4. Apr.

Algorithmische Mathematik II

Teil 1: Diskrete Stochastik
- Zufallsvariablen, bedingte Wahrscheinlichkeit, Monte Carlo Methoden.

Teil 2: Numerische Analysis
- Iterative Verfahren, Interpolation und Integration.

Vorlesung: Mo + Mi : 10–12 Uhr.

1) Diskrete Stochastik

1.1) Einleitung

- Ziel ist die Beschreibung und Untersuchung von Systemen, die einen Anteil von Unvorhersagbarkeit (Zufall) enthalten, d.h. die sich nicht 100% deterministisch verhalten.

Beispiele:

- Unvorhersagbarkeit / Zufall kann viele verschiedene Quelle haben:

  → Zu Komplex um jede Einzelnvariablen zu Analysieren
  (auch deterministisch)

  ⇒ Gesamteffekt sieht zufällig aus.
  (Z.B., Teilchenbewegung → Termische Rausch)

  → Fehlende Information (Z.B., Kartenspiele, Finanzmärkte, Umfragen)

  → Chaotische Systeme (Z.B., Lotto)

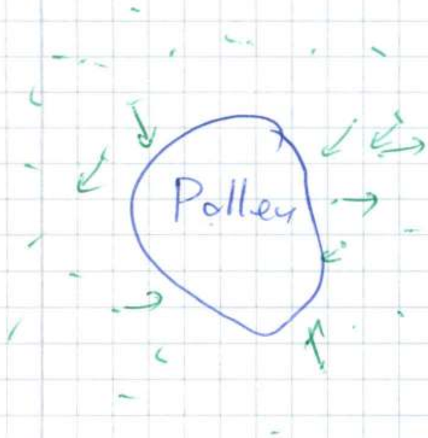
  → Intrinsisch unvorhersagbar. (Z.B., Radioaktive Zerfall) (Quantum Mechanik)

- Videos:
  - Geomag (chaotische System).
  - LorenzMoulin (").
  - Brownian Motion → Modellierung mit Zufall

- Image: . Stock Market → "Fluktuationen"

- Fragen:
  (1) Wie modelliert man ein System mit Zufall?
  (2) Wie simuliert " (⊕ "Zufallszahlen")
  (3) Welche Vorhersagen kann man machen?
  (4) Wie bestimmt man einen fairen Preis eines Produckts (stock, Versicherung)?

Beispiel: Physikalisch Braunsche Bewegung.



- Pollen ins Wasser (Siehe Video)
- 1 Pollen viel Grösser als die Wasserteilchen.
- $N = \mathcal{O}(10^{23})$ Wasserteilchen, die in Prinzip sich deterministisch Bewegen.

⇒ Systemgleichung mit $(N+1)\cdot 6$ Variablen ($6 = 3+3$: Positionen, Geschwindigkeiten).

⇒ Unlösbar; auch wenn wir die Anfangsbedienung kannten (der nicht den Fall ist).

(1) Modellierung:
- Was wollen wir Untersuchen?
- ⇒ Wir wollen die Bewegung vom Pollen beschreiben (nicht von den Wasserteilchen).

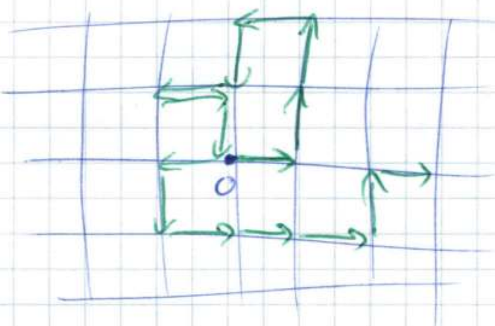
⇒ Statt (a priori deterministische) Stösse ersetzt man die mit "Zufällige" Stössen.

- Die Bewegung ist durch eine riesige Anzahl von kleinen Stösse ⇒ Gute Approximation ist durch die Mathematische Braunsche Bewegung, die ein Limes folgender diskrete Modell ist.

- Sei $X(n) \in \mathbb{Z}^3$ die Position unseren Pollen zur (diskrete) Zeit $n = 0, 1, 2, \ldots$
- O.b.d.A., nehmen wir $X(0) = 0$.
- $X(n+1) = X(n) + \xi_n$, wobei $\xi_n = \begin{cases} (1,0,0), & \text{Würfel} = 1 \\ (-1,0,0), & \text{"} \quad 2 \\ (0,1,0), & \text{"} \quad 3 \\ (0,-1,0), & \text{"} \quad 4 \\ (0,0,1), & \text{"} \quad 5 \\ (0,0,-1), & \text{"} \quad 6 \end{cases}$

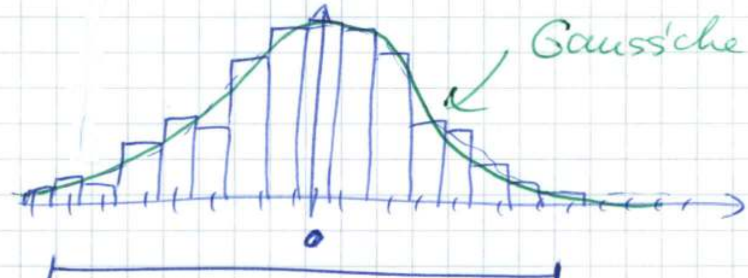
(Simulation mit Würfels oder Zufallszahlen)

- In 2 Dimensionen sieht die Trajektorie so aus:



- Wenn man eine Simulation oft wiederholt sieht man, dass typischerweise:
  - $X(n) = \mathcal{O}(\sqrt{n})$
  - Frequenz von $X_i(n)$, $i = 1, 2, 3$

Gauss'che Glocke.



$\mathcal{O}(\sqrt{n})$

⇒ Skalierung:

$$X(t) \text{ "}{:=}\text{" } \lim_{n \to \infty} \frac{X([n \cdot t])}{\sqrt{n}}$$ wird der Math. B.B.

- Vorhersagen:
  - Ist $X(t) \in$ Region A? Kann nicht beantwortet
  - Wenn man $X(t)$ beobachtet, wie häufig wird $X(t) \in$ Region A sein? Man kann es beantworten.

6. Apr.

1.2) Ereignisse und Wahrscheinlichkeit.

. Wahrscheinlichkeitsmodelle besitzen 3 Grundelementen:

(1) Die Menge Ω von möglichen Ergebnisse von einem Zufallsexperiment.
Elementen $\omega \in \Omega$ heissen auch Elementarereignisse.

(2) Die Menge $\mathcal{F}$ der Ereignissen, Ein Ereignis ist eine Eigenschaft, die an einer Teilmenge $G \subseteq \Omega$ assoziert ist, s.d. $\omega \in G \Leftrightarrow$ die Eigenschaft gilt.

(3) Eine Wahrscheinlichkeitsmass) Verteilung $\mathbb{P} : \mathcal{F} \to [0,1]$.
(oder W-Verteilung)

. Beispiel: Eine Urne ist mit 12 nummerierte Kugeln (von 1 bis 12).

. Zufallsexperiment: Eine Kugel ziehen und die Nummer notieren.

. $\Omega = \{1, 2, \dots, 12\}$ und ein Elementarereignis ist z.B. $\omega = 5$.

. Ereignissen sind z.B.:

. A = "Die Nummer ist gerade"
. B = "Die Nummer ist kleiner oder gleich 5"
. C = "Die Nummer ist 8"

. Assozierte Mengen: $A = \{2, 4, 6, 8, 10, 12\}$
$B = \{1, 2, 3, 4, 5\}$
$C = \{8\}$

. Wahrscheinlichkeiten: Unter die Annahme, dass keine Kugel wird bevorzugt, d.h. alle haben die gleiche "Chance" gezogen zu werden:

$$\mathbb{P}(G) = \frac{Card(G)}{Card(\Omega)} \equiv \frac{|G|}{|\Omega|}$$

$$\Rightarrow \quad \mathbb{P}(A) = \frac{6}{12} = \frac{1}{2} \; ; \; \mathbb{P}(B) = \frac{5}{12} \; ; \; \mathbb{P}(C) = \frac{1}{12}.$$

. Bem.: In dieser Vorlesung beschränken wir uns auf den Fall, dass Ω abzählbar ist ($\equiv$ diskret).

. Man kann **Kombinationen** von Ereignissen betrachten, z.B., $A \cap B$ = "Die Nummer ist gerade und ≤ 5".

. Notation: $A = \{\omega \in \Omega \mid \omega \in A\} = \{\omega \in A\} = \{A \text{ tritt ein}\}$.

oder A^c = "Die Nummer ist nicht gerade",
oder $A \cup B$ = "Die Nummer ist gerade oder ≤ 5", ...

$\Rightarrow \mathcal{F}$ muss mindestens eine Algebra sein.

. Seien $A, B, A_i \; i \in I$ Ereignisse. Dann,

. $A \cup B$: $\omega \in A \cup B \iff \omega \in A$ oder $\omega \in B$

$A \cup B$ tritt ein $\iff$ A tritt ein oder B tritt ein

(können auch beide eintreten).

- $\bigcup_{i\in I} A_i$: $\omega \in \bigcup_{i\in I} A_i \Leftrightarrow \exists$ (mindestens) ein $i \in I$ s.d. $\omega \in A_i$.

- $A \cap B \Leftrightarrow$ A <u>und</u> B treten ein.

- $\bigcap_{i\in I} A_i \Leftrightarrow$ jedes der A_i tritt ein.

$(A = \phi) \equiv (A^c = \Omega) \Leftrightarrow$ A tritt nicht ein.

- <u>Bemerkung:</u> $\mathcal{F}$ besteht aus Teilmengen von Ω:

$$\mathcal{F} \subseteq \mathcal{P}(\Omega) \quad , \mathcal{P}(\Omega) = \{A \mid A \subseteq \Omega\} \text{ ist}$$

die Potenzmenge von Ω.

- <u>Axiom 1:</u> $\mathcal{F} \subseteq \mathcal{P}(\Omega)$ <u>ist eine σ-Algebra</u>, d.h.,
  (1) $\Omega \in \mathcal{F}$,
  (2) $\forall A \in \mathcal{F},\ A^c \in \mathcal{F}$,
  (3) falls $A_1, A_2, \ldots \in \mathcal{F}$, dann $\bigcup_{i=1}^{\infty} A_i \in \mathcal{F}$

- <u>Bemerkung:</u> Punkt (3) ist mathematisch bequem, um im Fall unendlicher Mengen Ω nicht an ∞ Iterationen zu scheitern.

<u>Lemma 2:</u>
ⓐ $\phi \in \mathcal{F}$ (die leere Menge)
ⓑ $A, B \in \mathcal{F} \Rightarrow A \cup B \in \mathcal{F}$ und $A \cap B \in \mathcal{F}$
ⓒ $A_1, A_2, \ldots \in \mathcal{F} \Rightarrow \bigcap_{i=1}^{\infty} A_i \in \mathcal{F}$

<u>Beweis:</u>
ⓐ $\phi = \Omega^c \in \mathcal{F}$ nach (1) und (2).
ⓑ Nach (2) und (3): $A \cup B = A \cup B \cup \phi \cup \phi \cup \ldots \in \mathcal{F}$
ⓒ $\bigcap_{i=1}^{\infty} A_i = \left(\bigcup_{i=1}^{\infty} A_i^c\right)^c \in \mathcal{F}$.

