Zufallszahlen in Testbetten und Simulationen

Phillip Berndt

Institut für Informatik – FU Berlin

Zufall

Wofür brauchen wir Zufallszahlen?

Zufall

Wofür brauchen wir Zufallszahlen?

- Simulation von Dingen, die wir nicht genau beschreiben wollen

Zufall

Wofür brauchen wir Zufallszahlen?

- Simulation von Dingen, die wir nicht genau beschreiben wollen
- Simulation von Dingen, die wir nicht genau beschreiben können

Zufall

Beispiel

Wartezeit

Inhaltsverzeichnis

Wahrscheinlichkeitsmaß

Wie erfasst man Zufall mathematisch?

Wahrscheinlichkeitsmaß

Definition

Sei Ω die abzählbare Menge von möglichen Ergebnissen eines Experimentes. Eine Funktion

$$P : 2^{\Omega} \to [0, 1]$$
$$X \mapsto P(X)$$

heißt *Wahrscheinlichkeitsmaß*, wenn gilt:

1. $P(\Omega) = 1$
2. $A, B \in 2^{\Omega}, A \cap B = \emptyset \implies P(A \cup B) = P(A) + P(B)$

Der Übergang ins Kontinuierliche

- Statt ganz $\mathbb{R}$ betrachte kleine Intervalle

$$[x, x + \Delta x]$$

Der Übergang ins Kontinuierliche

- Statt ganz $\mathbb{R}$ betrachte kleine Intervalle

$$[x, x + \Delta x]$$

- Jetzt haben wir natürlich *abzählbar* viele Intervalle

Der Übergang ins Kontinuierliche

- Statt ganz $\mathbb{R}$ betrachte kleine Intervalle

$$[x, x + \Delta x]$$

- Jetzt haben wir natürlich *abzählbar* viele Intervalle
- Mit $\Delta x \to 0$ bekommen wir *infitesimale* Intervalle

$$[x, x + dx]$$

Der Übergang ins Kontinuierliche

- Wir nennen das Wahrscheinlichkeitsmaß nun auch *Dichtefunktion*.

Der Übergang ins Kontinuierliche

- Wir nennen das Wahrscheinlichkeitsmaß nun auch *Dichtefunktion*.
- Eine Punktweise Auswertung ergibt keinen Sinn mehr, da wir unechte Intervalle $[x, x + dx]$ haben

Der Übergang ins Kontinuierliche

- Wir nennen das Wahrscheinlichkeitsmaß nun auch *Dichtefunktion*.
- Eine Punktweise Auswertung ergibt keinen Sinn mehr, da wir unechte Intervalle $[x, x + dx]$ haben
- Stattdessen:

$$\int_a^b P([x, x + dx])dx = P([a, b])$$

Zufallsverteilungen

- Setze $b = -\infty$

Zufallsverteilungen

- Setze $b = -\infty$
- Dann ist

$$F(b) = \int_{-\infty}^{b} P([x, x + dx])dx$$

eine *Verteilungsfunktion*

Zufallsverteilungen

- Setze $b = -\infty$
- Dann ist

$$F(b) = \int_{-\infty}^{b} P([x, x + dx])dx$$

  eine *Verteilungsfunktion*
- Sie steigt monoton und es gilt

$$\lim_{b \to \infty} F(b) = 1$$

Zufallsverteilungen

- Setze $b = -\infty$
- Dann ist

$$F(b) = \int_{-\infty}^{b} P([x, x + dx])dx$$

  eine *Verteilungsfunktion*
- Sie steigt monoton und es gilt

$$\lim_{b \to \infty} F(b) = 1$$

- Sie gibt nun die Wahrscheinlichkeit für $x \leq b$ an

Gleichverteilung

- Falls $P(\{n\}) = c$ unabhängig von n haben wir eine *Gleichverteilung*

Gleichverteilung

- Falls $P(\{n\}) = c$ unabhängig von n haben wir eine *Gleichverteilung*
- Falls $P([x, x + dx]) = c$ unabhängig von x haben wir eine *Gleichverteilung*

Gleichverteilung

- Falls $P(\{n\}) = c$ unabhängig von n haben wir eine *Gleichverteilung*
- Falls $P([x, x + dx]) = c$ unabhängig von x haben wir eine *Gleichverteilung*
- Falls $f(x) = c$ unabhängig von x haben wir eine *Gleichverteilung*

