Algorithmen und Wahrscheinlichkeit

Zufall in der Informatik

Warum sollte jeder Informatiker Ahnung von Wahrscheinlichkeitstheorie haben?

QuickSort:

*Wodurch wird QuickSort zu **Quick**Sort?*

⇒ *wenn wir das Pivot-Element **zufällig wählen**,*

so hat er seinen Namen verdient …

Primzahltest:

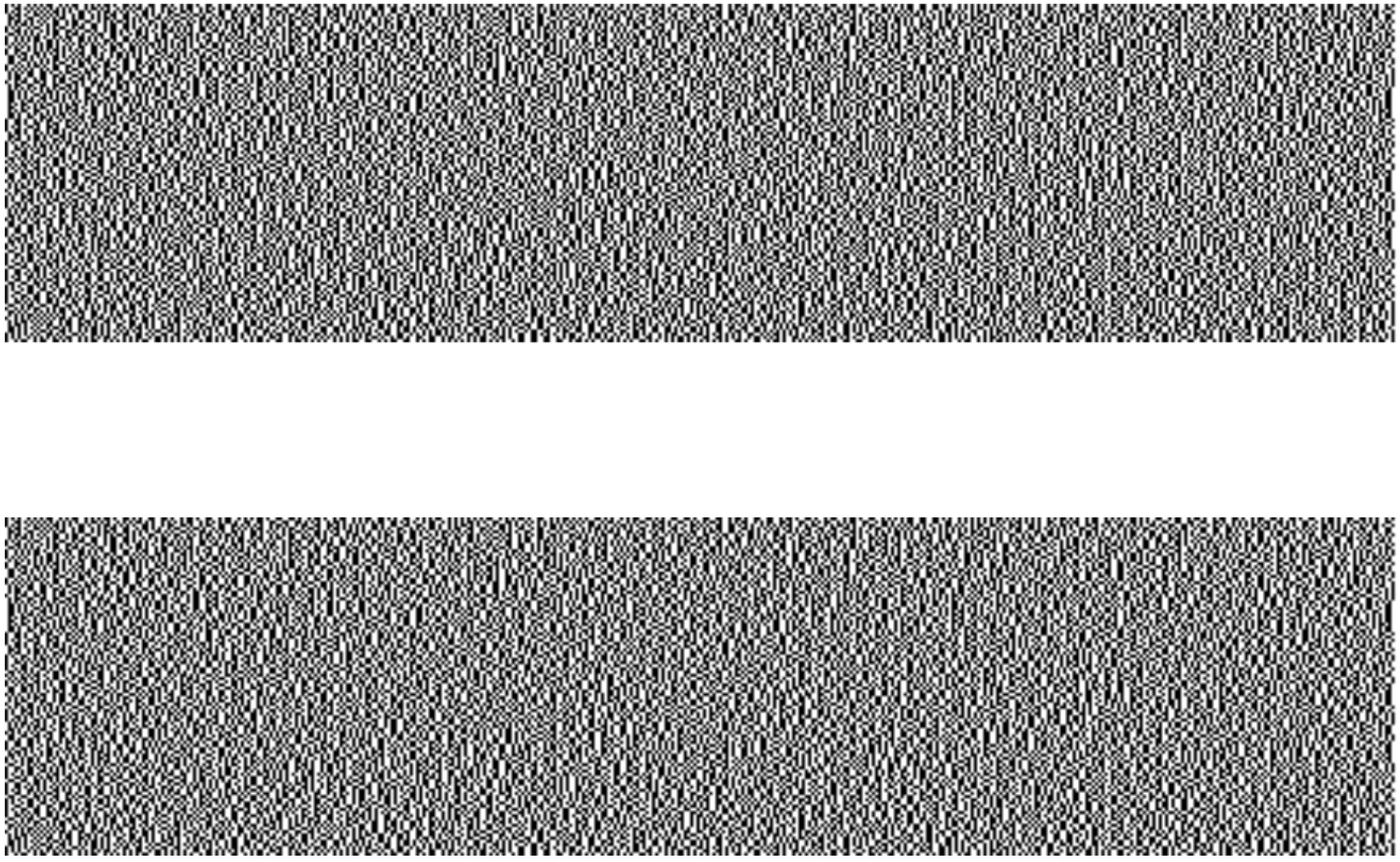
Gegeben natürliche Zahl n, ist n eine Primzahl?

⇨ essentiell für fast alle Probleme in der Kryptographie

⇨ Algorithmus:

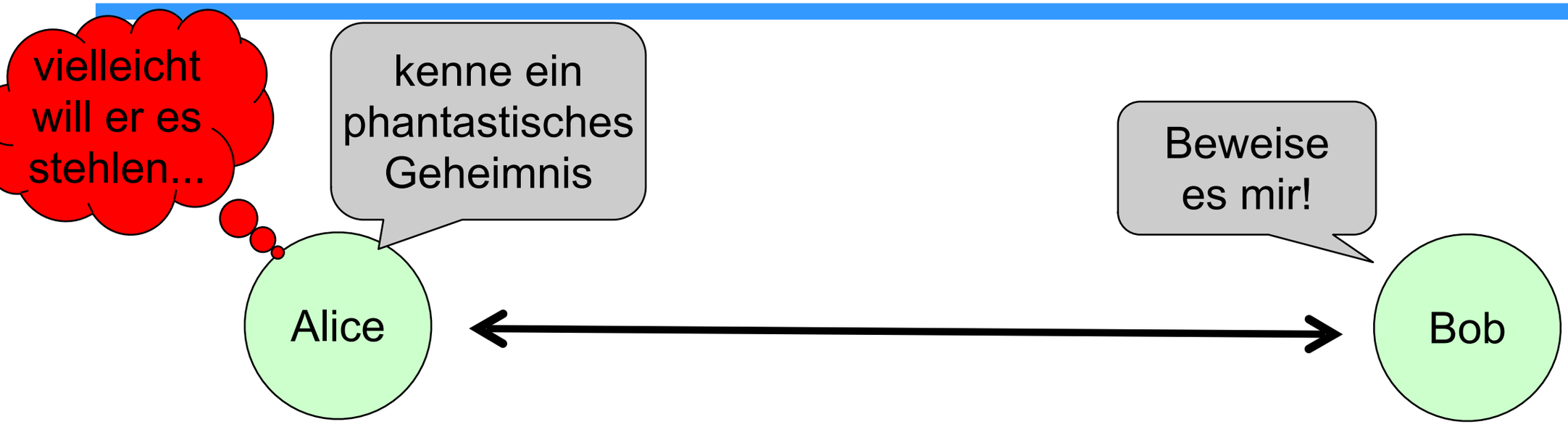
- wähle Zahl 1 ≦ x≦ n ***zufällig***
- prüfe ob x Zeuge für Zusammengesetztheit von n ist

Visual Cryptography:



taken from: www.codeproject.com

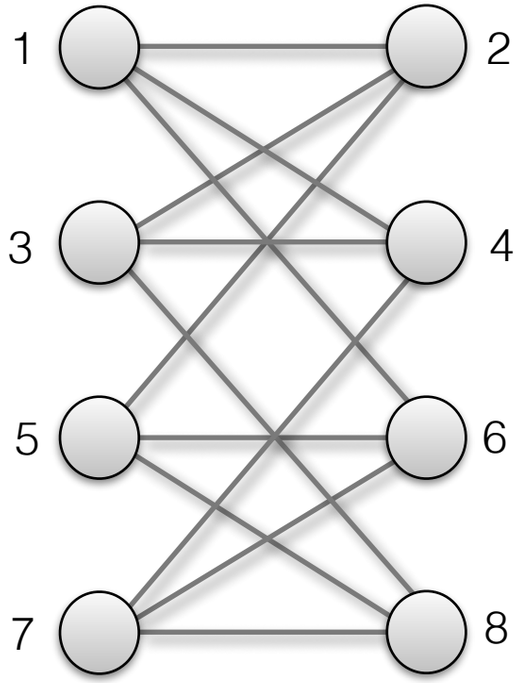
Anwendung: Zero-Knowledge-Protokolle

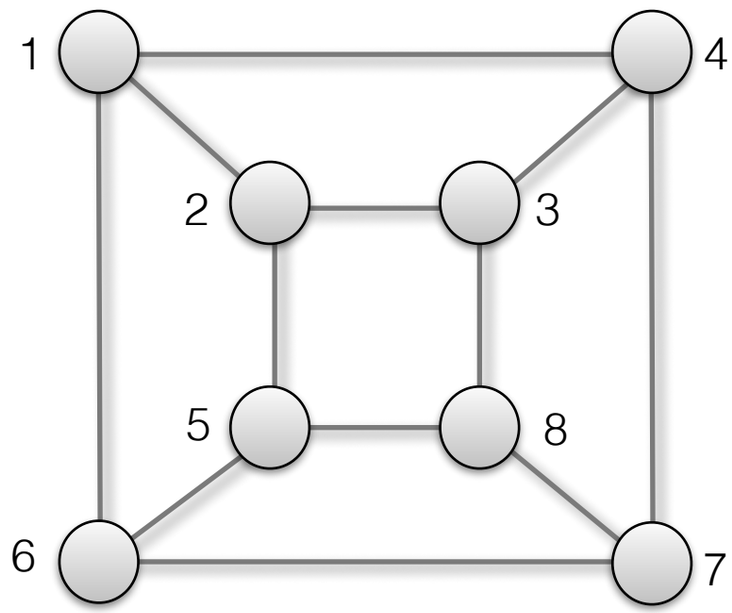


Ideale Welt: Alice kann Bob *beweisen*, dass sie das Geheimnis kennt, *ohne das Geheimnis zu verraten*.

Wir leben in einer idealen Welt!!

