

# Prinzipien zur Erzeugung von Zufallszahlen in der Informatik

Probevorlesung im Habilitationsverfahren an der  
Friedrich-Schiller-Universität Jena



Thomas Hinze

Brandenburgische Technische Universität Cottbus  
Institut für Informatik, Informations- und Medientechnik

`thomas.hinze@tu-cottbus.de`

11. Oktober 2012

# Was ist eigentlich Zufall?

Im Alltag: „Unabsichtlich passiert Unerklärliches.“  
Zufälle gaben Denkanstöße und verhalfen zu Entdeckungen



# Was ist eigentlich Zufall?

Im Alltag: „Unabsichtlich passiert Unerklärliches.“

Zufälle gaben Denkanstöße und verhalfen zu Entdeckungen

Bildquellen: wikipedia.org



C. Kolumbus, 1492  
"Amerika"

# Was ist eigentlich Zufall?

Im Alltag: „Unabsichtlich passiert Unerklärliches.“


Zufälle gaben Denkanstöße und verhalfen zu Entdeckungen

Bildquellen: wikipedia.org



C. Kolumbus, 1492  
"Amerika"






A. Kekule, 1865  
Benzolstruktur

# Was ist eigentlich Zufall?

Im Alltag: „Unabsichtlich passiert Unerklärliches.“

Zufälle gaben Denkanstöße und verhalfen zu Entdeckungen

Bildquellen: wikipedia.org


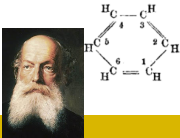
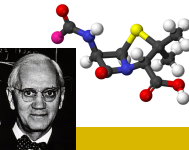
 <p>C. Kolumbus, 1492 "Amerika"</p>	 <p>A. Kekule, 1865 Benzolstruktur</p>	 <p>E. Fleming, 1928 Penicillin</p>
--	---	---

# Was ist eigentlich Zufall?

Im Alltag: „Unabsichtlich passiert Unerklärliches.“

Zufälle gaben Denkanstöße und verhalfen zu Entdeckungen

Bildquellen: wikipedia.org

 <p>C. Kolumbus, 1492 "Amerika"</p>	 <p>A. Kekule, 1865 Benzolstruktur</p>	 <p>E. Fleming, 1928 Penicillin</p>
--	---	---

## Begriff Zufall


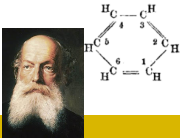
- an Auftreten oder Ausbleiben von *Ereignissen* gekoppelt
- einzelnes Ereignis oder Zusammentreffen mehrerer Ereignisse *ohne kausale Erklärung*

# Was ist eigentlich Zufall?

Im Alltag: „Unabsichtlich passiert Unerklärliches.“

Zufälle gaben Denkanstöße und verhalfen zu Entdeckungen

Bildquellen: wikipedia.org

 <p>C. Kolumbus, 1492 "Amerika"</p>	 <p>A. Kekule, 1865 Benzolstruktur</p>	 <p>E. Fleming, 1928 Penicillin</p>
--	---	---

## Begriff Zufall

- an Auftreten oder Ausbleiben von *Ereignissen* gekoppelt
- einzelnes Ereignis oder Zusammentreffen mehrerer Ereignisse *ohne kausale Erklärung*