#

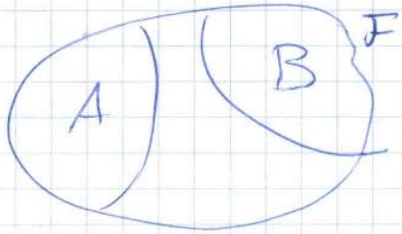
<u>Bemerkung:</u> $\mathcal{F} = \mathcal{P}(\Omega)$ ist eine σ-Algebra, die für <u>diskrete Modellen</u> gut ist.
<u>Aber</u> nicht für nicht-diskrete Modellen, weil wird es nicht möglich sein, eine Wahrscheinlichkeits(mass) Verteilung auf $\mathcal{P}(\Omega)$ zu definieren. (WT 1)

. Jetzt müssen wir schauen, was ein W-mass erfüllen muss.

. Seien $A, B \in \mathcal{F}$ mit $A \cap B = \emptyset$

$\Rightarrow$ Muss gelten: $\underline{\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)}$

(Diese Eigenschaft heisst "endliche Additivität".)



weil $\omega \in A \cup B$ mit $A \cap B = \emptyset$ bedeuted $\omega \in A$ oder (aber nicht gleichzeitig) $\omega \in B$.

. Anderseits $\Omega \in \mathcal{F}$ tritt immer ein $\Rightarrow$ $\underline{\mathbb{P}(\Omega) = 1 \ (=100\%)}$ (das ist die Normierung).

. Wir fordern etwas mehr als Additivität

<u>Definition 3:</u> Sei $(\Omega, \mathcal{F})$ ein Messraum. Eine Abbildung $\mathbb{P}: \mathcal{F} \to \mathbb{R}_+$ ist ein <u>W-(mass) Verteilung auf $(\Omega, \mathcal{F})$</u>
falls: (1) $\mathbb{P}(\Omega) = 1$

σ-Additivität $\rightarrow$ (2) Falls $A_1, A_2, \ldots \in \mathcal{F}$ mit $A_i \cap A_j = \emptyset$, $\forall i \neq j$, dann $\mathbb{P}\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mathbb{P}(A_i)$

Def. 4: Ein Wahrscheinlichkeitsraum $(\Omega, \mathcal{F}, \mathbb{P})$ besteht aus einer Menge Ω, einer σ-Algebra $\mathcal{F} \subseteq \mathcal{P}(\Omega)$ und ein Wahrscheinlichkeits (mass) Verteilung $\mathbb{P}$ auf $(\Omega, \mathcal{F})$.

- Konsequenzen:

Lemma 5: Sei $(\Omega, \mathcal{F}, \mathbb{P})$ ein W-raum.

(a) $\mathbb{P}(\emptyset) = 0$

(b) für $A, B \in \mathcal{F}$ mit $A \cap B = \emptyset$,
$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$$

(c) für $A, B \in \mathcal{F}$ mit $A \subseteq B$,
$$\mathbb{P}(B) = \mathbb{P}(A) + \mathbb{P}(B \setminus A)$$

$\Rightarrow$. $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$

. $\mathbb{P}(A) \leq \mathbb{P}(B) \leq 1$

(d) für $A, B \in \mathcal{F}$,
$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B) \leq \mathbb{P}(A) + \mathbb{P}(B).$$

(σ-Stetigkeit) (e) Wenn $A_n \uparrow A$ ($A_1 \subset A_2 \subset \dots$ und $A = \bigcup_{k=1}^{\infty} A_k$) oder $A_n \downarrow A$, dann $\lim_{n\to\infty} \mathbb{P}(A_n) = \mathbb{P}(\lim_{n\to\infty} A_n) = \mathbb{P}(A)$.

Beweis: (a) $1 = \mathbb{P}(\Omega)$ aber $\Omega = \Omega \cup \emptyset \cup \emptyset \dots$

$$\Rightarrow 1 = \mathbb{P}(\Omega \cup \emptyset \cup \emptyset \cup \dots) = \underbrace{\mathbb{P}(\Omega)}_{=1} + \underbrace{\mathbb{P}(\emptyset)}_{\geq 0} + \mathbb{P}(\emptyset) + \dots$$

$\Rightarrow \mathbb{P}(\emptyset) = 0$, sonst wäre $\leq \infty$.

(b) $\mathbb{P}(A \cup B) = \mathbb{P}(A \cup B \cup \emptyset \cup \emptyset \cup \dots)$

disjunkt $\overset{\sigma}{=} \mathbb{P}(A) + \mathbb{P}(B) + \mathbb{P}(\emptyset) + \dots$

$= \mathbb{P}(A) + \mathbb{P}(B)$.

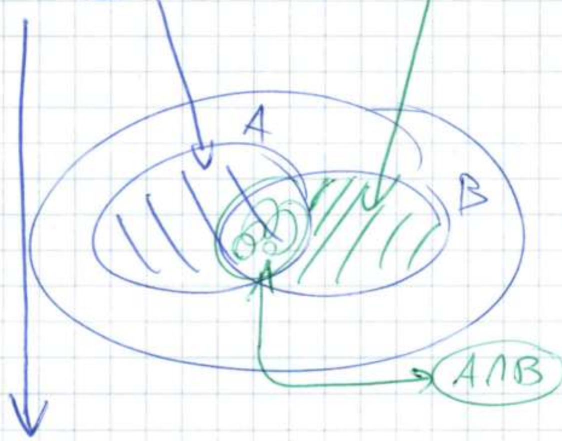
ⓒ $A \subseteq B \Rightarrow B = A \cup (B \setminus A)$ ist eine disjunkte Vereinigung

$$\Rightarrow \mathbb{P}(B) = \mathbb{P}(A) + \mathbb{P}(B \setminus A)$$

. Da $\mathbb{P}(B \setminus A) \geq 0$, folgt $\mathbb{P}(B) \geq \mathbb{P}(A)$.

. Mit $B = \Omega$, $1 = \mathbb{P}(\Omega) = \mathbb{P}(A) + \mathbb{P}(A^c) \geq \mathbb{P}(A)$.

ⓓ $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}((A \cup B) \setminus A)$



$$= \mathbb{P}(A) + \mathbb{P}(B \setminus (A \cap B))$$

$$= \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B). \ \#$$

ⓔ Übung.

Die Erweiterung von ⓓ für endlich viele Ereignisse ist die folgende:

Korollar 6: (Einschluss / Ausschluss Prinzip)

. Seien $A_1, A_2, \dots, A_n \in \mathcal{F}$. Dann,

$$\mathbb{P}(A_1 \cup A_2 \cup \dots \cup A_n) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \mathbb{P}(A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k})$$

Beweis: Wir zeigen es mit Induktion.

IV: Gilt für $n=1$: $\mathbb{P}(A_1) = \mathbb{P}(A_1)$.

IA: Sei Korollar für einen n gültig.

$$\text{Dann, } \mathbb{P}\Big(\bigcup_{k=1}^{n+1} A_k\Big) = \mathbb{P}\Big(\Big(\bigcup_{k=1}^{n} A_k\Big) \cup A_{n+1}\Big)$$

$$\underset{\text{Lemma 5(d)}}{=} \mathbb{P}\Big(\bigcup_{k=1}^{n} A_k\Big) + \mathbb{P}(A_{n+1}) - \mathbb{P}\Big(\Big(\bigcup_{k=1}^{n} A_k\Big) \cap A_{n+1}\Big)$$

$$= \mathbb{P}\Big(\bigcup_{k=1}^{n} A_k\Big) + \mathbb{P}(A_{n+1}) - \mathbb{P}\Big(\bigcup_{k=1}^{n} \underbrace{(A_k \cap A_{n+1})}_{=\tilde{A}_k}\Big)$$

$$\overset{\text{Induktion}}{=} \Big\{\sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k})\Big\}$$

$$+ \mathbb{P}(A_{n+1})$$

$$- \Big\{\sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k} \cap A_{n+1})\Big\}$$

Anderseits, $\displaystyle\sum_{k=1}^{n+1} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n+1} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k})$

$$= \sum_{k=1}^{n+1} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k}) \quad \leftarrow (i_k \le n)$$

$$+ \sum_{k=2}^{n+1} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_{k-1} \le n} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_{k-1}} \cap A_{n+1}) \quad \leftarrow \big(i_k = n+1,\ k \geq 2\big)$$

$$+ \mathbb{P}(A_{n+1}) \quad \leftarrow (i_k = n+1,\ k=1)$$

$$\overset{k-1=l}{=} -\sum_{l=1}^{n} (-1)^{l-1} \sum_{1 \le i_1 < \cdots < i_l \le n} \mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_l} \cap A_{n+1}).$$

#

11. Apr.

1.3) Diskrete Verteilungen

. Jetzt betrachten wir Ω endlich oder abzählbar unendlich. Dann setzen wir i.a. $\mathcal{F} = \mathcal{P}(\Omega)$.
$\left(\mathrm{Card}(\mathcal{P}(\Omega)) = 2^{\mathrm{Card}(\Omega)}\right)$.

. Beispiel: Münzwurf (nicht unbedingt faire Münze).

$$\Omega = \{\text{Kopf}, \text{Zahl}\} \text{ und } \mathcal{F} = \{\{K\}, \{Z\}, \{K, Z\}, \emptyset\}$$

. Sei p die W-keit Kopf zu erhalten.

$$\Rightarrow \mathbb{P}(\{K\}) = p \quad , \quad \mathbb{P}(\{Z\}) = 1 - p,$$
$$\mathbb{P}(\emptyset) = 0 \quad , \quad \mathbb{P}(\Omega = \{K, Z\}) = 1.$$

. Wie sieht es eine W-Verteilung wenn $\mathrm{Card}\,\Omega \leq \mathrm{Card}\,\mathbb{N}$?

. Satz 7) (a) Sei $p(\omega) \in [0,1]$, $\forall \omega \in \Omega$, s.d.

$$\sum_{\omega \in \Omega} p(\omega) = 1 \quad \text{(d.h., eine Gewichtung).}$$

Dann $\mathbb{P} : (\Omega, \mathcal{F}) \to [0,1]$ definiert durch

$$\mathbb{P}(A) := \sum_{\omega \in A} p(\omega) \quad , \forall A \subseteq \Omega, \quad (*)$$

ist eine W-verteilung.

(b) Jede W-Verteilung $\mathbb{P}$ auf $(\Omega, \mathcal{F})$ hat die Form $(*)$ mit $p(\omega) = \mathbb{P}(\{\omega\})$, $\omega \in \Omega$.

Bem.: $p : \Omega \to [0,1]$ von Satz 7 heisst Massenfunktion der diskreten W-Verteilung $\mathbb{P}$.

(Bem.: (b) Gilt nicht für Ω unabzählbar.).

. Laut Def. 3, müssen wir die σ-Additivität von $\mathbb{P}$ zeigen (und $\mathbb{P}(\Omega)=1$).

Bemerkung: Die Summe von positiven Summanden hängt nicht um die Summierordnung:

. Für A abzählbar, $p(\omega)\geq 0 \ \forall \omega\in A$,

$$\sum_{\omega\in A} p(\omega) := \sum_{k=1}^{\infty} p(\omega_k)$$

wobei $\omega_1, \omega_2, \ldots$ ist eine beliebige Abzählung von A ist

.(Vorbereitungslemma 8)

ⓐ Sei $p(\omega)\in[0,1]$. Dann $\sum_{\omega\in A} p(\omega)\in[0,\infty]$ ist wohldefiniert.

Deshalb setzen wir $\mathbb{P}(A) := \sum_{\omega\in A} p(\omega)$.

Dazu, es gilt: $$\mathbb{P}(A) = \sup_{\substack{F\subseteq A\\ |F|<\infty}} \mathbb{P}(F) \quad (**)$$

und $$\mathbb{P}(A)\leq \mathbb{P}(B) \ , \forall A\subseteq B. \quad (***)$$

ⓑ Ist $A=\dot{\bigcup}_{k=1}^{\infty} A_k$ eine disjunkte Zerlegung, dann

$$\mathbb{P}(A) = \sum_{k=1}^{\infty} \mathbb{P}(A_k).$$

(σ-Add. von $\mathbb{P}$).

