

Die Laufzeit von randomisierten (zufallsgesteuerten) Algorithmen hängt von gewissen zufälligen Ereignissen ab (Beispiel Quicksort).

Um die Laufzeiten dieser Algorithmen untersuchen zu können, studieren wir im Folgenden „zufällige“ Ereignisse oder Prozesse und die Grundlagen der Wahrscheinlichkeitstheorie.

Erwartete Laufzeiten

Was benötigen wir dafür?

Was ist wie wahrscheinlich?

» eine **Menge von Ereignissen**

Wie wahrscheinlich ist etwas?

» ein **Maß** für die Wahrscheinlichkeit eines Ereignisses

Wie kann ich mit Wahrscheinlichkeiten rechnen?

» einige **Rechenregeln** für diese Wahrscheinlichkeiten

Beispiel [1]:

Wir betrachten einen Wurf mit einem Würfel. Nach der Landung des Würfels sehen wir auf der Oberseite des Würfels 1, 2, 3, 4, 5 oder 6 Punkte.

Die **Menge von Ereignissen** (möglichen Resultaten) ist

$$S = \{1, 2, 3, 4, 5, 6\}$$

Falls es sich um einen fairen Würfel handelt, erscheint jede der sechs Zahlen mit der gleichen „**Wahrscheinlichkeit**“ (**WSK**).

Beispiel [2]:

Wir betrachten das Beispiel Münzwurf. Nach der Landung der Münze sehen wir entweder die eine Seite der Münze (K = Kopf) oder die andere Seite (Z = Zahl).

Die **Menge von Ereignissen** (möglichen Resultaten) ist

$$S = \{K, Z\}$$

Falls es sich bei der Münze um eine faire Münze handelt, erscheinen Kopf und Zahl mit der gleichen Wahrscheinlichkeit.

Definition [1]:

Sei S eine endliche Menge und sei p eine reellwertige Funktion:
 (S, p) heißt ein **Wahrscheinlichkeitsraum**, wenn die folgenden Axiome (Kolmogorov'sche Axiome) erfüllt sind:

$$1. \quad p(A) \geq 0 \quad \forall A \subseteq S$$

$$2. \quad p(S) = 1$$

3. σ -Additivität: Sind die Mengen A_i , $i \in \mathbb{N}$, paarweise disjunkt, so gilt:

$$p\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} p(A_i)$$

- Die endliche Menge S heißt der **Ereignisraum**.
- Die Funktion p heißt die **Wahrscheinlichkeitsverteilung**.
- Eine Teilmenge $A \subseteq S$ heißt eine **Ereignis** (event).
- Enthält A genau ein Element s der Menge S , so sprechen wir von einem **Elementarereignis s** .
- Sind alle Elementarereignisse gleich wahrscheinlich, so sprechen wir von einem **fairen Zufallsexperiment**.

Fortsetzung Beispiel [1]: Würfel

$$S = \{1,2,3,4,5,6\}$$

Falls es sich um einen fairen Würfel handelt, erscheint jede der sechs Zahlen mit der gleichen WSK.

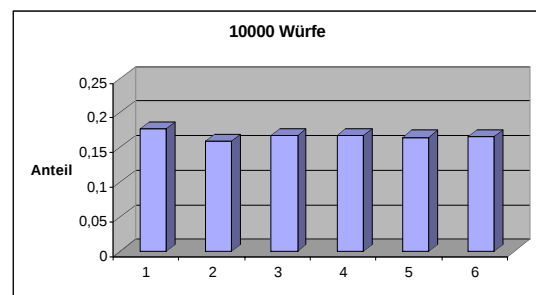
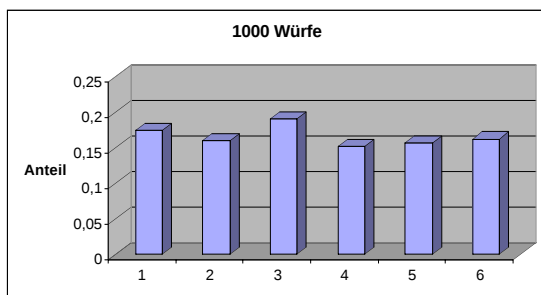
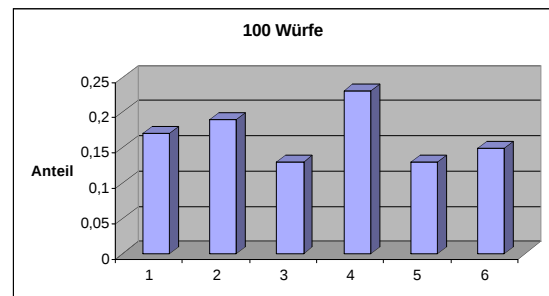
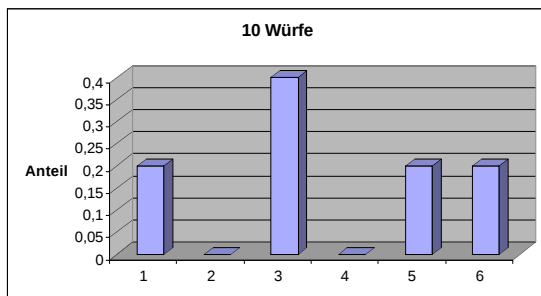
$$p(S) = \sum_{i=1}^6 p(i) = 6 * p(j) = 1 \quad \forall j \in \{1,2,3,4,5,6\}$$