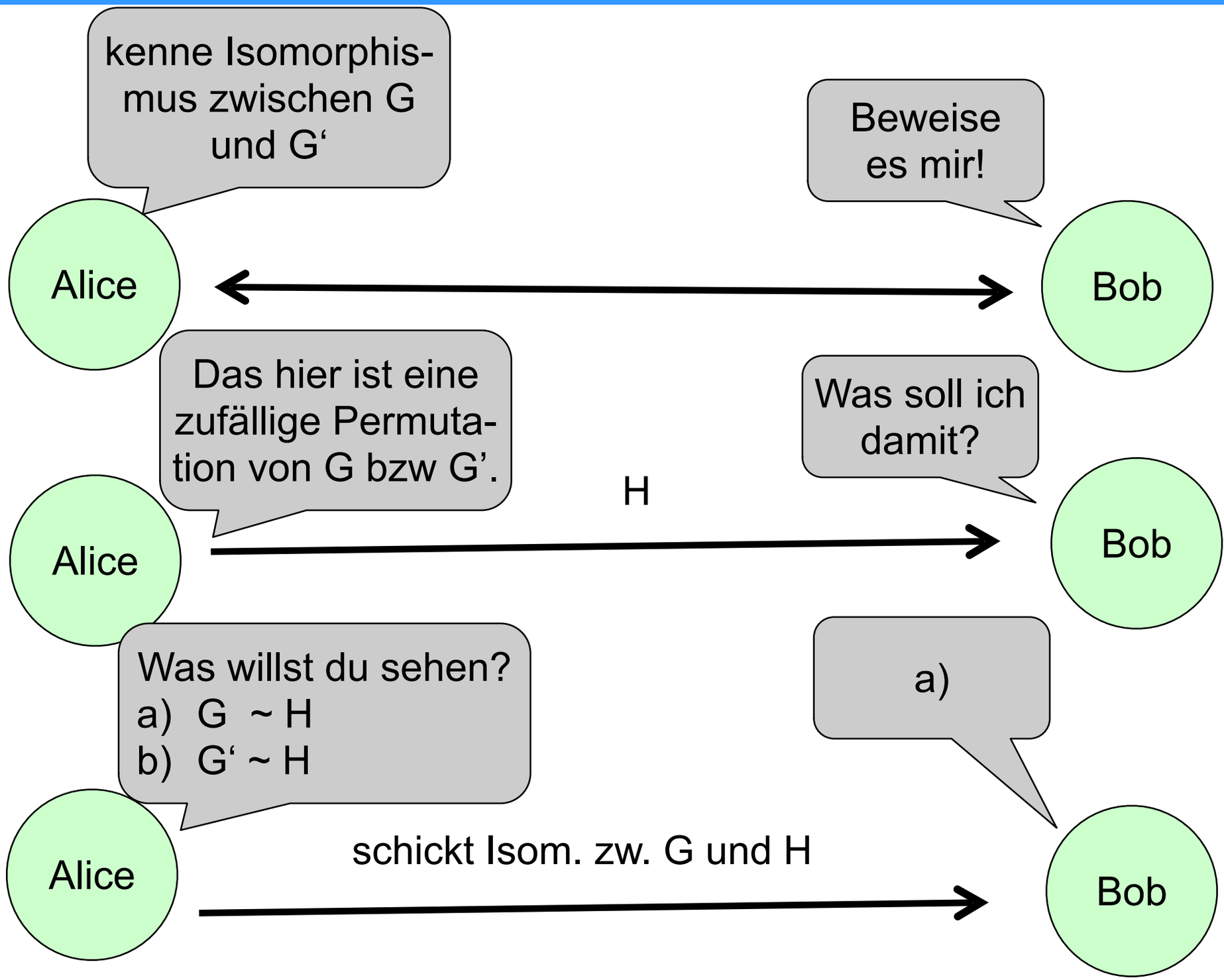
Anwendung: Zero-Knowledge-Protokolle



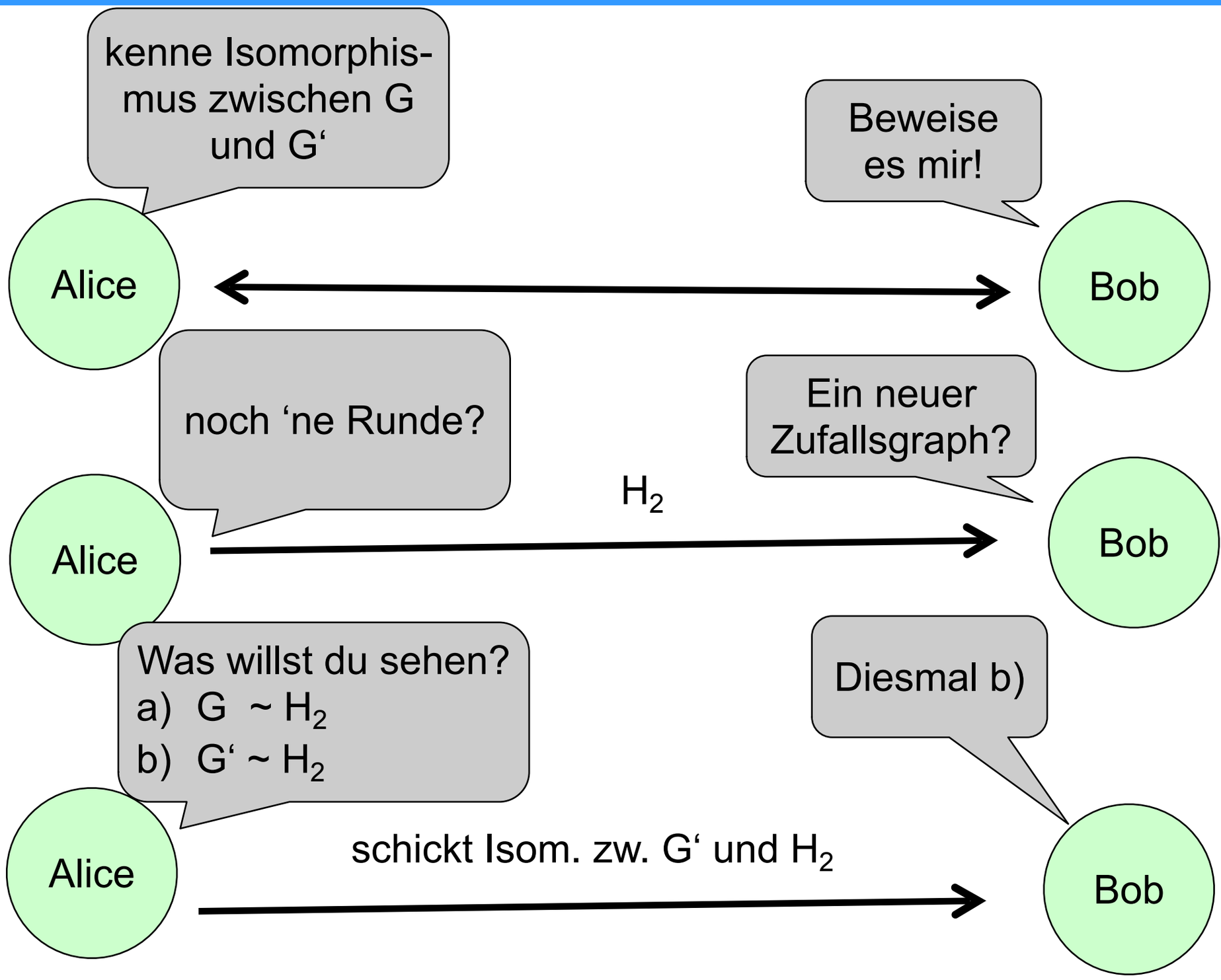


Es ist kein polynomieller Algorithmus bekannt, um zu entscheiden, ob zwei Graphen isomorph sind.

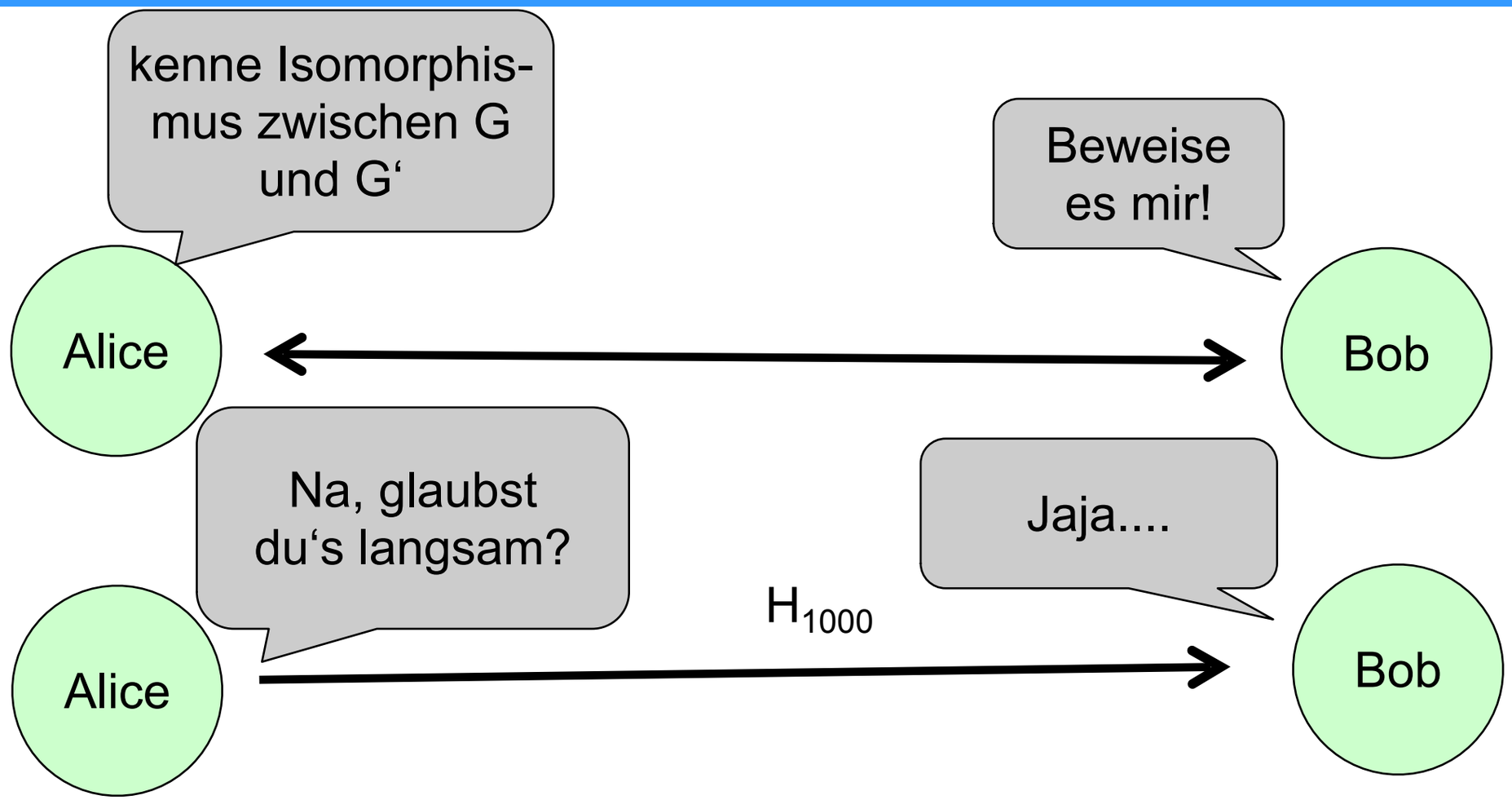
Anwendung: Zero-Knowledge-Protokolle



Anwendung: Zero-Knowledge-Protokolle



Anwendung: Zero-Knowledge-Protokolle



Elektronisches Geld:

00100100010011 1
00101111101100 10
10101000100100 0
10101010101010 1

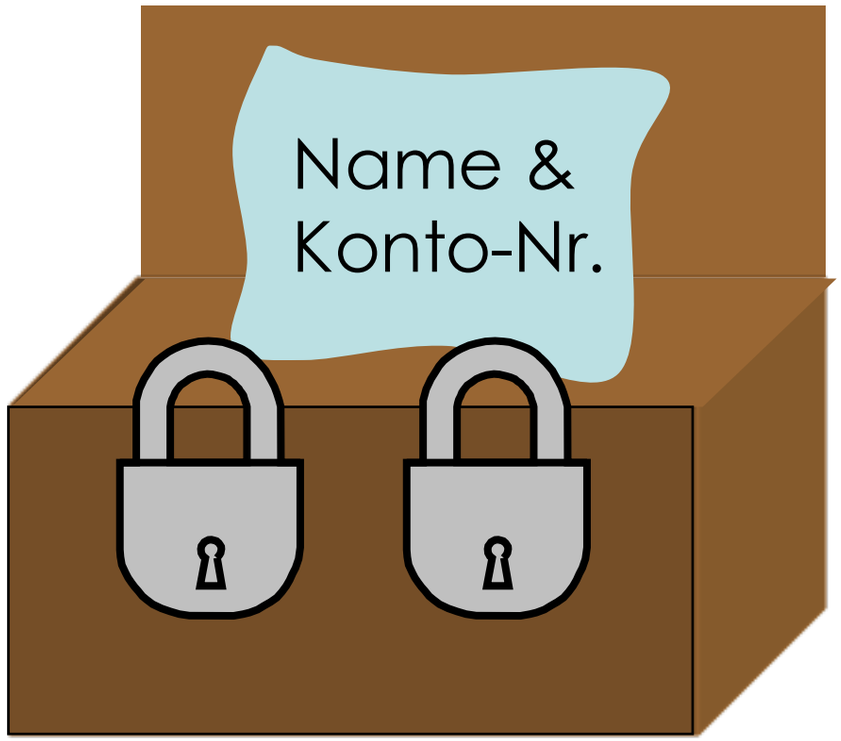
Erwünschte Eigenschaften:

Kunde: Anonymität

Bank: Kenntnis des Kunden, falls dieser betrügt
(Geldschein mehrfach verwendet)

Erzeugen eines elektronischen Geldscheins:

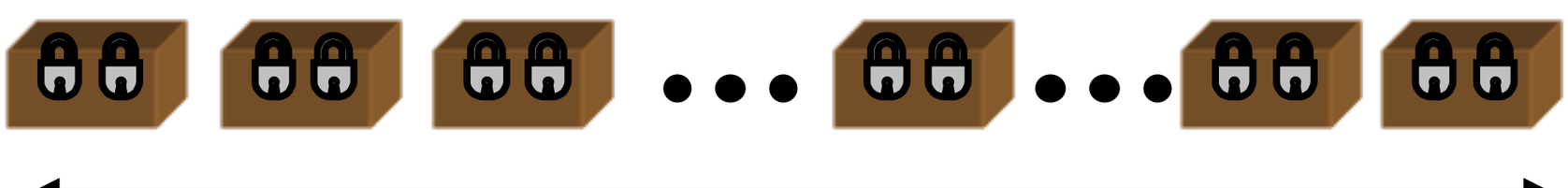
Kunde:



40 mal

Erzeugen eines elektronischen Geldscheins:

Kunde liefert der Bank:



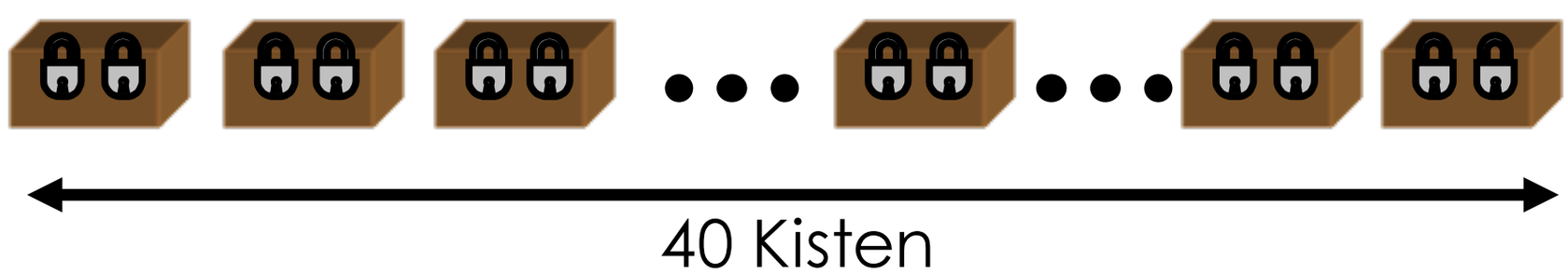
40 Kisten

Bank wählt 20 Kisten ***zufällig*** aus und bittet Kunden, diese Kisten aufzuschliessen.

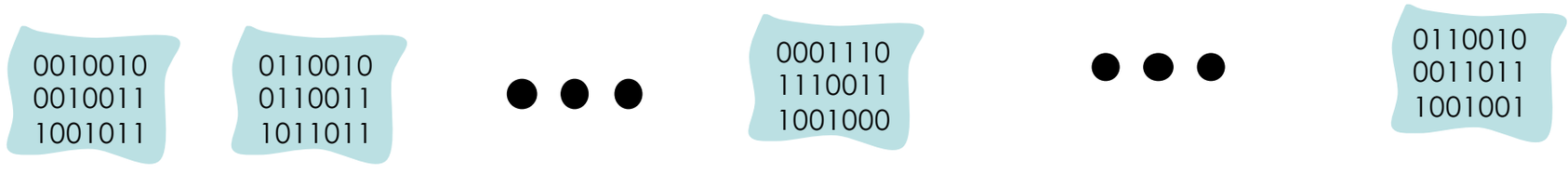
Falls in einer der ausgewählten Kisten, der Zettel mit Name und Konto-Nr. des Kunden fehlt oder falsch ist, bricht die Bank die Geschäftsverbindung mit dem Kunden ab.

Erzeugen eines elektronischen Geldscheins:

Kunde liefert der Bank:



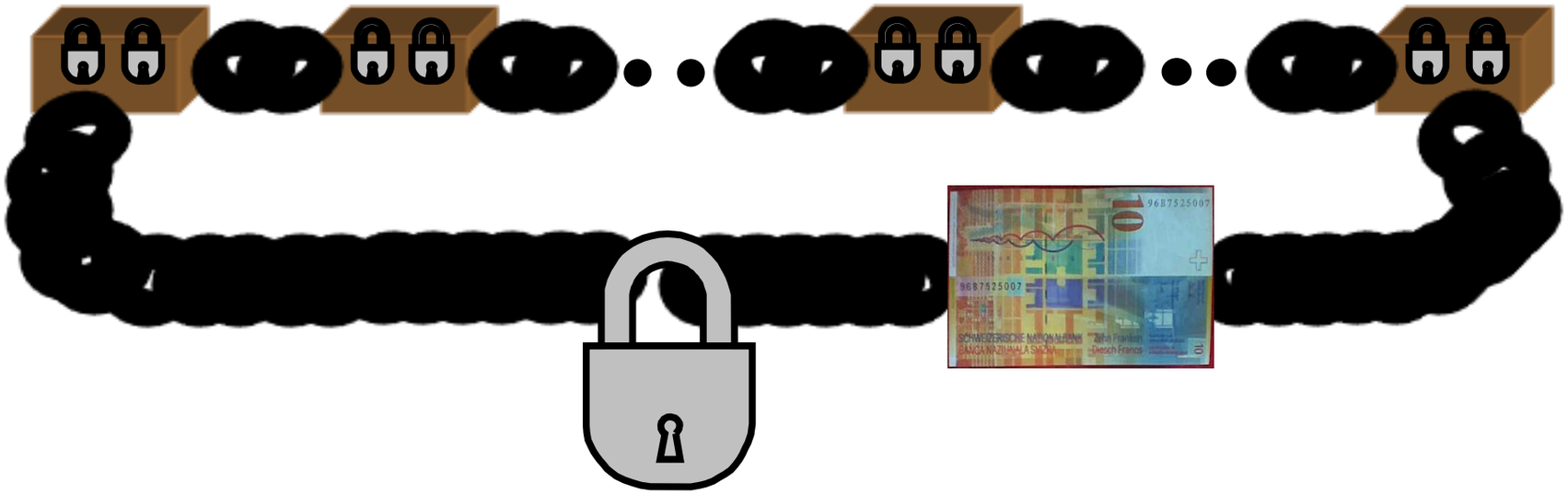
Notwendigkeit dieses Schrittes:



Bank bekommt vom Kunden 40 Bitstrings. Insbesondere kann die Bank beim Zuschliessen nicht „zusehen“.

Erzeugen eines elektronischen Geldscheins:

Bank liefert dem Kunden:



→ **elektronischer Geldschein**

Verwenden eines elektronischen Geldscheins:

Bezahlen:

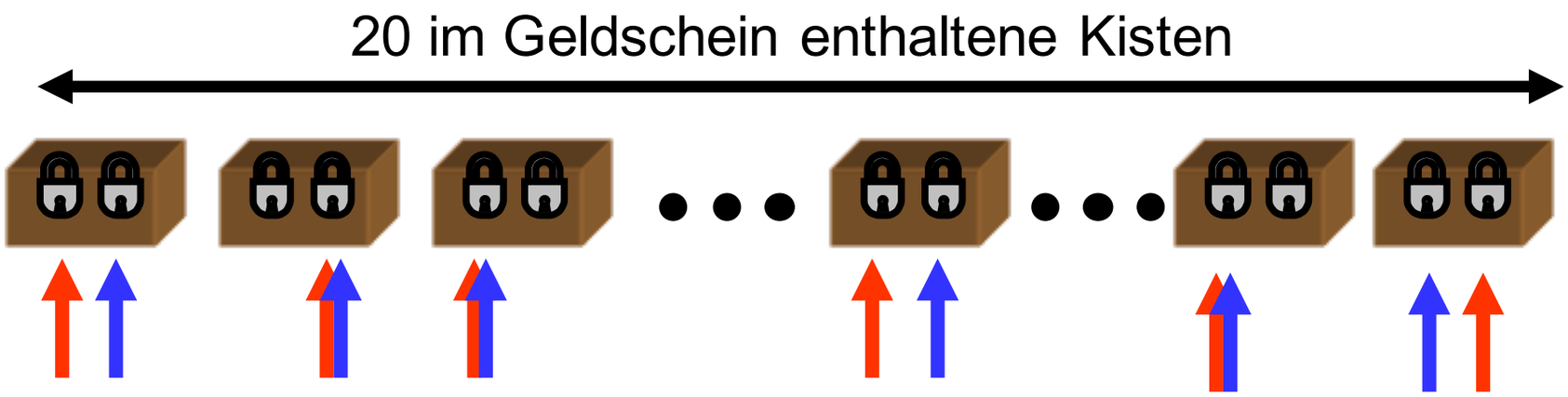
Geschäft verlangt vom Kunden für jede der 20 Kisten *einen* der beiden Schlüssel.

Welcher Schlüssel verlangt wird (linker oder rechter) wird vom Geschäft ***zufällig*** ausgewählt.

Geschäft liefert Geldschein zusammen mit den eingesammelten Schlüsseln an die Bank.

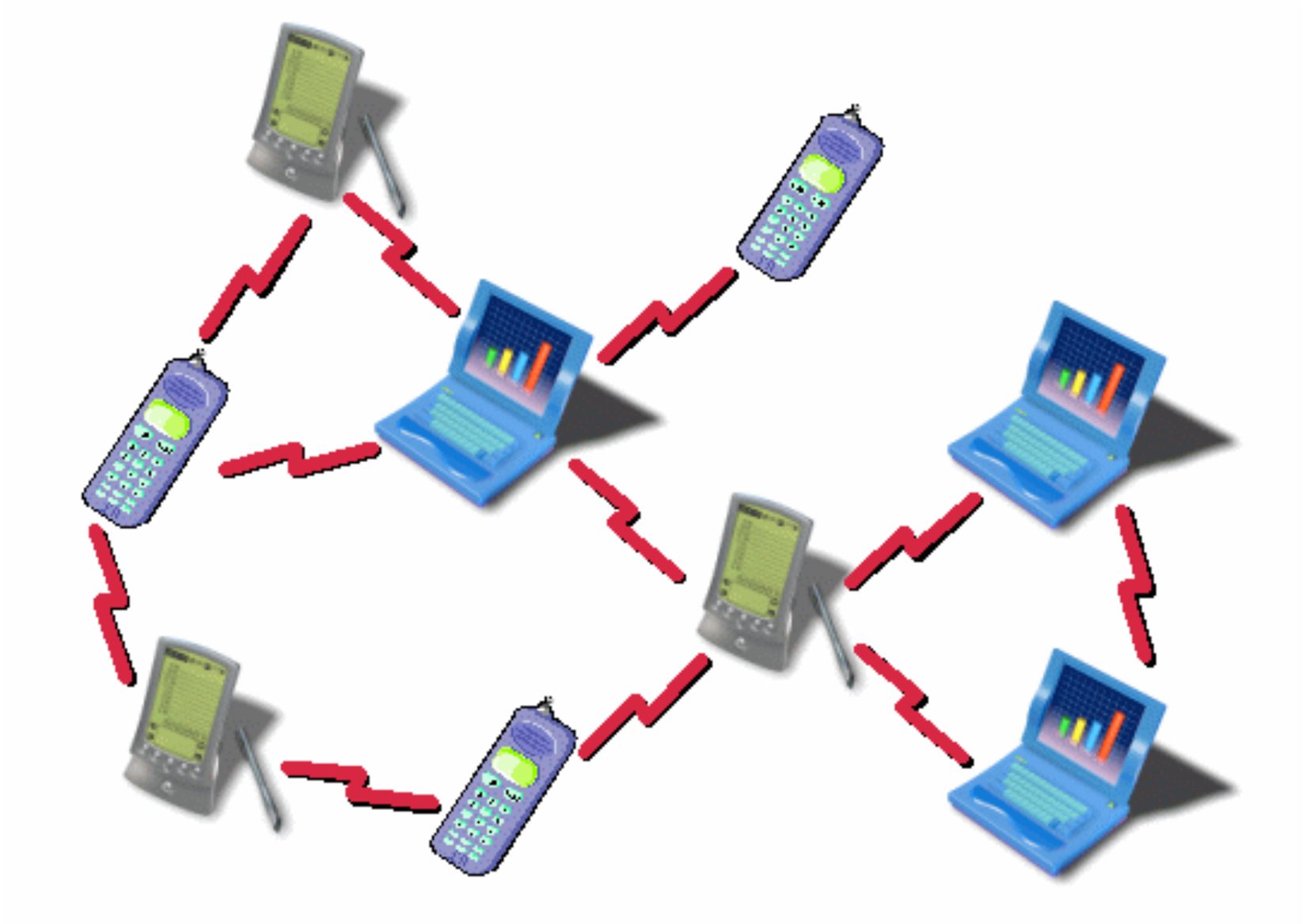
Verwenden eines elektronischen Geldscheins:

Bezahlen: angenommen der Kunde gibt Geldschein mehrmals aus:



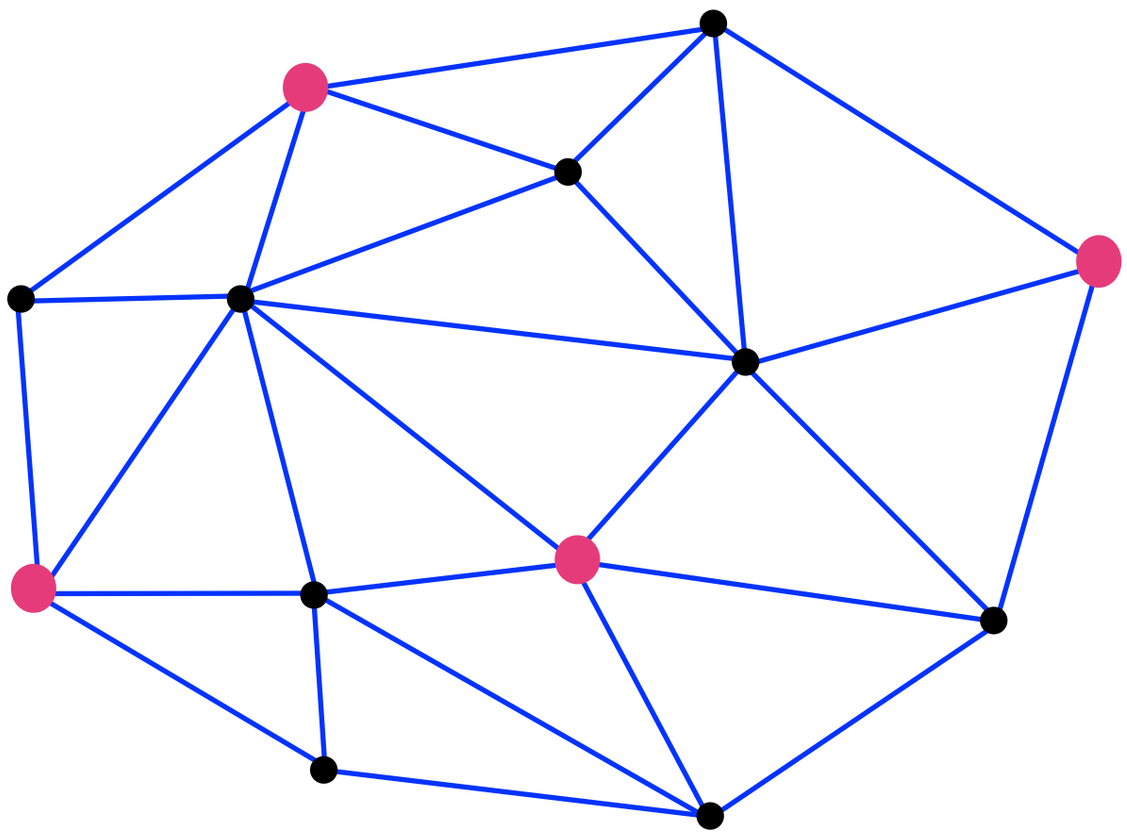
Bank wird von etwa der Hälfte der Kisten *beide* Schlüssel bekommen!

Verteiltes Rechnen



Ziel: Knoten/Rechner sollen gemeinsam eine Aufgabe lösen

z.B: Bestimme eine möglichst grosse stabile Menge



stabile Menge $\triangleq$ Knoten, die nicht durch Kanten verbunden sind

Wir stellen fest:

Alle Knoten mit Abstand k vom Rand sehen nach k Runden die exakt gleiche Umgebung.

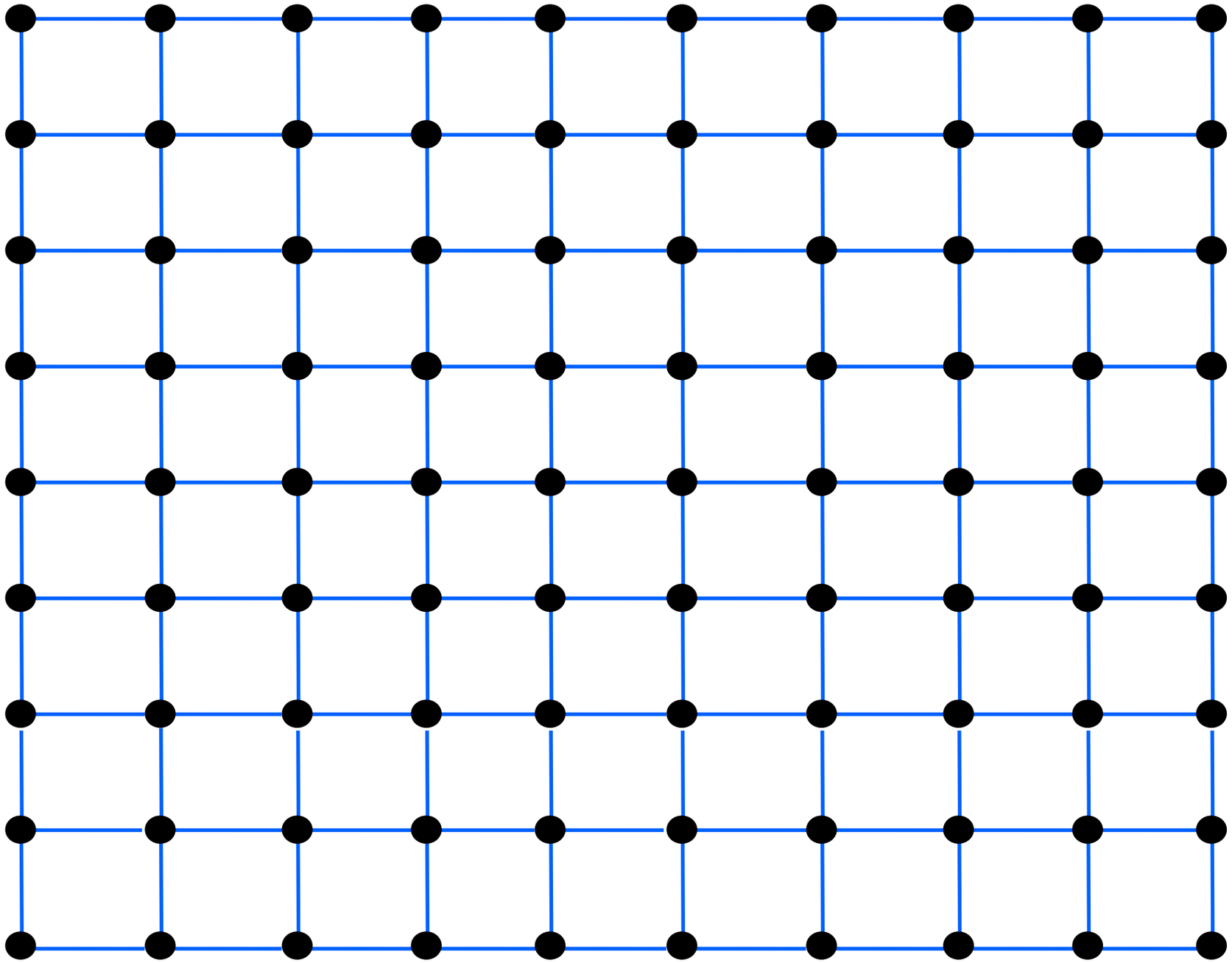
Jeder deterministische Algorithmus führt daher zur exakt gleichen Entscheidung ... die „ich gehöre nicht zur stabilen Menge“ sein muss.

Folgerung:

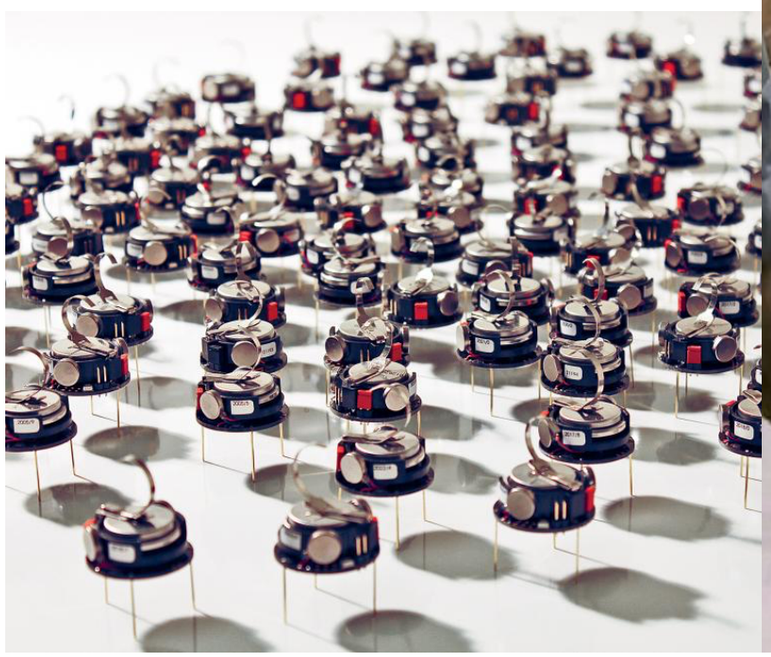
Einen „schnellen“ Algorithmus, der eine „grosse“ stabile Menge findet, kann es nicht geben.

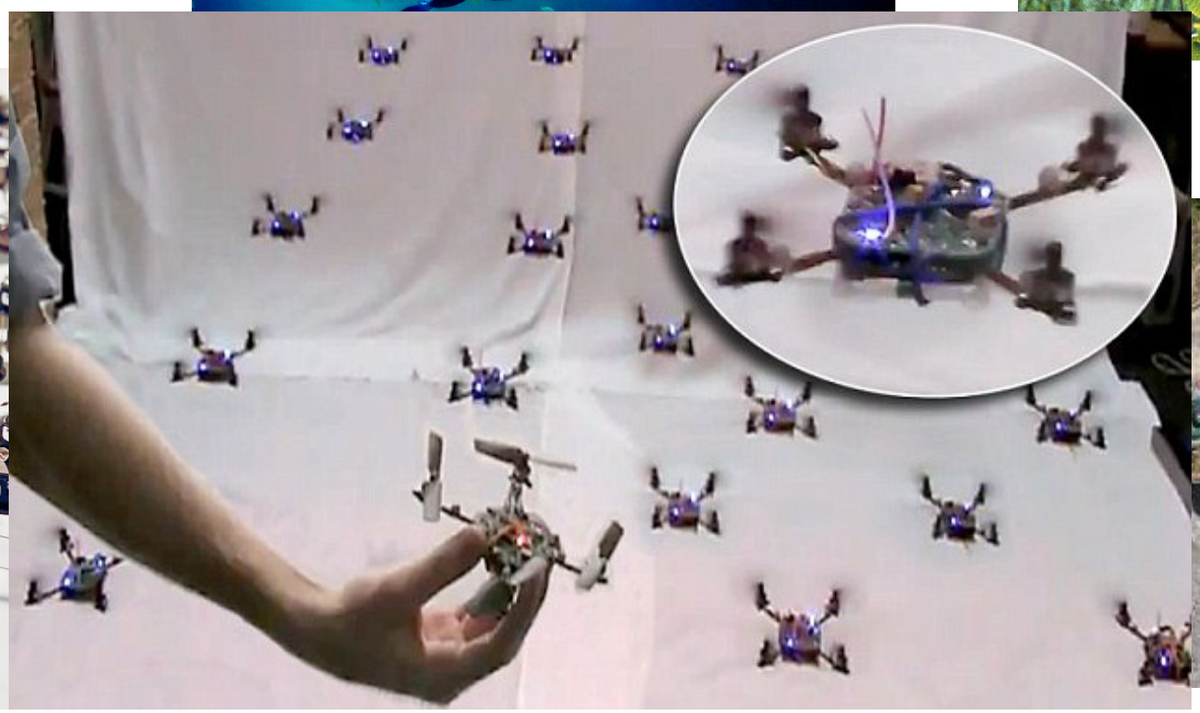
2. Runde:

alle noch vorhandenen Kanten: „lösche“ einen Knoten zufällig



Swarm Computing





Wahrscheinlichkeitsraum

Definition 2.1. Ein *diskreter Wahrscheinlichkeitsraum* ist bestimmt durch eine *Ergebnismenge* $\Omega = \{\omega_1, \omega_2, \ldots\}$ von *Elementarereignissen*. Jedem Elementarereignis ω_i ist eine *(Elementar-)Wahrscheinlichkeit* $\Pr[\omega_i]$ zugeordnet, wobei wir fordern, dass $0 \leq \Pr[\omega_i] \leq 1$ und

$$\sum_{\omega \in \Omega} \Pr[\omega] = 1.$$

Eine Menge $E \subseteq \Omega$ heisst *Ereignis*. Die Wahrscheinlichkeit $\Pr[E]$ eines Ereignisses ist definiert durch

$$\Pr[E] := \sum_{\omega \in E} \Pr[\omega].$$

Ist E ein Ereignis, so bezeichnen wir mit $\bar{E} := \Omega \setminus E$ das *Komplementärereignis* zu E.

