1. Zufallszahlen

- Systeme mit sehr vielen FG enthalten statistische Elemente

  ▶ Tatsächliche Fluktuationen:

  - thermische Fluktuationen: Diffusion, Wärmeleitung, Transport
  - Quantenfluktuationen: Teilchenphysik, Feldtheorie
  - zufälliges Verhalten einzelner Konstituenten

  ▶ Algorithmische Zufallsvariablen in streng deterministischen Systemen

  - statistische Physik / Thermodynamik: Zeitmittel = Scharmittel
  - Stochastische Prozesse / Monte-Carlo
  - Genetische Algorithmen
  - Statistische Analysen cf. heatmap

1.1. Klassen von Zufallszahlen

[1] Echte Zufallszahlen

- erzeugt durch echt zufällige Prozesse, z.B. radioaktiver Zerfall (Poisson!)
- aufwändig, kurze Sequenzen, nicht konfigurierbar, wenig unabh. Sequenzen

[2] Pseudo-Zufallszahlen

- nicht zufällig (determiniert → Algorithmus)
- (weitgehend) unkorreliert
- Echtzeit generierbar, lange Sequenzen, viele unabh. Sequenzen, schnell
- versteckte Korrelationen nicht leicht auffindbar → Stat. Tests

[3] Quasi-Zufallszahlen

- nicht zufällig (determiniert)
- (maximal) korreliert
- raumfüllend (ergodisch)
- Echtzeit generierbar, lange Sequenzen, (mittel-) schnell, aufwändig in hohen Dimensionen
- können MC Verfahren beschleunigen

1.2. Gleichverteilte Pseudozufallszahlen (RNG)

Prototyp: Linear-Kongruenter Generator

$X \in [0, M-1]$ natürliche Zufallszahl

Sequenz: $\boxed{X_{j+1} = a \cdot X_j + c \quad (\text{mod } M)}$

- Periode = # Schritte bis ein X_j wieder auftritt
  maximal M

- gute Wahl von a, c, M entscheidend (maximale Periode)

- Korrelationen:
  k aufeinanderfolgende X_j, bilde $\vec{x} = (t_1, \dots, t_k)$ $\quad t_i = X_i / M \in [0,1]$
  $\{\vec{x}\}$ nicht dicht im $\mathbb{R}^k$, sondern auf $(k-1)$-dim. Hyperebenen!
  höchstens $M^{1/k}$ solcher Ebenen, oft viel weniger!!

  Bsp: IBM mainframe, RANDU:
  $M = 2^{31} \approx 32\,768$, $\quad a = 65539 \longrightarrow \vec{x} = (t_j, t_{j+1}, t_{j+2}) \in [0,1]^3$
  auf 11 (!) Ebenen im $\mathbb{R}^3$!

Vorsicht mit OS-implementierten Zufallszahlen !

- brauchbare Linear-kongruente Generatoren

  - $a = 7^5 = 16807$, $c = 0$, $M = 2^{31}-1$ } Lewis, Goodman, Miller (1969)

  - Kombiniere Sequenzen mit verschiedenem M, z.B.

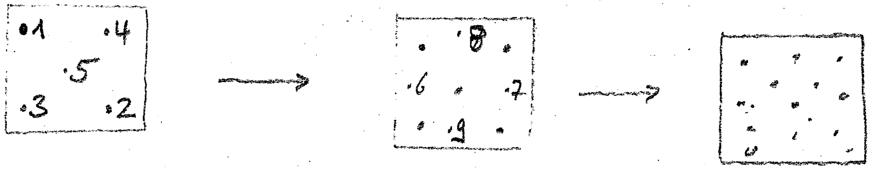
    $$X_j = \left[X_j^{(1)} + X_j^{(2)}\right] \bmod M \quad ; \quad M \in \{M_1, M_2\}$$ (L'Ecuyer)

- Best Practice: Verwende <u>gut getestete RNG-Bibliotheken/Algorithmen</u> !

  - ran3 (D. Knuth, s. Numerical Recipes)
  - ran4 (Verschlüsselung, basiert auf DES)
  - ranlux (M. Lüscher, exzellent, relativ langsam)
  - mersenne twister (Nishimura & Matsumoto, exzellent, schnell, riesige Periode $2^{19937}-1$
  - s. NVidia CURAND für weitere (auch CPU-basiert)

1.3. Quasi-Zufallszahlen

- deterministisch, korreliert



Quasi-Zufallszahlen „stoßen sich ab" → gleichverteilt + effizient raumfüllend

⇒ Können stat. Algorithmen beschleunigen!