Dann gilt:

$$p(1) = p(2) = p(3) = p(4) = p(5) = p(6) = \frac{1}{6}$$

(S, p) ist ein WSKraum mit Ereignisraum $S = \{1,2,3,4,5,6\}$ und WSKsverteilung p.

Wahrscheinlichkeitsrechnung



Fortsetzung Beispiel [1]:

Für jede Teilmenge $A \subseteq S$ gilt nach der Definition eines WSKsraums (S, p) :

$$p(A) = \sum_{s \in A} p(s)$$

Wir betrachten nun das Ereignis, dass bei einem Wurf mit dem Würfel entweder 1, 2 oder 6 gewürfelt wird:

$$A = \{1, 2, 6\} = \{1\} \cup \{2\} \cup \{6\} \subseteq S$$

$$\begin{aligned} p(A) &= p\left(\bigcup_{s \in A} \{s\}\right) = \sum_{s \in A} p(s) = \sum_{s \in \{1, 2, 6\}} p(s) \\ &= p(1) + p(2) + p(6) = 3 \cdot \frac{1}{6} = \frac{1}{2} \end{aligned}$$

Das Ereignis A tritt dann auf, wenn das Resultat des zufälligen Prozesses ein in A enthaltenes Elementarereignis ist.

Fortsetzung Beispiel [2]:

Wir betrachten das Beispiel Münzwurf. Nach der Landung der Münze sehen wir entweder die eine Seite der Münze (K = Kopf) oder die andere Seite (Z = Zahl).

$$S = \{K, Z\}$$

Falls es sich bei der Münze um eine faire Münze handelt, erscheinen Kopf und Zahl mit der gleichen Wahrscheinlichkeit.

$$p(S) = p(K) + p(Z) = 1$$

Hieraus folgt:

$$p(K) = p(Z) = \frac{1}{2}$$

(S, p) ist ein Wahrscheinlichkeitsraum mit Ereignisraum $S = \{K, Z\}$ und Wahrscheinlichkeitsverteilung p .

Seien A und B zwei Teilmengen von S

$$\begin{aligned} p(A \cup B) &= p\left(\bigcup_{s \in A \cup B} \{s\}\right) = \sum_{s \in A \cup B} p(s) \\ &= \sum_{s \in A} p(s) + \sum_{s \in B} p(s) - \sum_{s \in A \cap B} p(s) \\ &= p(A) + p(B) - p(A \cap B) \end{aligned}$$

Definition [2]:

Seien A und B Ereignisse mit $p(B) \neq 0$. Wir definieren die **bedingte Wahrscheinlichkeit $P(A|B)$** von A unter der Bedingung (Hypothese) B als

$$p(A|B) = \frac{p(A \cap B)}{p(B)}$$

Die bedingte WSK $p(A|B)$ ist die WSK,

- dass ein Elementarereignis $s \in A$ eintritt, unter der Annahme,
- dass die Hypothese B wahr ist, d.h., dass das eintretende Elementarereignis s mit Sicherheit ein Elementarereignis von B ist.

Ist der Durchschnitt $A \cap B$ der Ereignisse A und B leer, so ist $p(A|B) = 0$.

Ist B in A enthalten, so ist $p(A|B) = 1$.