⇒ Vier Arten des Zustandekommens von Zufall

# Woraus entsteht Zufall?

## 1. Ein Ereignis geschieht objektiv ohne Ursache

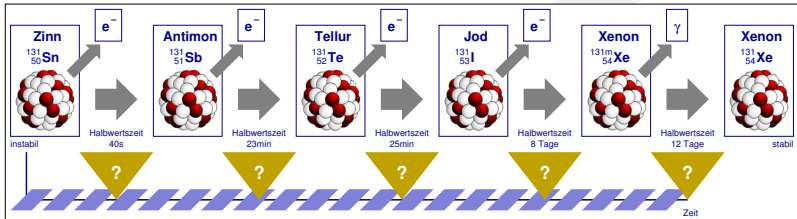




# Woraus entsteht Zufall?

## 1. Ein Ereignis geschieht objektiv ohne Ursache

vermutlich bei Quantenphänomenen und radioaktivem Zerfall

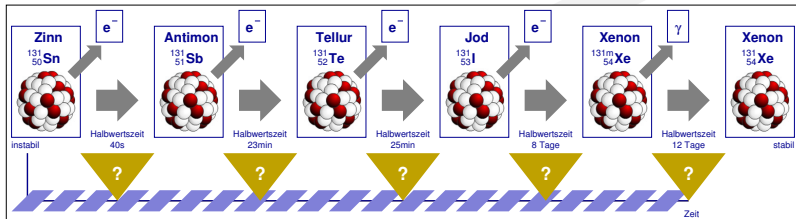


Zerfallskette von radioaktivem Zinn

# Woraus entsteht Zufall?

## 1. Ein Ereignis geschieht objektiv ohne Ursache

vermutlich bei Quantenphänomenen und radioaktivem Zerfall



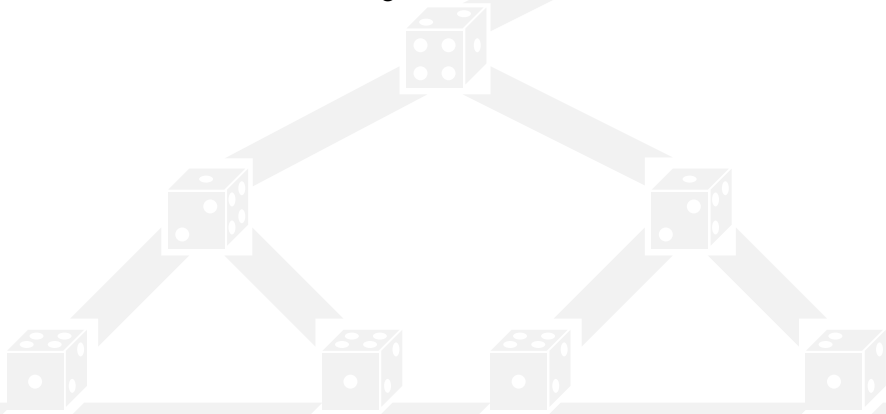
Zerfallskette von radioaktivem Zinn

- Vorhersage der spontanen Zerfallszeitpunkte eines konkreten Isotops unmöglich
- jedoch statistische Aussagen über viele Isotope möglich

# Woraus entsteht Zufall?

## 2. Ein Ereignis geschieht ohne erkennbare Ursache

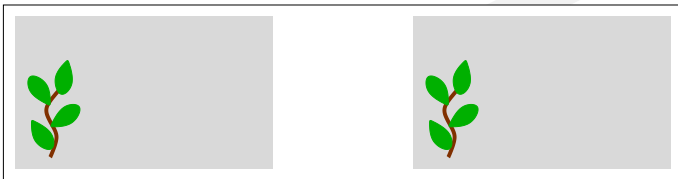
Ein Teil der Ursache-Wirkungs-Kette ist unbekannt



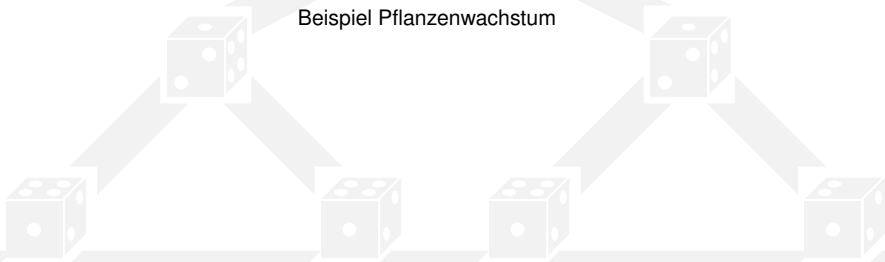
# Woraus entsteht Zufall?

## 2. Ein Ereignis geschieht ohne erkennbare Ursache

Ein Teil der Ursache-Wirkungs-Kette ist unbekannt



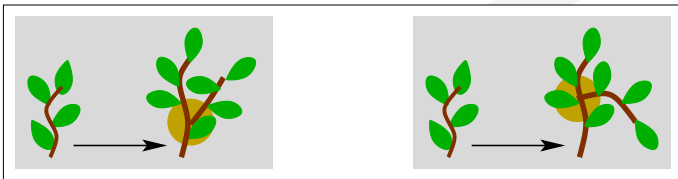
Beispiel Pflanzenwachstum



# Woraus entsteht Zufall?

## 2. Ein Ereignis geschieht ohne erkennbare Ursache

Ein Teil der Ursache-Wirkungs-Kette ist unbekannt



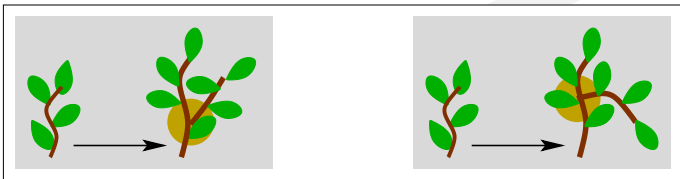
Warum Verästelung gerade an der beobachteten Stelle?