Gleichverteilung

- Die Gleichverteilung kennen wir aus der Schule, z.B. von Würfeln

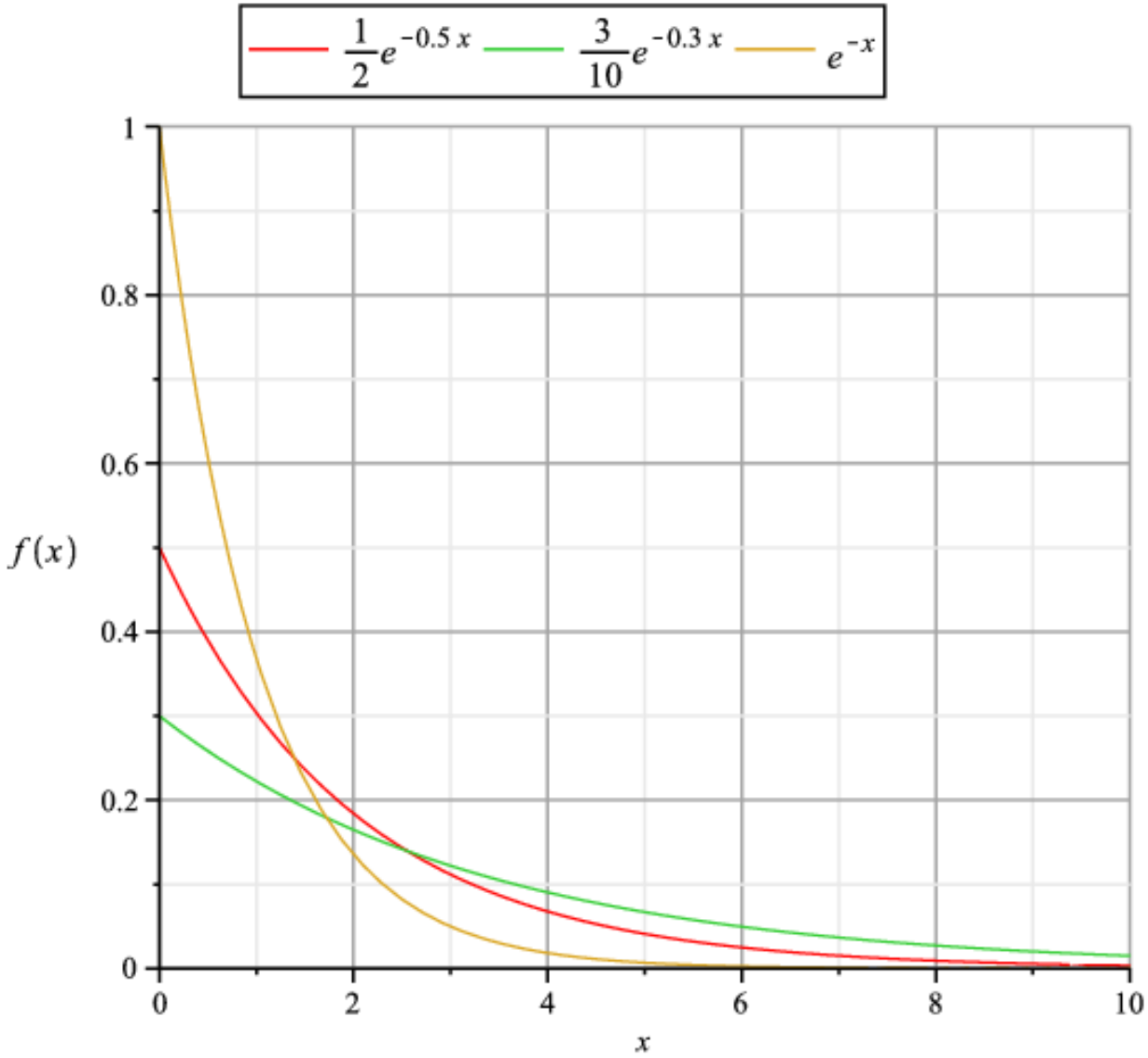
Gleichverteilung

- Die Gleichverteilung kennen wir aus der Schule, z.B. von Würfeln
- Wir können sie einfach simulieren!

Exponentialverteilung

- Die für uns interessante Verteilung ist die *Exponentialverteilung*

$$f_\lambda(x) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$


$\frac{1}{2}e^{-0.5\,x}$
$\frac{3}{10}e^{-0.3\,x}$
e^{-x}
1
0.8
0.6
0.4
0.2
0
$f(x)$
0
2
4
6
8
10
x

Exponentialverteilung

- Die für uns interessante Verteilung ist die *Exponentialverteilung*

$$f_\lambda(x) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

- Sie modelliert z.B. Lebensdauern und Zerfallsprozesse

Exponentialverteilung

- Die für uns interessante Verteilung ist die *Exponentialverteilung*

$$f_\lambda(x) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

- Sie modelliert z.B. Lebensdauern und Zerfallsprozesse
- Wir werden eine Möglichkeit sehen, sie zu simulieren!