Fortsetzung von Beispiel [1]:

Ein Wurf mit einem Würfel. $A = \{1, 2, 3\}$ und $B = \{3, 4, 5\}$.

$$p(A|B) = \frac{p(3)}{p(\{3, 4, 5\})} = \frac{1}{3}$$

Sei $A \subseteq S$ ein Ereignis. A^C ist das **komplementäre Ereignis**.

$$A^C = S \setminus A = \{s \in S \mid s \notin A\}$$

Satz [1] (Bayes'sche Regel):

Seien A und B Ereignisse mit den folgenden Eigenschaften:

$$p(A) \neq 0 \quad p(B^C) \neq 0 \quad p(B) \neq 0$$

Dann gilt:

$$p(B|A) = \frac{p(B)p(A|B)}{p(B)p(A|B) + p(B^C)p(A|B^C)}$$

Beweis:

$$p(B)p(A|B) = p(B) \frac{p(A \cap B)}{p(B)} = p(A \cap B) \quad \text{und}$$

$$p(B)p(A|B) + p(B^C)p(A|B^C) = p(A \cap B) + p(A \cap B^C) = p(A)$$



Beispiel [3]:

Gegeben eine faire Münze und eine gefälschte Münze, die immer Kopf zeigt. Wir wählen eine der beiden Münzen mit Wahrscheinlichkeit $\frac{1}{2}$ und werfen diese Münze zweimal.

A = zwei Köpfe beobachtet

B = gefälschte Münze gewählt

$$p(A) = p(B)p(A|B) + p(B^C)p(A|B^C) \quad p(B) = \frac{1}{2}$$

$$p(A|B) = 1 \quad p(A|B^C) = \frac{1}{4} \quad p(A) = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}$$

$$p(B|A) = \frac{p(B)p(A|B)}{p(B)p(A|B) + p(B^C)p(A|B^C)} = \frac{1/2 * 1}{1/2 * 1 + 1/2 * 1/4} = \frac{4}{5}$$

Beispiel [4]:

Wir werfen eine faire Münze n mal. Das Resultat von n Würfeln ist eine Folge der Länge n der folgenden Form:

$KZZKKKZKZK...ZZKZKK$

$$S = \{K, Z\}^n$$

Wie viele verschiedene Elementarereignisse (Folgen von Ks und Zs der Länge n) gibt es?

$$\#S = 2^n$$

Jedes Elementarereignis $s \in S$ tritt mit der gleichen WSK auf:

$$p(s) = \frac{1}{2^n}$$

Es gilt dann:

$$p(S) = \sum_{s \in S} p(s) = 2^n \frac{1}{2^n} = 1$$

Geordnete Stichproben mit Zurücklegen:

- Gegeben eine Urne mit n Kugeln, die von 1 bis n nummeriert sind.
- Wir ziehen k Kugeln nacheinander aus der Urne, wobei die gezogene Kugel wieder zurückgelegt wird.
- “Geordnet” bedeutet, dass die Reihenfolge der Ziehungen berücksichtigt wird:

$$3, 5, 3 \neq 3, 3, 5$$

- Es gibt

$$n^k$$

verschiedene geordnete Stichproben mit Zurücklegen.

Geordnete Stichproben ohne Zurücklegen:

- Gegeben eine Urne mit n Kugeln, die von 1 bis n nummeriert sind.
- Wir ziehen k Kugeln nacheinander aus der Urne, wobei die gezogene Kugel **nicht** wieder zurückgelegt wird.
- “Geordnet” bedeutet, dass die Reihenfolge der Ziehungen berücksichtigt wird:

$$3, 5, 1 \neq 1, 3, 5$$

- Es gibt

$$n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1) = n! / (n-k)!$$

geordnete Stichproben ohne Zurücklegen.

Ungeordnete Stichproben ohne Zurücklegen:

- Gegeben eine Urne mit n Kugeln, die von 1 bis n nummeriert sind.
- Wir ziehen k Kugeln nacheinander aus der Urne, wobei die gezogene Kugel **nicht** wieder zurückgelegt wird.
- “**Ungeordnet**” bedeutet, dass die Reihenfolge der Ziehungen **nicht** berücksichtigt wird:

$$3, 5, 1 = 1, 3, 5$$

Ungeordnete Stichproben ohne Zurücklegen:

- Es gibt

$$n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1) = n! / (n-k)!$$
 geordnete Stichproben ohne Zurücklegen.
- Da wir die Reihenfolge der Ziehungen nicht berücksichtigen dürfen, müssen wir die obige Größe durch die Zahl $k!$ der möglichen Reihenfolgen von k Elementen dividieren:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Binomialkoeffizient von n über k .