- Bsp: (Halton)

  - j als Zahl zur Basis b
  - Kehre Reihenfolge der b-Ziffern um
  - Dezimalpunkt (Basis b) vor umgedrehte Zahl
  - Schreibe Zahl zurück zur Basis 10

  ⇒ Halton-Zahl H_j

$b = 3$

$j = 17$

- $17 = (122)_3$
- $(221)_3$
- $(0.221)_3$
- $2 \cdot 3^{-1} + 2 \cdot 3^{-2} + 1 \cdot 3^{-3}$
- $H_{17} = \frac{25}{27} = 0.90123457$

$j = 18$

$H_{18} = (0.002)_3 = \frac{2}{27} \approx 0.074 \ldots$

- Verbesserung durch Sobol (→ primitive Polynome mod 2)

  s. nVidia CURAND

1.4 Ungleichmäßige Verteilungen

- Suche Zufallszahl $\xi \in I \subseteq \mathbb{R}$ verteilt mit vorgegebener Dichte $\rho(\xi)$
- Annahme: Gleichverteilte Zufallszahlen $x \in \Omega \subseteq \mathbb{R}$ können erzeugt werden (RNG)

- Erzeugung von ξ:
  - [1] Transformationsmethode
  - [2] Ablehnungsmethode
  - [3] Spezielle Algorithmen für geeignete ρ

- [1] Transformationsmethode

> Sei x auf $[x_1, x_2]$ gleichverteilt und $g: [x_1, x_2] \to [a,b]$ diffbar und streng monoton
> Dann ist $\xi = g(x)$ Zufallsvariable auf $[a,b]$ mit Verteilung $\rho(\xi) = |f'(\xi)|$
> wobei $f = g^{-1} : [a,b] \to [x_1, x_2]$ die Umkehrfunktion ist.

Um das "richtige" f bzw. g zu finden (bei vorgegebener Zieldichte ρ) muss $\rho = f'$ integriert werden. d.h. man muss die Stammfunktion von ρ analytisch kennen

Bsp: $\rho(\xi) = \lambda \cdot e^{-\lambda \xi}$, $\xi \in \mathbb{R}$ (Poisson)

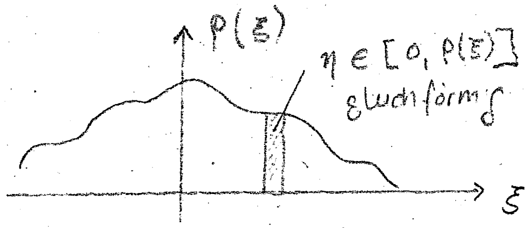
$|f'(\xi)| = \rho(\xi) = \lambda e^{-\lambda\xi} \rightarrow f(\xi) = \pm e^{-\lambda\xi}$

wähle '-' und $g(x) = f^{-1}(x) = + \lambda^{-1} \ln(-x)$

$\Rightarrow$ x auf $[x_1, x_2]$ gleichverteilt mit $x_1 = -e^{-\lambda a}$, $x_2 = -e^{-\lambda b}$

dann ist $\xi = \lambda^{-1} \ln(-x)$ auf $[a, b]$ mit $\rho(\xi) = \lambda e^{-\lambda\xi}$ verteilt.

[2] Ablehnungsmethode



$\rho(\xi)$ groß: ξ dicht in $\Delta\xi$
η dünn in $[0, \rho(\xi)]$
$\Rightarrow (\xi, \eta)$ gleichverteilt

Wähle Punkt (ξ, η) unter der Fläche von ρ gleichförmig

$\rightarrow \xi$ ist gesuchte Zufallsvariable !

Begründung: Flächendichte für Punkt $(\xi, \eta) = 1$

$1 =$ Dichte von $\xi \cdot$ Dichte von η

$=$ Dichte von $\xi \cdot \dfrac{1}{\rho(\xi)}$

Dichte von $\xi = \rho(\xi)$

Gleichförmige Punktverteilung

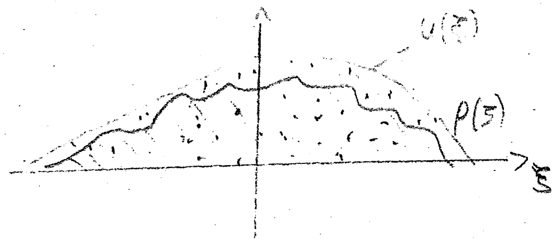
Falls $F(\xi) = \int_{-\infty}^{\xi} dx\, \rho(x)$ analytisch bekannt und $A = F(\infty) = \int_{-\infty}^{\infty} dx\, \rho(x)$

Wähle $t \in [0, A]$ gleichförmig $\rightarrow \xi = F^{-1}(t)$
$\eta \in [0, \rho(\xi)]$ gleichmäßig

$\Big\}$ (ξ, η) gleichförmig unter ρ verteilt

Problem: Muss Stammfunktion analytisch kennen

Besser: Wähle analytisch angenehme Vergleichsfkt. $u(\xi)$ mit $F(\xi) = \int_{-\infty}^{\xi} dx\, u(x)$ und $A = F(\infty)$