Beispiel: Betrachte Würfel

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

$Pr[1] = Pr[2] = Pr[3] = Pr[4] = Pr[5] = Pr[6] = 1/6$

A	:=	„Augenzahl ist gerade“	$A = \{2,4,6\}$	$Pr[A] = 3/6$
B	:=	„Augenzahl ist Primzahl“	$B = \{2,3,5\}$	$Pr[B] = 3/6$
C	:=	„Augenzahl ist durch 6 teilbar“	$C = \{6\}$	$Pr[C] = 1/6$

Wahrscheinlichkeitsraum

Lemma 2.2. Für Ereignisse $A, B, A_1, A_2, \ldots$ gilt:

1. $\Pr[\emptyset] = 0$, $\Pr[\Omega] = 1$.
2. $0 \leq \Pr[A] \leq 1$.
3. $\Pr[\bar{A}] = 1 - \Pr[A]$.
4. Wenn $A \subseteq B$, so folgt $\Pr[A] \leq \Pr[B]$.
5. *(Additionssatz)* Wenn die Ereignisse $A_1, \ldots, A_n$ paarweise disjunkt sind (also wenn für alle Paare $i \neq j$ gilt, dass $A_i \cap A_j = \emptyset$), so folgt

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{i=1}^{n} \Pr[A_i].$$

Für eine unendliche Menge von disjunkten Ereignissen $A_1, A_2, \ldots$ gilt analog

$$\Pr\left[\bigcup_{i=1}^{\infty} A_i\right] = \sum_{i=1}^{\infty} \Pr[A_i].$$

Vereinigung von Ereignissen

(Additionssatz) Wenn die Ereignisse $A_1, \ldots, A_n$ paarweise disjunkt sind (also wenn für alle Paare $i \neq j$ gilt, dass $A_i \cap A_j = \emptyset$), so folgt

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{i=1}^{n} \Pr[A_i].$$

beliebig

Satz 2.4. *(Boolesche Ungleichung)* Für Ereignisse $A_1, \ldots, A_n$ gilt

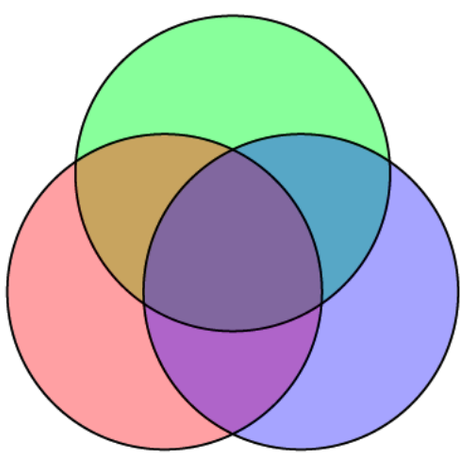
$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] \leq \sum_{i=1}^{n} \Pr[A_i].$$

Vereinigung von Ereignissen

Satz 2.3. *(Siebformel, Prinzip der Inklusion/Exklusion)*
Für Ereignisse $A_1, \ldots, A_n$ $(n \geq 2)$ gilt:

$$\begin{aligned}\Pr\left[\bigcup_{i=1}^{n} A_i\right] &= \sum_{i=1}^{n} \Pr[A_i] - \sum_{1 \leq i_1 < i_2 \leq n} \Pr[A_{i_1} \cap A_{i_2}] + - \ldots \\ &+ (-1)^{l+1} \sum_{1 \leq i_1 < \ldots < i_l \leq n} \Pr[A_{i_1} \cap \ldots \cap A_{i_l}] + - \ldots \\ &+ (-1)^{n+1} \cdot \Pr[A_1 \cap \ldots \cap A_n].\end{aligned}$$

n=3:



$$\begin{aligned}&\Pr[A \cup B \cup C] \\ &\quad = \Pr[A] + \Pr[B] + \Pr[C] \\ &\qquad - \Pr[A \cap B] - \Pr[A \cap C] - \Pr[B \cap C] + \Pr[A \cap B \cap C]\end{aligned}$$

Vereinigung von Ereignissen

Satz 2.3. *(Siebformel, Prinzip der Inklusion/Exklusion)*
Für Ereignisse $A_1, \ldots, A_n$ $(n \geq 2)$ gilt:

$$\begin{aligned}\Pr\left[\bigcup_{i=1}^{n} A_i\right] &= \sum_{i=1}^{n} \Pr[A_i] - \sum_{1 \leq i_1 < i_2 \leq n} \Pr[A_{i_1} \cap A_{i_2}] + - \ldots \\ &+ (-1)^{l+1} \sum_{1 \leq i_1 < \ldots < i_l \leq n} \Pr[A_{i_1} \cap \ldots \cap A_{i_l}] + - \ldots \\ &+ (-1)^{n+1} \cdot \Pr[A_1 \cap \ldots \cap A_n].\end{aligned}$$

Satz 2.4. *(Boolesche Ungleichung)* Für Ereignisse $A_1, \ldots, A_n$ gilt

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] \leq \sum_{i=1}^{n} \Pr[A_i].$$

Vereinigung von Ereignissen

Beispiel: Betrachte Würfel

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

A := „Augenzahl ist gerade“ $A = \{2,4,6\}$ $Pr[A] = 3/6$

B := „Augenzahl ist Primzahl“ $B = \{2,3,5\}$ $Pr[B] = 3/6$

C := „Augenzahl ist durch 6 teilbar“ $C = \{6\}$ $Pr[C] = 1/6$

$$Pr[A \cup B \cup C]$$
$$= Pr[A] + Pr[B] + Pr[C]$$
$$- Pr[A \cap B] - Pr[A \cap C] - Pr[B \cap C] + Pr[A \cap B \cap C]$$
$$= 3/6 + 3/6 + 1/6 - 1/6 - 1/6 - 0 + 0 = 5/6$$

Laplace-Raum

$$C = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\} \times \{2, 3, \ldots, 9, 10, B, D, K, A\}$$

Laplace-Raum: endlicher Wahrscheinlichkeitsraum, in dem alle Elementarereignisse gleich wahrscheinlich sind.

Beispiel: Mische und ziehe eine Karte:

$\Omega = C$ und $Pr[\omega] = 1/|\Omega| = 1/52$ für alle $\omega \in \Omega$

In einem Laplace-Raum gilt für jedes Ereignis E: $$\Pr[E] = \frac{|E|}{|\Omega|}.$$

zusammengesetzte W'räume

$C = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\} \times \{2, 3, \ldots, 9, 10, B, D, K, A\}$

Szenario 1: Wir mischen ein Kartenspiel und ziehen zwei Karten.

$$\Omega := \{X \mid X \subseteq C, |X| = 2\} \qquad \Omega' := \{(x_1, x_2) \mid x_1 \in C, x_2 \in C, x_2 \neq x_1\}$$

Sind Ereignisse in Ω', z.B.
X= {🂱,🃂}
ist das Ereignis {ω₁,ω₂} mit
ω₁= (🃂,🂱) und ω₂= (🂱,🃂).

alle 52 Karten sind gleich wahrscheinlich

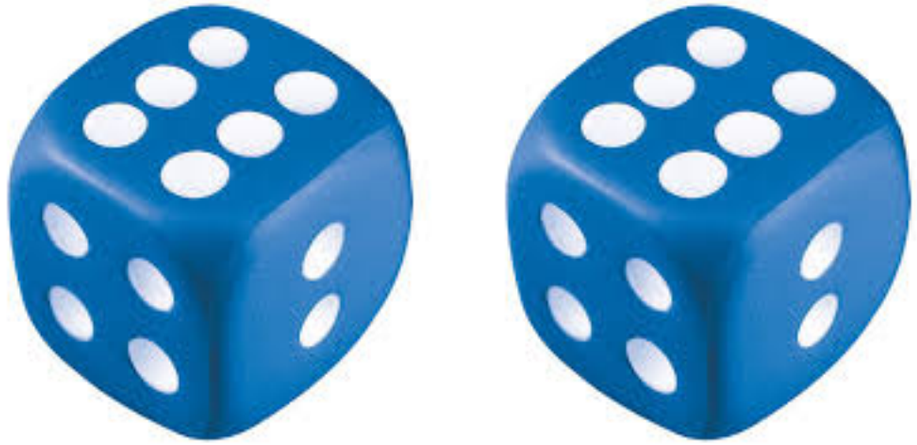
Nach Ziehen von x_1 sind alle 51 verbleibenden Karten gleich wahrscheinlich.

⇒ **Laplaceraum** mit $|\Omega'| = 52 \cdot 51$.

Jedes X aus Ω hat dieselbe Wahrscheinlichkeit $\Pr[X] = \frac{2}{|\Omega'|} = \frac{2}{52 \cdot 51}$.

zusammengesetzte W'räume

Szenario 2: Wir werfen zwei Würfel und addieren die Augenzahlen.



$\Omega := \{2, 3, 4, \ldots, 12\}$

Sind Ereignisse in Ω', z.B.
X = 10
ist das Ereignis $\{\omega_1, \omega_2, \omega_3\}$ mit
ω_1= (6,4), ω_2= (5,5), ω_3= (4,6).

$\Omega' := \{(x_1, x_2) \mid x_1, x_2 \in \{1, 2, 3, 4, 5, 6\}\}$

alle 6 Augen-zahlen gleich wahrscheinlich

Nach Werfen von x_1 sind für x_2 immer noch alle Augen-zahlen gleich wahrscheinlich.

$\Rightarrow$ **Laplaceraum** mit $|\Omega'| = 6 \cdot 6$.

