3 Generierung und Bewertung von Zufallszahlen

Warum brauchen wir den Zufall in der Simulation?

Unsere Wahrnehmung der Realität ist i.d.R. nicht deterministisch

Beispiele:

- Ausfallzeit und Reparaturzeit einer Maschine
- Ankunftszeiten von Kunden
- Einschlagstellen von Blitzen, ……

Einsatz von Zufall, wenn

- Komplexität vermieden werden soll
- Details nicht bekannt sind
- Zusammenhänge nicht bekannt sind
- zufällige Prozesse in der Natur auftreten

Zufall ist ein zentrales Element der diskreten Simulation

Damit sind auch Wahrscheinlichkeitsrechnung und mathematische Statistik unverzichtbar

Ziele dieses Kapitels:

- Kurze Einführung in die Wahrscheinlichkeitsrechnung und Statistik (Wiederholung!)
- Kennen lernen, wie Zufall im Rechner gehandhabt wird
- Wissen wie aus Zufallszahlen einer bestimmten Verteilung generiert werden
- Wissen was gute Zufallszahlen sind und wie man diese erkennen kann
- Grenzen der Darstellung kennen lernen

Gliederung

3.1 Grundlagen der Wahrscheinlichkeitsrechnung
(eine Wiederholung!?)

3.2 Grundlagen der Generierung von Zufallszahlen

3.1 Grundlagen der Wahrscheinlichkeitsrechnung

Zufallsexperiment ist ein Prozess, dessen Ausgang wir nicht mit Gewissheit vorhersagen können

- Die Menge der möglichen einander ausschließenden Ausgänge S heißt die Menge der Elementarereignisse
- E ist eine Ereignismenge, falls gilt
  - $\emptyset \in E$ und $S \in E$
  - $A \in E \Rightarrow S \backslash A \in E$
  - $A_i \in E \Rightarrow \cup_i A_i \in E$ und $\cap_i A_i \in E$
- Wahrscheinlichkeitsmaß P(A) bildet $A \in E$ auf reelle Zahlen ab, so dass
  - $0 \leq P(A) \leq 1$, $P(S)=1$ und $P(\emptyset)=0$
  - falls $A \cap B = \emptyset \Rightarrow P(A \cup B) = P(A)+P(B)$

Allgemein gilt $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

A|B beschreibt, dass A eintritt unter der Bedingung, dass B eintritt/eingetreten ist

Es gilt dann $P(A|B) = P(A \cap B) / P(B)$

Sei $B = A_1 \cup A_2 \cup \ldots \cup A_K$ und alle A_k seien disjunkt, dann

Satz von der totalen Wahrscheinlichkeit

$P(B) = \Sigma_{k=1,\ldots,K} P(B|A_k) \cdot P(A_k)$

Satz von Bayes

$P(A|B) = P(B|A) \cdot P(A) / P(B)$

Zwei Ereignisse A und B heißen unabhängig, wenn eine der folgenden Bedingungen gilt

$P(A|B) = P(A)$ oder $P(B|A) = P(B)$ oder $P(A \cap B) = P(A) \cdot P(B)$

Zufallsvariable (ZV) ist eine Variable, deren Wert durch den Ausgang eines Zufallsexperiments bestimmt ist und eine reelle Zahl ist.

Bezeichnung für ZVs: X, Y, Z, ...

Bezeichnung für den Wert einer ZVs: x, y, z, ...

Unterscheidung in

diskrete Zufallsvariablen mit endlichem oder abzählbarem Wertebereich

Beispiele: Münzwurf, Würfeln, Anzahl eingehender Telefonanrufe, ...

kontinuierliche Zufallsvariablen mit überabzählbarem Wertebereich

Beispiele: Zwischenankunftszeit, Bedienzeit, Regenmenge, ...

Charakterisierung von Zufallsvariablen

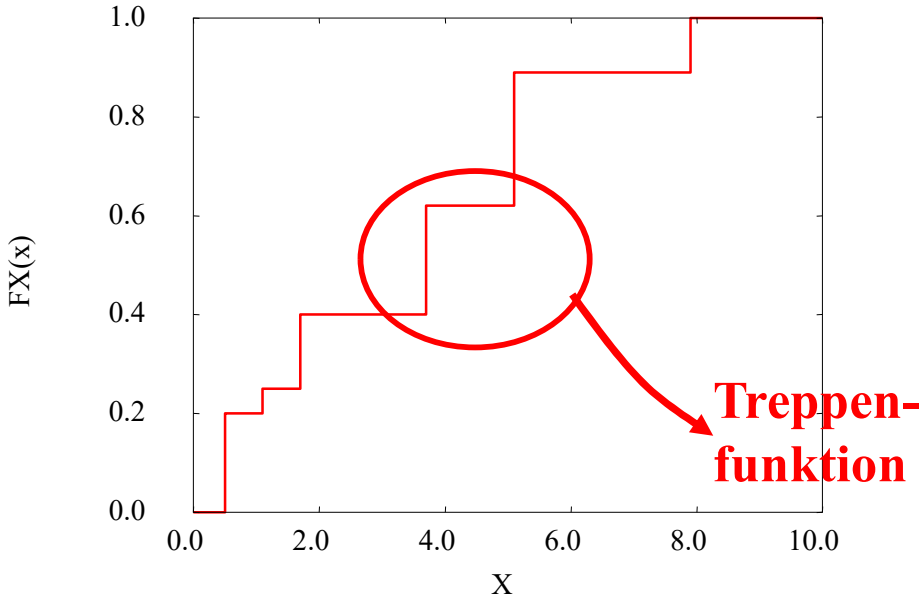
Verteilungsfunktion (Vfkt) $F(x)=P[X \leq x]$ für $-\infty \leq x \leq \infty$

Es gilt:

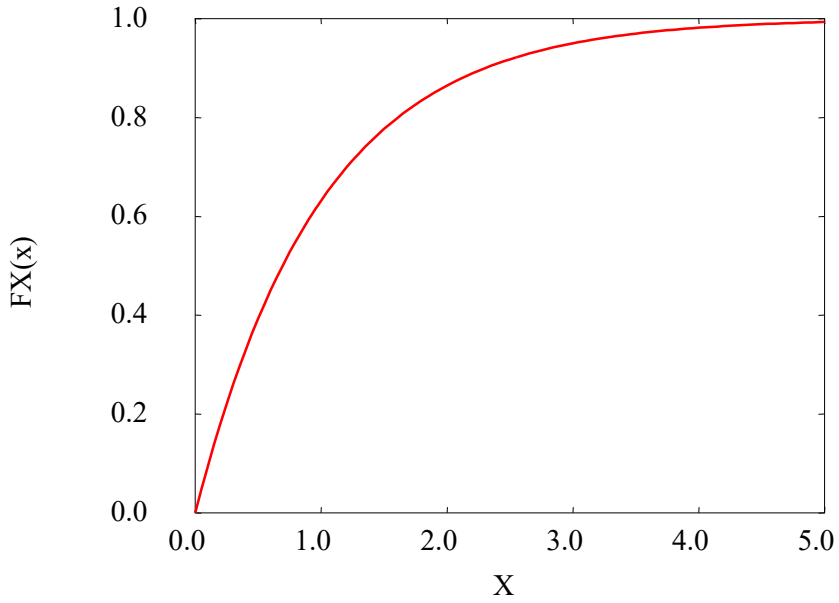
- $0 \leq F(x) \leq 1$
- $x_1 < x_2 \Rightarrow F(x_1) \leq F(x_2)$
- $\lim_{x \to \infty} F(x) = 1$ und $\lim_{x \to -\infty} F(x) = 0$

Graphische Repräsentation

diskrete ZV



kontinuierliche ZV

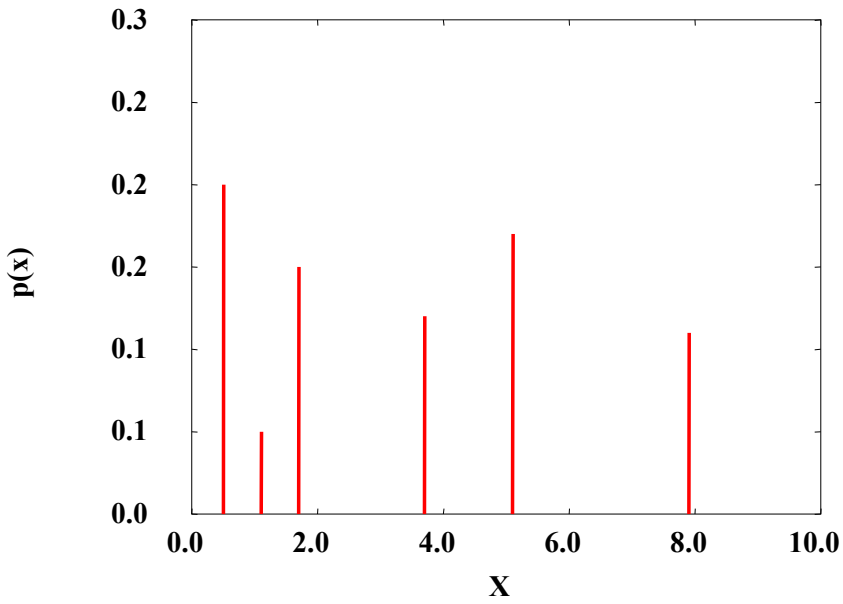


Diskrete ZV X mit Wertebereich W_X

Wahrscheinlichkeit p(x)=P[X=x], es gilt

- $p(x)=0$ für $x \notin W_X$
- $0 \leq p(x) \leq 1$ für $x \in W_X$
- $\sum_{x \in W_X} p(x) = 1.0$
- $\sum_{x \in W_X \wedge x \leq y} p(x) = F(y)$

Graphische Repräsentation



Momente der Verteilung

- $E(X^i) = \sum_{x \in W_X} p(x) \cdot x^i$ i-tes Moment
- $E(X) = E(X^1)$ erstes Moment oder Erwartungswert

Beispiel fairer Würfel: $p(x) = 1/6$ für $x = 1,\ldots,6$

Damit gilt $E(X) = \Sigma_{x=1,\ldots,6}\, x/6 = 7/2$

Einige Identitäten für Erwartungswerte:

- $E(c \cdot X) = c \cdot E(X) \quad (c \in \mathbb{R})$
- $E\big(h(X)\big) = \sum_{x \in W_X} p(x) \cdot h(x)$
- $E(\sum_{i=1}^{n} c_i \cdot X_i) = \sum_{i=1}^{n} c_i \cdot E(X_i) \qquad (c_i \in \mathbb{R})$
  (gilt auch für abhängige X_i !)

Weitere Maßzahlen:

- $\sigma^2(X) \quad = E\big((X - E(X))^2\big) \qquad = \sum_{x \in W_X} p(x) \cdot (x - E(X))^2$
  $\qquad\qquad = \sum_{x \in W_X} p(x) \cdot x^2 - E(X)^2 \quad = E(X^2) - E(X)^2$
  Varianz und σ(X) Standardabweichung
- $VK(X) = \frac{\sigma(X)}{E(X)}$ Variationskoeffizient
- $C(X,Y) = E((X - E(X)) \cdot (Y - E(Y))) = E(X \cdot Y) - E(X) \cdot E(Y)$ Kovarianz

Typische/Wichtige diskrete Verteilungen

Bernoulli-Verteilung
Parameter $p \in [0,1]$:

$$p(x) = \begin{cases} p & \text{falls } x = 1 \\ 1-p & \text{falls } x = 0 \\ 0 & \text{sonst} \end{cases}$$

$$F(x) = \begin{cases} 0 & \text{falls } x < 0 \\ 1-p & \text{falls } 0 \le x < 1 \\ 1 & \text{falls } 1 \le x \end{cases}$$

$E(X)=p$

$\sigma^2(X)=p\cdot(1-p)$

Anwendung:
binäre Entscheidungen

Geometrische-Verteilung
Parameter $p \in (0,1]$:

$$p(x) = \begin{cases} p \cdot (1-p)^x & \text{falls } x \in \{0,1,2,\ldots\} \\ 0 & \text{sonst} \end{cases}$$

$$F(x) = \begin{cases} 1-(1-p)^{\lfloor x \rfloor+1} & \text{falls } x \ge 0 \\ 0 & \text{sonst} \end{cases}$$

$E(X)=(1-p)/p$

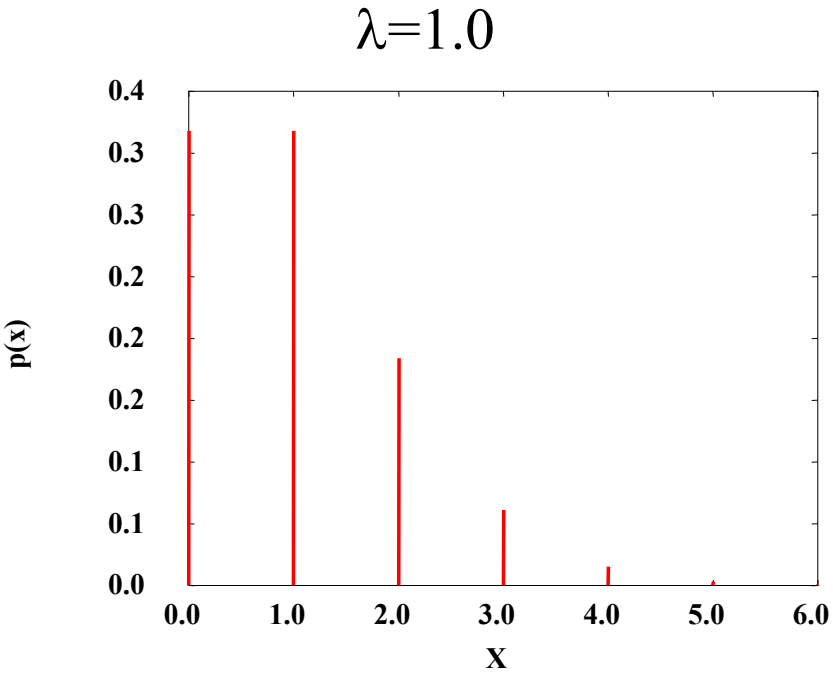
$\sigma^2(X)=(1-p)/p^2$

Anwendung:
Anzahl erfolgloser Versuche bis zum Erfolg bei Erfolgswahrscheinlichkeit p

