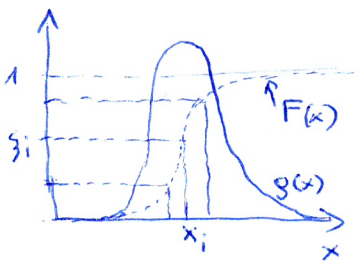
Generování náhodných čísel s určitým rozdělením

- máme-li k dispozici generátor pseudonáhodných čísel s rovnoměrným rozdělením na intervalu $\langle 0,1\rangle$ (povětšinou jako funkci v daném program. jazyce) můžeme generovat náhodná čísla s jiným rozdělením buď speciálními technikami pro specifická rozdělení, nebo univerzálními metodami (von Neumann, Metropolis), které ovšem nemusí být moc efektivní, nebo generovaná náhodná čísla můžou být korelovaná (je třeba hlídat)

1) metoda založená na inverzi kumulativní distribuční funkce

- potřebujeme-li generovat proměnnou x s pravděpodobnostním rozdělením $g(x)$, lze využít inverzi funkce



$$F(x) = P(X \le x) = \int_{-\infty}^{x} g(t)\,dt$$

pokud ovšem umíme inverzi F^{-1} spočítat (vyjádřit)

- pak jednoduše vygenerujeme $\xi_i \in (0,1)$ a položíme

$$\boxed{x_i = F^{-1}(\xi_i)}$$

- náhodná čísla jsou pak preferenčně vybírána tam, kde je $g(x)$ největší (nejstrmější růst $F(x)$)

příklady: a) exponenciální rozdělení na $\langle 0,\infty\rangle$

- pro $g(x) = \lambda e^{-\lambda x}$ dostaneme $\int_0^\infty g(x)\,dx = 1$

a $F(x) = 1 - e^{-\lambda x}$ a tedy $F^{-1}(\xi) = -\frac{1}{\lambda}\ln(1-\xi)$

- pokud $\xi \in \langle 0,1)$, pak i $1-\xi \in \langle 0,1)$ a obvykle se bere $\boxed{x_i = -\frac{1}{\lambda}\ln\xi_i}$, které bude mít rozdělení $g(x)$ na $\langle 0,\infty\rangle$

b) náhodné body na sféře

- normovaný element sféry je dán jako (pro poloměr R)

$$dS = \frac{1}{4\pi} R^2 \,d\varphi \sin\theta \,d\varphi$$

a tedy pro jednotkovou sféru chceme generovat body

s rozdělením $g(\theta,\varphi) = \frac{\sin\theta}{4\pi}$ $\left(\Rightarrow \int_0^{2\pi} d\varphi \int_0^{\pi} d\theta \frac{\sin\theta}{4\pi} = 1 \right)$

kumulativní distribuční funkce

$$F(\theta,\varphi) = \int_0^{\varphi} d\varphi' \int_0^{\theta} d\theta' \frac{\sin\theta'}{4\pi} = \frac{\varphi}{2\pi} \cdot \frac{1-\cos\theta}{2} = F_\varphi \cdot F_\theta$$

a generujeme

$\xi_1 \in \langle 0,1)$ $\Rightarrow$ $\varphi_i = F_\varphi^{-1}(\xi_1) = 2\pi\,\xi_1$

a $\xi_2 \in \langle 0,1)$ $\Rightarrow$ $\theta_i = F_\theta^{-1}(\xi_2) = \arccos(1-2\xi_2)$

c) <u>normální rozdělení</u>

- lze využít přímo centrální limitní větu
  x_i jako součet dostatečného počtu (>10) náhodných čísel s rovnoměrným rozdělením
- nebo trikem Boxe a Mullera (Ann. Math. Stat. 29 (1958) 610)

přes dvourozměrné normální rozdělení

$$g(x,y) = \frac{1}{2\pi} e^{-\frac{x^2+y^2}{2}}$$

a přechodem k polárním souřadnicím

$$g(x,y)\,dx\,dy = g_p(r,\varphi)\,dr\,d\varphi = \frac{1}{2\pi} e^{-\frac{r^2}{2}} r\,dr\,d\varphi$$

pro něž $F_r(r,\varphi) = \frac{\varphi}{2\pi} \int_0^r r' e^{-\frac{r'^2}{2}} dr' = \frac{\varphi}{2\pi}\left(1-e^{-\frac{r^2}{2}}\right) = F_\varphi \cdot F_r$

atedy z $\xi_1 \in \langle 0,1)$ $\Rightarrow$ $r_i = \sqrt{-\ln(1-\xi_1)}$ nebo $r_i = \sqrt{-\ln\xi_1}$