Beweis: ⓐ Sei $\omega_1, \omega_2, \ldots$ eine beliebige Abzählung von A.

Da $p(\omega_k)\geq 0, \ \forall k\in\mathbb{N}$,

$$n \longmapsto \sum_{k=1}^{n} p(\omega_k) \text{ ist monoton wachsend.}$$

$$\Rightarrow \sum_{k=1}^{\infty} p(\omega_k) = \sup_{n\in\mathbb{N}} \sum_{k=1}^{n} p(\omega_k) \in [0,\infty].$$

. Setzen wir deshalb $\mathbb{P}(A) := \sum_{k=1}^{\infty} p(\omega_k)$. (14)

<u>Zu zeigen:</u> $\sup_{n\in\mathbb{N}} \sum_{k=1}^{n} p(\omega_k) = \sup_{\substack{F\subseteq A\\|F|<\infty}} \underbrace{\sum_{\omega\in F} p(\omega)}_{\mathbb{P}(F)}$ ist unabhängig von der Abzählung von A. $\{\omega_1,\omega_2,\dots\}$

$\leq$: $\forall n\in\mathbb{N}$, $\sum_{k=1}^{n} p(\omega_k) = \underbrace{\sum_{\omega\in\tilde F_n} p(\omega)}_{\mathbb{P}(\tilde F_n)} \leq \sup_{\substack{F\subseteq A\\|F|<\infty}} \underbrace{\sum_{\omega\in F} p(\omega)}_{\mathbb{P}(F)}$.

Sei $\tilde F_n = \{\omega_1,\dots,\omega_n\}$

$$\Rightarrow \sup_{n\in\mathbb{N}} \sum_{k=1}^{n} p(\omega_k) \leq \sup_{\substack{F\subseteq A\\|F|<\infty}} \underbrace{\sum_{\omega\in F} p(\omega)}_{\mathbb{P}(F)}.$$

$\geq$: F in "$\sup_{\substack{F\subseteq A\\|F|<\infty}}$" ist endlich $\Rightarrow \exists\, n\in\mathbb{N}$ s.d. $F\subseteq\{\omega_1,\dots,\omega_n\}$.

Deshalb: $\overbrace{\sum_{\omega\in F} p(\omega)}^{\mathbb{P}(F)} \leq \sum_{k=1}^{n} p(\omega_k) \leq \overbrace{\sum_{k=1}^{\infty} p(\omega_k)}^{=\mathbb{P}(A)}$,

$\forall$ endlich $F\subseteq A$. $\Rightarrow \underbrace{\sum_{k=1}^{\infty} p(\omega_k)}_{\mathbb{P}(A)} = \sup_{n\in\mathbb{N}} \sum_{k=1}^{n} p(\omega_k) \geq \sup_{\substack{F\subseteq A\\|F|<\infty}} \underbrace{\sum_{\omega\in F} p(\omega)}_{\mathbb{P}(F)}$.

. Da $\mathbb{P}(A) \leq \mathbb{P}(B)$ ist klar, weil

$$\mathbb{P}(A) = \sup_{\substack{F\subseteq A\\|F|<\infty}} \mathbb{P}(F) \leq \sup_{\substack{F\subseteq B\\|F|<\infty}} \mathbb{P}(F) = \mathbb{P}(B).$$

$A\subseteq B$

(b) (b.1) <u>Fall $|A|<\infty$:</u> $\exists\, n\in\mathbb{N}$ s.d. $A = \bigcup_{k=1}^{n} A_k$.

Dann, $\mathbb{P}(A) = \sum_{\ell=1}^{|A|} p(\omega_\ell) = \sum_{\ell=1}^{|A|}\sum_{k=1}^{n} p(\omega_\ell)\,\mathbb{1}_{[\omega_\ell\in A_k]}$

$$= \sum_{k=1}^{n} \underbrace{\sum_{\ell=1}^{|A|} p(\omega_\ell)\,\mathbb{1}_{[\omega_\ell\in A_k]}}_{=\mathbb{P}(A_k)} = \sum_{k=1}^{n} \mathbb{P}(A_k).$$

b.2) Fall $|A| = \infty$.

"$\leq$": $P(A) \overset{(**)}{=} \sup_{\substack{F \subseteq A \\ |F| < \infty}} P(F)$.

Da $F \subseteq A$ endlich ist, $F = \overset{\infty}{\underset{k=1}{\dot{\bigcup}}} (F \cap A_k)$ ist eine disjunkte Vereinigung mit nur endlich viele $F \cap A_k \neq \phi$.

Deshalb (aus Fall $|A| < \infty$) folgt:

(man benutzt nicht σ-Add.).

$$P(F) = \sum_{k=1}^{\infty} P(F \cap A_k)$$

$$\overset{(**)}{\leq} \sum_{k=1}^{\infty} P(A_k) \quad \text{weil } F \cap A_k \subseteq A_k.$$

$$\Rightarrow P(A) = \sup_{\substack{F \subseteq A \\ |F| < \infty}} P(F) \leq \sum_{k=1}^{\infty} P(A_k).$$

"$\geq$": Jetzt versuchen wir den supremum auf jede einzeln A_k zu bestimmen.

So, seien $F_k \subseteq A_k$ endlich.

Aus $A_k \cap A_l = \phi$ für $l \neq k \Rightarrow F_k \cap F_l = \phi$ für $l \neq k$.

So, $\forall n \in \mathbb{N}$,

$$\sum_{k=1}^{n} P(F_k) \underset{(\text{Fall } |A| < \infty)}{=} P\left(\overset{n}{\underset{k=1}{\dot{\bigcup}}} F_k\right) \underset{(***)}{\leq} P\left(\overset{\infty}{\underset{k=1}{\dot{\bigcup}}} F_k\right)$$

$$\underset{(***)}{\leq} P\left(\overset{\infty}{\underset{k=1}{\dot{\bigcup}}} A_k\right) = P(A).$$

Deshalb, $\sum_{k=1}^{n} P(A_k) \overset{(**)}{=} \sum_{k=1}^{n} \sup_{\substack{F_k \subseteq A_k \\ |F_k| < \infty}} P(F_k) \leq P(A)$, $\forall n \in \mathbb{N}$.

$$\Rightarrow \sum_{k=1}^{\infty} P(A_k) \leq P(A).$$

#

• Wir haben praktisch schon Satz 7 bewiesen, ausser die Normierung.

Beweis von Satz 7:

ⓐ Nach Voraussetzungen gilt $\sum_{\omega\in\Omega} p(\omega) = \mathbb{P}(\Omega) = 1$

und aus Lemma 8 ist $\mathbb{P}$ σ-additiv.

$\Rightarrow \mathbb{P}(A) := \mathbb{P}(A)$ ist eine W-Verteilung.

ⓑ Da $\mathbb{P}$ σ-additiv ist, $\forall A \subseteq \Omega$,

$$\mathbb{P}(A) = \mathbb{P}\Big(\bigcup_{\omega\in A} \{\omega\}\Big) \overset{\downarrow}{=} \sum_{\omega\in A} \mathbb{P}(\{\omega\})$$

hat die Form ⊛ mit $p(\omega) = \mathbb{P}(\{\omega\})$. #

1.4) Einige Beispiele

1.4.1) Gleichverteilung: Sei Ω endlich ($\Omega \neq \emptyset$),

dann kann man setzen $\mathcal{F} = \mathcal{P}(\Omega)$ und ein (uniform) Gewicht auf die Elementarereignissen, d.h.,

$\forall \omega \in \Omega$, $p(\omega) = \mathbb{P}(\{\omega\}) = \frac{1}{|\Omega|}$.

Dann $\mathbb{P}$ heisst Gleichverteilung.

. Es folgt dann aus Satz 7, dass für $A \subseteq \Omega$,

$$\mathbb{P}(A) = \sum_{\omega\in A} p(\omega) = \frac{1}{|\Omega|}\cdot|A| = \frac{\#\,\omega \text{ wo } A \text{ tritt ein}}{\#\,\omega}.$$

Beispiele: (a) Faire Würfeln, n mal geworfen.

$\Omega = \{1,2,3,4,5,6\}^n$, dann $|\Omega| = 6^n$

so hat die Gleichverteilung $\mathbb{P}$ die Gewichte $p(\omega) = \frac{1}{6^n}$.

(b) Zufällige Permutationen.

. Eine Permutation $\sigma \in S_n$ von $\{1,..,n\}$ ist eine bijektive Abbildung von $\{1,..,n\}$ nach $\{1,..,n\}$.

. Sei $\Omega = S_n$, die Menge aller Permutationen von $\{1,..,n\} \Rightarrow |\Omega| = n!$

. Falls $\mathbb{P}$ die Gleichverteilung ist, dann $\mathbb{P}(A) = \frac{|A|}{n!}$.

Kleine Übung: Sei n die Anzahl von Karten eines Kartenspiel, die "gut gemischt" sind, d.h., jede Reihenfolge gleich wahrscheinlich ist.

$\omega(k)$ = Position von Karte k.

(1) Q: $\mathbb{P}$(Karte k ist auf ℓte Stelle) = ?

A: $= \mathbb{P}(\{\omega \in S_n \mid \omega(k) = \ell\}) = \frac{(n-1)!}{n!} = \frac{1}{n}$ (weil 1 ist fest).

(2) Q: $\mathbb{P}$(ist eine Karte "auf ihre Stelle") = ?

A: $= \mathbb{P}(\{\exists k \text{ s.d. } \omega(k) = k\})$.

Sei das Ereignis $A_k = \{\omega \mid \omega(k) = k\}$.

Dann,

$$\mathbb{P}(\{\exists k \text{ s.d. } \omega(k)=k\}) = \mathbb{P}\left(\bigcup_{k=1}^{n} A_k\right)$$

$$\overset{\text{Kor. 6}}{=} \sum_{k=1}^{n} (-1)^{k-1} \sum_{1\le i_1<\dots<i_k\le n} \underbrace{\mathbb{P}(A_{i_1}\cap\dots\cap A_{i_k})}_{=\frac{(n-k)!}{n!}} \quad \text{(da } k \text{ sind fest)}$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \underbrace{\sum_{1\le i_1<\dots<i_k\le n}}_{\binom{n}{k}} \frac{(n-k)!}{n!}$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \frac{(n-k)!}{n!} \cdot \binom{n}{k} = -\sum_{k=1}^{n} \frac{(-1)^k}{k!}.$$

$$= \underbrace{\sum_{k=0}^{\infty} \frac{(-1)^k}{k!}}_{} - \frac{1}{e} - \sum_{k=1}^{n} \frac{(-1)^k}{k!}$$

$$= 1 - \frac{1}{e} + \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \xrightarrow[n\to\infty]{} 1 - \frac{1}{e}.$$

1.4.2) Empirische Verteilung.

- Aus einer empirische Beobachtung kann man eine W-Verteilung definieren, die <u>empirische Verteilung</u> heisst.

- Seien $x_1, \dots, x_n \in \Omega$ die (n) Beobachtungen.
  Sei dazu
  $N(A) = |\{k \in \{1,\dots,n\} \mid x_i \in A\}|$ die Anzahl der Beobachtungen in A.

Dann, $\mathbb{P}(A) := \frac{N(A)}{n}$, die relative Häufigkeit in A ist eine W-Verteilung (die empirische Verteilung).