Poisson-Prozess (Parameter $\lambda>0$)

$$p(x)=\begin{cases}\dfrac{e^{-\lambda}\cdot\lambda^{x}}{x!} & \text{falls } x\in\{0,1,2,\ldots\}\\ 0 & \text{sonst}\end{cases}$$

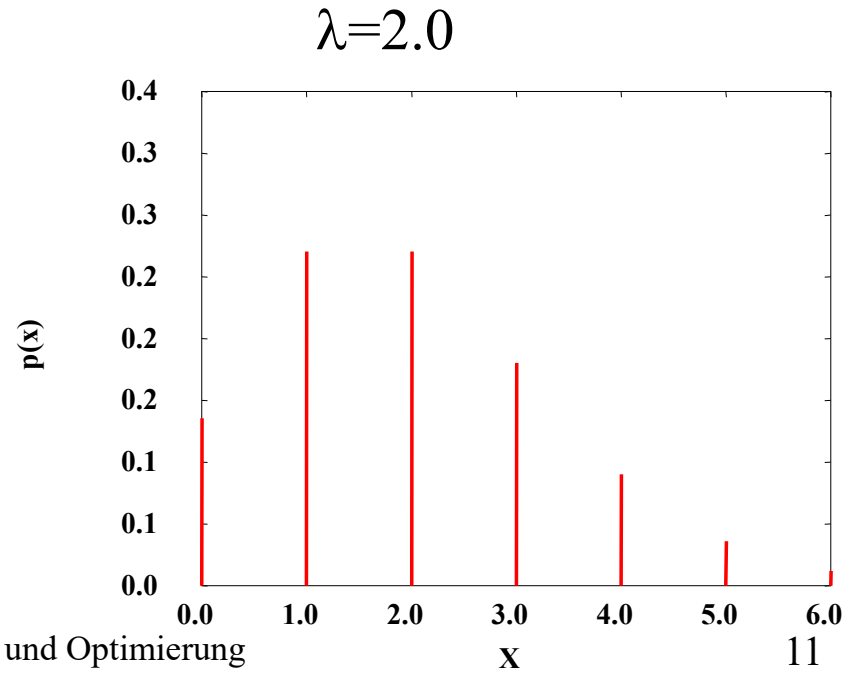
$$F(x)=\begin{cases}e^{-\lambda}\displaystyle\sum_{i=0}^{\lfloor x\rfloor}\frac{\lambda^{i}}{i!} & \text{falls } x\geq 0\\ 0 & \text{sonst}\end{cases}$$



Es gilt $\lim_{x\to\infty} F(x) = 1$, da

$$\sum_{i=0}^{\infty}\frac{\lambda^{i}}{i!}=e^{\lambda}$$

$$E(X)=\lambda$$
$$\sigma^{2}(X)=\lambda$$



Anwendungen des Poisson-Prozesses:

Angenommen wir hätten ein Intervall, in dem zufällig Ereignisse auftreten.
Dieses Intervall kann so in Subintervalle partitioniert werden, dass

1. die Wahrscheinlichkeit, dass mehr als ein Ereignis im Subintervall auftritt vernachlässigbar ist,
2. die Wahrscheinlichkeit, dass ein Ereignis in einem Subintervall auftritt, für alle Subintervalle identisch ist und
3. die Ereignisse unabhängig in den Subintervallen auftreten

dann entspricht die Verteilung der Ereignisse im Intervall einem Poisson Prozess

Anwendungsbeispiele:

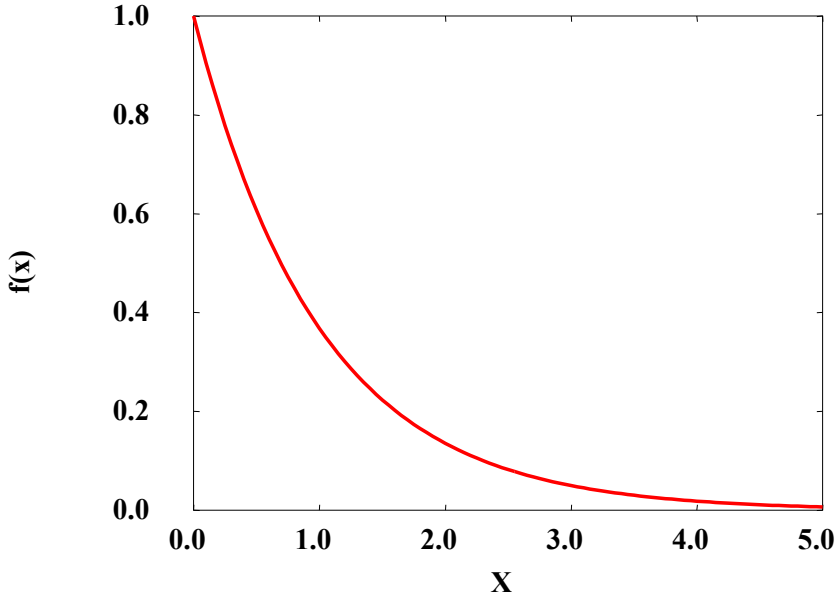
- Telefonanrufe an einer Vermittlungsstelle
- Fehler in einer Fertigung
- …

Kontinuierliche ZV X mit Wertebereich W_X

Dichtefunktion (Dfkt) $f(x)$, es gilt

- $f(x) = 0$ für $x \notin W_X$
- $0 \leq f(x)$ für $x \in W_X$
- $\int_{x \in W_X} f(x)dx = 1.0$
- $\int_{x \in W_X \wedge x \leq y} f(x)dx = F(y)$
- $\int_y^z f(x)dx = F(z) - F(y)$ falls $z \geq y$

Graphische Repräsentation



Momente $E(X^i) = \int_{x \in W_X} f(x) \cdot x^i dx$

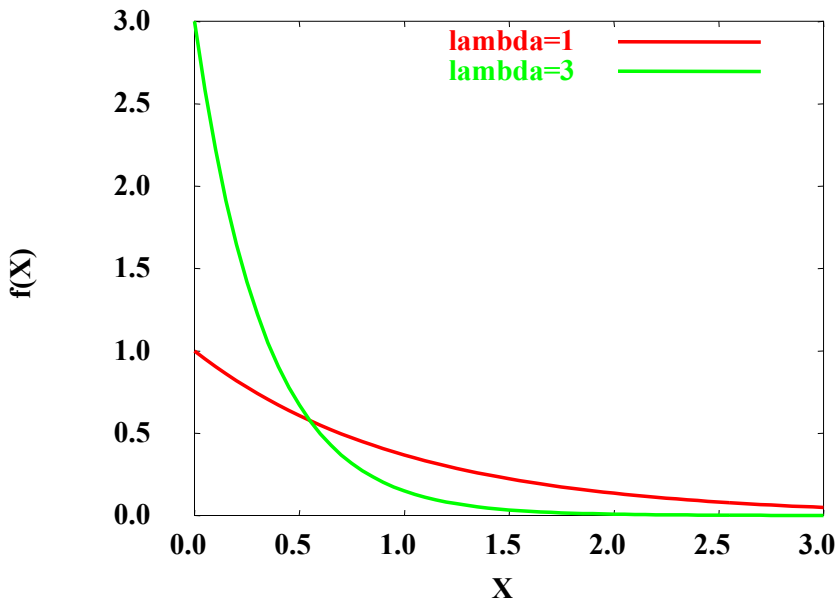
$$\sigma^2(X) = \int_{x \in W_X} f(x) \cdot \big(x - E(X)\big)^2 dx = \int_{x \in W_X} f(x) \cdot x^2 dx - E(X)^2$$

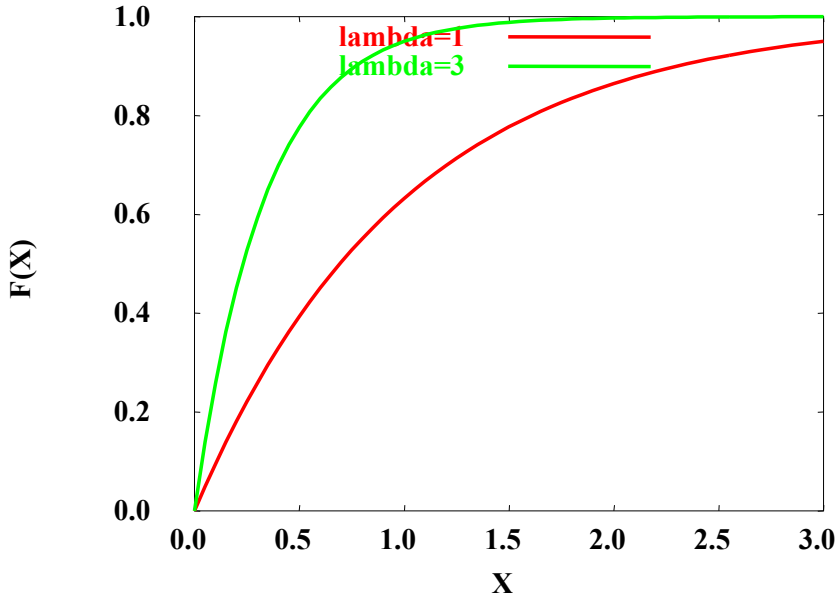
Wichtige kontinuierliche Verteilungen

Exponentialverteilung (Parameter $\lambda>0$)

$$f(x)=\begin{cases}\lambda\cdot e^{-\lambda x} & \text{falls } x\geq 0\\ 0 & \text{sonst}\end{cases}$$

$$F(x)=\begin{cases}1-e^{-\lambda x} & \text{falls } x\geq 0\\ 0 & \text{sonst}\end{cases}$$





- $E(X)=1/\lambda$
- $\sigma^2(X)=1/\lambda^2$

$\Rightarrow VK(X)=1$

Anwendung:

Addition vieler seltener Ereignisse,
z.B. Zwischenankunftszeiten

Gedächtnislosigkeitseigenschaft der Exponentialverteilung:

Falls eine ZV X exponentialverteilt ist, so gilt

$P[X > t + s \mid X > t] = P[X > s]$, da

$P[X > t + s \mid X > t] = e^{-\lambda(s+t)} / e^{-\lambda t} = e^{-\lambda s} = P[X > s]$

Dies hat zur Folge, dass die Restzeit einer Exponentialverteilung immer exponentialverteilt ist mit einer festen Rate

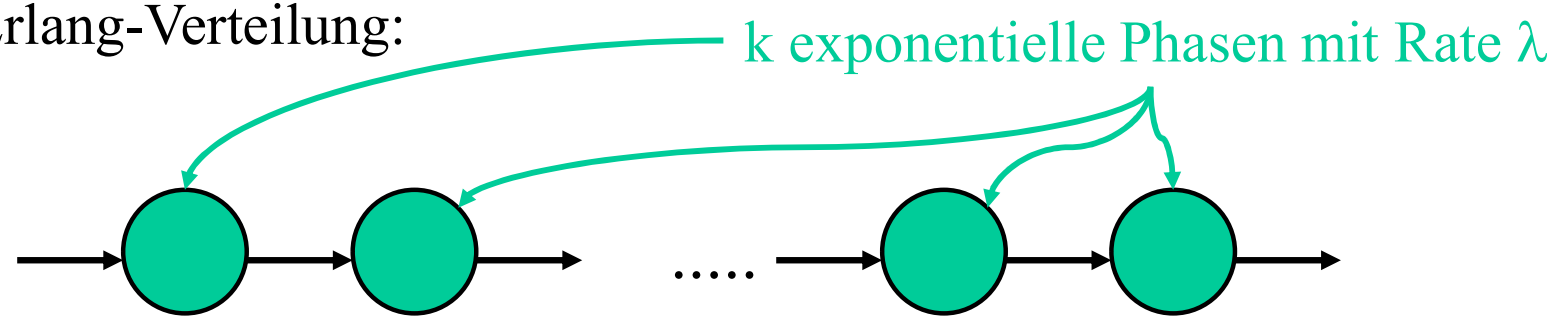
Damit ist die Exponentialverteilung für analytische Berechnungen interessant

Falls Ereignisse mit einer exponentialverteilten Generierungszeit mit Rate λ erzeugt werden, so entspricht die Anzahl der Ereignisse, die in einem Intervall $[0,t]$ erzeugt werden, einem Poisson-Prozess mit Rate λt.