a $\xi_2 \in \langle 0,1)$ $\Rightarrow$ $\varphi_i = 2\pi\,\xi_2$

dostaneme dva body

$x_i = r_i \cos\varphi_i$

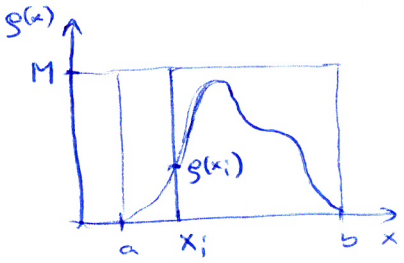
$y_i = r_i \sin\varphi_i$

které budou mít normální rozdělení

Pozn: pro jednorozměrné normální rozdělení nelze jednoduše invertovat $F(x) = \frac{1}{2}\left[1 + \mathrm{Erf}\left(\frac{x-m}{\sqrt{2\sigma^2}}\right)\right]$

2) univerzální von Neumannova metoda

- ilustrace na jednorozměrném případě, ale přímočaře lze zobecnit do více dimenzí, kde ale typicky rychle klesá její efektivita



- vygenerujeme dvě náhodné proměnné $\xi_i, \eta_i \in \langle 0,1 \rangle$ s rovnoměrným rozdělením a namapujeme je na intervaly $\langle a,b \rangle$ a $\langle 0,M \rangle$

$$x_i = a + \xi_i (b-a)$$

$$y_i = M \eta_i$$

kde M musí splňovat $g(x) \leq M$ pro $\forall x \in \langle a,b \rangle$ (volíme co nejmenší)

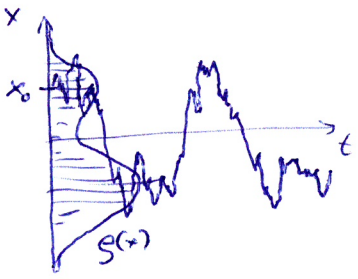
- pokud $y_i \leq g(x_i)$, pak x_i použijeme (přijmeme)
a pokud $y_i > g(x_i)$, pak x_i nepoužijeme (odmítneme)

a tedy pravděpodobnost přijetí bodu z $\langle x, x+dx \rangle$ je úměrná $g(x)\,dx$, neboť ξ_i jsou rovnoměrně rozdělené na $\langle a,b \rangle$

- pokud je $g(x)$ lokalizovaná do malé oblasti, pak je zlomek přijetí poměrně malý a ztrácí se efektivita $\Rightarrow$ lépe použít např. Metropolisův alg. i za cenu větší korelace

- Metropolisův - Hastingsův algoritmus

- základní myšlenka: jít „náhodnou" procházkou v prostoru v závislosti na hustotě pravděpodobnosti, tj. jsme-li v bodě x_k, učiníme náhodný krok o délce $\delta x_k = \xi_k \delta$, kde $\xi_k \in \langle -1, 1 \rangle$ a δ je fixní parametr procházky (musí být vhodně nastaven, aby bylo případně možno překlenout oblasti s malou hustotou),



a tento krok učiníme, pokud $g(x_k + \delta x_k) \geq g(x_k)$, nebo je-li $g(x_k + \delta x_k) < g(x_k)$, pak vygenerujeme náhodné $\eta \in \langle 0, 1 \rangle$ a krok učiníme, pokud $g(x_k + \delta x_k) / g(x_k) > \eta$.

- pokud krok neudělámě, pak zůstaneme a $x_{k+1} = x_k$.
- v d-rozměrném prostoru bude algoritmus vypadat takto:

procedura vracející další bod, jsme-li v x(:)

```
r(:) = random(:)          ← generátor na intervalu <0,1>
xtrial(:) = x(:) + δ(2r(:) - 1)   ← posun na <-1,1>
ratio = g(xtrial) / g(x)
if ( ratio ≥ 1 or ratio > random) then
        x = xtrial
return x(:)
```

- v limitě dlouhé náhodné procházky tento algoritmus opravdu generuje body rozložené podle g(x)
  - označíme-li $N_n(x)$ hustotu náhodných nezávislých chodců startujících v různých bodech po n krocích, pak počet chodců jdoucích z x do y v následujícím kroku je

$$\Delta N(x) = N_n(x) P(x \to y) - N_n(y) P(y \to x) =$$

$$= N_n(y) P(x \to y) \left[\frac{N_n(x)}{N_n(y)} - \frac{P(y \to x)}{P(x \to y)} \right]$$

kde $P(x \to y)$ je pravděpodobnost, že chodec přejde z x do y

- rovnováha nastává pro

$$\frac{N_n(x)}{N_n(y)} = \frac{P(y \to x)}{P(x \to y)}$$

a lze ukázat, že pro velká n jde $N_n(x) \to N_e(x)$, což je rovnovážné rozdělení chodců v x