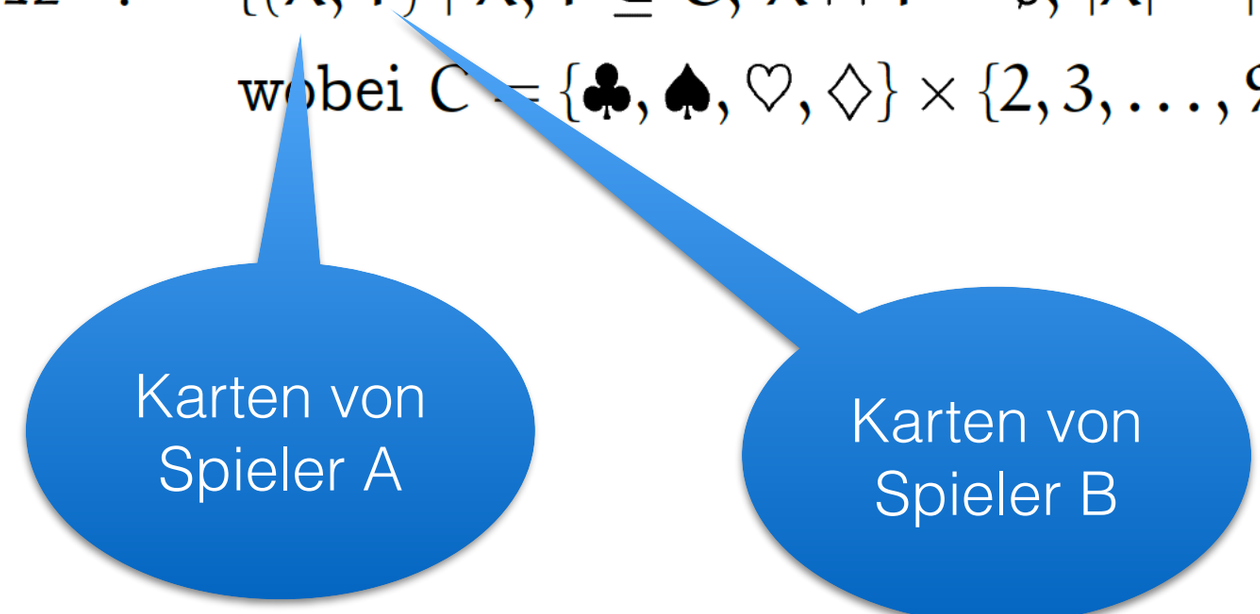
Verschiedene X aus Ω haben unterschiedliche Wahrscheinlichkeiten, z.B.

$$\Pr[2] = \frac{1}{|\Omega'|} = \frac{1}{36}, \qquad \Pr[7] = \frac{6}{|\Omega'|} = \frac{6}{36}, \qquad \Pr[10] = \frac{3}{|\Omega'|} = \frac{3}{36}.$$

Beispiel: Kartenspiel

Szenario: Wir mischen die Karten und geben
Spieler A und B jeweils fünf Karten.

$$\Rightarrow \quad \Omega := \{(X, Y) \mid X, Y \subseteq C,\ X \cap Y = \emptyset,\ |X| = |Y| = 5\},$$
$$\text{wobei } C = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\} \times \{2, 3, \ldots, 9, 10, B, D, K, A\}\}. \qquad |C|=52$$



$|\Omega| = ?$

Wdh: Kombinatorik

Anzahl Möglichkeiten k Elemente aus einer n-elementigen Menge zu ziehen

	geordnet	ungeordnet
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

Beispiel: k=2 Elemente aus S={1,2,3} ziehen (n=3)

	geordnet	ungeordnet
mit Zurücklegen	$(1,1),(1,2),(1,3)$ $(2,1),(2,2),(2,3)$ $(3,1),(3,2),(3,3)$	$\{1,1\}, \{1,2\}, \{1,3\}$ $\{2,2\}, \{2,3\}, \{3,3\}$
ohne Zurücklegen	$(1,2), (1,3), (2,1)$ $(2,3), (3,1), (3,2)$	$\{1,2\}, \{1,3\}, \{2,3\}$

Wdh: Kombinatorik

Anzahl Möglichkeiten k Elemente aus einer n-elementigen Menge zu ziehen

	geordnet	ungeordnet
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

geordnet, mit Zurücklegen (Tupel)

5 7 5 1 2

_ _ _ _ _ . . .

n Möglichkeiten

n Möglichkeiten

n Möglichkeiten

$$\underbrace{n \cdot n \cdot \ldots \cdot n}_{k \text{ mal}}$$

Wdh: Kombinatorik

Anzahl Möglichkeiten k Elemente aus einer n-elementigen Menge zu ziehen

	geordnet	ungeordnet
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

geordnet, ohne Zurücklegen (Tupel ohne Wiederholung)

5 7 3 1 2

— — — — —

n Möglichkeiten

n-1 Möglichkeiten

n-2 Möglichkeiten

. . .

n-k+1 Möglichkeiten

$$n^{\underline{k}} := \underbrace{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}_{k \text{ Faktoren}}$$

Wdh: Kombinatorik

Anzahl Möglichkeiten k Elemente aus einer n-elementigen Menge zu ziehen

	geordnet	ungeordnet
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

Zähle erst **geordnet**, ohne Zurücklegen: $n^{\underline{k}}$

ungeordnet, ohne Zurücklegen (Menge)

5 7 3 1 2

_ _ _ _ _

Problem: Haben Lösungen mehrfach gezählt! z.B. {1,2,3,5,7} als 12357, 53217, 12537, 75312, …

Wie oft? Jede **un**geordnete Lösung genau $k^{\underline{k}} = k!$ mal.

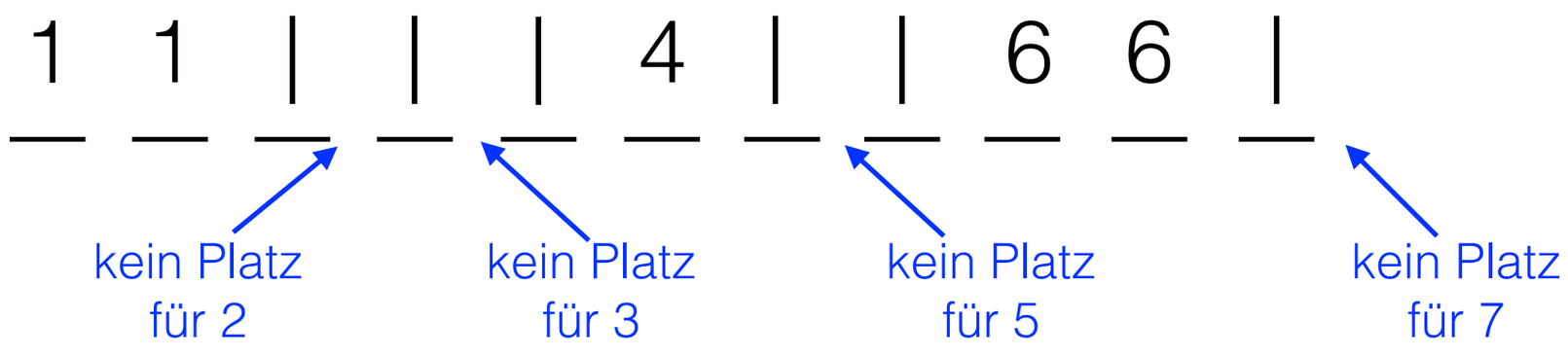
$$\binom{n}{k} := \frac{n^{\underline{k}}}{k!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-1) \cdot \ldots \cdot 1} = \frac{n!}{k! \cdot (n-k)!}$$

Wdh: Kombinatorik

Anzahl Möglichkeiten k Elemente aus einer n-elementigen Menge zu ziehen

	geordnet	ungeordnet
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

ungeordnet, mit Zurücklegen (Multimenge) (Beispiel für k=5, n=7)



Trick:

1) Füge n-1 Zusatzplätze ein, sodass insgesamt n+k-1 Plätze zur Verfügung stehen.
2) Wähle n-1 der Plätze aus und schreibe | auf diese Plätze. → n Bereiche
3) Fülle den ersten Bereich mit “1” aus, den zweiten mit “2”, usw.

Mit diesem Trick wird jede Möglichkeit exakt einmal gezählt! $\rightarrow \binom{n+k-1}{n-1}$

Beispiel: Kartenspiel

Szenario: Wir mischen die Karten und geben
Spieler A und B jeweils fünf Karten.

$$\Rightarrow \quad \Omega := \{(X,Y) \mid X,Y \subseteq C,\ X \cap Y = \emptyset,\ |X| = |Y| = 5\},$$
$$\text{wobei } C = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\} \times \{2,3,\ldots,9,10,B,D,K,A\}\}. \qquad |C|=52$$

$$|\Omega| = \begin{cases} 52^5 \cdot 52^5 \\ \binom{52}{10} \cdot \binom{10}{5} \\ \frac{52!}{5! \cdot 5! \cdot 42!} \\ \binom{52}{5} \cdot \binom{47}{5} \end{cases}$$

Beispiel: Kartenspiel

Szenario: Wir mischen die Karten und geben
Spieler A und B jeweils fünf Karten.

$$\Rightarrow \quad \Omega := \{(X, Y) \mid X, Y \subseteq C,\ X \cap Y = \emptyset,\ |X| = |Y| = 5\},$$
$$\text{wobei } C = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\} \times \{2, 3, \ldots, 9, 10, B, D, K, A\}\}. \qquad |C|=52$$

$$|\Omega| = \begin{cases} 52^5 \cdot 52^5 & \text{✗} \\ \binom{52}{10} \cdot \binom{10}{5} & \text{✓} \\ \frac{52!}{5! \cdot 5! \cdot 42!} & \text{✓} \\ \binom{52}{5} \cdot \binom{47}{5} & \text{✓} \end{cases}$$

Beispiel: Kartenspiel

Szenario: Wir mischen die Karten und geben
Spieler A und B jeweils fünf Karten.

$$\Omega := \{(X, Y) \mid X, Y \subseteq C,\ X \cap Y = \emptyset,\ |X| = |Y| = 5,$$
$$\text{wobei } C = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\} \times \{2, 3, \ldots, 9, 10, B, D, K, A\}\}.$$

Beispiel für ein Ereignis: $E :=$ „Spieler A hat vier Asse“

$$\text{Prob[E]} = \frac{\text{Anzahl Möglichkeiten in denen Spieler A vier Asse hat}}{\text{Anzahl aller Möglichkeiten}}$$

$$= \frac{48 \cdot \binom{47}{5}}{|\Omega|}$$

bedingte Wahrscheinlichkeit

Wir betrachten dieses Ereignis nun aus der Sicht von Spieler B:

Jetzt hängt die Wahrscheinlichkeit, dass A vier Asse hat, von den Karten von B ab. D.h. Spieler B interessiert sich für:

Pr[„A hat vier Asse“ | „Karten von B“]

bedingte Wahrscheinlichkeit

bedingte Wahrscheinlichkeit

Definition 2.7. A und B seien Ereignisse mit $\Pr[B] > 0$. Die *bedingte Wahrscheinlichkeit* $\Pr[A|B]$ von A gegeben B ist definiert durch

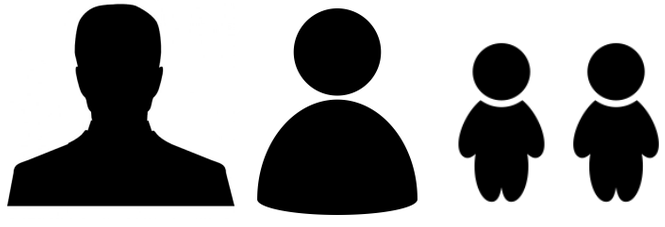
$$\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}.$$

die W'keit, dass Ereignis A eintrifft, *wenn wir schon wissen*, dass Ereignis B eingetreten ist

so rechnen wir diese W'keit aus

Beispiel: Zwei-Kinder-Problem

Familie X hat zwei Kinder



$\Omega = \{mm,mw,wm,ww\}$

1.Stelle: Geschlecht des älteren Kindes,
2.Stelle: Geschlecht des jüngeren Kindes

$Pr[\text{„beide Kinder sind Mädchen“}] = 1/4$

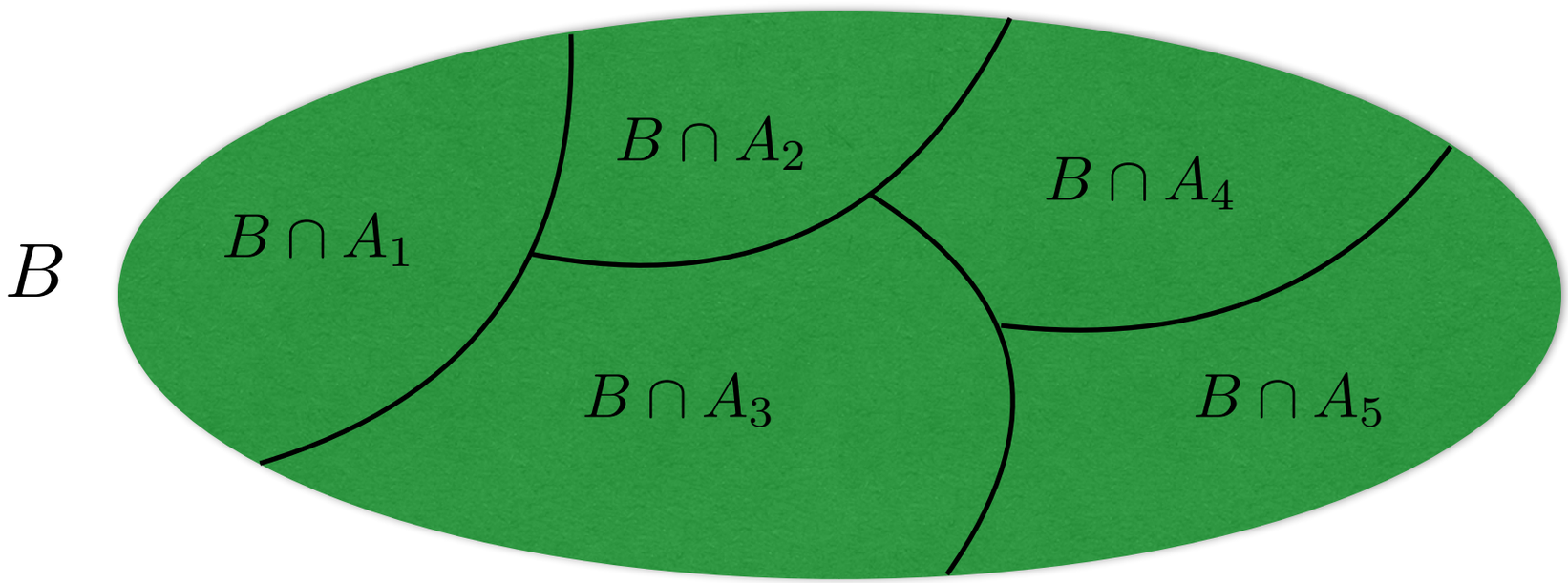
$Pr[\text{„beide Kinder sind Mädchen“} \mid \text{„ein Kind ist Mädchen“}] = 1/3$