Erweiterung der Modellierungsmächtigkeit der Exponentialverteilung:

- Kombination von exponentiellen Phasen

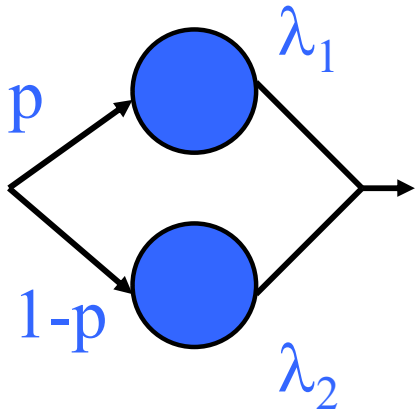
Erlang-Verteilung:



$E(X)=k/\lambda$, $\sigma^2(X)=k/\lambda^2$ und $VK(X)=1/k^{1/2}$

(weniger variabel als Exp.-Verteilung)

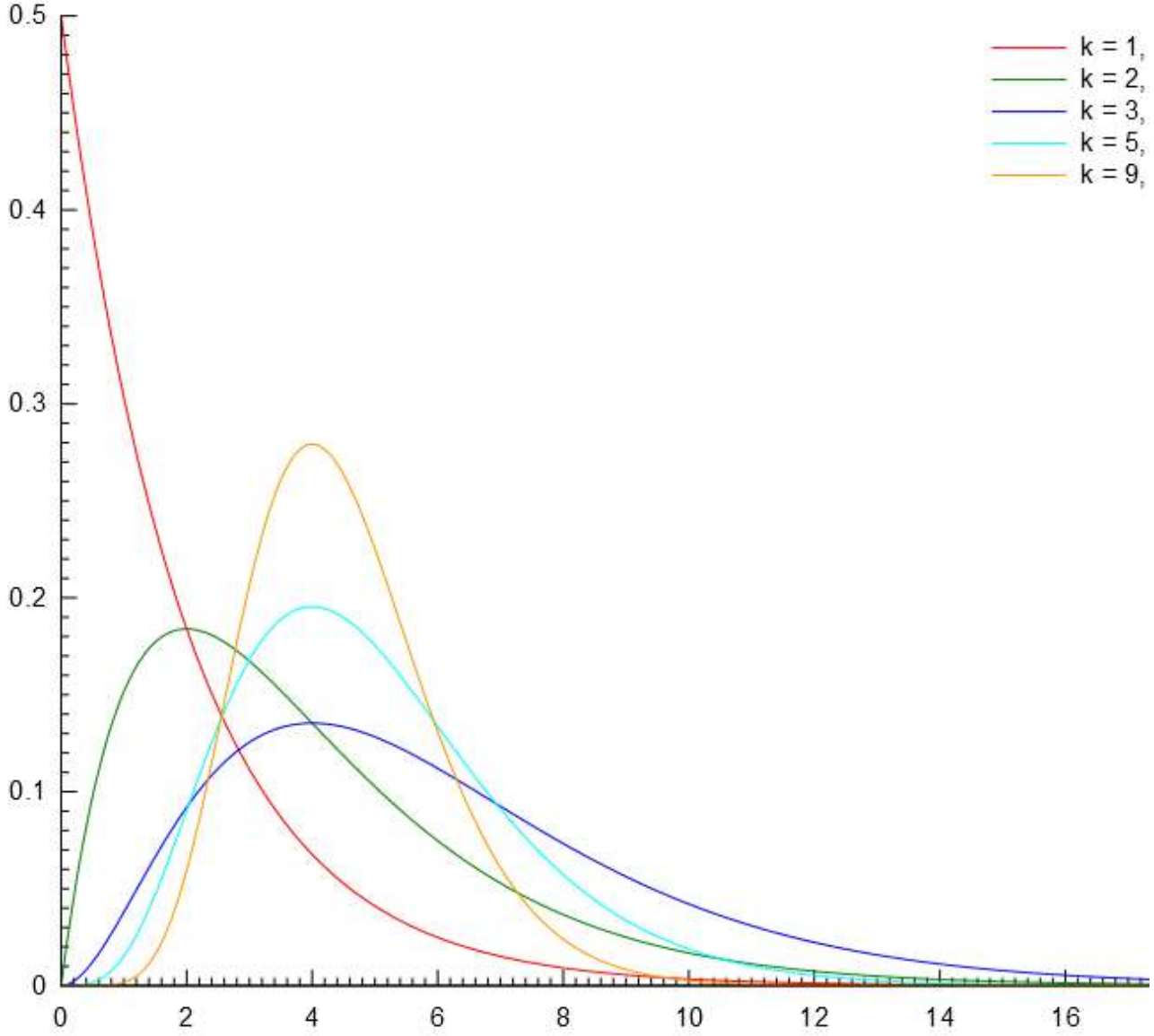
Hyperexponential-Verteilung:



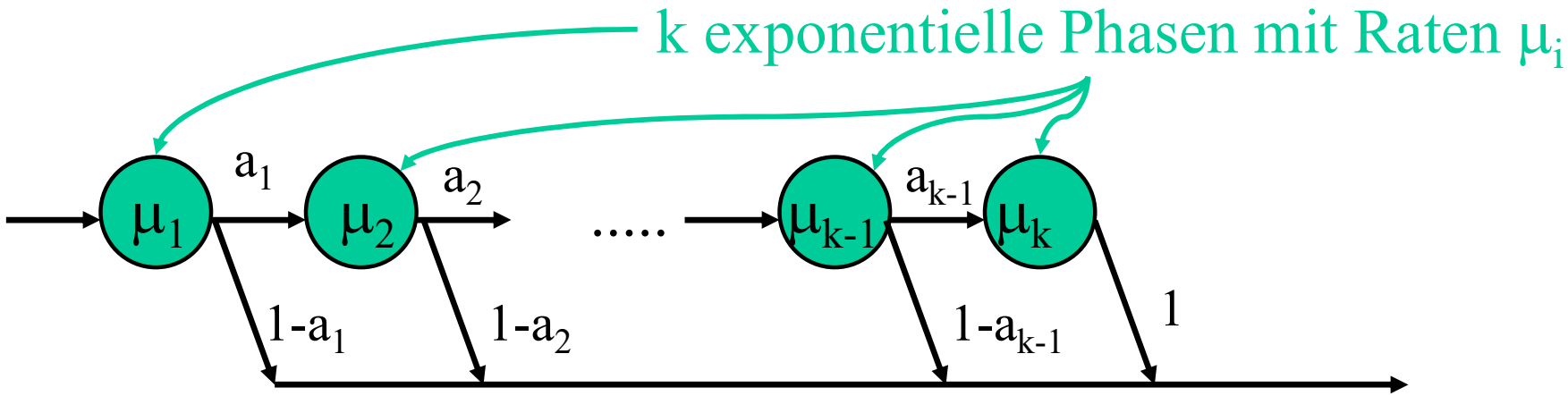
- $E(X)=p/\lambda_1+(1-p)/\lambda_2$,
- $\sigma^2(X)=p(2-p)/\lambda_1^2 + (1-p^2)/\lambda_2^2 - 2p(1-p)/(\lambda_1\lambda_2)$

(mindestens so variabel wie Exp.-Verteilung, beliebige VK≥1 realisierbar)

Erlang-Verteilung



Cox-Verteilungen als Erweiterung der Phasenverteilungen



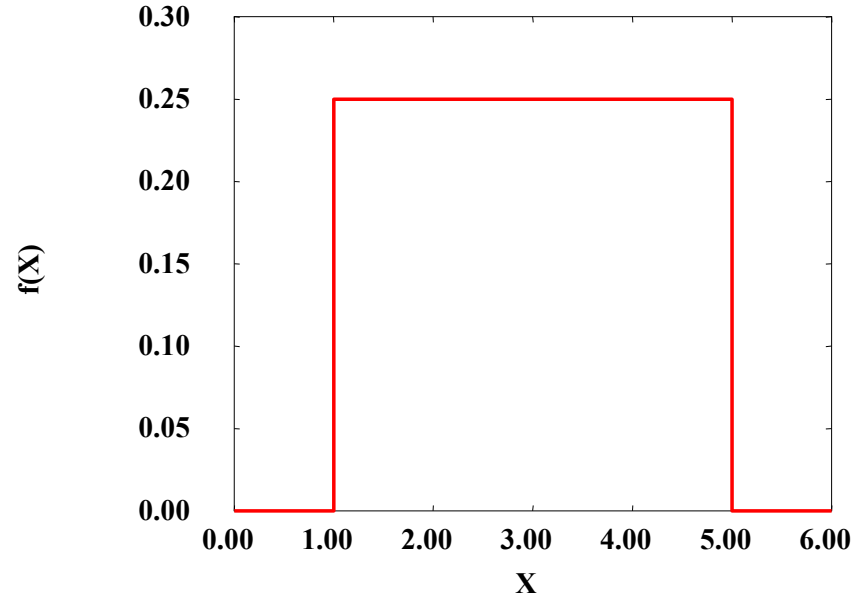
$$E(X) = \sum_{i=1}^{k} \left(\prod_{j=1}^{i-1} a_j \right) \frac{1}{\mu_i} \qquad \text{und} \qquad VK(X) \geq \frac{1}{\sqrt{k}}$$

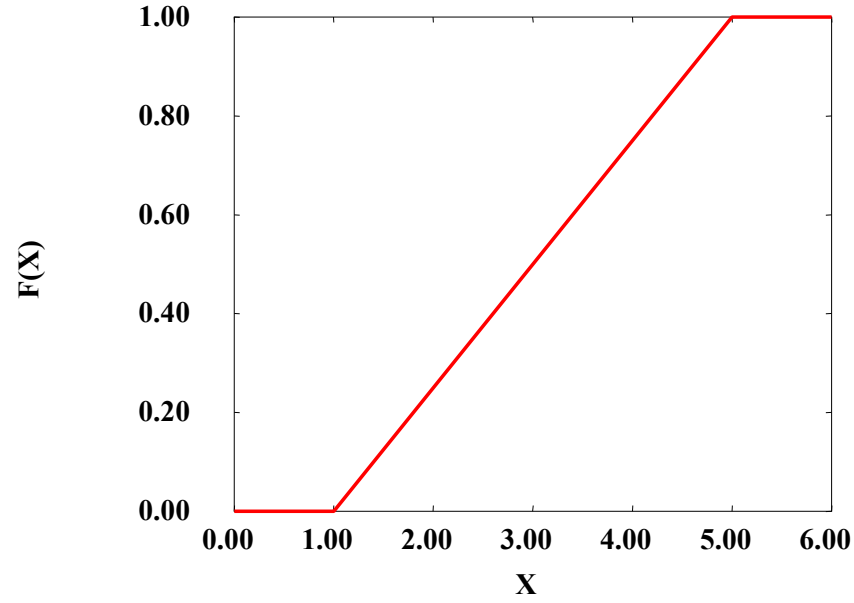
Jede Erlang- oder Hyperexponentialverteilung mit k Phasen kann durch eine Cox-Verteilung mit k Phasen dargestellt werden.

Gleichverteilung (Parameter a,b)

$$f(x) = \begin{cases} \dfrac{1}{b-a} & \text{falls } a \le x \le b \\ 0 & \text{sonst} \end{cases}$$

$$F(x) = \begin{cases} 0 & \text{falls } x < a \\ \dfrac{x-a}{b-a} & \text{falls a} \le \text{x} < \text{b} \\ 1 & \text{falls b} \le \text{x} \end{cases}$$





- E(X)=(a+b)/2 $\Rightarrow$ VK(X)≈1.73
- $\sigma^2(X)=(b-a)^2/12$

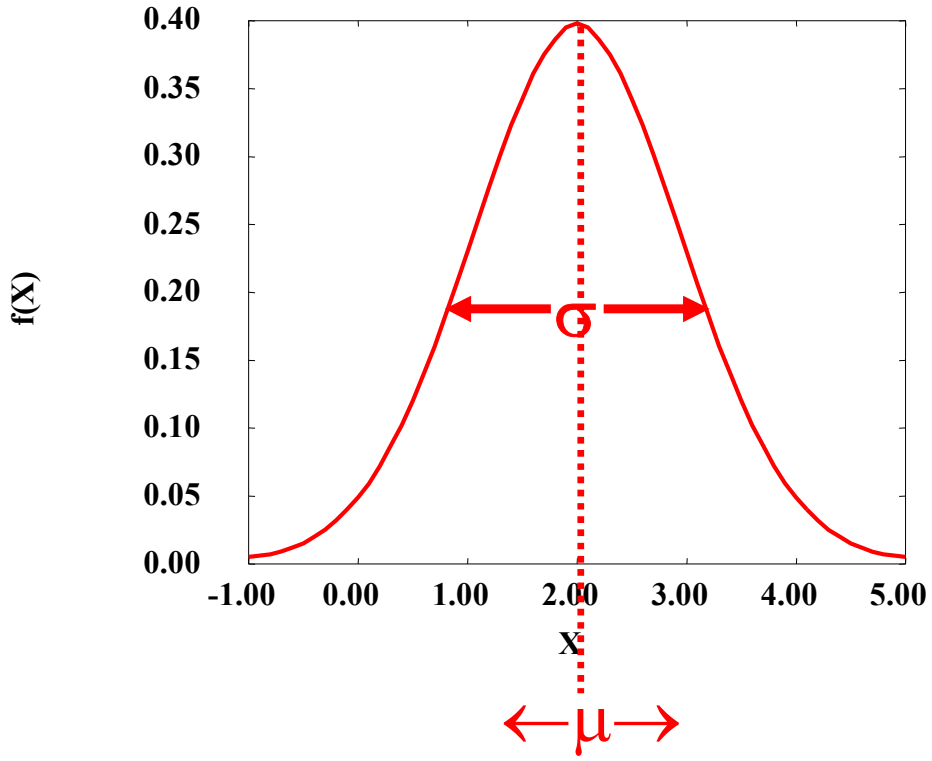
Anwendung:

[0,1]-Gleichverteilung ist die Basis zur Generierung allg. Verteilungen.

Normalverteilung (Parameter μ,σ)

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}$$

Keine geschlossene Form für F(X)



- E(X)=μ
- $\sigma^2(X)=\sigma^2$

Normalverteilt mit Parametern μ, σ ⇒
Schreibweise $X \sim N(\mu, \sigma^2)$

Falls $X \sim N(0, 1) \Rightarrow Y = \mu + \sigma \cdot X \sim N(\mu, \sigma^2)$

N(0, 1) ist die Standardnormalverteilung, aus ihr können Realisierungen für beliebige Normalverteilungen erzeugt werden

Zentraler Grenzwertsatz:

Sei $X_1,\ldots,X_n$ eine Menge identisch unabhängig verteilter ZVs mit Erwartungswert μ und Standardabweichung σ, dann gilt für den Mittelwert $\tilde{X}_n = \frac{1}{n}\sum_{i=1}^{n} X_i$:

$$\lim_{n\to\infty} \frac{\tilde{X}_n - \mu}{\sigma/\sqrt{n}} \sim N(0,1).$$

Anwendungen:

Durch mehrfaches/vielfaches Beobachten einer Zufallsvariablen können Aussagen über die Verteilung des Mittelwertschätzers gemacht werden, ohne die Verteilung der ZV zu kennen!