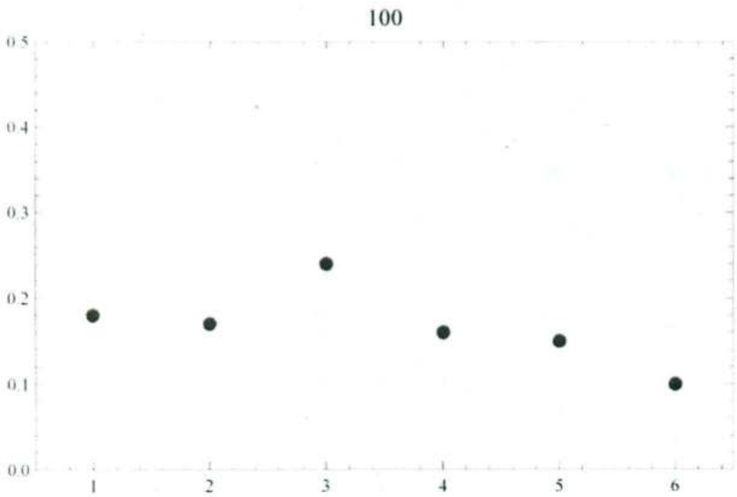
und $p(\omega) = \frac{N(\{\omega\})}{n}$ ist <u>die relative Häufigkeit</u> von $\omega \in \Omega$.

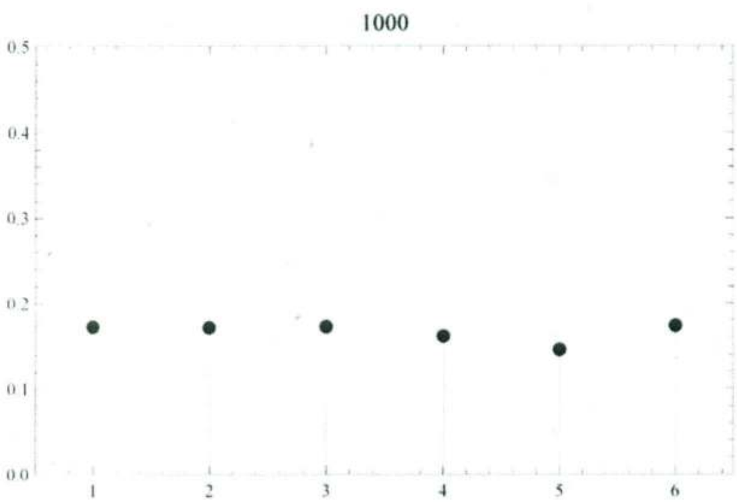
Beispiel: Empirische Verteilung von n Zufallswürfen eines Würfels.

- $x_1, \dots, x_n$ Zufallszahlen auf $\{1, 2, 3, 4, 5, 6\}$.

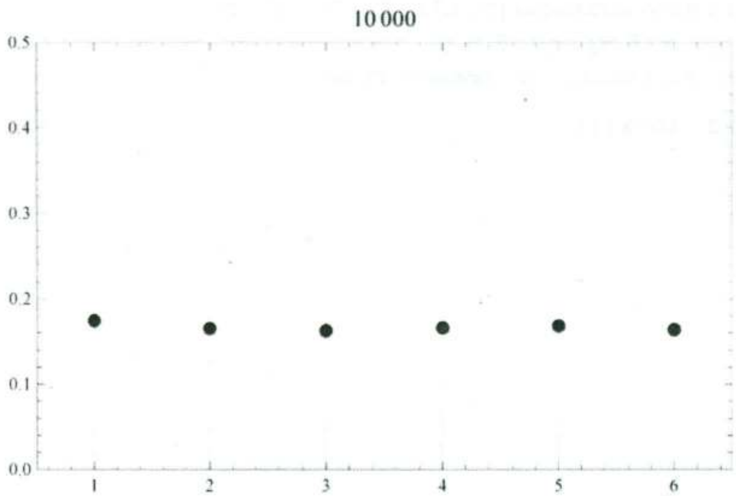
→ Siehe File $\boxed{\text{01 EmpirischeVerteilungen.nb}}$

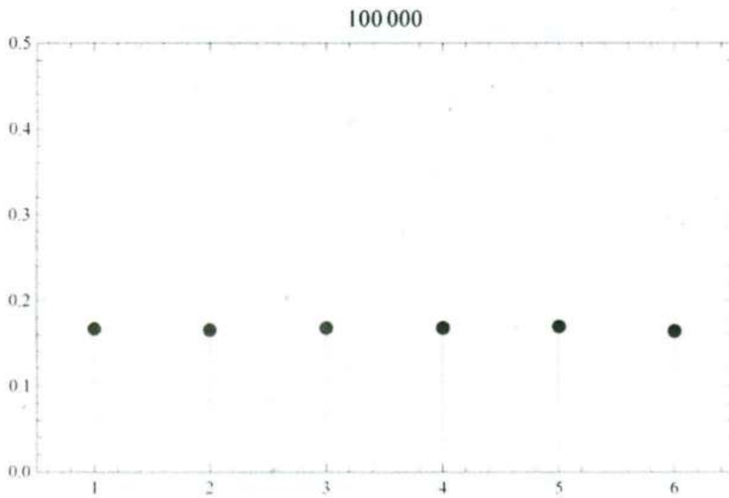
```
In[27]:= P[n_] := ListPlot[BinCounts[(1 + RandomInteger[5, n]), {1, 7, 1}] / n,
           Filling → Axis, PlotRange → {{0.5, 6.5}, {0, 0.5}},
           PlotStyle → PointSize[Large], PlotLabel → n, Frame → True]

In[28]:= For [k = 1, k < 6, k++, Print[P[10 × 10^k]]]
```

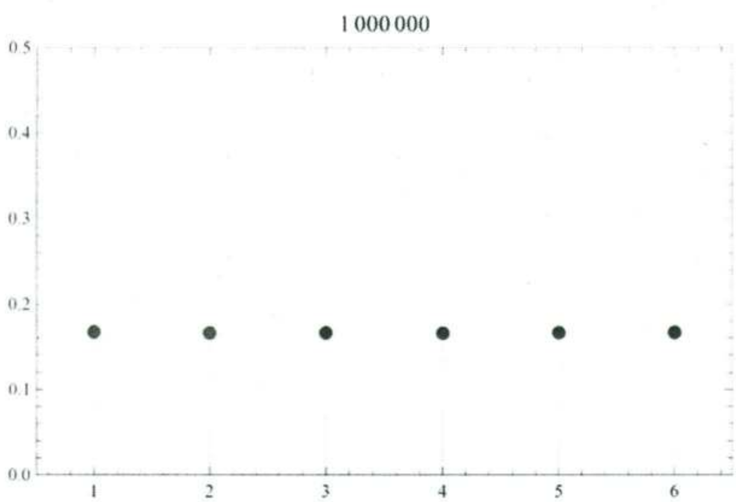




196


10 000
0.5
0.4
0.3
0.2
0.1
0.0
1
2
3
4
5
6


100 000
0.5
0.4
0.3
0.2
0.1
0.0
1
2
3
4
5
6


1 000 000
0.5
0.4
0.3
0.2
0.1
0.0
1
2
3
4
5
6

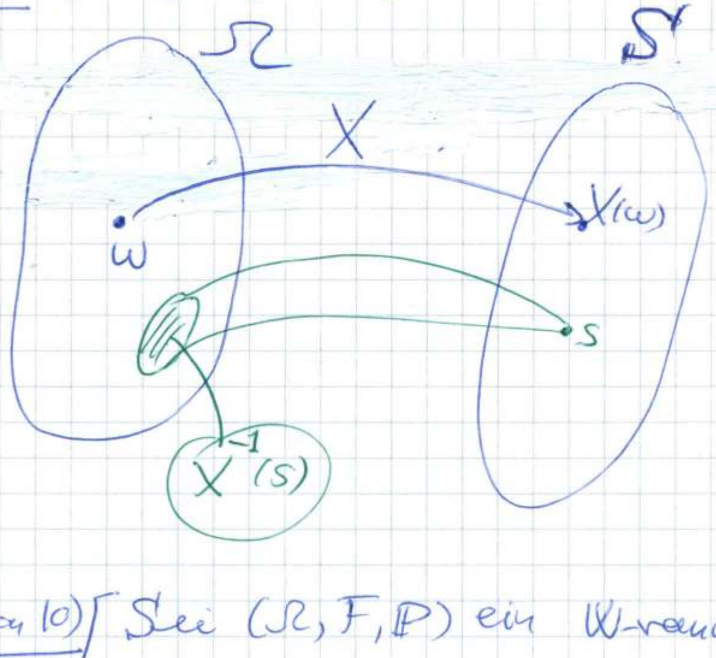
1.5) Zufallsvariablen

• <u>Definition 9)</u> Sei $(\Omega, \mathcal{F}, \mathbb{P})$ ein W-raum.

Eine <u>diskrete Zufallsvariable</u> ist eine Abbildung $X : \Omega \to S$ mit S abzählbar, so dass $\forall s \in S$,

$$X^{-1}(s) := \{\omega \in \Omega \mid X(\omega) = s\} \in \mathcal{F}.$$

• <u>Notation:</u> $X^{-1}(s) \equiv \{X = s\}$.



<u>Definition 10)</u> Sei $(\Omega, \mathcal{F}, \mathbb{P})$ ein W-raum und $X : \Omega \to S$ eine diskrete ZV. Dann die <u>Verteilung von X</u> ist die W-Verteilung μ_X auf $(S, \tilde{\mathcal{F}} = \mathcal{P}(S))$ s.d.

$$\forall \tilde{A} \in \tilde{\mathcal{F}}, \quad \mu_X(\tilde{A}) := \mathbb{P}(X^{-1}(\tilde{A})) = \mathbb{P}(\{X \in \tilde{A}\}),$$

d.h. μ_X hat gewichte p_X : <u>$p_X(s) = \mathbb{P}(X = s)$.</u>

Bemerkungen: (a) $\forall s \in S',\ p_X(s) \geq 0$.

(b) Die Ereignisse $\{X = s\}$ für verschiedene $s \in S'$ sind disjunkt.

$$\Rightarrow \sum_{s \in S'} p_X(s) = \sum_{s \in S'} \mathbb{P}(X=s) = \mathbb{P}\Big(\bigcup_{s \in S'} \{X=s\}\Big) = \mathbb{P}(\Omega) = 1$$

Beispiele: Werfen von n Münzen.

Sei $\Omega = \{\omega = (\omega_1, \dots, \omega_n) \mid \omega_k \in \{0,1\}\}$

wobei $\omega_k = \begin{cases} 0 & \text{, falls Zahl,} \\ 1 & \text{, falls Kopf.} \end{cases}$

Sei $\mathcal{F} = \mathcal{P}(\Omega)$ und $\mathbb{P}$ die Gleichverteilung.

(1) $X_k : \Omega \to \{0,1\} = S'$

$\omega \mapsto \omega_k$

ist eine diskrete ZV mit Verteilung μ_{X_k} (mit Gewichte)

$$p_{X_k}(s) = \mathbb{P}(X_k = s) = \frac{2^{n-1}}{2^n} = \frac{1}{2},\quad s \in \{0,1\}.$$

Noch Gleichverteilt!

(2) $Y : \Omega \to \tilde{S'} := \{0, 1, \dots, n\}$.