$Pr[\text{„beide Kinder sind Mädchen“} \mid \text{„älteres Kind ist Mädchen“}] = 1/2$

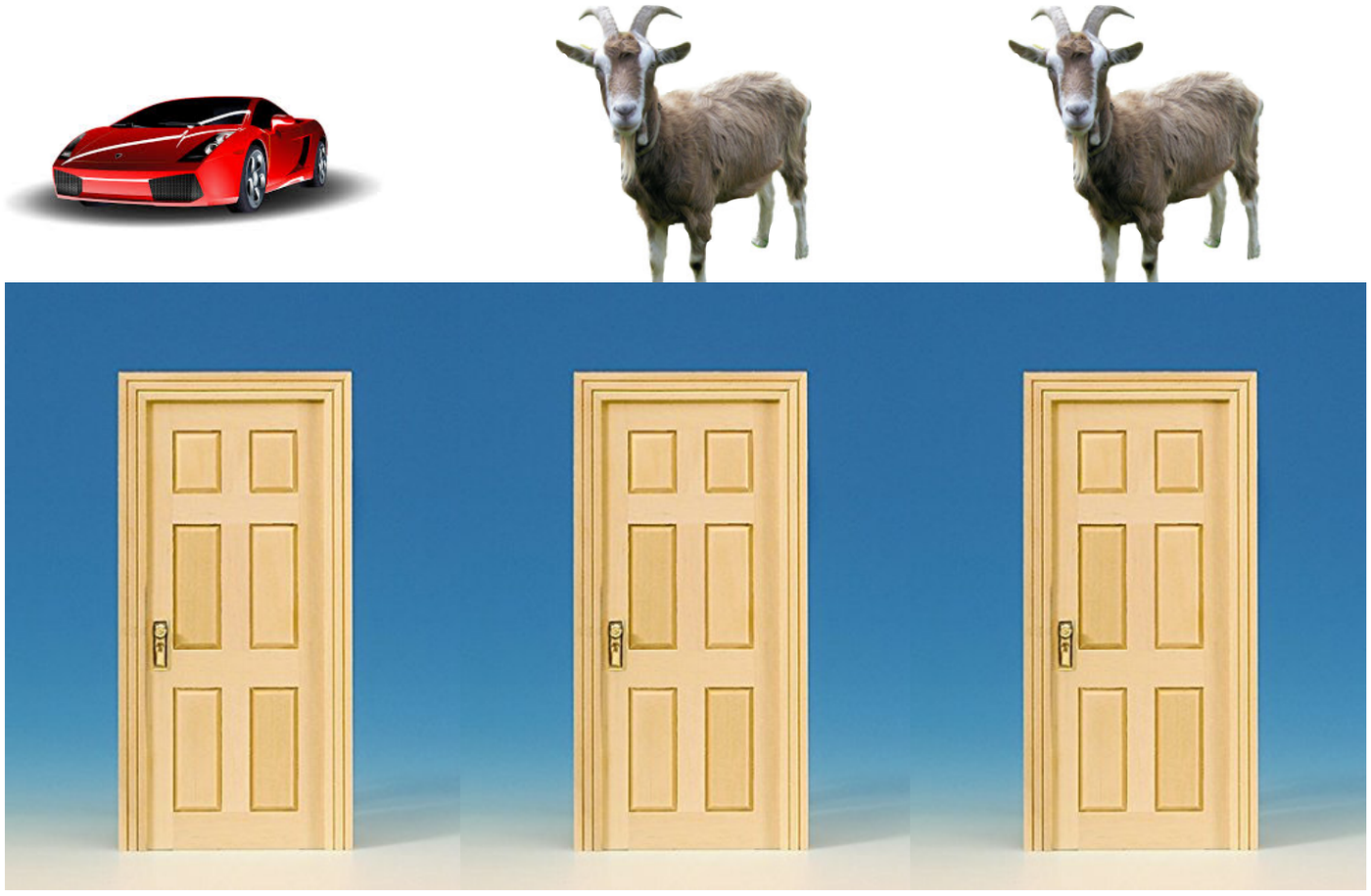
Satz von der totalen W'keit

Satz *(Satz von der totalen Wahrscheinlichkeit)* Die Ereignisse $A_1, \ldots, A_n$ seien paarweise disjunkt und es gelte $B \subseteq A_1 \cup \ldots \cup A_n$. Dann folgt

$$\Pr[B] = \sum_{i=1}^{n} \underbrace{\Pr[B|A_i] \cdot \Pr[A_i]}_{= \Pr[B \cap A_i]}.$$



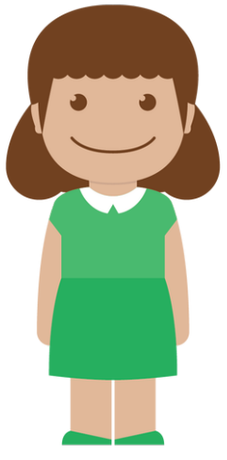
Ziegenproblem



drei Türen:
hinter zweien eine Ziege,
hinter dritten ein Auto

Kandidatin
- sucht sich eine Türe aus

Moderator
- öffnet Tür zu einer Ziege



Ziegenproblem

drei Türen:
hinter zweien eine Ziege,
hinter dritten ein Auto

Kandidatin
- sucht sich eine Türe aus

Moderator
- öffnet Tür zu einer Ziege

Frage: Soll Kandidatin die Türe wechseln?

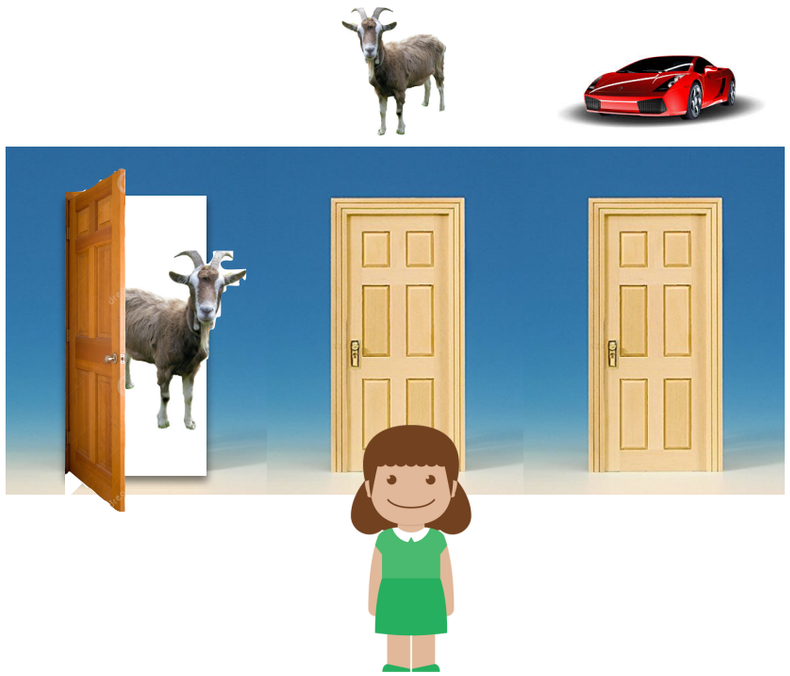
Ziegenproblem

A := „Kandidatin steht vor Tür mit Auto“

B := „Auto hinter dritter Tür“

Pr[A] = 1/3

Ziegenproblem



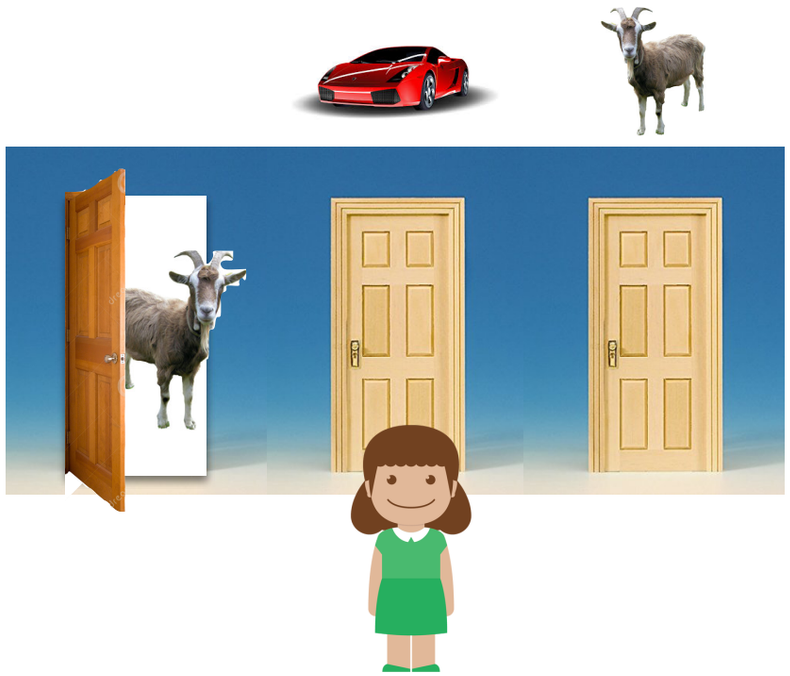
A := „Kandidatin steht vor Tür mit Auto“

B := „Auto hinter dritter Tür“

$$Pr[A] = 1/3$$

$$Pr[B \mid \overline{A}] = 1$$

Ziegenproblem



A := „Kandidatin wählt Tür mit Auto“

B := „Auto hinter dritter Tür“

$$\Pr[A] = 1/3$$

$$\Pr[B \mid \overline{A}] = 1$$

$$\Pr[B \mid A] = 0$$

Ziegenproblem

A := „Kandidatin wählt Tür mit Auto“

B := „Auto hinter dritter Tür“

$$\Pr[A] = 1/3$$

$$\Pr[B \mid \overline{A}] = 1$$

$$\Pr[B \mid A] = 0$$

$$\Pr[A] = 1/3$$

$$\Pr[B]$$

$$= \Pr[B \mid \overline{A}]\,\Pr[\overline{A}] + \Pr[B \mid A]\,\Pr[A]$$

$$= 1 \cdot 2/3 + 0 \cdot 1/3$$

$$= 2/3$$

Multiplikationssatz

Satz 2.10. *(Multiplikationssatz)* Seien die Ereignisse $A_1, \ldots, A_n$ gegeben. Falls $\Pr[A_1 \cap \cdots \cap A_n] > 0$ ist, gilt

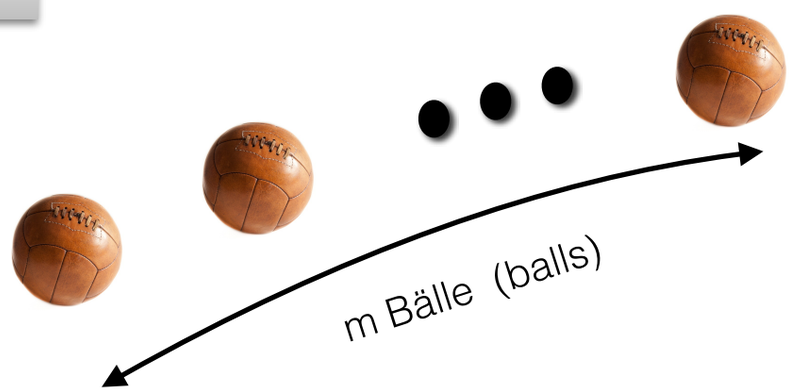
$$\Pr[A_1 \cap \cdots \cap A_n] = \Pr[A_1] \cdot \Pr[A_2|A_1] \cdot \Pr[A_3|A_1 \cap A_2] \cdots \Pr[A_n|A_1 \cap \cdots \cap A_{n-1}].$$