- Bestimmung von Konfidenzintervallen (Kap. 5)
- Testverfahren (Kap. 3, 4, 5, 8)
- …

Statistik in der Modellierung und Simulation

- mathematisches Modell zufälliger Prozesse $\Rightarrow$ Wahrscheinlichkeitsrechnung
- Modellierung realer Phänomene mit Hilfe des mathematischen Modells $\Rightarrow$
  1. Beobachte Realisierungen
  2. Finde eine passende mathematische Beschreibung

Daraus ergeben sich Fragen:

Wie oft/lange muss ich beobachten, bis ich genügend Informationen habe? (Beobachtungen schwanken!)

Welche Aussagen darf ich aus einer endlichen Zahl von Beobachtungen ableiten?

Ist mein gewähltes Modell für die Beobachtungsdaten passend?

Stichproben und Schätzer

Sei X eine ZV mit unbekannter Verteilung

$x_1,..., x_n$ sei eine Menge von Beobachtungen von X (eine Stichprobe)

alle Beobachtungen seien unabhängig und aus derselben Verteilung

Oft sollen Aussagen über Parameter Θ der Verteilung von X mit Hilfe von $x_1,..., x_n$ gewonnen werden

Ein Schätzer $\widetilde{\Theta}$ für einen Parameter Θ der Verteilung einer ZV X auf Basis einer Stichprobe $x_1,..., x_n$ ist eine Funktion

$$g(x_1, \cdots, x_n) \rightarrow \widetilde{\Theta} \quad (g \text{ ist die Schätzfunktion, } \widetilde{\Theta} \text{ ist eine ZV}).$$

heißt

- erwartungstreu, wenn $E(\widetilde{\Theta}) = \Theta$
- asymptotisch erwartungstreu, wenn $\lim_{n\to\infty} E(\widetilde{\Theta}) = \Theta$
- konsistent, wenn $\lim_{n\to\infty} P\left[\left|\widetilde{\Theta} - \Theta\right| > \varepsilon\right] = 0$ für jedes $\varepsilon > 0$

Auswertungen und Tests

Ziel ist eine formalere Überprüfung über die Gültigkeit von Modellen

Beispiele:

- Sei Θ ein Schätzwert für den Erwartungswert einer Größe, der aus einer endlichen Stichprobe geschätzt wurde.
  Wie groß ist der Unterschied zwischen dem wahren Wert und dem Schätzwert?
- Können wir auf Basis einer Stichprobe entscheiden, dass ein Wert nie größer als eine vorgegebene Schranke wird?

Ohne zusätzliche Informationen können endliche Stichproben zu falschen Aussagen/Schlüssen führen!

Die Wahrscheinlichkeit einer falschen Aussage fällt meistens mit einer steigenden Zahl verfügbarer Beobachtungen!

Methoden der Statistik:

➢ Konfidenzintervalle und Testverfahren

3.2 Grundlagen der Generierung von Zufallszahlen

Ziel: Realisierungen einer ZV X sollen generiert werden

„Ziehen von Zufallszahlen (ZZ)“

- Gesucht Methode $zz(X) \rightarrow x$, so dass
  für so erzeugte x, $P(x<y)=P(X<y)$ für alle y
  $(\Rightarrow E(x^i)=E(X^i)$ für alle i)
- Eine Sequenz $x_1,x_2, \ldots$ liefere *unabhängige* ZZs

Schritte der Erzeugung von ZZs:

1. Erzeugung von gleichverteilten ganzzahlige ZZs im Intervall [0,m)
2. Transformation in (approximativ) [0,1)-gleichverteilte ZZs
3. Transformation in ZZs der gewünschten Verteilung

Basis aller ZZ-Generatoren: Erzeugung von [0,1)-gleichverteilten ZZs

Echte Zufallszahlen:

- Münzwurf (Z=1, K=0)
- Würfeln (Zahlen 1,..6)
- Physikalische Messungen (z.B. radioaktiver Zerfall)

echte ZZs sind nicht reproduzierbar!

Pseudozufallszahlen:

Sequenz von ZZs, die für einen Beobachter zufällig aussieht

- Tafeln mit ZZs (z.B. Tippett 1927, 41600 gleichvert. Zahlen aus Daten der Finanzverwaltung)
- Generierungsalgorithmus der Form $x_i=g(s_i)$ und $s_{i+1}=f(s_i)$

Pseudo-ZZs sind reproduzierbar!

In der Simulation werden fast nur Pseudozufallszahlen eingesetzt

(Reproduzierbarkeit von Programmläufen, ...)

Jeder Generierungsalgorithmus erzeugt eine endliche Sequenz von ZZs

Anforderungen

1. Generierte ZZs müssen gleichverteilt sein
2. Generierte ZZs müssen unabhängig sein
   (d.h. Kenntnis von n ZZs darf keine zusätzliche Information über die n+1te ZZ liefern, ohne dass der Generierungsalgorithmus bekannt ist)
3. die Sequenzlänge bis zur Wiederholung muss groß sein
4. die Erzeugung muss effizient sein
5. der Algorithmus muss portabel sein

Unterschiedliche Klassen von Generatoren existieren, wir betrachten nur die am weitesten verbreitete Klasse!

Ein erster Versuch: Midsquare Methode (von Neumann 1940)

1. Wähle eine vierstellige Zahl
2. Quadriere diese
   ($\Rightarrow$ achtstellige Zahl, u.U. von Links mit 0 auffüllen)
3. Wähle die mittleren vier Stellen als Nachkommastellen einer ZZ und fahre mit der Zahl bei 1. fort

Beispiel:

7182	$\rightarrow$	51581124	ZZ: 0.5811
5811	$\rightarrow$	33767721	ZZ: 0.7677
7677	$\rightarrow$	58936329	ZZ: 0.9363
9363	$\rightarrow$	87665769	ZZ: 0.6657
6657	$\rightarrow$	44315649	ZZ: 0.3156

usw.

Generierte Zufallszahlen sind sehr schlecht!

Lineare Kongruenzgeneratoren (Lehmer 1951)

Eine Funktion $x_i = \left(\sum_{j=1}^{r} a_j \cdot x_{i-j} + c\right) (\mathrm{mod}\, m)$

mit $x_0, x_1, \cdots, x_{r-1}, a_1, \cdots, a_r, c \in \mathbb{N}$

heißt linearer Kongruenzgenerator (LCG)

Heute meist verwendet $x_i = (a \cdot x_{i-1} + c) (\mathrm{mod}\, m)$

Falls c=0 multiplikativer Generator, sonst gemischter Generator!

x_0 ist die Saat des Generators

Eigenschaften:

- $x_i \in [0,m)$ falls c>0 und $x_i \in (0,m)$ falls c=0 (notwendigerweise)
- $x_i = x_j \Rightarrow x_{i+k} = x_{j+k}$ für alle k≥0 (Generator beginnt von vorn)
- $\kappa = \min_{|i-j|} (x_i = x_j)$ heißt die Periode des LCGs

Ein einfaches Beispiel:

a=5, c=0 und m=17 also $x_{i+1} = (5x_i)(\text{mod } 17)$ mit Saat $x_0=5$

i	0	1	2	3	4	5	6	7	8
$5x_i$	25	40	30	65	70	10	50	80	60
x_{i+1}	8	6	13	14	2	10	16	12	9
i	9	10	11	12	13	14	15	16	
$5x_i$	45	55	20	15	75	35	5	25	
x_{i+1}	11	4	3	15	7	1	5	8	

Maximale Periode 1,...,16 wird erreicht!

Beispiele für (einige ältere) Generatoren:

- Unix $m=2^{32}$, $a=1103515245$, $c=12345$
- RANDU $m=2^{31}$, $a=65539$
- Simula/Univac $m=2^{31}$, $a=5^{13}$
- SIMPL-I (IBM) $m=2^{31}-1$, $a=48271$
- SIMSCRIPT II.5 $m=2^{31}-1$, $a=630360016$
- L'Ecuyer $m= 2^{63}-25$, $a=4645906587823291368$

schlechte LCGs!

Anforderungen an einen guten LCG:

1. große Periode (großes m)
2. effiziente Berechnung
3. generierte ZZs bestehen statistische Tests

Große Periode eines LCG $\Rightarrow$ möglichst m oder m-1 Werte!

Ein gemischter LCG hat genau dann volle Periodenlänge, wenn:

1. ggT(m,c) = 1 (c und m sind relativ prim)
2. a mod p_i = 1 für alle Primfaktoren p_i von m
3. a mod 4 = 1 falls 4 Faktor von m ist

Ein multiplikativer LCG hat genau dann volle Periodenlänge, wenn

1. Falls $m = 2^b$, dann ist der maximale Wert für $\kappa = m/4 = 2^{b-2}$, wird erreicht für ungerade Saaten und a = 3 + 8k oder a = 5 + 8k mit
   k = 0,1 , …
2. Falls m eine Primzahl ist, dann wird κ = m-1 erreicht, falls die kleinste Zahl k, für die a^k-1 durch m ganzzahlig dividiert werden kann, gleich m-1 ist
   (d.h. a ist Primitivwurzel von m)

Effizienz der Generierung

Division ist aufwändig ⇒ Effizienz erfordert wenige/keine Divisionen!

Falls $m=2^e$, kann mod durch „Weglassen“ von Stellen realisiert werden! (shiften auf Bitebene)

Beispiel: $10111011 \bmod 2^6 = 00111011$

in Dezimaldarstellung $187 \bmod 64 = 59$

Aber $m=2^e$ bedingt Zyklen der niederwertigen Bits (schlechte ZZs!)
Beispiel: $x_{i+1} = (5x_i + 1) \bmod 16$

i	0	1	2	3	4	5	6	7
x_i	1	6	15	12	13	2	11	8
b_0	1	0	1	0	1	0	1	0
b_1b_0	01	10	11	00	01	10	11	00
$b_2b_1b_0$	001	110	111	100	101	010	011	000

Alternative: Wähle $m = 2^e - 1$

Effiziente Berechnung ohne Division:

Gesucht $z = (a \cdot x) \pmod{2^e - 1}$

Sei $y = (a \cdot x) \pmod{2^e}$ (effizient berechenbar)

Es gilt:

$$z = \begin{cases} y + k & \text{falls } y + k < 2^e - 1 \\ y + k - (2^e - 1) & \text{sonst} \end{cases}$$

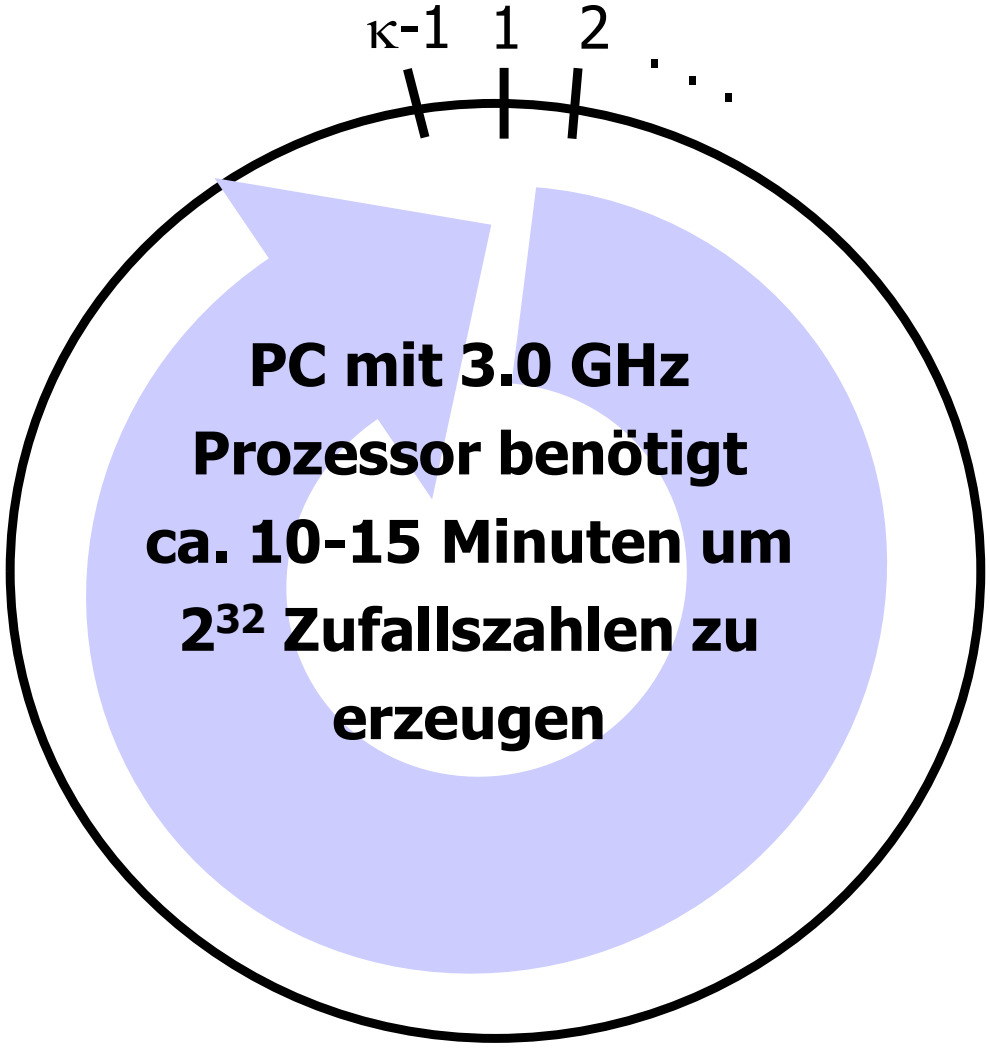
mit $k = \lfloor a \cdot x / 2^e \rfloor$

Ähnlich effizient, aber mit besseren Eigenschaften als 2^e!