$\omega \mapsto Y(\omega) = \omega_1 + \dots + \omega_n \quad (= X_1(\omega) + \dots + X_n(\omega))$

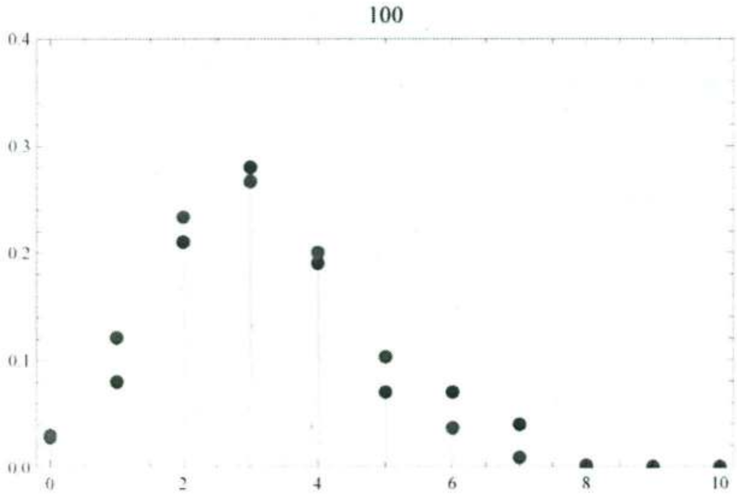
Dann, μ_Y hat Gewichte

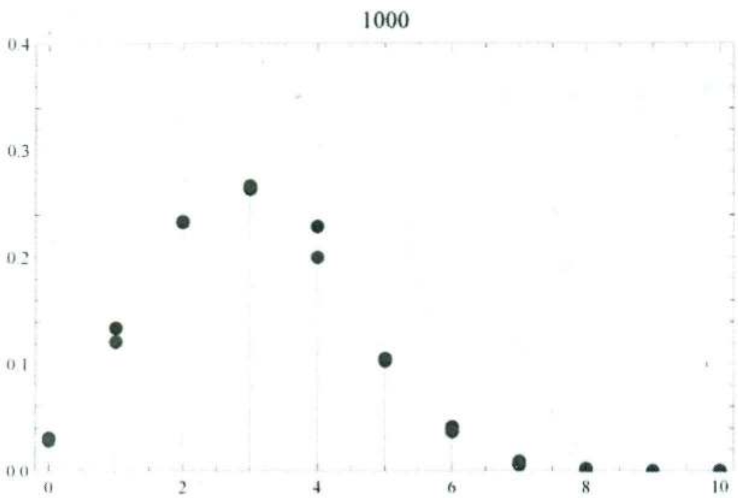
$$p_Y(s) = \binom{n}{s} \cdot \frac{1}{2^n},\quad s \in \{0,1,\dots,n\}$$

$\longrightarrow$ Nicht mehr Gleichverteilt!

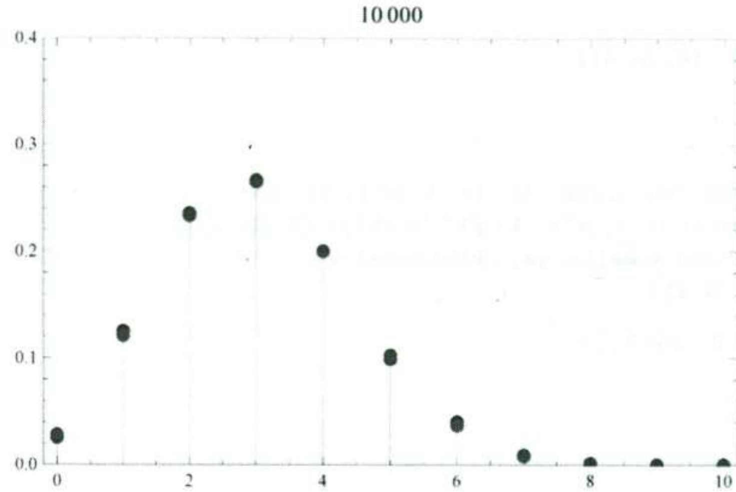
22a

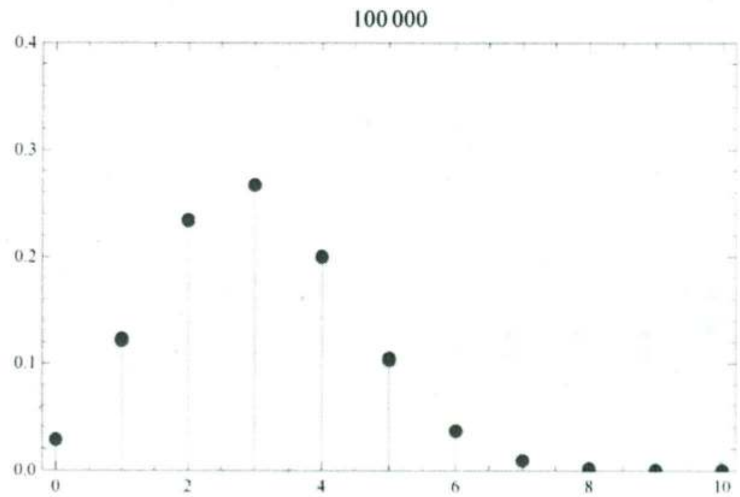
```
In[3]:= L[p_, x_] := If[x ≤ p, 1, 0]

In[4]:= Y[p_, n_] := Sum[L[p, Random[]], {k, 1, n}]

In[30]:= p = 0.3; n = 10;

In[33]:= P[m_] :=
  ListPlot[{Table[{k, (BinCounts[Table[Y[p, n], {k, 1, m}], {0, n + 1, 1}] / m)[[k + 1]]},
     {k, 0, n}], Table[{k, Binomial[n, k] p^k (1 - p)^(n - k)}, {k, 0, n}]},
   Filling → Axis, PlotStyle → PointSize[Large], PlotLabel → m,
   Frame → True, PlotRange → {0, 0.4}]

In[34]:= For [k = 1, k < 5, k++, Print[P[10 × 10^k]]]
```





(22b)





1.5.1) Binomialverteilung.

Definition 11) Seien $n \in \mathbb{N}$ und $p \in [0,1]$ gegeben. Die W-Verteilung auf $\{0,1,\dots,n\}$ mit Massenfunktion

$$P_{n,p}(k) = \binom{n}{k} p^k (1-p)^{n-k}$$

heisst Binomialverteilung mit Parametern n und p (Notation: $Bin(n,p)$).

. Wo taucht diese Verteilung auf?

(a) Würfeln einer Münze , die mit W-keit p Kopf gibt (n mal). Dann die Verteilungen von Y (wie oben) ist $Bin(n,p)$.

(b) Ziehen wir n Mal eine Zufallszahl auf $[0,1]$, (Gleichverteilt)

$\Rightarrow \omega = (\omega_1, \dots, \omega_n) \Rightarrow$ Sei $Y(\omega) = \sum_{k=1}^{n} \mathbb{1}_{[\omega_k \leq p]}$

$\Rightarrow$ Siehe 02 Binomial. ub.

(c) Ziehen mit Zurücklegen.

. Seien m Kugeln in einer Urne, davon $p \cdot m$ Weisse und $(1-p)m$ Schwarze.

. Wir ziehen eine Kugel und legen die wieder zurück (+ Gut mischen).

. Wir machen insgesamt n Ziehungen

. Sei $\omega = (\omega_1, \dots, \omega_n) \in \Omega = \{0,1\}^n$ mit

$$\omega_k = \begin{cases} 1, & \text{falls die Kugel ist weiss.} \\ 0, & \text{sonst.} \end{cases}$$

. Dann, $\mathbb{P}(\omega_k = 1) = \frac{p \cdot m}{m} = p = 1 - \mathbb{P}(\omega_k = 0)$, $k = 1, \dots, n$.

Sei $X(\omega) = \sum_{k=1}^{n} \omega_k$. Dann hat X die Bin(n,p) Verteilung.

. In der Tat, $\left|\{\omega \in \Omega \mid X(\omega) = \ell\}\right| = \binom{n}{\ell} \cdot (pm)^{\ell} ((1-p)m)^{n-\ell}$

\# möglichkeiten für $\omega_k = 1$, $\forall k$ \# möglichkeiten für $\omega_k = 0$, $\forall k$

$$\Rightarrow \mathbb{P}(X(\omega) = \ell) = \frac{|X = \ell|}{|\Omega|} = \frac{\binom{n}{\ell} p^{\ell} (1-p)^{n-\ell} \cdot \cancel{m^n}}{\cancel{m^n}}.$$

<u>Definition 12)</u> Ereignisse $E_1, \dots, E_n$ heissen <u>unabhängig</u>,

falls $\forall\, 2 \le k \le n$, $1 \le i_1 < i_2 < \dots < i_k \le n$ gilt
$$\mathbb{P}(E_{i_1} \cap \dots \cap E_{i_k}) = \mathbb{P}(E_{i_1}) \cdots \mathbb{P}(E_{i_k}).$$

. Falls $E_1, \dots, E_n$ unabhängig sind und $\mathbb{P}(E_i) = p$, dann

$$\circledast \quad \mathbb{P}(k \text{ von } E_1, \dots, E_n \text{ eintreten}) = \binom{n}{k} p^k (1-p)^{n-k}.$$

In der Tat, sei $A_{(i_1, \dots, i_k)} = \{\omega \in \Omega \mid E_{i_1}, \dots, E_{i_k}$ eintreten und die andere $E_\cdot$ nicht eintreten$\}$.

$\Rightarrow \underbrace{\bigcup_{1 \le i_1 < \dots < i_k \le n} A_{(i_1, \dots, i_k)}}$ ist ~~eine~~ disjunkte Vereinigung

und so $\circledast = \mathbb{P}(\downarrow) = \underbrace{\sum_{1 \le i_1 < \dots < i_k \le n}}_{\binom{n}{k} \text{ Terms}} \underbrace{\mathbb{P}(A_{(i_1, \dots, i_n)})}_{= p^k (1-p)^{n-k}} \overset{\text{unab.}}{=} p^k (1-p)^{n-k} \binom{n}{k}.$

1.5.2) Poissonverteilung.

Definition 13) Die W-Verteilung auf $\{0,1,2,\ldots\}$ mit Massenfunktion

$$p(k) = \frac{\lambda^k}{k!} e^{-\lambda}, \quad k = 0,1,2,\ldots$$

heisst Poissonverteilung mit Parameter λ.

. Woher sieht man diese Verteilung?

@Warteschlange:

. Annahme: Kunden in einer Warteschlange kommen unabhängig voneinander zu zufälligen gleichverteilten Zeiten.

. Wir nehmen eine Zeiteinheit $\delta = \frac{1}{n}$ klein genug so dass zwischen 2 Zeiten kommt höchstens ein Kunde.

. Sei $E_k = \{$ein Kunde in $[(k-1)\delta, k\cdot\delta]$ ankommt$\}$.

~~$\tilde{E}_k = \{$2 Kunden in $[(k-1)\delta, k\delta]$ ankommt$\}$.~~

. Wenn ein Kunde kommt in $\Theta(1)$ Zeit, dann wird $\mathbb{P}(E_k) = \Theta(\delta)$ sein für klein δ.