Beweis: Die rechte Seite ist:

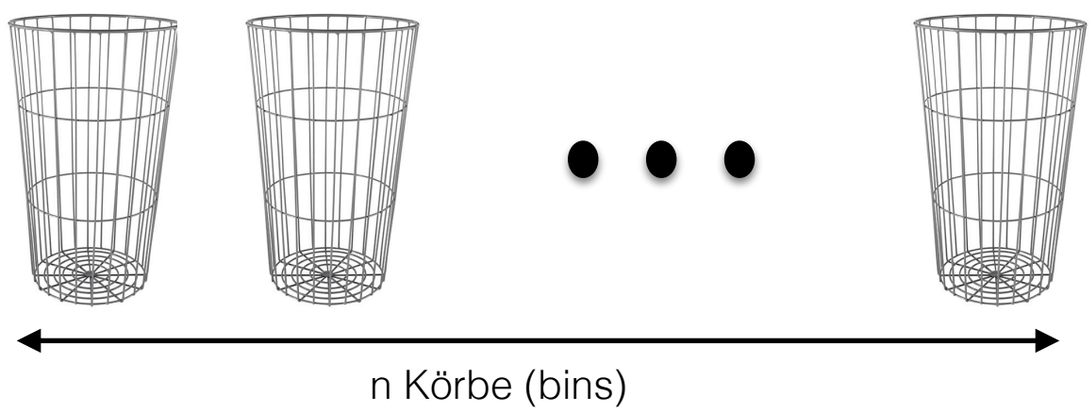
$$\frac{\Pr[A_1]}{1} \cdot \frac{\Pr[A_1 \cap A_2]}{\Pr[A_1]} \cdot \frac{\Pr[A_1 \cap A_2 \cap A_3]}{\Pr[A_1 \cap A_2]} \cdot \ldots \cdot \frac{\Pr[A_1 \cap \ldots \cap A_n]}{\Pr[A_1 \cap \ldots \cap A_{n-1}]}$$

Geburtstagsproblem

Umformulierung:



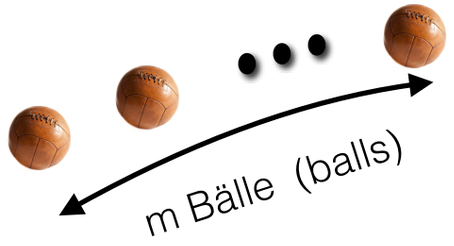
zufällig



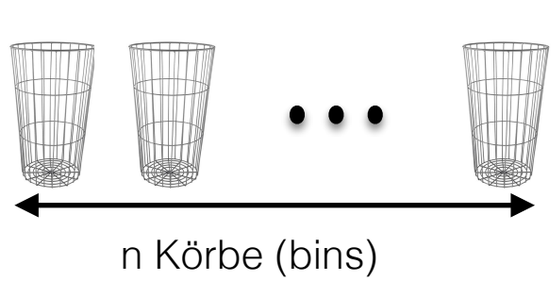
n = 365
m = Anzahl Personen

Geburtstagsproblem

A_i := i-ter Ball landet in einem Korb in dem noch kein Ball liegt



zufällig



$Pr[A_1] = 1$

$Pr[A_2 \mid A_1] = (n-1) / n$

allgemein:

$Pr[A_i \mid A_1 \cap \ldots \cap A_{i-1}] = (n-(i-1)) / n$

$$Pr[A_1 \cap \ldots \cap A_m] = 1 \cdot \frac{n-1}{n} \cdot \ldots \cdot \frac{n-(m-1)}{n}$$

Satz von Bayes

Satz *(Satz von Bayes)* Die Ereignisse $A_1, \ldots, A_n$ seien paarweise disjunkt. Ferner sei $B \subseteq A_1 \cup \ldots \cup A_n$ ein Ereignis mit $\Pr[B] > 0$. Dann gilt für ein beliebiges $i = 1, \ldots, n$

$$\Pr[A_i|B] = \frac{\Pr[A_i \cap B]}{\Pr[B]} = \frac{\Pr[B|A_i] \cdot \Pr[A_i]}{\sum_{j=1}^{n} \Pr[B|A_j] \cdot \Pr[A_j]}.$$

$\Longrightarrow$ Der Satz von Bayes ermöglicht es das Ereignis auf das wir bedingen und das dessen W'keit wir berechnen wollen zu vertauschen.

Satz von Bayes

Satz *(Satz von Bayes)* Die Ereignisse $A_1, \ldots, A_n$ seien paarweise disjunkt. Ferner sei $B \subseteq A_1 \cup \ldots \cup A_n$ ein Ereignis mit $\Pr[B] > 0$. Dann gilt für ein beliebiges $i = 1, \ldots, n$

$$\Pr[A_i|B] = \frac{\Pr[A_i \cap B]}{\Pr[B]} = \frac{\Pr[B|A_i] \cdot \Pr[A_i]}{\sum_{j=1}^{n} \Pr[B|A_j] \cdot \Pr[A_j]}.$$

Klassisches Anwendungsbeispiel: Test auf eine Krankheit ….

bekannt aus statistischen Untersuchungen:

Pr[„Test ist positiv“ I „Patient hat Krankheit X“]
Pr[„Test ist positiv“ I „Patient hat Krankheit X nicht“]

was uns interessiert

Pr[„habe Krankheit X“ I „Test ist positiv“]

Satz von Bayes

Satz *(Satz von Bayes)* Die Ereignisse $A_1, \ldots, A_n$ seien paarweise disjunkt. Ferner sei $B \subseteq A_1 \cup \ldots \cup A_n$ ein Ereignis mit $\Pr[B] > 0$. Dann gilt für ein beliebiges $i = 1, \ldots, n$

$$\Pr[A_i|B] = \frac{\Pr[A_i \cap B]}{\Pr[B]} = \frac{\Pr[B|A_i] \cdot \Pr[A_i]}{\sum_{j=1}^{n} \Pr[B|A_j] \cdot \Pr[A_j]}.$$

Beweis:

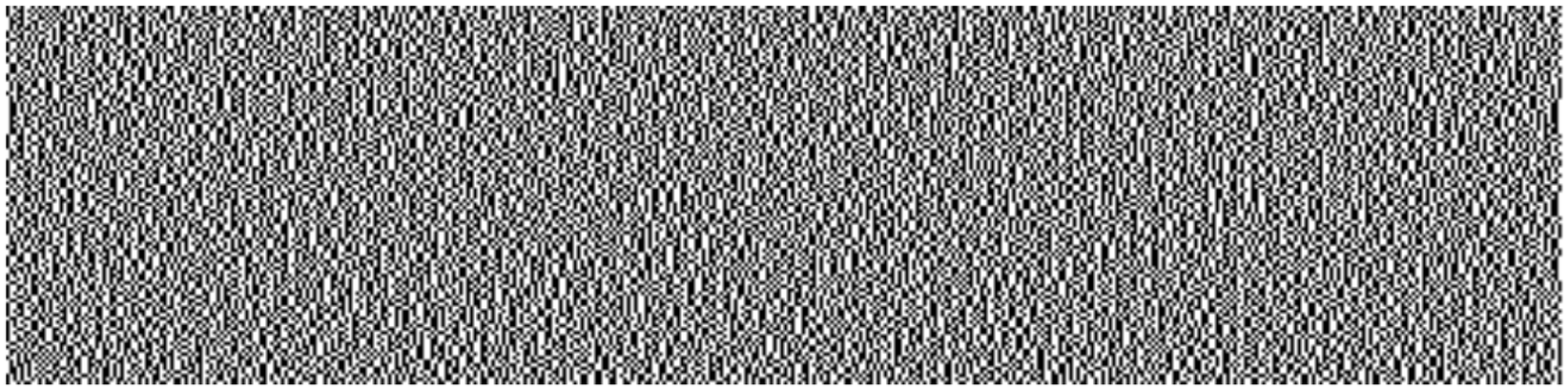
Zähler: $\text{Prob}[A_i \cap B] = \text{Prob}[B \cap A_i] = \text{Prob}[B \mid A_i] \cdot \text{Prob}[A_i]$

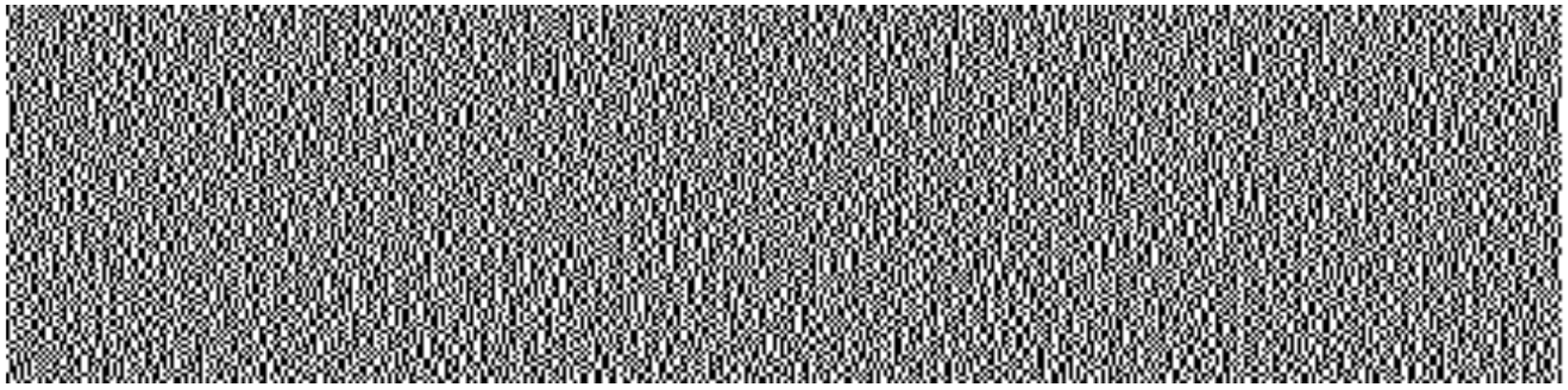
Nenner: $\text{Prob}[B] =$ *... wende Satz von der totalen Wahrscheinlichkeit an ...*

Kapitel 2.3

Unabhängigkeit

Visuelle Kryptographie

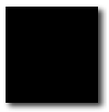




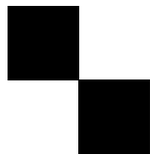
Codierung

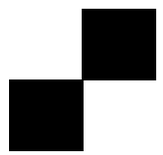
Bild 1 Bild 2 Bild 1+2

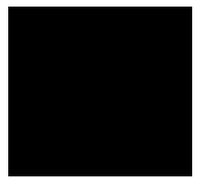
schwarzes Pixel

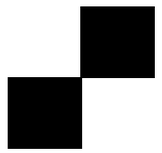


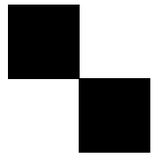
oder



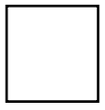




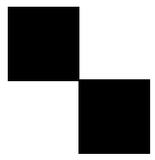


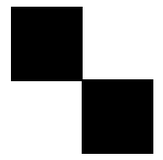


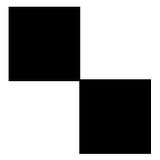
weisses Pixel

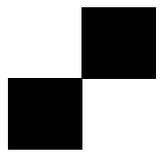


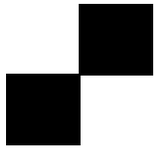
oder

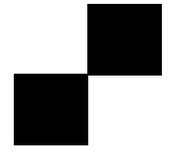












Visuelle Kryptographie

	Bild 1	Bild 2	Bild 1+2
schwarzes Pixel			
weisses Pixel			

Visuelle Kryptographie