Wie groß sollte/muss m heute sein?

Periode vieler heutiger Generatoren $\kappa \approx 2^{31}\text{-}2^{32}$

$$\left(\prod_{i=1}^{k}(m_i - 1)\right) \Big/ 2^{k-1}$$



Vergrößerung der Periode z.B. durch Kombination von Generatoren:

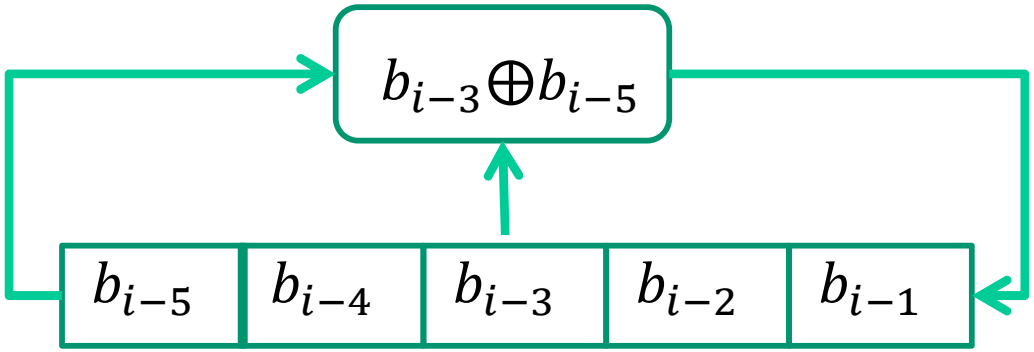
- k Generatoren mit Periode und Modul m_j für den j-ten Generator
- sei $x_{i,j}$ i-ter Wert des j-ten Generators
- $x_i = \left(\sum_{j=1}^{k}(-1)^{j-1}x_{i,j}\right)(\mathrm{mod}\ m_1 - 1)$

  ist $[0, m_1\text{-}2]$-gleichverteilt
- maximal erreichbare Periode

$$\left(\prod_{i=1}^{k}(m_i - 1)\right) \Big/ 2^{k-1}$$

Linear feedback shift Register (LFSR) Generatoren

- $W = b_1 b_2 \ldots b_L$ Binärdarstellung einer natürlichen Zahl (Länge L)
- $W_1, W_2, \ldots$ ist eine Sequenz solcher Zahlen, die als eine Bitsequenz aufgefasst werden
- Die i-te Binärstelle entsteht aus der (i-q)-ten und (i-r)-ten Binärstelle $(1 \leq r < q < i)$ durch $b_i = (b_{i-r} + b_{i-q}) mod\ 2 = b_{i-r} \oplus b_{i-q}$
  Realisierung für r=3, q=5 in einem shift Register



Rekurrenz
$W_i = W_{i-r} \oplus W_{i-q}$

- Statistische Eigenschaften der Basisvariante nicht gut, deshalb Erweiterung
  $Y_i = Y_{i-r} \oplus AY_{i-q}$ wobei Y_j Vektoren der Länge L und A $L \times L$ Matrix

Aktueller Generator: Mersenne-Twister Generator

Erste Publikation 1998, seitdem kontinuierlich weiterentwickelt, heute MT19937

Generierung auf Basis so genannter Matrixrekurrenzen

Relativ komplexe Generierungsvorschrift, die allerdings auf XOR und shift-Operationen basiert und dadurch effizient ist (vergleichbar mit LCGs mit großem m)

Eigenschaften:

- Periodenlänge $2^{19937}-1 \approx 10^{6000}$
- Gleichverteilung in 623 Dimensionen
- Besteht viele statistische Tests
- aber es wurden auch Schwächen entdeckt

Rekurrenz $x_{k+n} = x_{k+m} \oplus (x_k^{u} \mid x_{k+1}^{l})A \quad (k=0,1,\ldots)$

Code für den Mersenne-Twister Generator

Step 0. $\mathbf{u} \leftarrow \underbrace{1\cdots1}_{w-r}\underbrace{0\cdots0}_{r}$;(bitmask for upper $w-r$ bits)

$\mathbf{ll} \leftarrow \underbrace{0\cdots0}_{w-r}\underbrace{1\cdots1}_{r}$;(bitmask for lower r bits)

$\mathbf{a} \leftarrow a_{w-1}a_{w-2}\cdots a_1 a_0$;(the last row of the matrix A)

Step 1. $i \leftarrow 0$

$\mathbf{x}[0], \mathbf{x}[1], \cdots, \mathbf{x}[n-1] \leftarrow$ "any non-zero initial values"

Step 2. $\mathbf{y} \leftarrow (\mathbf{x}[i]$ AND $\mathbf{u})$ OR $(\mathbf{x}[(i+1) \bmod n]$ AND $\mathbf{ll})$;(computing $(\mathbf{x}_i^u|\mathbf{x}_{i+1}^l)$)

Step 3. $\mathbf{x}[i] \leftarrow \mathbf{x}[(i+m) \bmod n]$ XOR $(\mathbf{y} >> 1)$

$$\text{XOR} \begin{cases} 0 & \text{if the least significant bit of } \mathbf{y} = 0 \\ \mathbf{a} & \text{if the least significant bit of } \mathbf{y} = 1 \end{cases}$$;(multiplying A)

Step 4. ;(calculate $\mathbf{x}[i]T$)

$\mathbf{y} \leftarrow \mathbf{x}[i]$

$\mathbf{y} \leftarrow \mathbf{y}$ XOR $(\mathbf{y} >> u)$;(shiftright $\mathbf{y}$ by u bits and add to $\mathbf{y}$)

$\mathbf{y} \leftarrow \mathbf{y}$ XOR $((\mathbf{y} << s)$ AND $\mathbf{b})$

$\mathbf{y} \leftarrow \mathbf{y}$ XOR $((\mathbf{y} << t)$ AND $\mathbf{c})$

$\mathbf{y} \leftarrow \mathbf{y}$ XOR $(\mathbf{y} >> l)$

output $\mathbf{y}$

Step 5. $i \leftarrow (i+1) \bmod n$

Step 6. Goto Step 2.

Weitere Anwendung für Pseudozufallszahlen:

- Schlüsselgenerierung in Verschlüsselungsalgorithmen
  Schlüssel müssen zufällig sein
  Pseudozufallszahlen müssen nicht reproduzierbar sein

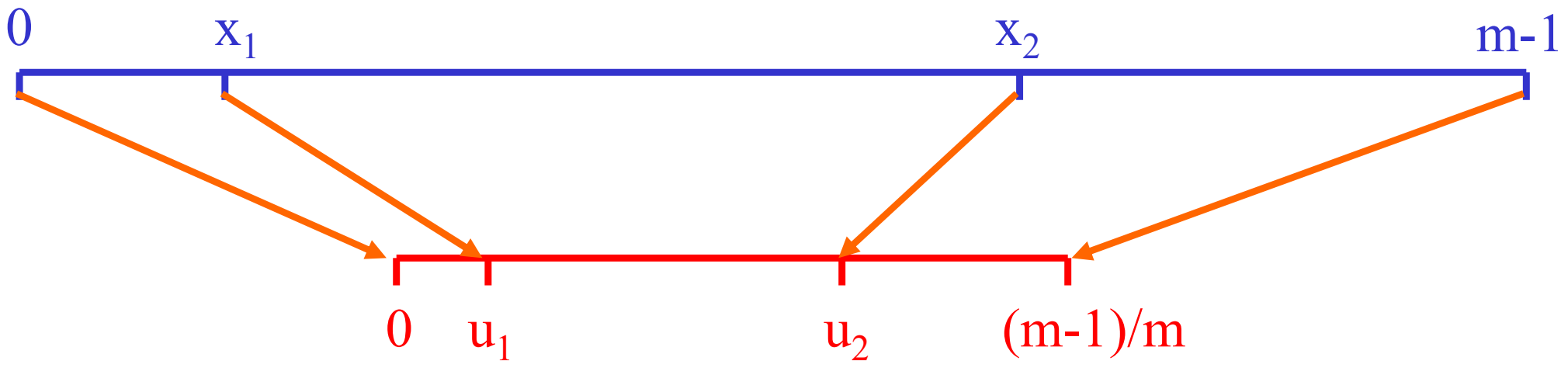
Notwendigkeit deterministische Algorithmen zur Generierung zu nutzen entfällt

Oft werden physikalische Phänomene genutzt

- LavaRand Bläschenbildung bei Lavalampen wird simuliert
- Weißes Rauschen
- Zeitverschiebung bei Hardware-Uhren

Für die Simulation auf Grund der fehlenden Reproduzierbarkeit nicht geeignet!

Generierung von [0,1)-gleichverteilten reellwertigen ZZs aus [0,m)-gleichverteilten ganzzahligen ZZs



Streng genommen werden nur diskrete Werte i/m aus [0,1) erzeugt

- aber die Werte liegen sehr dicht
  (bei Beachtung der Maschinendarstellung sogar optimal dicht)
- d.h. bei voller Periode sind alle im Intervall darstellbaren Zahlen enthalten

Testverfahren für Zufallszahlen

[0,1)-gleichverteilte ZZs sind die Basis für weitere (oft exakte) Transformationen
$\Rightarrow$ gute [0,1)-Gleichverteilung ist notwendig

Anforderungen an generierte ZZs:

- Sie müssen gleichverteilt in [0,1) sein
- Sie müssen von unabhängigen ZZs nicht unterscheidbar sein

Testverfahren dienen zur Bewertung dieser Eigenschaften

Man unterscheidet:

- Empirische Testverfahren
  Bewertung der ZZ auf Basis einer Stichprobe
- Theoretische Testverfahren
  Bewertung aller generierten ZZ (oft schwieriger)

Testen von Zufallszahlengeneratoren:

Grundsätzliches Vorgehen beim Testen:

Aufstellen einer Hypothese H_0. Hier z.B.

- mit Generator G erzeugte ZZs sind unabhängig, identisch [0,1)-gleichverteilt

  oder

- mit Generator G erzeugte ZZs sind nicht unabhängig, identisch [0,1)-gleichverteilt

H_0 heißt **Nullhypothese**, $H_1 = \neg H_0$ heißt **Alternativhypothese**

Testverfahren dienen dazu herauszufinden, ob H_0 gilt

Auf Grund statistischer Schwankungen von Stichproben, können falsche Folgerungen gezogen werden (Tests sind keine Beweise!)

Mögliche Fehler

(statistischer) Fehler der 1. Art (α Fehler): H_1 wird angenommen, obwohl H_0 gegeben (fälschliches Verwerfen der Nullhypothese)

(statistischer) Fehler der 2. Art (β Fehler): H_0 wird angenommen, obwohl H_1 gegeben (fälschliches Annehmen der Nullhypothese)

Impliziert ein bestimmter Test mit Wahrscheinlichkeit $\leq \alpha$ Fehler der
1. Art, so heißt er „Test zum (Signifikanz-)Niveau α“

unabhängig (!) von der Wahrscheinlichkeit eines Fehlers der 2. Art!

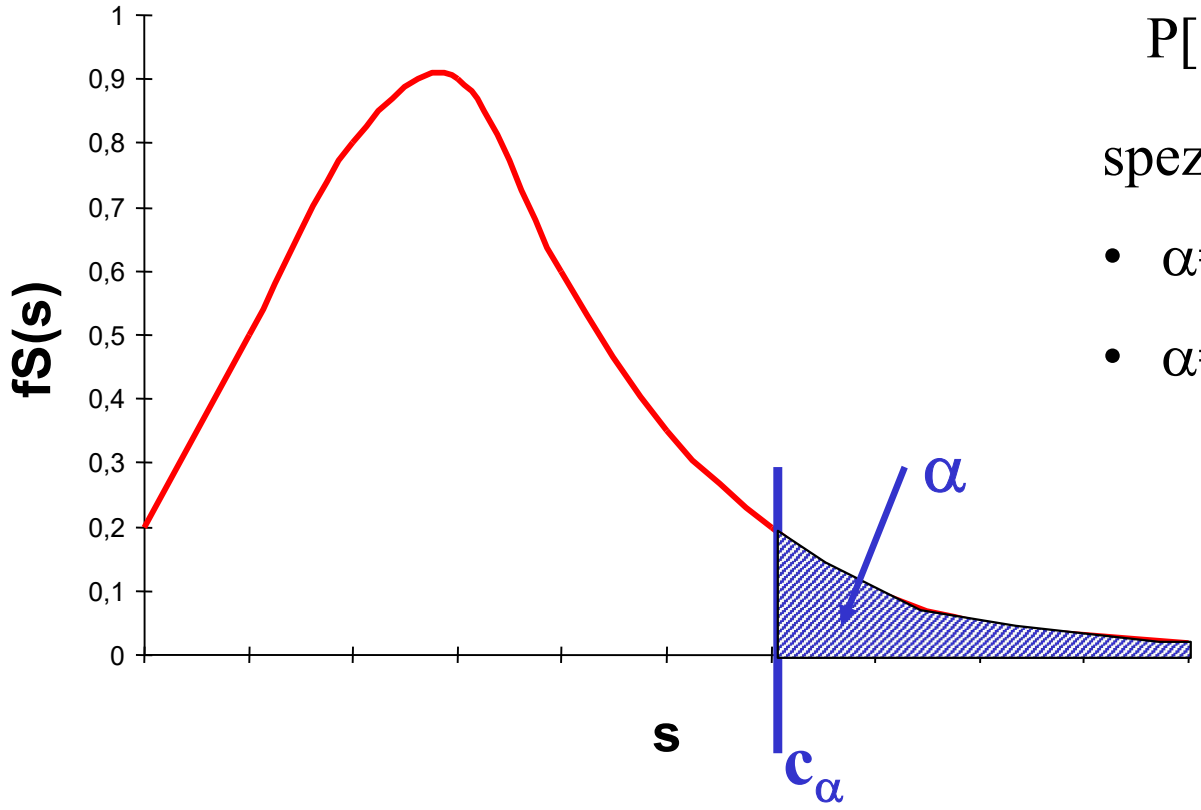
Vorgehen beim Testen auf Basis einer Stichprobe
(d.h. einer Realisierung der ZVs $Y_1, ..., Y_n$):

Teststatistik $S(Y_1, ..., Y_n)$ „bewertet“ die Stichprobe, je größer der Wert, desto unwahrscheinlicher H_0
(und implizit je wahrscheinlicher H_1)

Zur Anwendung erforderlich:

- Bestimme die Verteilung von S
  (unter der Voraussetzung, dass H_0 gilt)
- Ermittlung der kritischen Werte c_α (oder $c_{1-\alpha}$) ab denen H_0 zum Niveau α verworfen wird

Skizze des Prinzips



c_α so bestimmt, dass

$$P[S(Y_1,\ldots,Y_n)>c_\alpha|H_0] = \alpha$$

spezielle α-Werte:

- α=0.05 signifikant
- α=0.01 hochsignifikant

Verteilung sagt nichts über den Fehler 2. Art aus

Testverfahren können schlechte Generatoren identifizieren, nicht aber die generelle Güte eines Generators nachweisen!