Definition [3]:

Gegeben ein WSKraum (S, p) . Eine Funktion, die jedem Elementar-

$$X : S \rightarrow \mathfrak{R}$$

ereignis $s \in S$ eine reelle Zahl zuordnet, heißt **Zufallsvariable**.

Mittels Zufallsvariablen kann man zum Beispiel jedem Elementarereignis s Kosten zuordnen, die durch das zufällige „Auftreten“ von s verursacht werden. Im Folgenden werden wir oft Zufallsvariablen betrachten, deren Kosten den „Laufzeiten“ von Algorithmen (mit einer Zufallskomponente) entsprechen.

Für ein vorgegebenes $x \in \mathfrak{R}$ betrachten wir häufig die Menge:

$$\{s \in S \mid X(s) = x\}$$

Als Kurzschreibweise für diese Menge verwenden wir

$$\{X = x\}$$

Beispiel [5]:

Wir werfen zweimal hintereinander mit einem Würfel. Die Elementarereignisse sind Paare (a,b) mit $a,b \in \{1,2,3,4,5,6\}$. Die „Kosten“ $X(s)$ eines Elementarereignisses $s = (a,b)$ sind gleich der Summe $a+b$ der Augenzahlen.

$$X(s = (a,b)) = a + b \quad p(s = (a,b)) = \frac{1}{36}$$

Definition [4]:

Gegeben ein WSKraum (S, p) und eine Zufallsvariable $X: S \rightarrow \mathbb{R}$.
Der **Erwartungswert der Zufallsvariablen** X ist definiert als:

$$E[X] = \sum_{s \in S} p(s)X(s)$$

Repräsentiert die Zufallsvariable X eine Art Kostenfunktion, so kann der Erwartungswert als die (mittleren) zu erwartenden Kosten interpretiert werden. Siehe Beispiel [4]:

Beispiel [5]:

Wir werfen zweimal hintereinander mit einem Würfel. Die Elementarereignisse sind Paare (a, b) mit $a, b \in \{1, 2, 3, 4, 5, 6\}$. Die „Kosten“ $X(s)$ eines Elementarereignisses $s = (a, b)$ seien gleich der Summe $a + b$ der Augenzahlen.

$$X(s = (a, b)) = a + b \quad p(s = (a, b)) = \frac{1}{36}$$

$$\begin{aligned} E[X] &= \sum_{s \in S} p(s)X(s) \\ &= \sum_{s \in S} \frac{1}{36} X(s) = \frac{1}{36} \sum_{s \in S} X(s) \\ &= \frac{1}{36} \sum_{a=1}^6 \sum_{b=1}^6 (a + b) \\ &= \frac{1}{36} \sum_{a=1}^6 (6a + \sum_{b=1}^6 b) = \frac{1}{36} \sum_{a=1}^6 (6a + 21) \\ &= \frac{12 \cdot 21}{36} = \frac{12 \cdot 7}{12} = 7 \end{aligned}$$

$X(s) = a + b = k$	2	3	4	5	6	7	8	9	10	11	12
$p(\{X=k\})$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

Man beachte:

$$E[X] = \sum_{s \in S} p(s)X(s) = \sum_{k \in X(S)} p(\{X = k\}) * k$$

Fortsetzung von Beispiel [4]: Wir werfen eine faire Münze n mal.

Die Zufallsvariable X ordnet einem Elementarereignis $s \in S = \{K, Z\}^n$ die Anzahl der Würfe mit Resultat Kopf in s zu.

a) Jedes Elementarereignis $s \in S = \{K, Z\}^n$ hat WSK $2^{-n} = 1/2^n$.

b) Wie viele Elementarereignisse gibt es, die genau an k „Positionen“ „Kopf“ zeigen ?

Ungeordnete Stichprobe ohne Zurücklegen! $\binom{n}{k}$

c) Wie groß ist die WSK, dass man genau k Köpfe in einer Folge von n Würfeln erhält?

$$p(\{X = k\}) = \binom{n}{k} 2^{-n}$$

d) Welchen Wert hat der Erwartungswert $E[X]$ von X ?

$$\begin{aligned}
 E[X] &= \sum_{k=0}^n \binom{n}{k} 2^{-n} k & k \binom{n}{k} &= n \binom{n-1}{k-1} \\
 &= \sum_{k=1}^n \binom{n-1}{k-1} n 2^{-n} \\
 &= \sum_{k=0}^{n-1} \binom{n-1}{k} n 2^{-n} \\
 &= n 2^{-n} \sum_{k=0}^{n-1} \binom{n-1}{k} = n 2^{-n} 2^{n-1} = \frac{n}{2}
 \end{aligned}$$