~~und $\mathbb{P}(\tilde{E}_k) = \Theta(\delta^2)$~~

Sei $$\lambda = \lim_{\delta \downarrow 0} \frac{\mathbb{P}(E_k)}{\delta} \in (0,\infty).$$

$\Rightarrow N =$ Anzahl der angekommenden Kunden in $[0,t]$. (eine ZV).

$$\Rightarrow \mathbb{P}(N=\ell) \underset{\delta \text{ klein}}{\approx} \mathbb{P}(\text{genau } \ell \text{ der } [t\cdot n]\ E_k \text{ eintreten})$$

$$\underset{\delta \text{ klein}}{\approx} P^{V.}_{n t, \frac{\lambda}{n}}(\ell) \xrightarrow[\substack{n\to\infty \\ (\delta \to 0)}]{} \frac{(\lambda t)^{\ell} e^{-\lambda t}}{\ell!}.$$

Siehe

Satz 14) Sei $\lambda \in (0,\infty)$. Dann,

$$\lim_{n\to\infty} P_{n,\frac{\lambda}{n}}(k) = \frac{\lambda^k e^{-\lambda}}{k!}, \quad k=0,1,2,\dots$$

Beweis: $\forall$ festes k

$$P_{n,\frac{\lambda}{n}}(k) = \frac{n!}{k!(n-k)!}\cdot\left(\frac{\lambda}{n}\right)^k \left(1-\frac{\lambda}{n}\right)^{n-k}$$

$$= \frac{1}{k!}\overbrace{\frac{n(n-1)\cdots(n-k+1)}{n^k}}^{\to 1}\lambda^k \overbrace{\left(1-\frac{\lambda}{n}\right)^n}^{\to e^{-\lambda}} \overbrace{\frac{1}{\left(1-\frac{\lambda}{n}\right)^k}}^{\to 1}$$

$$\xrightarrow[n\to\infty]{} \frac{\lambda^k}{k!} e^{-\lambda}. \qquad \#$$

Bsp.: Nuklear Zerfall mit Aktivität A.

$$\Rightarrow \mathbb{P}(\#\text{ Zerfälle in Zeit } [0,t] = k) = \frac{e^{-At}}{k!}(At)^k, \quad k \geq 0.$$

$\boxed{\text{Aktivität} := \text{Anzahl der Kernzerfälle pro Zeiteinheit.}}$

18. April

1.6) Simulation von Gleichverteilungen.

- Wie simuliert man "Zufallszahlen"?

- Computer können nicht echte Zufallszahlen erzeugen, nur "Pseudozufallszahlen".

- Ein Zufallszahlgenerator gibt eine Folge von ganzen Zahlen $x_1, x_2, \ldots \in \{0, 1, \ldots, m-1\}$, die deterministisch aus ein (oder mehrere) Anfangswert entstehen.

- Typischerweise: $x_{n+1} = f(x_n, x_{n-1}, \ldots, x_{n-k+1})$, $n = k, k+1, \ldots$

  aus Startwerten $x_1, x_2, \ldots, x_k$.

- Welche Startwert? → Computerzeit !
- Ob ein Zufallsgenerator gut oder schlecht ist, wird durch statistischen Test entschieden.

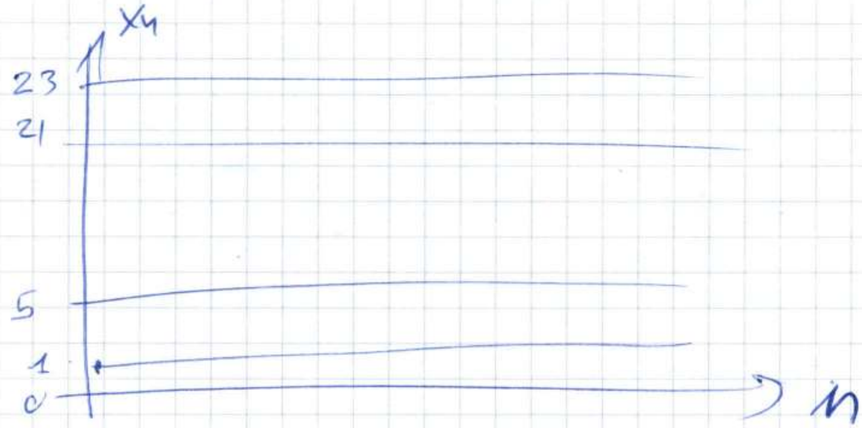
1.6.1) Lineare Kongruenzgeneratoren (LCG)

$$\begin{cases} X_0 \text{ gegeben}; \ a, c, m \in \mathbb{N}. \\ X_{n+1} = (a \cdot x_n + c) \bmod m \end{cases}$$

Beispiele:

	m	a	c
ZX81	$2^{16}+1$	75	0
RANDU	2^{31}	65539 $=2^{16}+3$	0
Marsaglia	2^{32}	69069	1
Langlands	2^{48}	142412, 40584757	11

. Ein schlechtes LCG: ($x_0 = 1$); $a = 4$, $c = 1$, $m = 31$



. $x_1 = f(1) = 5$
. $x_2 = f(5) = 21$
. $x_3 = f(21) = 23$
. $x_4 = f(23) = 0$
. $x_5 = f(0) = 1$

↳ Siehe 03 RandomNumbers.nb

$\Rightarrow$. Mit Anfangswert $x_0 = 1$ hat Periode 5.

. Anzahl von möglichen Zahlen $= m = 31 \gg 5$.

. Wie sollte man $\underline{a}$ und $\underline{c}$ wählen, um Periodizität $< m$ zu vermeiden?

Lemma 15 (Knuth) Die Periode eines LCG ist gleich m $\Leftrightarrow$

ⓐ $\underline{c}$ und $\underline{m}$ sind teilerfremd,
ⓑ jeder Primfaktor von $\underline{m}$ ist ein Teiler von $a-1$,
ⓒ falls 4 teilt m, dann 4 teilt $a-1$.

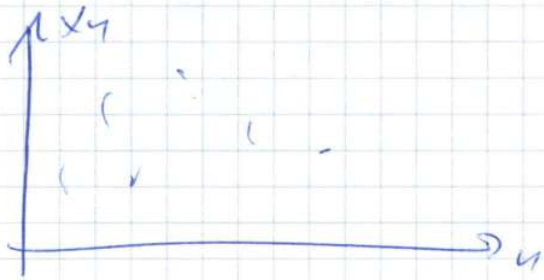
(Ohne Beweis).

Beispiel: ZX81: $m = 2^{16}+1$ ist Primzahl

$\Rightarrow$ (a) ✓.

$\Rightarrow$ (b) ✓. $(m > a)$

$\Rightarrow$ (c) ✓.

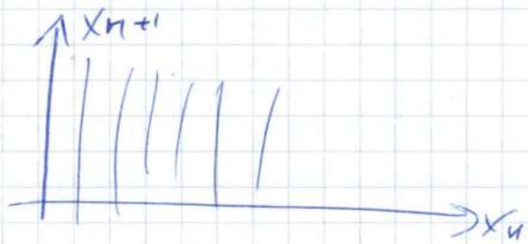


Sieht gut aus.

$\Rightarrow$ Gut wenn man 1 Zahl mit

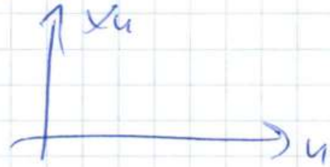
$X_0 = \text{Zeit(von Rechner)} \bmod m$.

Ist es auch gut wenn man eine Folge von Zufallszahlen will?

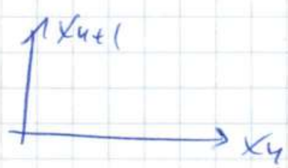


$\hookrightarrow$ Struktur $\Rightarrow$ nicht gut.

Beispiel: RANDU



✓.



✓.

(x_n, x_{n+1}, x_{n+2}): bad (rotate the plot 3D).

Weil: Man kann zeigen, dass

$$x_{n+2} = 6x_{n+1} - 9x_n$$

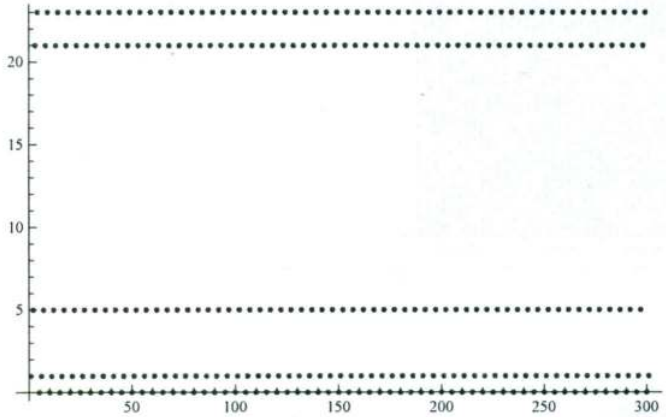
$\Rightarrow$ Starke Korrelationen

29a

```
f[x_] := Mod[a x + c, m]
```

Bad LCG Random generator

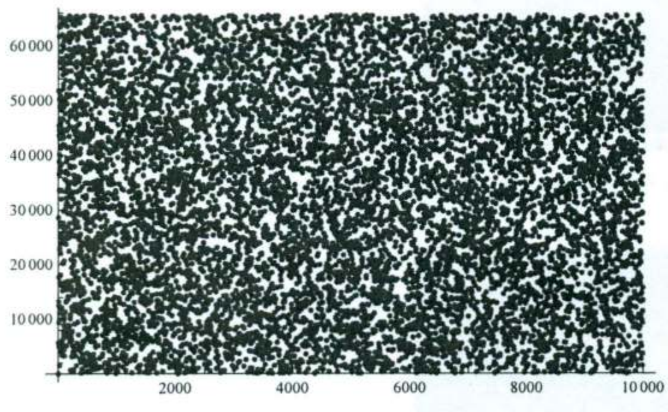
```
a = 4; c = 1; m = 31; x0 = 1;
BadRandom = NestList[f, x0, 300];
ListPlot[BadRandom]
```



ZX81 Generator

```
m = 2^16 + 1; c = 0; a = 75; x0 = 1;
FactorInteger[m]
ZX81Random = NestList[f, x0, 10 000];
ListPlot[ZX81Random]
```

```
{{65 537, 1}}
```

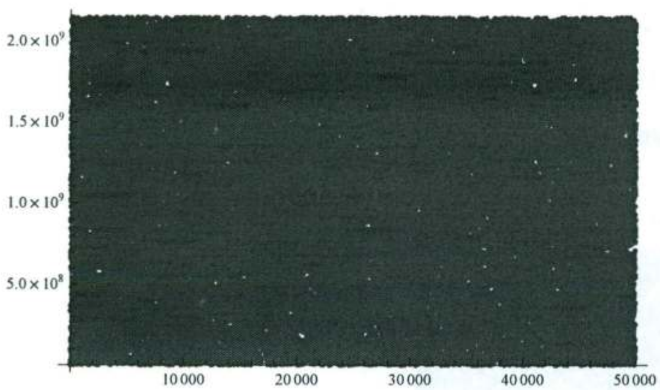


296

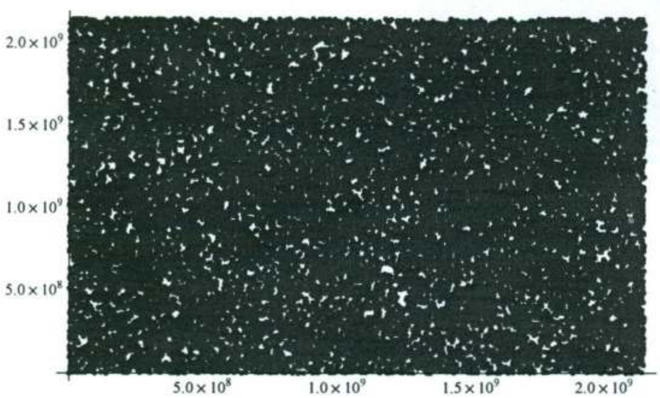
```
blocks = Partition[ZX81Random, 2];
ListPlot[blocks]
```

RANDU

```
m = 2^31 ; c = 0; a = 65539; x0 = 1;
RANDURandom = NestList[f, x0, 50000];
ListPlot[RANDURandom]
```

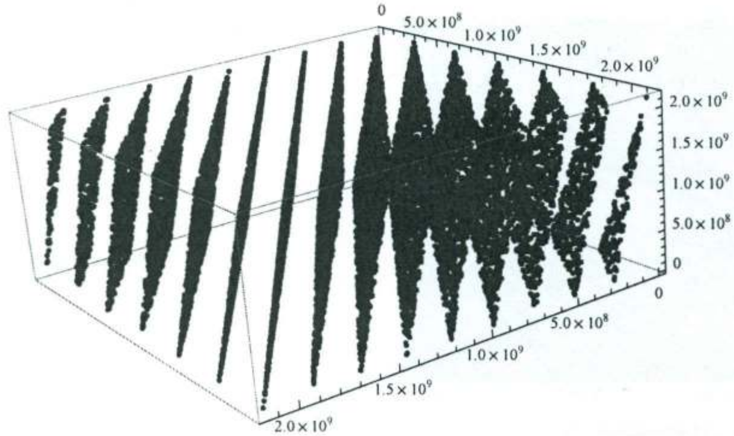


```
blocks = Partition[RANDURandom, 2];
ListPlot[blocks]
```



29c

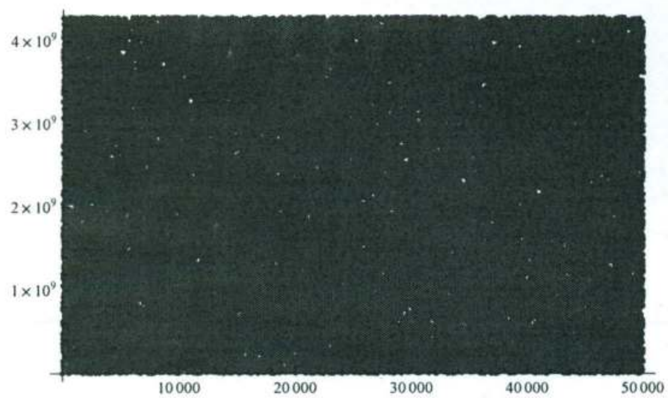
```
blocks3 = Partition[RANDURandom, 3];
ListPointPlot3D[blocks3]
```



Rotate the 3d picture in case you do not see the planes ...