Runs Test

Paare aufeinander folgender ZZs werden in Klassen unterteilt:

- Ein Paar fällt in Klasse +, wenn der erste Wert kleiner als der zweite ist
- Ansonsten fällt das Paar in Klasse –

Ein run ist eine Folge identischer Zeichen + oder –

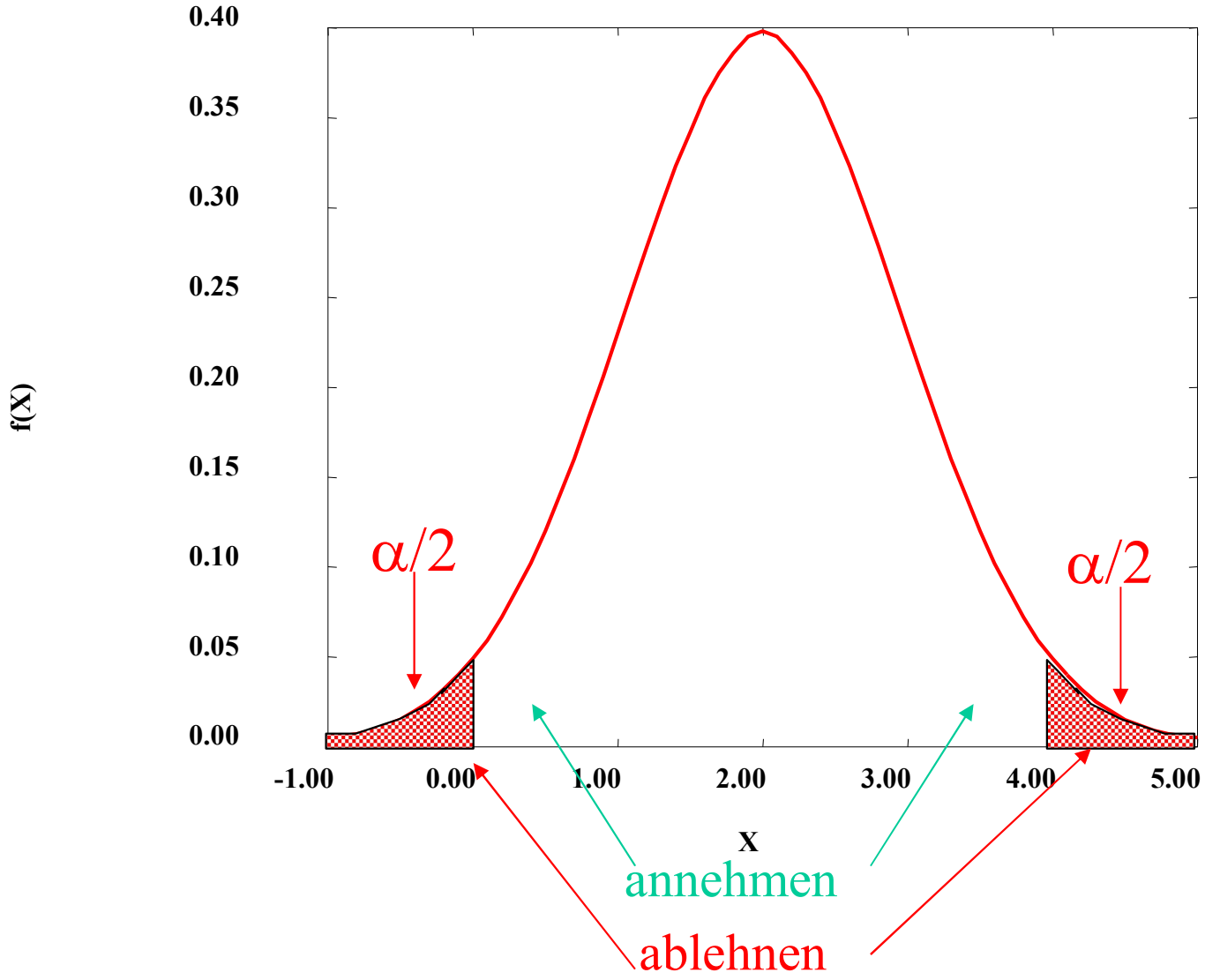
Sei R_n die Anzahl der runs, n die Größe der Stichprobe, dann ist

die Anzahl der runs für große n normalverteilt mit

- Erwartungswert $E(R) = (2n - 1)/3$
- Varianz $\sigma^2(R) = (16n – 29)/90$

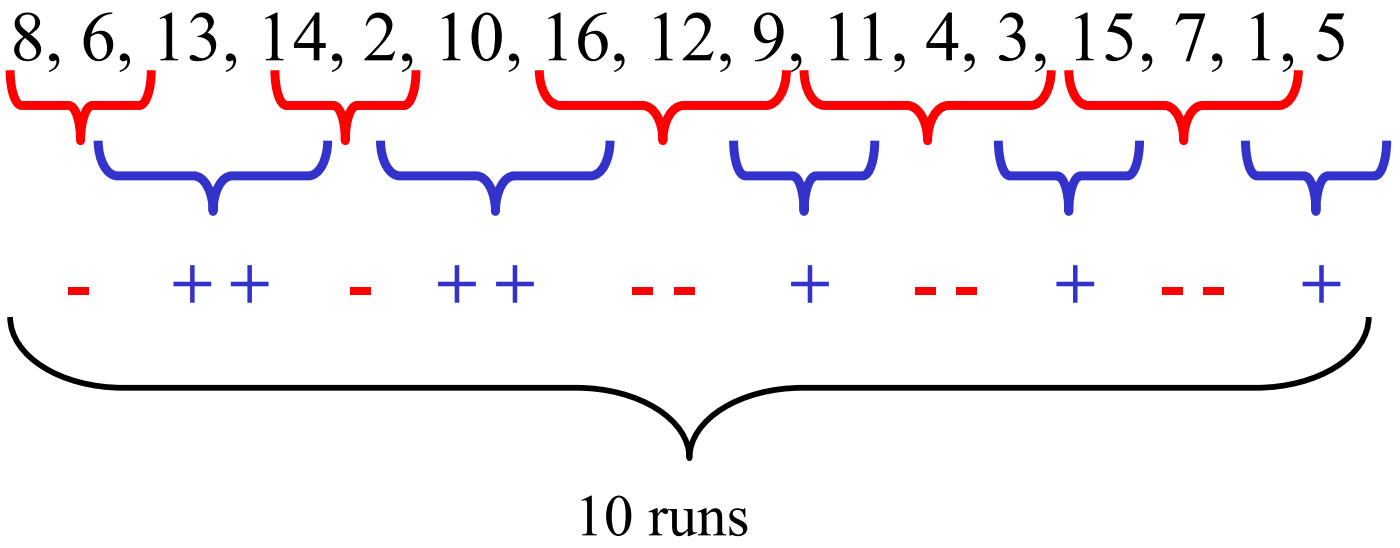
Auf Basis der kritischen Werte der Normalverteilung kann ein statistischer Test durchgeführt werden und damit die Hypothese „unabhängige [0,1)-verteilte ZZs“ abgelehnt oder angenommen werden

Skizze des Prinzips



Beispiel $x_{i+1} = (5 \cdot x_i) \pmod{17}$

Generierte ZZs für x_0=5:



Laut Theorie: $E(R_{16}) = (2 \cdot 16 - 1)/3 = 10.333$
(Gute Übereinstimmung)

Für α=0.05 würde die Hypothese unabhängig [0,1)-verteilt (H_0)
für 8 bis 13 runs akzeptiert!

Verschiedene ähnliche Tests existieren
(zum Teil auch unter dem Namen runs-Test)

Test der Autokorrelation

Seien $X_1, ..., X_n$ ZVs mit Erwartungswert μ und Varianz σ^2

Der Autokorrelationskoeffizient der Ordnung s $\rho(s)$ ist definiert als

$$\rho(s) = \frac{\sum_{i=1}^{n-s}(X_{i+s} - \mu)(X_i - \mu)}{\sum_{i=0}^{n-s}(X_i - \mu)^2} = \frac{C(X_i, X_{i+s})}{\sigma^2(X)} = \frac{C_s}{C_0}$$

Es gilt:

- $-1 \leq \rho(s) \leq 1$
- falls X_i und X_{i+s} unabhängig, so gilt $\rho(s) = 0$

Für [0,1)-verteilte ZV X gilt ferner

- $E(X) = 1/2$ und $\sigma^2(X) = C_0 = 1/12$,

Da $C_s = E(X_iX_{i+s}) - E(X_i)E(X_{i+s})$ gilt in diesem Fall auch

$$\rho(s) = \frac{E(X_iX_{i+s}) - E(X_i)E(X_{i+s})}{\sigma^2(X)} = \frac{E(X_iX_{i+s}) - {}^1/_4}{{}^1/_{12}} = 12E(X_iX_{i+s}) - 3$$

Ein Schätzer für ρ(s) lautet:

$$\tilde{\rho}(s) = \frac{12}{h+1}\sum_{k=0}^{h}\left(X_{1+ks}X_{1+(k+1)s}\right) - 3 \;\; mit\; h = \left\lfloor\frac{n-1}{s}\right\rfloor - 1$$

Einsetzen der konkreten Werte x_i statt der Zufallsvariablen X_i liefert den konkreten Schätzwert $\hat{\rho}(s)$.

Für unabhängige [0,1)-verteilte X_i ist $\tilde{\rho}(s)$ normalverteilt mit Erwartungswert 0 und Standardabweichung $\sqrt{13h+7}/_{h+1}$

Testverfahren untersuchen, ob $\rho(s) \approx 0$ gilt ($H_0: \rho(s) = 0$), indem

$$z = \frac{\hat{\rho}(s)\cdot(h+1)}{\sqrt{13h+7}}$$

gegen die kritischen Werte einer N(0,1)-Verteilung getestet wird

Theoretische Testverfahren

Erkennung der Struktur der generierten Sequenzen von ZZs:

Sei x_1, x_2, ... die Sequenz der erzeugten ZZs

Überlappende d-Tupel $(x_1,...,x_d)$, $(x_2,...,x_{d+1})$, ... definieren jeweils Punkte im d-dimensionalen Hyperraum

Beobachtung: Punkte fallen auf „relativ wenige“ Hyperebenen der Dimension d-1

Im zweidimensionalen Fall liegen die Punkte auf einem Gitter

Punkte außerhalb des Gitters sind nicht erreichbar

Anzahl der Gitterlinien bestimmt die Qualität des Generators

Verfahren wie der Spektraltest oder Gittertest bestimmen die Abdeckung des Hyperraums durch den Generator!

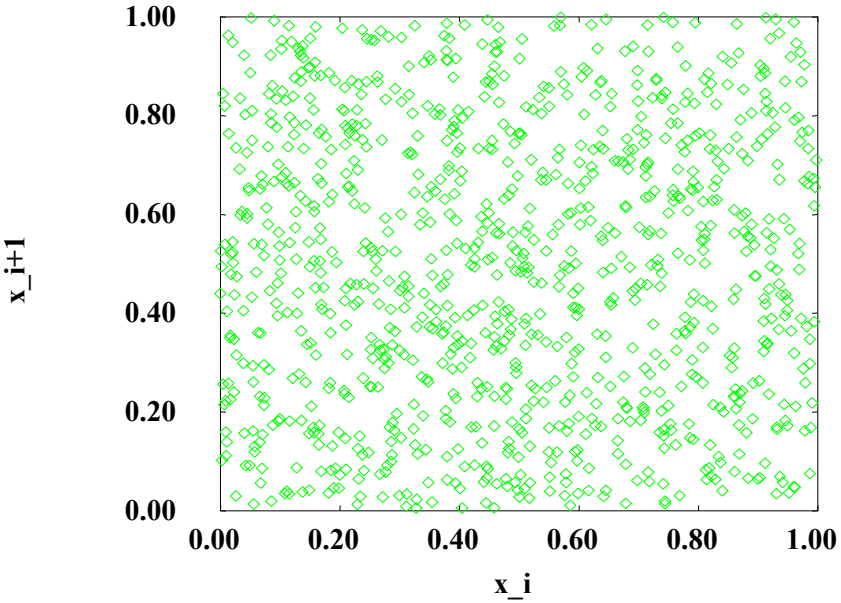
Visuelle Darstellung durch überlappende Tupel ..., (x_i, x_{i+1}), (x_{i+1}, x_{i+2}), ...

oder Tripel ..., (x_i, x_{i+1}, x_{i+2}), $(x_{i+1}, x_{i+2}, x_{i+3})$, ...