Satz[2]:

Seien X und Y Zufallsvariablen über dem gleichen Ereignisraum S , dann gilt:

$$E[X + Y] = E[X] + E[Y]$$

Beweis:

$$\begin{aligned}
 E[X + Y] &= \sum_{s \in S} p(s)(X + Y)(s) = \sum_{s \in S} p(s)(X(s) + Y(s)) \\
 &= \sum_{s \in S} p(s)X(s) + \sum_{s \in S} p(s)Y(s) = E[X] + E[Y]
 \end{aligned}$$



Beispiel [5]: 2 Würfe mit einem Würfel (Elementarereigniss = EE)

$X: S \rightarrow \mathbb{R}$ bildet ein EE auf die Augensumme ab.

$X_1: S \rightarrow \mathbb{R}$ bildet ein EE auf die Augenzahl des ersten Wurfes ab.

$X_2: S \rightarrow \mathbb{R}$ bildet ein EE auf die Augenzahl des zweiten Wurfes ab.

$$X = X_1 + X_2 \quad \Rightarrow \quad E[X] = E[X_1 + X_2] = E[X_1] + E[X_2] = 3.5 + 3.5 = 7$$

Fortsetzung Beispiel [4]: n Würfe mit einer fairen Münze:

$$X_i = \begin{cases} 1 & \text{falls } i\text{-ter Wurf Kopf} \\ 0 & \text{falls } i\text{-ter Wurf Zahl} \end{cases} \longrightarrow \begin{cases} E[X_i] = \frac{1}{2} \\ \text{für alle } i \in \{1, \dots, n\} \end{cases}$$

$$X = X_1 + X_2 + \dots + X_n \longrightarrow E[X] = n/2$$

Vorsicht: Im allgemeinen ist $E[XY] \neq E[X]E[Y]$. Es gibt jedoch Ausnahmen:

Definition [5]:

Zwei Zufallsvariablen X und Y über dem gleichen Ereignisraum heißen unabhängig, wenn für alle $x, y \in \mathfrak{R}$ gilt:

$$p(\{X = x\} \wedge \{Y = y\}) = p(\{X = x\}) * p(\{Y = y\})$$

Satz [3]:

Wenn X und Y unabhängig sind, dann gilt: $E[XY] = E[X]E[Y]$.

Beweis:

$$\begin{aligned} E[XY] &= \sum_{s \in \mathfrak{S}} p(s)(XY)(s) \\ &= \sum_{z \in \mathfrak{R}} p(\{XY = z\})z \\ &= \sum_{z \in \mathfrak{R}} \sum_{x,y; xy=z} p(\{X = x\} \wedge \{Y = y\})xy \\ &= \sum_{x,y} p(\{X = x\} \wedge \{Y = y\})xy \end{aligned}$$

$$\begin{aligned}
&= \sum_{x,y} p(\{X = x\}) * p(\{Y = y\})xy \\
&= \sum_x p(\{X = x\})x \sum_y p(\{Y = y\})y \\
&= E[X]E[Y]
\end{aligned}$$

**Definition [6]:**

Sei X eine Zufallsvariable. Dann heißt $\text{Var}[X] := E[(X - E[X])^2]$ die Varianz von X . Die positive Wurzel der Varianz heißt Standardabweichung und wird mit σ bezeichnet.

Fortsetzung Beispiel [4]: n Würfe mit einer fairen Münze.

$X_i = 1$, falls der i -te Wurf gleich Kopf ist, und 0 sonst.

$$\text{Var}[X_i] = \frac{1}{2} \left(1 - \frac{1}{2}\right)^2 + \frac{1}{2} \left(0 - \frac{1}{2}\right)^2 = \frac{1}{4}$$

Lemma [1]:

$$\text{Var}[X] = E[X^2] - (E[X])^2$$

Beweis:

$$\begin{aligned}
E[(X - E[X])^2] &= E[X^2 - 2E[X]X + (E[X])^2] \\
&= E[X^2] - 2E[X]E[X] + (E[X])^2 \\
&= E[X^2] - (E[X])^2
\end{aligned}$$



Satz [4]:

Wenn X und Y unabhängig sind, dann ist $\text{Var}[X+Y] = \text{Var}[X] + \text{Var}[Y]$.