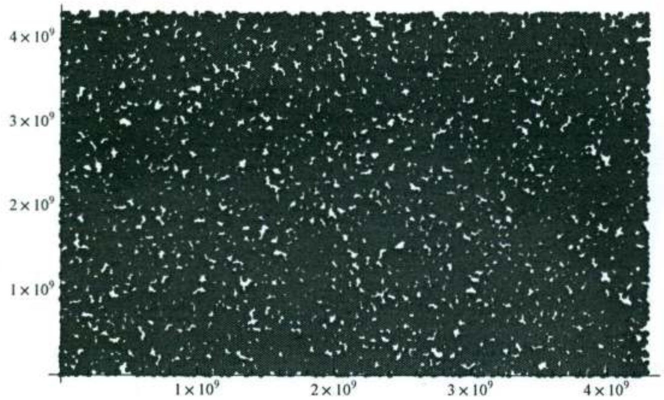
Marsaglia

```
m = 2^32 ; c = 1; a = 69069; x0 = 1;
MarsagliaRandom = NestList[f, x0, 50000];
ListPlot[MarsagliaRandom]
```

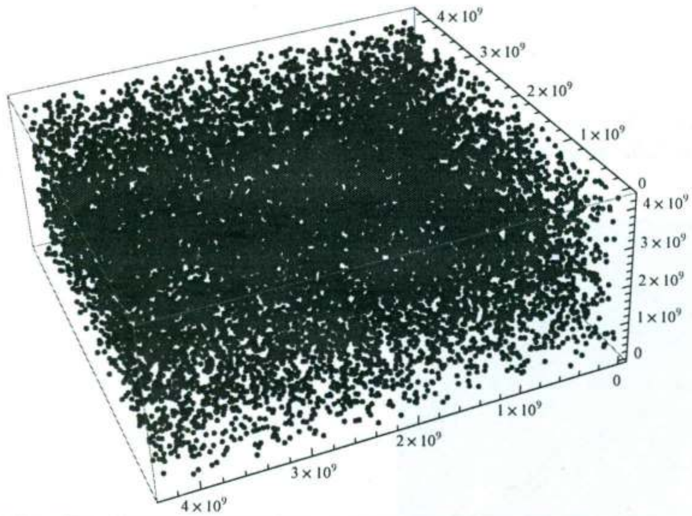


29d

```
blocks = Partition[MarsagliaRandom, 2];
ListPlot[blocks]
```




```
blocks3 = Partition[MarsagliaRandom, 3];
ListPointPlot3D[blocks3]
```



Random Permutations

```
RandomPerm[n_] := Module[{x = Range[n], k, a},
  Do[
    k = RandomInteger[{i, n}];
    a = x[[i]]; x[[i]] = x[[k]]; x[[k]] = a;
    , {i, 1, n - 1}]
   Print[x]
 ]
```

```
RandomPerm[10]
```

```
{8, 4, 5, 3, 7, 6, 9, 10, 2, 1}
```

```
Null^2
```

Beispiel: Marsaglia: Alle 3 Test sind gut.

1.6.2) Zufallszahlen aus $[0,1)$.

- Sei $(x_n)_n$ eine Folge von Pseudozufallszahlen aus $\{0, \dots, m-1\}$.

Dann $\left(U_n := \frac{x_n}{m}\right)_{n \geq 1}$ ist ein Folge von

"Pseudozufallszahlen in $[0,1)$".

1.6.3) Zufallspermutationen.

- Algorithmus: Random Permutation von $\{1, \dots, n\}$.

    - $\sigma_0 = \{1, 2, \dots, n\}$
    - For $i=1$ to $n-1$:
      - { . Choose $k \in \{i, \dots, n\}$ Random; (Gleichverteilt)
      - . $\sigma_i = \tau_{i,k} \circ \sigma_{i-1}$, with $\tau_{i,k}$ = Transposition of (i,k);
      - }

Lemma (6)

- Dieser Algorithmus erzeugt eine zufällige Permutation mit Gleichverteilung.

<u>Beweis:</u> Wir haben eine Gleichverteilung auf $\Omega_n = \{1, 2, \dots, n\} \times \{2, 3, \dots, n\} \times \dots \times \{n-1, n\}$, wobei $\omega = (\omega_1, \dots, \omega_{n-1})$ sind die Zufallszahlen aus dem Algorithmus.

<u>"Zufallsvariable":</u>

$$\sigma(\omega) = \tau_{n-1, \omega_{n-1}} \circ \dots \circ \tau_{1, \omega_1} \circ \begin{pmatrix} 1, 2, \dots, n \\ 1, 2, \dots, n \end{pmatrix}, \text{ mit}$$

- $\tau_{i,j}$ = Transposition von i und j.

<u>Zu zeigen:</u>

- $\sigma : \Omega_n \to S_n'$ ist eine Bijektion.

Dann die Gleichverteilung folgt.

(a) $|\Omega_n| = |S_n| = n!$ ✓.

(b) Seien $\omega \neq \tilde{\omega}$ und $k = \min\{j \mid \omega_j \neq \tilde{\omega}_j\}$.

Dann, $\sigma(\omega)_k \neq \sigma(\tilde{\omega})_k$ (trivial).

$\Rightarrow$ wegen (a) und (b) σ ist eine Bijektion. #

1.7) Erwartungswert und Varianz.

- Jetzt betrachten wir reellwertige (diskrete) Zufallsvariable, d.h., $X: \Omega \to S \subset \mathbb{R}$ (S abzählbar).

- Frage: Wir wollen eine Sorte von Mittelwert definieren, die berücksichtig die W-keit der Ausgänge (von X).
  - Wir fordern:
    - (a) Falls $X(\omega) = a \in S$ $\forall \omega$, dann Mittelwert von X muss gleich a sein.
    - (b) Jedes Ausgang von X muss gewichted bzgl der W-keit.

Definition 17)

Der Erwartungswert von X (bzgl. $\mathbb{P}$) ist definiert durch

$$\mathbb{E}(X) := \sum_{s \in S} s \cdot \mathbb{P}(X = s) \equiv \sum_{s \in S} s \cdot p_X(s).$$

(Er ist wohldefiniert falls $\sum_{s \in S} |s| \cdot p_X(s) < \infty$).

Bemerkung: Nicht alle W-Verteilungen haben endlichen Mittelwert. Als Beispiel, sei X eine ZV auf $\{1, 2, \dots\}$ mit

$$p_X(s) = \frac{(\pi^2/6)^{-1}}{s^2}, \quad s = 1, 2, \dots$$

Dann $\mathbb{E}(X) = \sum_{s \geq 1} s \cdot p_X(s) = \infty$.

<u>Beispiel:</u> <u>Zufallsvariablen mit Werten in $\{0,1\}$</u> (<u>Bernoulli ZV.</u>)

. Sei $A \in \mathcal{F}$ ein Ereignis und

$$X(\omega) := \mathbb{1}_A(\omega) \equiv \begin{cases} 1, & \text{falls } \omega \in A, \\ 0, & \text{falls } \omega \in A^c. \end{cases}$$

Dann $\underline{\mathbb{E}(X) = \mathbb{P}(A)}$.

In der Tat, $\mathbb{E}(X) = 1 \cdot \mathbb{P}(X = 1) + 0 \cdot \mathbb{P}(X=0)$
$= \mathbb{P}(A)$.

<u>Beispiel:</u> <u>(Binomialverteilung)</u>

. Sei X eine ZV. mit

$X \sim Bin(n,p)$ (d.h., mit Verteilung $Bin(n,p)$).

Dann, $\underline{\mathbb{E}(X) = np}$

. In der Tat,

$$\mathbb{E}(X) = \sum_{x=0}^{n} \binom{n}{x} \cdot p^x (1-p)^{n-x} \cdot x.$$

<u>Trick:</u> Aus der Binomialformeln:

$$\sum_{x=0}^{n} \binom{n}{x} p^x q^{n-x} = (p+q)^n$$

Folgt: $p \cdot \frac{d}{dp} \sum_{x=0}^{n} \binom{n}{x} p^x q^{n-x} = \sum_{x=0}^{n} \binom{n}{x} p^x q^{n-x} \cdot x$

$= p \cdot n \cdot (p+q)^{n-1}$.

$$\sum_{x=0}^{n} \binom{n}{x} p^x q^{n-x} x = p \cdot \frac{d}{dp} \sum_{x=0}^{n} \binom{n}{x} p^x \cdot q^{n-x}$$

$$= p \cdot n \cdot (p+q)^{n-1}$$

$\Rightarrow$ Setze dann $q = 1-p \Rightarrow \underline{\mathbb{E}(X) = p \cdot n}$. ✓.

<u>Beispiel</u>: (<u>Poissonverteilung</u>)

. Sei $X \sim Poi(\lambda)$. Dann,

$\underline{\mathbb{E}(X) = \lambda}$.

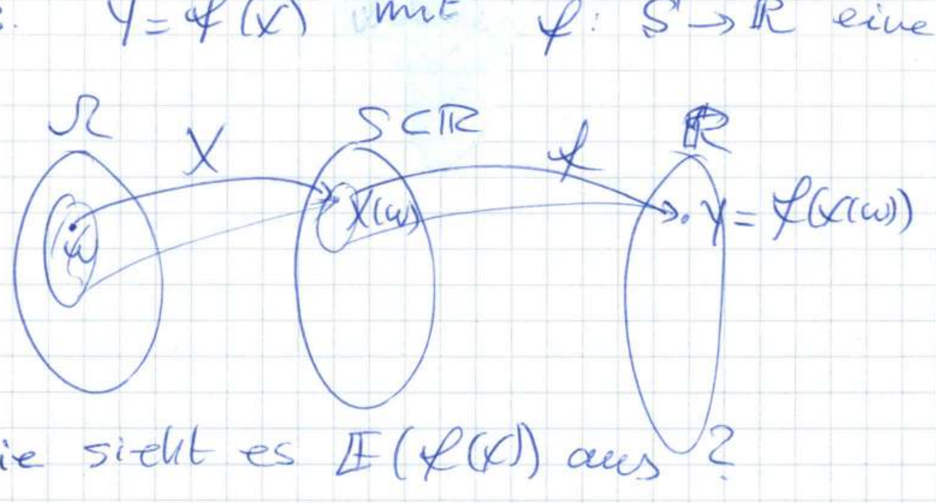
<u>In der Tat</u>: $\mathbb{E}(X) = \sum_{k \geq 0} \frac{e^{-\lambda} \lambda^k}{k!} \cdot k$

$$= \sum_{k \geq 1} \frac{e^{-\lambda} \lambda^{k-1} \cdot \lambda}{(k-1)!} = \lambda.$$

---

20. April

. Wenn wir eine Zufallsvariable X haben, kann man andere ZV aus X definieren, z.B. $Y = f(X)$ mit $f: S \to \mathbb{R}$ eine Funktion.