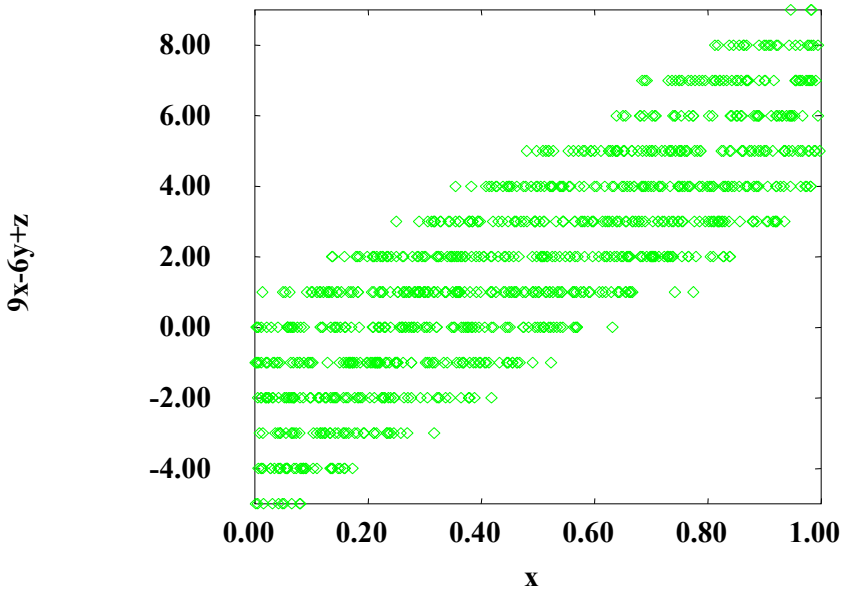
Beispiel für einen schlechten Generator RANDU

$$(x_{i+1} = 65539 \cdot x_i)(\mathrm{mod}\ 2^{31})$$

Darstellung für Tupel



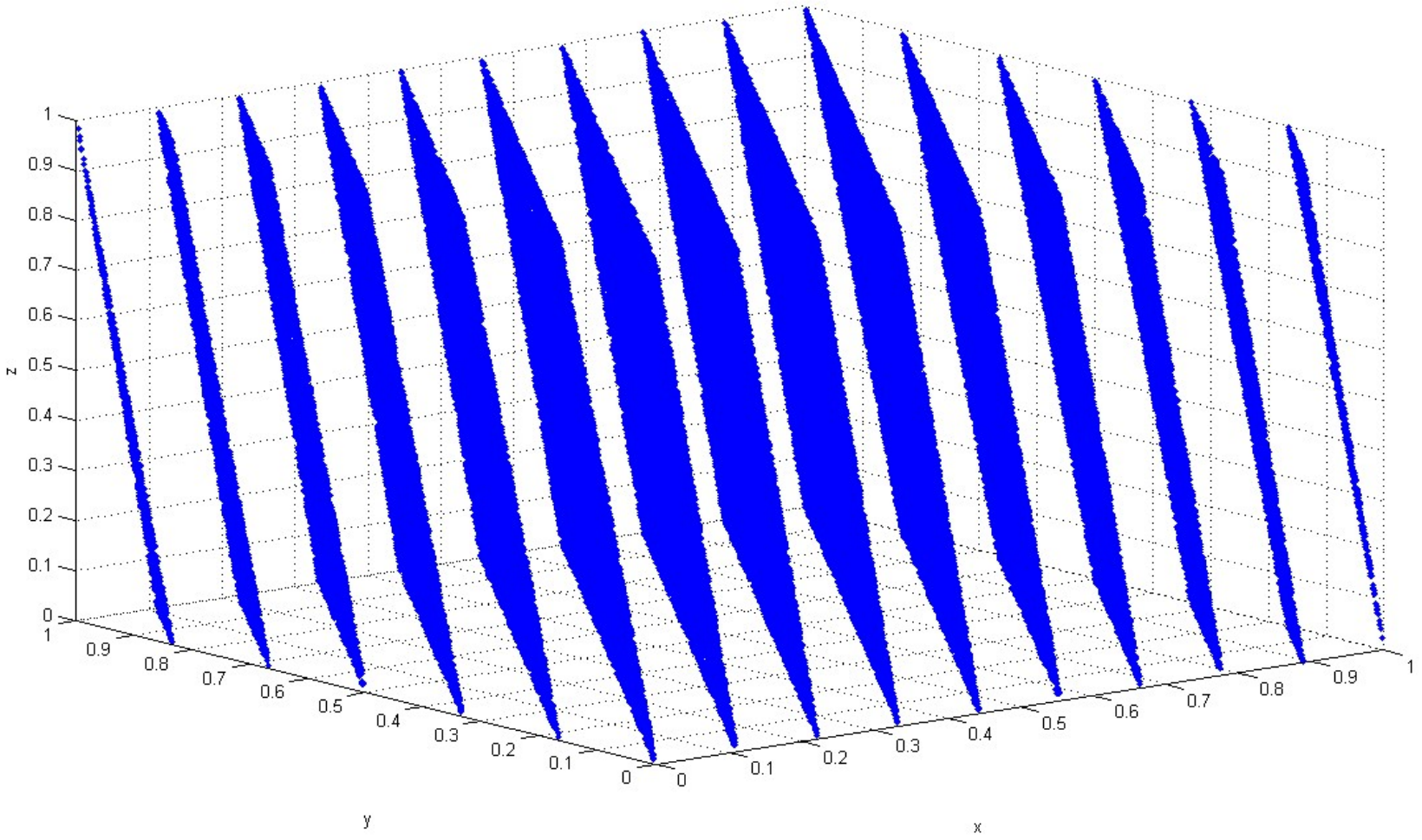
Darstellung von Tripeln (x,y,z) als 9x-6y+z



Alle Werte liegen auf einer von 15 Hyperebenen, die durch die Gleichung 9x-6y+z gegeben sind

Bei einem guten Generator würden die Werte in einem Band um die Diagonale verteilt liegen!

Dreidimensional Darstellung der ZZ aus dem Generator RANDU

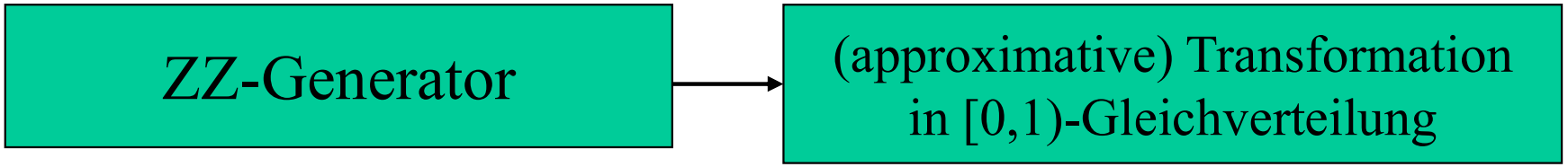


Aussagen zu Testverfahren und der Qualität von Generatoren:

- Es existiert eine Vielzahl von Testverfahren, aber es ist unklar, welcher Test das beste Ergebnis liefert
- Test können keine beweisbar guten Zufallsgeneratoren liefern, sondern nur schlechte aussondern
- Einige Generatoren wurden aufwändig getestet und haben sich bzgl. dieser Tests als „gut“ erwiesen. Möglichst diese Generatoren in der Simulation verwenden.
- Durch Nutzung mehrerer unterschiedlicher Generatoren, können Verzerrungen durch einzelne Generatoren aufgedeckt werden.

Generierung von Zufallszahlen der gewünschten Verteilung

Bisherige Schritte



Also $$FU(u) = \begin{cases} 0 & \text{falls } u < 0 \\ u & \text{falls } 0 \le u < 1 \\ 1 & \text{falls } u \ge 1 \end{cases} \qquad fU(u) = \begin{cases} 1 & \text{falls } 0 \le u < 1 \\ 0 & \text{sonst} \end{cases}$$

Benötigt werden aber ZZs mit Verteilungsfunktion FX(x)

$\Rightarrow$ Transformation der [0,1)-gleichverteilten ZZs u_i in ZZs x_i, die nach $F_X(x)$ verteilt sind

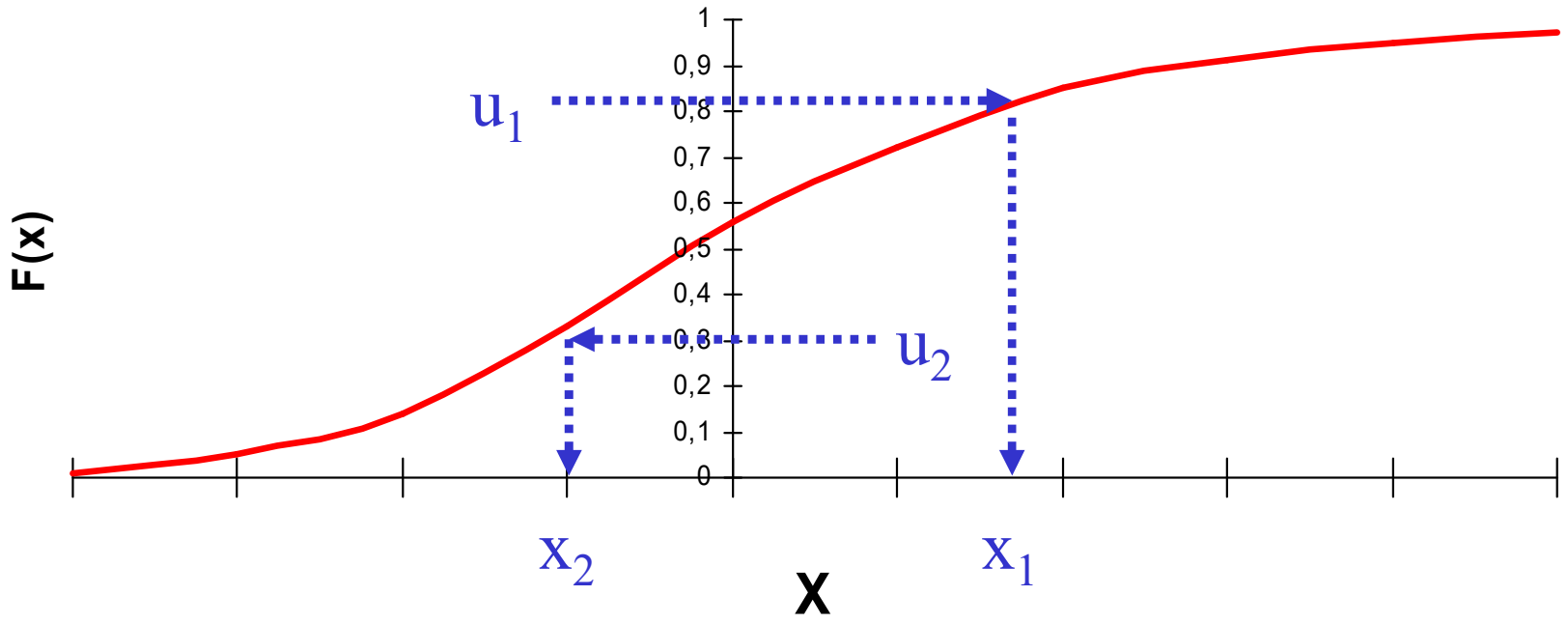
Wir beginnen mit kontinuierlichen Verteilungen, so dass für

$x_1<x_2$ mit $0 < F(x_1) \leq F(x_2) \leq 1$ auch $F(x_1) < F(x_2)$ gelte

Damit existiert die Umkehrfunktion F^{-1} von F

Naheliegendes Vorgehen (**Inverse Transformation**):

1. Generiere u aus [0,1)-Gleichverteilung
2. Transformiere $x = F^{-1}(u)$



Formal gilt: $P[X \leq x] = P[F^{-1}(U) \leq x] = P[U \leq F(x)] = F(x)$

Beispiel: Exponentialverteilung

Für $x \geq 0$: $F(x) = 1 - e^{-\lambda x}$ Sei u ZZ aus (0,1)-Gleichverteilung

Transformationsschritte:

$$1 - e^{-\lambda x} = u \Rightarrow e^{-\lambda x} = 1 - u \Rightarrow -\lambda x = \ln(1-u) \Rightarrow x = (\ln(1-u))/-\lambda$$

Da 1-u ebenfalls (0,1)-gleichverteilt, kann es durch u ersetzt werden!

Erzeugung exponentiell vert. ZZs:

1. Generiere u aus (0,1)-Gleichverteilung
2. Transformiere $x = \ln(u)/(-\lambda)$

Funktioniert dies für alle kontinuierlichen Verteilungen?