Wahrscheinlichkeit für (ξ, η):

$$u(\xi) \cdot \frac{\rho(\xi)}{u(\xi)} = \rho(\xi)$$

- Wähle Punkt (ξ, η) unter Vergleichsfunktion $u(\xi)$ wie oben
- Falls (ξ, η) unter ρ, d.h. $\eta < \rho(\xi)$ akzeptiere Punkt (ξ, η), sonst verwerfe und ziehe neuen Kandidat (ξ, η), solange bis akzeptiert
- $\Rightarrow$ nächster Punkt (ξ, η)
- ξ ist nach $\rho(\xi)$ verteilt

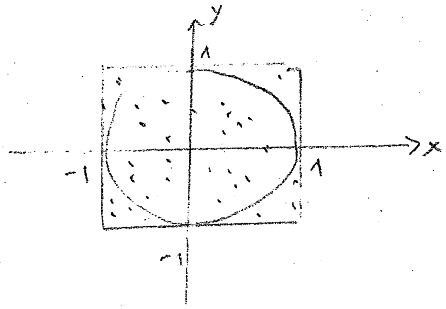
[3] Spezielle Methoden

Bsp: $\boxed{\text{Box-Müller}}$ für Gauß-Verteilung

- z_1, z_2 gleichverteilt auf $[0,1]$
- $\xi_1 = \sqrt{-2 \ln z_1} \cdot \cos(2\pi z_2)$
  $\xi_2 = \sqrt{-2 \ln z_1} \cdot \sin(2\pi z_2)$
- ξ_1, ξ_2 auf $\mathbb{R}$ Gauß-verteilt, $\rho(\xi) = \frac{1}{\sqrt{2\pi}} e^{-\xi^2/2}$

1.4 Einfache Monte-Carlo Methode

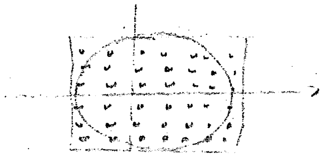
- Basiert auf Ablehnungsmethode



- Kreisfläche / Quadratfläche $= \pi/4$
- Würfle $(x, y) \in$ Quadrat gleichförmig
- Zähle „Treffer" in Kreis
- $\frac{\pi}{4} \approx \frac{\#\text{ Treffer im Kreis}}{\#\text{ Versuche}}$

1. Kann zu jedem Zeitpunkt mit Näherung für $\pi/4$ abgebrochen werden
2. Konvergenz sehr langsam, $|\text{Näherung} - \pi/4| = O(N^{-1/2})$ $N = \#$ Versuche

vgl. regelmäßiges Gitter für Testpunkte



- Skaliert wie $O(N^{-1})$
- Kann nicht jederzeit abgebrochen werden!

ÜA Ersetze Pseudo-Zufallszahl im MC oder durch Quasi-Zufallszahlen
Wie ändert sich die Konvergenzgeschwindigkeit?

1.5. Das Monte-Carlo Theorem

Betrachte n-dim Integral $I = \int_\Omega d^n x \, f(\vec{x})$ mit $\Omega = \Omega_1 \times \dots \times \Omega_n$ und $f \geq 0$

1. Sei $\vec{\xi} \in \Omega$ Zufallsvektor, so daß jede Komponente ξ_k in Ω_k gleichverteilt ist.
   Dann Stichprobe $\{\vec{\xi}^{(i)}\}$ vom Umfang N

$$\boxed{I = |\Omega| \cdot \left\{ \langle f \rangle \pm \sigma_f \right\}}$$

Standardfehler

mit $\langle f \rangle = \frac{1}{N} \sum_{i=1}^{N} f(\vec{\xi}^{(i)})$ arithm. Mittel

$$\sigma_f^2 = \frac{1}{|\Omega|^2} \int_\Omega d^n x \left[f(\vec{x}) - I/|\Omega| \right]^2$$

2. Der beste Schätzwert für die Varianz σ_f^2 ist

$$\sigma_f^2 \cong \frac{1}{N-1} \left\{ \langle f^2 \rangle - \langle f \rangle^2 \right\} = \frac{1}{N(N-1)} \sum_{i=1}^{N} \left[f(\vec{\xi}^{(i)}) - \langle f \rangle \right]^2$$

Insbesondere ist $\sigma_f \sim O(N^{-1/2})$ für $N \to \infty$.

3. Verallgemeinerung für nicht gleichverteilte Zufallsvektoren:

$$\frac{I}{|\Omega|} = \frac{1}{|\Omega|} \int_\Omega d^n x \, \rho(\vec{x}) \cdot f(\vec{x}) \approx \langle f \rangle \pm \left[\frac{\langle f^2 \rangle - \langle f \rangle^2}{N-1} \right]^{1/2}$$

wobei $\langle \omega \rangle = \frac{1}{N} \sum_{i=1}^{N} \omega(\vec{\xi}^{(i)})$ und $\vec{\xi}$ in Ω nach Dichte $\rho(\vec{\xi})$ verteilt