. Wie sieht es $\mathbb{E}(f(X))$ aus?

Satz 18) Es gilt

$$\mathbb{E}(f(X)) = \sum_{s\in S'} f(s)\cdot \mathbb{P}(X=s)$$

(klar, falls $\sum_{s\in S'} |f(s)|\,\mathbb{P}(X=s) < \infty$; sonst ist nicht wohldefiniert).

Beweis:

$$\mathbb{E}(f(X)) \overset{def}{=} \sum_{y\in f(S')} y\cdot \mathbb{P}(f(X)=y)$$

$$= \sum_{y\in f(S')} y\cdot \mathbb{P}\Big(\bigcup_{s\in f^{-1}(y)} \{X=s\}\Big)$$

$$= \sum_{y\in f(S')} y\cdot \sum_{s\in f^{-1}(y)} \mathbb{P}(X=s)$$

$\{s\in S'\} = \bigcup_{y\in f(S')} \{s\in S' \mid f(s)=y\}$

$$= \sum_{y\in f(S')} \sum_{s\in f^{-1}(y)} \overset{=y}{f(s)}\, \mathbb{P}(X=s)$$

$$= \sum_{s\in S'} f(s)\, \mathbb{P}(X=s).$$

#

- Der Erwartungswert hat eine wichtige Eigenschaft, er ist nämlich Linear.

Satz 19) Seien $X_1 : \Omega \to S_1$ und $X_2 : \Omega \to S_2$ zwei reellwertige Z.V. auf $(\Omega, \mathcal{F}, \mathbb{P})$. Falls $\mathbb{E}(|X_1|) < \infty$, $\mathbb{E}(|X_2|) < \infty$, dann $\forall \lambda_1, \lambda_2 \in \mathbb{R}$,

$$\mathbb{E}(\lambda_1 X_1 + \lambda_2 X_2) = \lambda_1 \mathbb{E}(X_1) + \lambda_2 \mathbb{E}(X_2).$$

Beweis: Sei $f: S_1 \times S_2 \to \mathbb{R}$
$(x_1, x_2) \to \lambda_1 x_1 + \lambda_2 x_2$.

$$\mathbb{E}(\lambda_1 X_1 + \lambda_2 X_2) = \mathbb{E}(f(X_1, X_2))$$
$$= \sum_{\substack{x_1 \in S_1' \\ x_2 \in S_2'}} f(x_1, x_2)\, \mathbb{P}(X_1 = x_1, X_2 = x_2) \quad (*)$$
$$= \sum_{\substack{x_1 \in S_1' \\ x_2 \in S_2'}} (\lambda_1 x_1 + \lambda_2 x_2)\, \mathbb{P}(X_1 = x_1, X_2 = x_2)$$

$\{X_1 = x_1\} = \bigcup_{x_2 \in S_2'} \{X_1 = x_1, X_2 = x_2\}$ disjunkt

$$= \lambda_1 \sum_{x_1 \in S_1'} x_1 \cdot \Big(\sum_{x_2 \in S_2'} \mathbb{P}(X_1 = x_1, X_2 = x_2) \Big)$$
$$+ \lambda_2 \sum_{x_2 \in S_2'} x_2 \cdot \Big(\sum_{x_1 \in S_1'} \mathbb{P}(X_1 = x_1, X_2 = x_2) \Big)$$
$$= \lambda_1 \cdot \sum_{x_1 \in S_1'} x_1 \, \mathbb{P}(X_1 = x_1) + \lambda_2 \cdot \sum_{x_2 \in S_2'} x_2 \, \mathbb{P}(X_2 = x_2)$$
$$= \lambda_1 \cdot \mathbb{E}(X_1) + \lambda_2 \cdot \mathbb{E}(X_2).$$

Die Summe $(*)$ konvergiert absolut, weil wegen $|\lambda_1 x_1 + \lambda_2 x_2| \leq |\lambda_1| \cdot |x_1| + |\lambda_2| \cdot |x_2|$ erhält man

$$|\mathbb{E}(\lambda_1 X_1 + \lambda_2 X_2)| \leq \underbrace{|\lambda_1| \cdot \mathbb{E}(|X_1|) + |\lambda_2| \cdot \mathbb{E}(|X_2|)}_{< \infty \text{ nach Voraussetzung}}. \quad \#$$

- Die 2. Eigenschaft ist Monotonie.

Korollar 19) Seien X_1 und X_2 wie im Satz 18.
Dazu, sei $\forall \omega \in \Omega$,
$$X_1(\omega) \leq X_2(\omega).$$
Dann, $\mathbb{E}(X_1) \leq \mathbb{E}(X_2)$.

Beweis: Da $X_2(\omega) - X_1(\omega) \geq 0$,

$\mathbb{E}(X_2 - X_1) \geq 0$ und wegen Linearität,

$$0 \leq \mathbb{E}(X_2 - X_1) = \mathbb{E}(X_2) - \mathbb{E}(X_1). \quad \#$$

Beispiel: Seien $A_1, \dots, A_n \in \mathcal{F}$ Ereignisse mit $\mathbb{P}(A_k) = p$, $k = 1, \dots, n$.

- Setze: $X_k = \mathbb{1}_{A_k}$, $k = 1, \dots, n$.

Dann $X_k \sim \text{Bernoulli}(p)$ $\quad (\mathbb{E}(X_k) = p)$

und $S_n := \sum_{k=1}^{n} X_k$ hat

Erwartungswert

$$\mathbb{E}(S_n) \underset{\substack{\uparrow \\ \text{Linearität}}}{=} \sum_{k=1}^{n} \mathbb{E}(X_k) = n \cdot p.$$

- Das verallgemeinert den Fall, dass $A_1, \dots, A_n$ unabhängig sind, wo $S_n \sim \text{Bin}(n, p)$.

Frage: Wie kann man sehen ob eine Summe von Bernoulli(p) Z.V. ist unabhängig oder nicht?

(Teilantwort):

- Es gibt andere Grössen, die man betrachten kann, wie die Varianz, die eine Messung der Streuung bzgl. den Erwartungswert ist.

Def. 20) Sei X eine reellwertige Z-V. auf $(\Omega, \mathcal{F}, \mathbb{P})$ mit $\mathbb{E}(X^2) < \infty$.
Dann, definiert man die Varianz von X (bzgl. $\mathbb{P}$) als

$$Var(X) := \mathbb{E}\left((X - \mathbb{E}(X))^2 \right).$$

Bemerkung: (Übung)

ⓐ $Var(X) \geq 0$ und $Var(X) = 0 \Leftrightarrow \mathbb{P}(X = \mathbb{E}(X)) = 1$,
d.h., X ist eine Konstante.

ⓑ Wegen Linearität von $\mathbb{E}$:

$$Var(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2.$$

und

$$Var(\lambda X) = \lambda^2 Var(X).$$

ⓒ Wenn $X_1, \dots, X_n$ unabhängig sind, dann

$$Var(X_1 + \dots + X_n) = Var(X_1) + \dots + Var(X_n)$$

Beispiel:

ⓐ $X \sim$ Bernoulli(p)

$\Rightarrow \mathbb{E}(X) = p$, $Var(X) = p(1-p)$

ⓑ $X \sim$ Binomial(n,p):

$\Rightarrow \mathbb{E}(X) = n \cdot p$, $Var(X) = np(1-p)$

ⓒ $X \sim Poi(\lambda)$:

$\Rightarrow \mathbb{E}(X) = \lambda$, $Var(X) = \lambda$.

Rechnungen: (a) $X \sim$ Bernoulli(p).

$$Var(X) = \sum_{k=0}^{1} k^2 \, \mathbb{P}(X=k) - (\mathbb{E}(X))^2$$

$$= p - p^2 = p(1-p)$$

(b) $X \sim$ Binomial(n, p).

Methode 1: $Var(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2$

mit $\mathbb{E}(X) = n \cdot p$

und $\mathbb{E}(X^2) = \sum_{k=0}^{n} k^2 \binom{n}{k} p^k (1-p)^{n-k}$

aber $\sum_{k=0}^{n} k^2 \binom{n}{k} p^k q^{n-k} =$

$$= \sum_{k=0}^{n} k(k-1) \binom{n}{k} p^k q^{n-k} + \sum_{k=0}^{n} k \binom{n}{k} p^k q^{n-k}$$

$$= p^2 \frac{d^2}{dp^2} \Big(\overbrace{\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k}}^{=(p+q)^n} \Big) + p \frac{d}{dp} \Big(\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \Big)$$

$$= p^2 \cdot n(n-1) \cdot (p+q)^{n-2} + p \cdot n \cdot (p+q)^{n-1}$$

Mit $q = 1-p$
$\Rightarrow \mathbb{E}(X^2) = n(n-1)p^2 + np = n^2p^2 + np(1-p)$.

$\Rightarrow Var(X) = np(1-p)$.

Methode 2: $X = \sum_{i=1}^{n} Y_i$ mit $Y_i \sim$ Bernoulli(p).

$\Rightarrow$ Wegen Eigenschaft (c),
$Var(X) = n \cdot Var(Y_1) = np(1-p)$.

• <u>Anwendung</u>: Beweis von Einschluss/Ausschlussprinzip:

$$\mathbb{P}(A_1 \cup \dots \cup A_n) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \mathbb{P}(A_{i_1} \cap \dots \cap A_{i_k}).$$

• Fangen wir an mit

$$\begin{aligned}
\mathbb{P}\left((A_1 \cup \dots \cup A_n)^c\right) &= \mathbb{P}(A_1^c \cap \dots \cap A_n^c) \\
&= \mathbb{E}\left(\mathbb{1}_{A_1^c \cap \dots \cap A_n^c}\right) \\
&= \mathbb{E}\left(\mathbb{1}_{A_1^c} \cdots \mathbb{1}_{A_n^c}\right) \\
&= \mathbb{E}\left((1 - \mathbb{1}_{A_1}) \cdots (1 - A_n)\right) \\
&\overset{\text{lin.}}{=} \sum_{k=0}^{n} (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} \underbrace{\mathbb{E}\left(\mathbb{1}_{A_{i_1}} \cdots \mathbb{1}_{A_{i_k}}\right)}_{\substack{= \mathbb{E}(\mathbb{1}_{A_{i_1} \cap \dots \cap A_{i_k}}) \\ = \mathbb{P}(A_{i_1} \cap \dots \cap A_{i_k})}} \\
&= \sum_{k=0}^{n} (-1)^k \cdot \sum_{1 \leq i_1 < \dots < i_k \leq n} \mathbb{P}(A_{i_1} \cap \dots \cap A_{i_k})
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \mathbb{P}(A_1 \cup \dots \cup A_n) &= 1 - \mathbb{P}\left((A_1 \cup \dots \cup A_n)^c\right) \\
&= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \mathbb{P}(A_{i_1} \cap \dots \cap A_{i_k}).
\end{aligned}$$