Nein, $F^{-1}(x)$ muss in geschlossener Form vorliegen oder einfach berechenbar sein! (gleich mehr dazu)

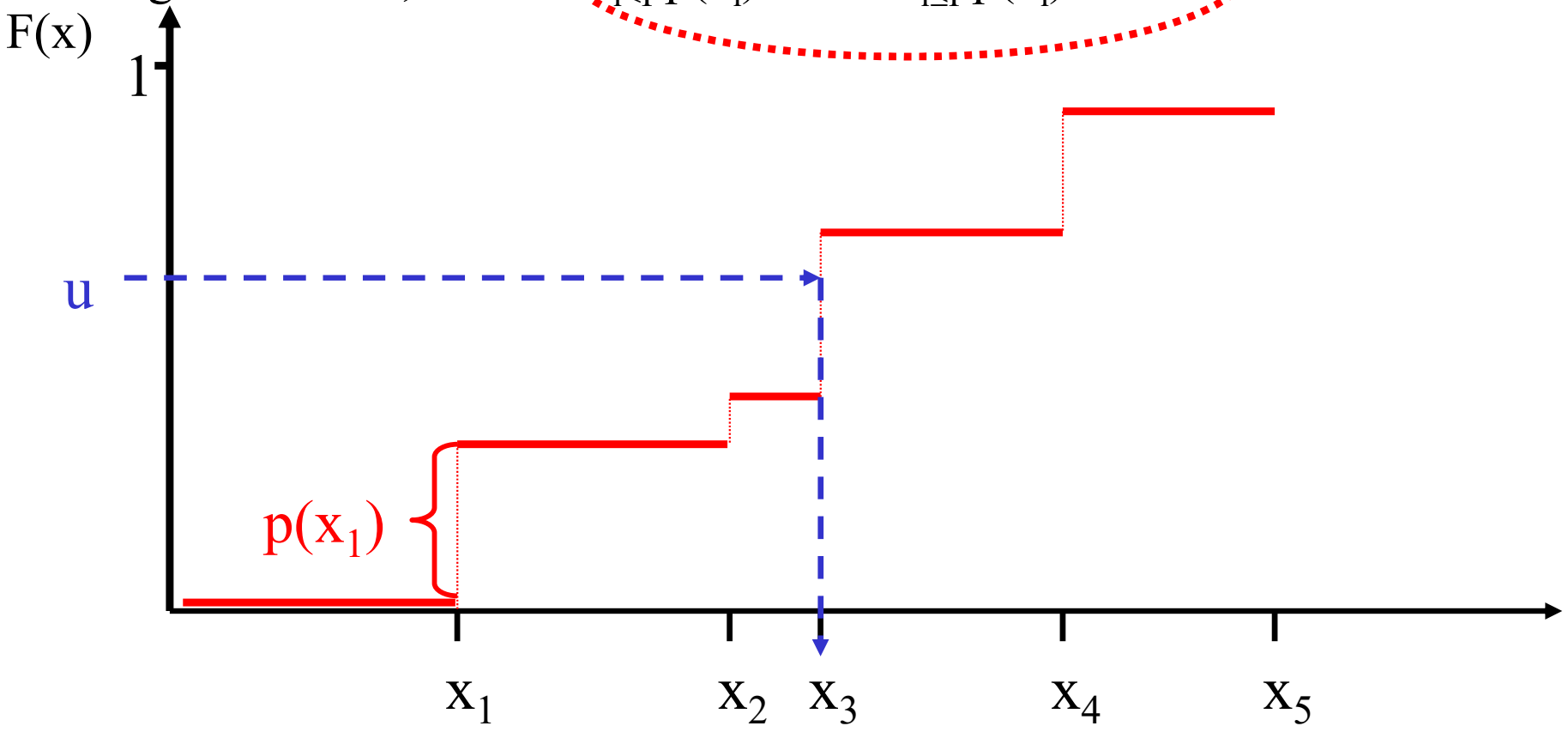
Inverse Transformation für diskrete Verteilungen

Es gilt $F(x) = P(X \leq x) = \Sigma_{x_i \leq x} p(x_i)$

Datenstrukturen zum effizienten Suchen verwenden

Generiere u aus [0,1)-Gleichverteilung

Finde ganze Zahl I, so dass $\Sigma_{i<I} p(x_i) < u \leq \Sigma_{i \leq I} p(x_i)$



Konvolutionsverfahren

Falls ZV X als Summe von ZVs X_i (i=1,...I) mit Vfkt. $F_i(x)$ darstellbar ist und Generatoren für die X_i existieren, so können Realisierungen von X wie folgt generiert werden:

```
x = 0 ;
for i=1 to I do
        ziehe ZZ y aus F_i(y) ;
        x = x + y ;
end for
return (x) ;
```

Beispiel: Erlang-Verteilung

Kompositionsverfahren

Falls ZV X eine Vfkt F(x) hat, die sich wie folgt darstellen lässt

$F(x) = \Sigma_{i \le I} \, p_i \cdot F_i(x)$

und Generatoren existieren, die Realisierungen X_i aus $F_i(x)$ erzeugen, so können Realisierungen von X wie folgt generiert werden:

```
generiere i gemäß Verteilung p_i ;
ziehe ZZ x aus F_i(x) ;
return(x) ;
```

Beispiel: Hyperexponentialvert.

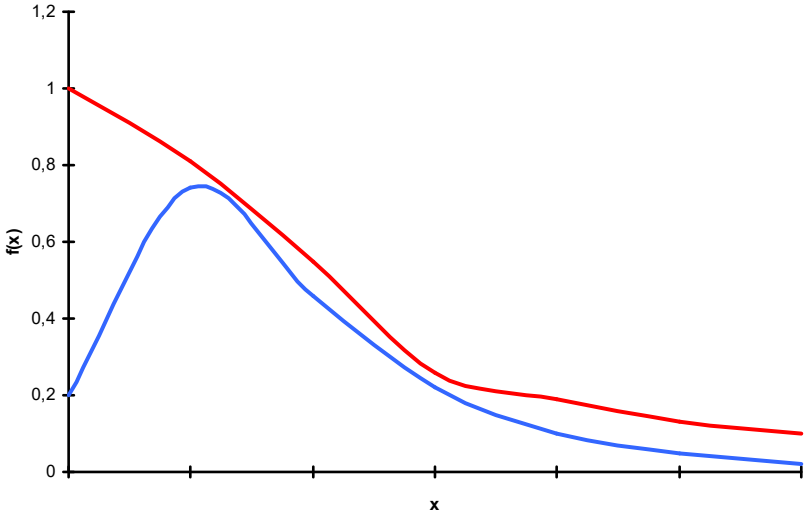
Verwerfungsmethode

Anwendbar für diskrete und kontinuierliche Verteilungen, wir betrachten den kontinuierlichen Fall!

Ges: Realisierungen ZV X mit bekannter Dfkt. $f_X(x)$

Voraussetzung: Generator für ZV Y mit Dfkt. $f_Y(x)$ bekannt und es existiert $\alpha \in (1,\infty)$ so dass für alle x gilt $f_X(x) \leq \alpha \cdot f_Y(x)$

Skizze:



Generierungsmethode:

repeat

  ziehe ZZ y gemäß $f_Y(x)$;

  ziehe ZZ x aus $[0,\alpha \cdot f_Y(y))$-Gleichv.;

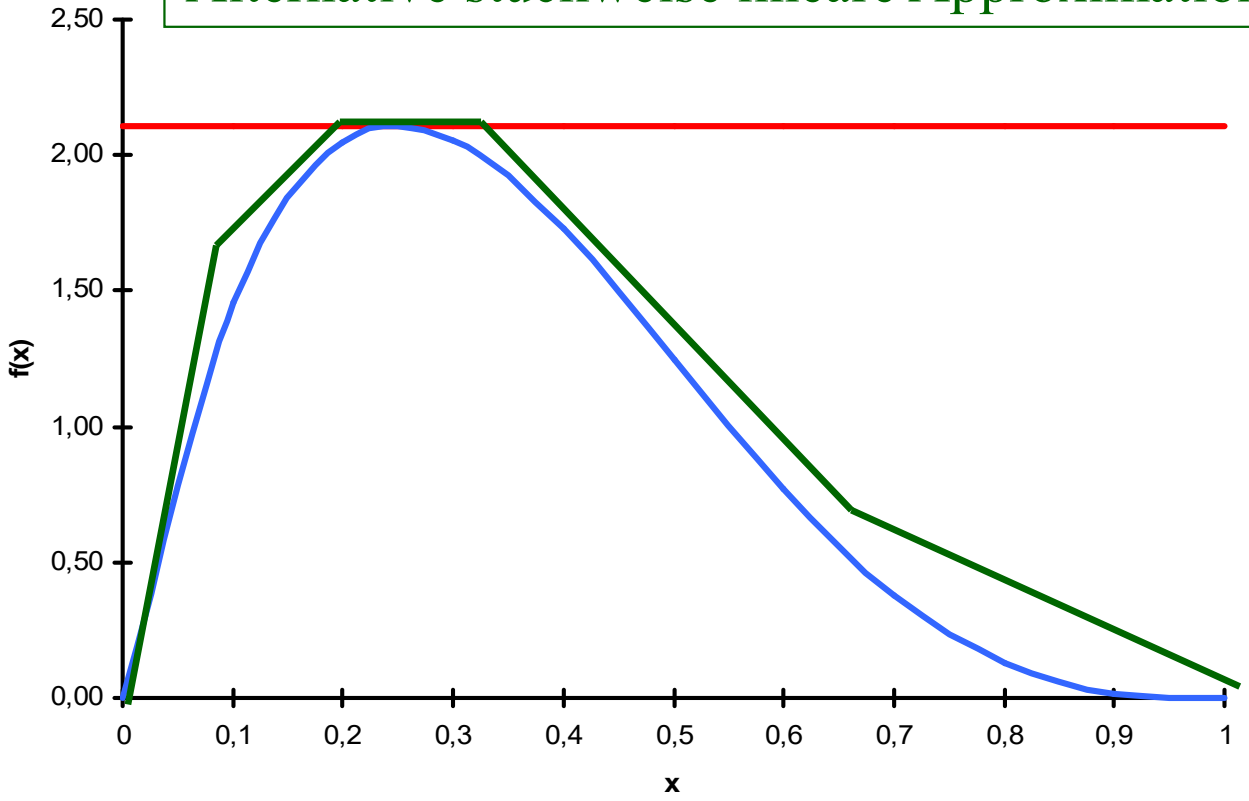
until $x \leq f_X(y)$;

return(y) ;

Beispiel: $\beta(2,4)$-Vert. mit $f(x) = 20 \cdot x \cdot (1-x)^3$ falls $0 \le x \le 1$ und 0 sonst

Dichtefunktion wird beschränkt durch Rechteck der Höhe 2.11

Alternative stückweise lineare Approximation



Generierungsmethode:

repeat
  ziehe y aus [0,1)-Gl.Vert. ;
  ziehe x aus [0,2.11)-Gl.Vert.;
until $x \le 20 \cdot y \cdot (1-y)^3$;

Effizienz der Methode hängt ab von

1. der W., dass eine ZZ akzeptiert wird $1 - \int(\alpha \cdot f_Y(x) - f_x(x))dx/\alpha$
2. der Effizienz der Generierung von ZZs mit Dfkt. $f_Y(x)$

Generierung von normalverteilten ZZs

Sei X eine N(0,1)-verteilte ZV, dann ist

$$Y = \mu + \sigma \cdot X \text{ eine } N(\mu,\sigma^2)\text{-verteilte ZV}$$

Methode zur Generierung von N(0,1)-verteilten ZZ ist ausreichend!

Verteilungsfunktion und auch inverse Verteilungsfunktion der Normalverteilung haben keine geschlossene Darstellung

$\Rightarrow$ inverse Transformation nicht einsetzbar!

Konvolution

(nach dem zentralen Grenzwertsatz!)

$$x = \frac{\left(\sum_{i=1}^{n} u_i\right) - n/2}{\sqrt{n/12}} \qquad \text{(oft n=12)}$$

u_i aus [0,1)-Gleichverteilung

$\Rightarrow$ x ist approx. aus N(0,1)

Methode von Box-Muller (1958)

$$x_1 = \cos(2\pi u_1)\sqrt{-2\ln(u_2)}$$

$$x_2 = \sin(2\pi u_1)\sqrt{-2\ln(u_2)}$$

u_i aus [0,1)-Gleichverteilung

$\Rightarrow x_i$ aus N(0,1)

Weitere Methoden existieren !!

Generierung von abhängigen Zufallsvariablen

Viele Parameter sind in der Realität korreliert, z.B.:

- Größe und Gewicht von Menschen
- Temperatur und Regenmenge
- Ein-/Ausgabeoperationen und CPU-Zeitbedarf

Dadurch bedingte Probleme:

- Verwendung unabhängiger Zufallsvariablen verfälscht Verhalten
- mehrdimensionale Verteilung muss spezifiziert werden
  - Abhängigkeiten sind schwer zu schätzen
  - in allgemeiner Form nicht kompakt darstellbar

Formale Darstellung als Zufallsvektor $(X_1,X_2,...,X_d)$ mit Verteilungsfunktion

$F_{X_1,X_2,...,X_d}(x_1,x_2,...,x_d)$

Alternativ: Darstellung als bedingte Verteilung mit $F_i(x_i \mid x_1,...,x_{i-1})$

- falls bedingte Verteilungen bekannt, dann Generierung einfach
- i.d.R. ist diese detaillierte Information aber kaum ermittelbar

Beispiel bivariate Normalverteilung

X_1 und X_2 sind korrelierte normalverteilte ZVs

- mit Erwartungswert μ_i und Standardabweichung σ_i
- und Korrelation $\rho = COV(X_1,X_2) / (\sigma_1\sigma_2)$

Erzeugung der ZZs:

1. Erzeuge z_1 und z_2 als unabhängige N(0,1) verteilte ZZs (z.B. mit der Box-Muller-Methode)
2. $x_1 = \mu_1 + \sigma_1 z_1$
3. $x_2 = \mu_2 + \sigma_2 \left(\rho z_1 + \sqrt{1-\rho^2} z_2\right)$

- Generalisierung auf multivariate Normalverteilungen möglich
- für andere Verteilungen sind andere Methoden notwendig
- oft verwendet stochastische Prozesse (MA-,AR-Modelle) etc.