithmus erzeugt werden (Pseudo-Zufallszahlen). Dies scheint zunächst ein Widerspruch zu sein, aber von einem praktischen Standpunkt aus kommt es ja nur darauf an, ob sich die erzeugten Zahlen ähnlich verhalten wie Realisationen von einer Folge $(U_1, U_2, \ldots)$ von uniformen Zufallsvariablen.

Der einfachste deterministische Zufallszahlengenerator, der auch heute noch verwendet wird (allerdings meist kombiniert mit anderen Verfahren) ist der linearer Kongruenzgenerator. Er ist von der Form $u_n = x_n/M$, wobei (x_n) der Rekursion

$$x_{n+1} \;=\; (ax_n \;+\; c) \bmod M$$

genügt mit $x_0, a, c, M \in \mathbb{N}$. Die Qualität des Generators hängt aber stark von den gewählten Parametern ab. Dies wollen wir in diesem Atelier etwas untersuchen und illustrieren.

Es ist klar, dass dieser Generator periodisch ist, ausser eventuell einem transienten Stück am Anfang, und dass die Periode maximal $= M$ ist. Also muss man sicher M gross wählen. Für die Implementation der Modulo Operation wählt man M oft gleich einer Zweierpotenz.

Es gibt Kriterien, die eine maximale Periode garantieren:

1. Falls $c \neq 0$ und $M = 2^k$, dann ist die Periode $= M$ für alle x_0 genau dann wenn c ungerade ist und $a \equiv 1 \bmod 4$.

2. Falls $c = 0$, dann ist die Periode $= M - 1$ für alle $x_0 \neq 0$ genau dann, wenn M prim ist und $a^{(M-1)/p} \neq 1 \bmod M$ für alle Primfaktoren p von $M - 1$.

Dies genügt jedoch nicht für einen guten Generator, es sollten auch die Paare (u_n, u_{n+1}) das Einheitsquadrat möglichst gleichmässig ausfüllen, die Trippel den Einheitswürfel etc.

Implementieren Sie einen linearen Kongruenzgenerator auf Ihrem Computer für $M = 2048$ $c = 1$ *und verschiedene Werte von* a*, und zeichnen Sie die Paare* (u_n, u_{n+1})*.*

Die d-Tupel eines linearen Kongruenzgenerators haben eine spezielle Struktur: Sie liegen auf Scharen von parallellen Hyperebenen. Bei einem guten Generator liegen diese Hyperebenen in allen Richtungen etwa gleich weit auseinander, bei einem schlechten Generator hat man in gewissen Richtungen grosse Lücken. Die folgende Theorie zeigt, wie man alle Normalenvektoren von Scharen von parallelen Hyperebenen berechnen kann.

Dafür brauchen wir das mathematische Konzept eines Gitters. Ein Gitter $L \subset \mathbb{R}^d$ besteht aus allen ganzzahligen Linearkombinationen von d linear unabhängigen Vektoren $g_i \in \mathbb{R}^d$:

$$L = \{x = t_1 g_1 + \ldots t_d g_d;\; t_i \in \mathbb{Z}\}.$$

Die Menge der g_i's heisst eine Basis von L, wobei es viele Basen des gleichen Gitters gibt. Ein Gitter ist eine Untergruppe von $(\mathbb{R}^d, +)$.

Die Punkte eines Gitters liegen auf parallelen gleichabständigen Hyperebenen. Mathematisch lässt sich das beschreiben mit dem Konzept des dualen (oder reziproken) Gitters

$$L^\perp = \{v \in \mathbb{R}^d;\ v^T x \in \mathbb{Z}\ \ \forall x \in L\}.$$

Wir zeigen, dass $L^\perp$ wieder ein Gitter ist und bestimmen eine Basis.

Lemma 1 *Wenn L ein Gitter ist mit Basisvektoren g_i, dann ist auch $L^\perp$ ein Gitter und die Menge der Vektoren h_i, welche $h_i^T g_k = 0$ für $i \neq k$ uand $h_i^T g_i = 1$ erfüllen, ist eine Basis von $L^\perp$. Das heisst, wenn G die Matrix ist mit Spaltenvektoren g_i, dann bilden die Spalten von $H = G^{-T}$ eine Bais von $L^\perp$.*

Beweis als Übung.

Um zu untersuchen, wie gut ein Gitter den Raum ausfüllt, bestimmt man also diejenige Richtung, in der die parallelen, gleichabständigen Hyperebenen, die L enthalten, möglichst grossen Abstand haben. *Welchem Element von $L^\perp$ entspricht diese Richtung, und wie gross ist der maximale Abstand ?*

Da Hauptresultat ist nun

Satz 1 *Sei (x_n) ein linearer Kongruenzgenerator mit $c > 0$ und maximaler Periode M. Dann ist für jedes d die Menge*

$$\{(x_n, x_{n+1}, \ldots, x_{n+d-1}); 0 \leq n < M\} - c(0, 1, 1+a, \ldots, (1+a+\cdots+a^{d-2}))^T$$

gleich $L \cap \{0, \ldots, M-1\}^d$. wobei L gleich dem Gitter mit Basis

$$g_1 = (1, a, a^2, \ldots, a^{d-1})^T, \quad g_j = (0, \ldots, \underbrace{M}_{j}, \ldots, 0)^T \quad (j = 2, 3, \ldots, d).$$

ist. Das duale Gitter $L^\perp$ hat die Basis

$$h_1 = (1, 0, \ldots, 0)^T, \quad h_j = \frac{1}{M}(-a^{j-1}, 0, \ldots, 1, \ldots, 0)^T \quad (j = 2, 3, \ldots, d).$$

Beweisen Sie dies in den Fällen $d = 2$ und $d = 3$. Für $c = 0$ gilt der Satz auch, wenn man $(0, 0, \ldots, 0)^T$ noch zu L hinzufügt.

Die Basis von $L^\perp$ im Theorem oben ist leider nicht optimal, um die Richtung mit den grössten Lücken zu finden. Dazu muss man Basisvektoren mit kürzerer Länge finden. Dies kann mit folgendem Algorithmus gemacht werden:

1. Wiederhole den folgenden Schritt für jedes Paar $i \neq j$ in einer fest gewählten Reihenfolge bis keine Änderung mehr auftritt
2. Nimm an, dass $||h_i|| \leq ||h_j||$ und berechne s = Rundung $h_i^T h_j / ||h_i||^2$ auf die nächstliegend ganze Zahl. Ersetze h_j durch $h_j - s h_i$.

Überlegen Sie, weshalb dieser Algorithmus die Länge der Basisvektoren von $L^\perp$ verkleinert. Programmieren Sie diesen Algorithmus für $d = 3$ und wenden Sie ihn an für einige Beispiele.