Vorgehensweise

Vorgehensweise

- Wir simulieren zunächst eine Gleichverteilung

Vorgehensweise

- Wir simulieren zunächst eine Gleichverteilung
- Aus der berechnen wir dann unsere gewünschte Verteilung

Anforderungen

Anforderungen

- Zufallszahlen müssen eine große Periode haben

Anforderungen

- Zufallszahlen müssen eine große Periode haben
- Zufallszahlen müssen unvorhersagbar sein

Anforderungen

- Zufallszahlen müssen eine große Periode haben
- Zufallszahlen müssen unvorhersagbar sein
- Zufallszahlen sollten einer bekannten Verteilung entsprechen

Eine mögliche Definition

Definition

$$\zeta : \Lambda \to \Lambda,\ \Lambda \subset \mathbb{N}$$
$$\psi : \Lambda \to \Omega$$

Eine mögliche Definition

Definition

$$\zeta : \Lambda \to \Lambda,\ \Lambda \subset \mathbb{N}$$
$$\psi : \Lambda \to \Omega$$

- ζ ist eine Zustandsüberführungsfunktion

Eine mögliche Definition

Definition

$$\zeta : \Lambda \to \Lambda,\ \Lambda \subset \mathbb{N}$$
$$\psi : \Lambda \to \Omega$$

- ζ ist eine Zustandsüberführungsfunktion
- ψ weist jedem Zustand eine Zahl zu

Lineare Kongurenzgeneratoren

Wahl von ψ und ζ

$$\psi(x) := \frac{\zeta(x)}{M}$$
$$\zeta(x) := a \cdot x + c \mod M$$

Lineare Kongurenzgeneratoren

Wahl von ψ und ζ

$$\psi(x) := \frac{\zeta(x)}{M}$$
$$\zeta(x) := a \cdot x + c \mod M$$

Eigenschaften

- Bei passender Wahl von a und c erzielen wir eine Periode von M
- Durch geschickte Kombination mehrerer Generatoren können wir die Eigenschaften noch verbessern

Der Algorithmus von Wichman-Hill

```
1  class WichmannHill(Random):
2      def seed(self, a):
3          a, x = divmod(a, 30268)
4          a, y = divmod(a, 30306)
5          a, z = divmod(a, 30322)
6          self._seed = int(x)+1, int(y)+1, int(z)+1
7      def random(self):
8          x, y, z = self._seed
9          x = (171 * x) % 30269
10         y = (172 * y) % 30307
11         z = (170 * z) % 30323
12         self._seed = x, y, z
13         return (x/30269.0 + y/30307.0 + z/30323.0) % 1.0
```

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wie erzeugen wir exponentialverteilte ($\lambda e^{-\lambda x}$) Zufallszahlen?

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wie erzeugen wir exponentialverteilte ($\lambda e^{-\lambda x}$) Zufallszahlen?
- Einfach: Die Verteilung $y(x) = 1 - e^{-\lambda x}$ umkehren

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wie erzeugen wir exponentialverteilte ($\lambda e^{-\lambda x}$) Zufallszahlen?
- Einfach: Die Verteilung $y(x) = 1 - e^{-\lambda x}$ umkehren
- $x(y) = -\frac{1}{\lambda} \ln(1 - y)$

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wie erzeugen wir exponentialverteilte ($\lambda e^{-\lambda x}$) Zufallszahlen?
- Einfach: Die Verteilung $y(x) = 1 - e^{-\lambda x}$ umkehren
- $x(y) = -\frac{1}{\lambda} \ln(1 - y)$
- Wende die Funktion auf die Ausgabe eines Gleichverteilungsgenerators an

Erzeugung nicht-gleichverteilter Zufallszahlen

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wähle je zwei gleichverteilte Zufallszahlen auf dem Bereich

$$\left\{(u, v) \in \mathbb{R}^2 : 0 \leq u \leq f^{0.5}\left(\frac{u}{v}\right)\right\}$$

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wähle je zwei gleichverteilte Zufallszahlen auf dem Bereich

$$\left\{(u, v) \in \mathbb{R}^2 : 0 \leq u \leq f^{0.5}\left(\frac{u}{v}\right)\right\}$$

- Teile v durch u

Erzeugung nicht-gleichverteilter Zufallszahlen

- Wähle je zwei gleichverteilte Zufallszahlen auf dem Bereich

$$\left\{(u, v) \in \mathbb{R}^2 : 0 \leq u \leq f^{0.5}\left(\frac{u}{v}\right)\right\}$$

- Teile v durch u
- Das Ergebnis ist nach der Dichtefunktion f verteilt!