- pro M-H algoritmus je $N_e(x) \sim g(x)$, neboť

$P(x \to y)$ lze vyjádřit jako

$$P(x \to y) = T(x \to y)\, A(x \to y)$$

kde $T(x \to y)$ je pravděpodobnost náhodného vykročení z x do y a $A(x \to y)$ je pravděpodobnost přijetí tohoto kroku

- pokud tedy bude

$$\frac{g(x)}{g(y)} = \frac{P(y \to x)}{P(x \to y)} = \frac{T(y \to x)\, A(y \to x)}{T(x \to y)\, A(y \to x)}$$

pak $N_e(x)$ bude $\sim g(x)$

- pro vhodně zvolené δ, kdy lze y dosáhnout v jediném kroku, tj. $y \in \langle x-\delta, x+\delta \rangle$, pak $T(x \to y) = T(y \to x)$

a dále pro $g(x) \geq g(y)$ bude

$$A(y \to x) = 1 \quad \text{a} \quad A(x \to y) = \frac{g(y)}{g(x)}$$

a pro $g(x) \leq g(y)$ bude

$$A(x \to y) = 1 \quad \text{a} \quad A(y \to x) = \frac{g(x)}{g(y)}$$

tedy celkem v každém případě

$$\frac{A(y \to x)}{A(x \to y)} = \frac{g(x)}{g(y)}$$

a tedy vskutku $\frac{N_e(x)}{N_e(y)} = \frac{g(x)}{g(y)}$

Generátory (pseudo) náhodných čísel (random numbers)

- deterministické programy generující posloupnost čísel, které splňují jistá kritéria (testy) náhodnosti
- při stejných počátečních podmínkách generují tytéž náhodná čísla
  - poč. pod. = random seed (náhodné semínko)
- vzhledem ke konečné aritmetice počítačů a deterministickému chování nejde o náhodná čísla, ale o pseudonáhodná
- většinou generována jako posloupnost čísel $\{x_0, x_1, x_2 \dots\}$ → nutná periodicita, kvůli konečné aritmetice ⇒ perioda generátoru = nejmenší k takové, že $x_i = x_{i+k}$ pro i

Základní generátory

- lineární kongruentní generátor (LCG) - velmi rychlý algoritmus

$$x_{i+1} = (a x_i + c) \bmod m$$

maximální (optimální) perioda = m, většinou menší

speciální případ - multiplikativní LCG, když $c = 0$ (navržen D. H. Lehmerem)

byl velmi často používán v historii, ale má často zásadní nedostatky pro aplikace ve více dimenzích, neboť n-tice $(x_i, x_{i+1}, \dots x_{i+n-1})$ se nacházejí na relativně malém počtu $(n-1)$-rozm. nadplochách

Př. Nechvalně známý generátor RANDV

$a = 65539$, $c = 0$, $m = 2^{31}$ splňuje rekur. vztah $x_{i+2} = (2^{16}+3) x_{i+1} \bmod 2^{31}$

$$x_{i+2} = (2^{32} + 6 \cdot 2^{16} + 9) x_i \bmod 2^{31} = (6 x_{i+1} - 9 x_k) \bmod 2^{31}$$

a lze ukázat, že trojice bodů se nacházejí na 15 paralelních rovinách

Marsaglia: Random Numbers Fall Mainly in the Planes, PNAS 61 (1968) 25

Teorel pro MLCG: Pokud $c_1, \dots c_n$ jsou přirozená čísla taková, že

$$c_1 + c_2 a + c_3 a^2 + \dots c_n a^{n-1} = 0 \pmod m$$

pak body $P_1 = (u_1, u_2, \dots u_n)$, $P_2 = (u_2, \dots u_{n+1}), \dots$ (kde $u_i = x_i/m$) leží v jedné z paralelních nadploch

$$c_1 z_1 + c_2 z_2 + \dots + c_n z_n = 0, \pm 1, \pm 2, \dots$$

Navíc nanejvýše $|c_1| + |c_2| + \dots + |c_n|$ těchto rovin protíná krychli $0 < z_1 < 1, \dots, 0 < z_n < 1$ a vždy lze vybrat takové $c_1, \dots c_n$, že body budou v méně než $(n! m)^{1/n}$ nadplochách.