Beweis:

$$\begin{aligned}
 \text{Var}[X + Y] &= E[(X + Y)^2] - (E[X + Y])^2 \\
 &= E[X^2 + 2XY + Y^2] - (E[X] + E[Y])^2 \\
 &= E[X^2] + 2E[XY] + E[Y^2] - (E[X])^2 - 2E[X]E[Y] - (E[Y])^2 \\
 &= E[X^2] - (E[X])^2 + E[Y^2] - (E[Y])^2 + 2E[XY] - 2E[X]E[Y] \\
 &\quad \boxed{\text{Satz[3]: } X \text{ und } Y \text{ unabhängig}} \\
 &= E[X^2] - (E[X])^2 + E[Y^2] - (E[Y])^2 + 2E[X]E[Y] - 2E[X]E[Y] \\
 &\quad \boxed{\text{Lemma [1]}} = \text{Var}[X] + \text{Var}[Y]
 \end{aligned}$$

**Fortsetzung von Beispiel [4]:**

n Würfe mit einer fairen Münze.

Sei $X = X_1 + X_2 + \dots + X_n$ die Zahl der Köpfe.

Da die Zufallsvariablen X_i sind unabhängig, gilt:

$$\text{Var}[X] = \sum_{i=1}^n \text{Var}[X_i] = \sum_{i=1}^n \frac{1}{4} = \frac{n}{4}$$

Satz [5] (Markow Ungleichung):

Sei X eine nicht-negative Zufallsvariable. Dann gilt für alle Konstanten $t \geq 1$:

$$p(\{X \geq t * E[X]\}) \leq \frac{1}{t}$$

Beweis:

$$\begin{aligned} E[X] &= \sum_{s \in S} p(s) * X(s) \geq \sum_{s \in S, X(s) \geq tE[X]} p(s) * X(s) \\ &\geq \sum_{s \in S, X(s) \geq tE[X]} p(s) * t * E[X] \\ &= t * E[X] \sum_{s \in S, X(s) \geq tE[X]} p(s) \\ &= t * E[X] * p(\{X \geq t * E[X]\}) \end{aligned}$$

Bemerkung:

Die obige Abschätzung ist sehr schwach. Wenn man etwas über die Varianz weiß, dann kann man bessere Abschätzungen erhalten.

Satz [6] (Chebychev Ungleichung):

$$\begin{aligned} p(\{|X - E[X]| \geq t\}) &\leq \frac{\text{Var}[X]}{t^2} \\ \text{oder} \\ p(\{|X - E[X]| \geq t * \sqrt{\text{Var}[X]}\}) &\leq \frac{1}{t^2} \end{aligned}$$

Beweis:

$$\begin{aligned} \text{Var}[X] &= E[(X - E[X])^2] = \sum_{s \in S} p(s)(X(s) - E[X])^2 \\ &= \sum_{s \in S} p(s)(X(s) - E[X])^2 \\ &\geq \sum_{s \in S, |X(s) - E[X]| \geq t} p(s) * t^2 = t^2 \sum_{s \in S, |X(s) - E[X]| \geq t} p(s) \\ &= t^2 p(\{|X - E[X]| \geq t\}) \end{aligned}$$

Fortsetzung Beispiel [4]: n Würfe mit einer fairen Münzen

Für die Anzahl X der Köpfe gilt: $E[X] = n/2$ und $\text{Var}[X] = n/4$

Damit ist $\sigma = (n/4)^{1/2}$ und daher gilt für $t = 10$:

$$p(\{|X - \frac{n}{2}| \geq 5\sqrt{n}\}) \leq \frac{1}{100}$$

Daher ist X mit Wahrscheinlichkeit $1 - (1/100)$ in dem folgenden Intervall:

$$X \in \left[\frac{n}{2} - 5\sqrt{n}, \frac{n}{2} + 5\sqrt{n} \right]$$

Satz [7] (Chernoff Schranke):

Sei X die Anzahl der Köpfe in n Würfeln einer fairen Münze und sei $\varepsilon \geq 0$. Dann gilt:

$$p(\{|X - \frac{n}{2}| \geq \varepsilon * \frac{n}{2}\}) \leq 2 * e^{-\varepsilon^2 \frac{n}{4}}$$

Beweis: Buch von Motwani/Ragharan über Randomized Algorithms. ■

Fortsetzung von Beispiel [4]: (n faire Münzen) Für $\varepsilon = 10/(n)^{1/2}$

$$p(\{|X - \frac{n}{2}| \geq 5\sqrt{n}\}) \leq 2 * e^{-25}$$

Diese Abschätzung ist erheblich stärker als die Chebychef Schranke.