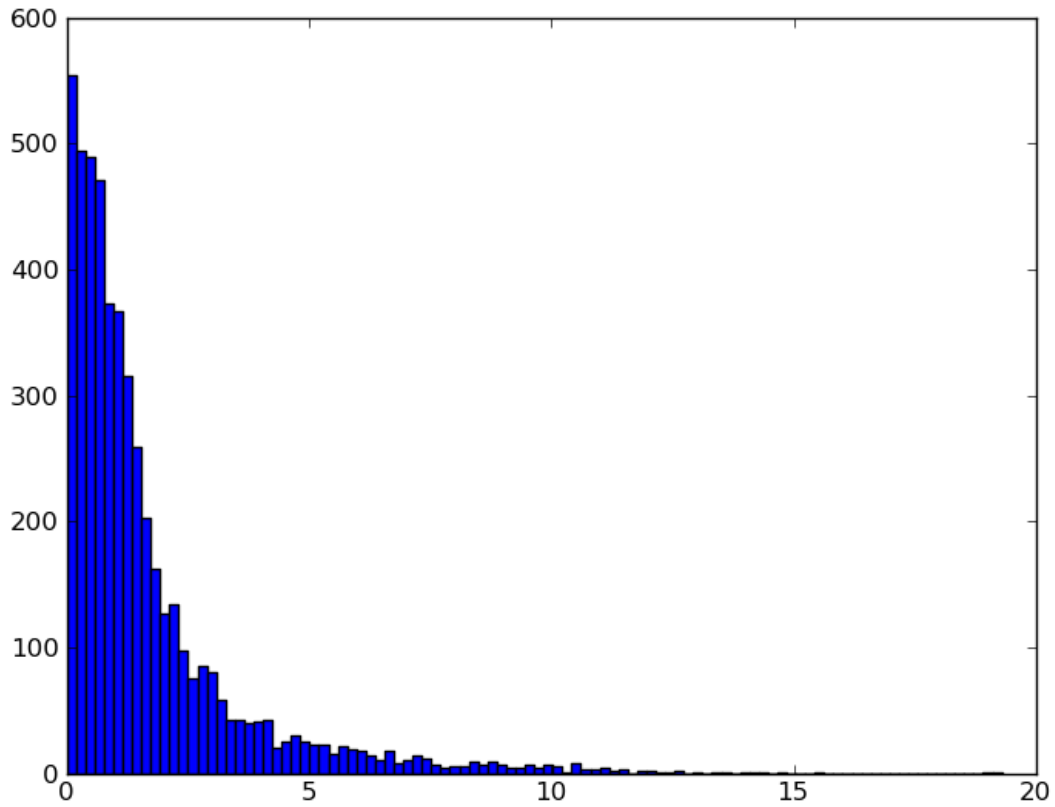
- Unser Beispiel war $f(x) = e^{-\lambda x}$

- Unser Beispiel war $f(x) = e^{-\lambda x}$
- Dann haben wir eingesetzt

$$0 \leq u \leq 1,\ v = -\frac{2}{\lambda} u \ln(u)$$

Erzeugung nicht-gleichverteilter Zufallszahlen

```
1 def exponential(_lambda):
2     while 1:
3     u1 = random()
4     u2 = 1.0 - random()
5     if u2 <= -2 / _lambda * u1 * log(u1):
6         break
7     return u2/u1
```


600
500
400
300
200
100
0
0
5
10
15
20

Weiterführendes

- Wo kann ich nach Code suchen?

Weiterführendes

- Wo kann ich nach Code suchen?
- Simulationswerkzeuge (NS-2)

Weiterführendes

- Wo kann ich nach Code suchen?
- Simulationswerkzeuge (NS-2)
- Publikationsorte

Ende

Weitere Details:
`http://page.mi.fu-berlin.de/pberndt/prngs/`

Ende

Weitere Details:
`http://page.mi.fu-berlin.de/pberndt/prngs/`

Und Danke für eure Aufmerksamkeit :-)