# Woraus entsteht Zufall?

## 2. Ein Ereignis geschieht ohne erkennbare Ursache

Ein Teil der Ursache-Wirkungs-Kette ist unbekannt



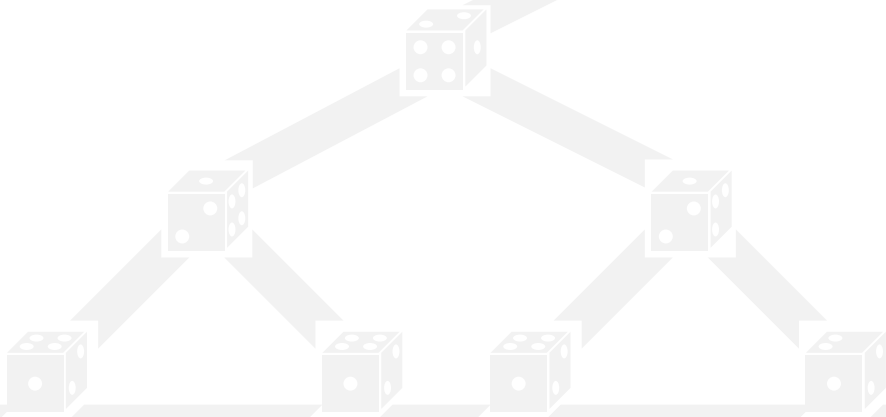
Warum Verästelung gerade an der beobachteten Stelle?

- unzureichendes Wissen über Einflussfaktoren, die ein konkretes Ereignis bewirken
- häufig wiederum statistische Aussagen über viele ähnliche Ereignisse möglich

## Woraus entsteht Zufall?

3. Ein Ereignis mit bekannten Einflussfaktoren geschieht, aber man kann diese nicht genau genug messen oder steuern, so dass das Ergebnis nicht vorhersagbar ist

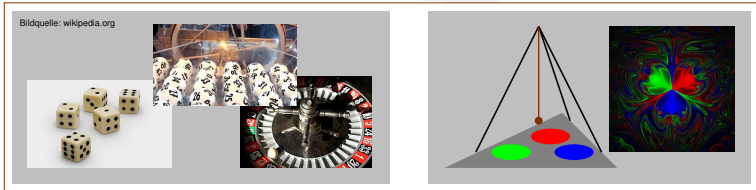
Glücksspiel und deterministisches Chaos



# Woraus entsteht Zufall?

**3. Ein Ereignis mit bekannten Einflussfaktoren geschieht, aber man kann diese nicht genau genug messen oder steuern, so dass das Ergebnis nicht vorhersagbar ist**

Glücksspiel und deterministisches Chaos



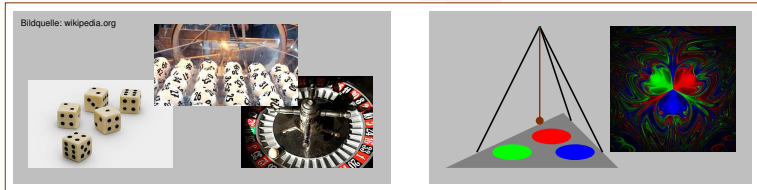
Würfel, Lotto, Roulette (links); Magnetpendel (rechts)



# Woraus entsteht Zufall?

## 3. Ein Ereignis mit bekannten Einflussfaktoren geschieht, aber man kann diese nicht genau genug messen oder steuern, so dass das Ergebnis nicht vorhersagbar ist

Glücksspiel und deterministisches Chaos



Würfel, Lotto, Roulette (links); Magnetpendel (rechts)

- entsprechende Systeme oft leicht konstruierbar
- gern zur Erzeugung echter Zufallszahlen genutzt
- statistische Aussagen möglich

# Woraus entsteht Zufall?

## 4. Zwei Ereignisse stehen in keinem (bekanntem) kausalen Zusammenhang

Zusammenhang zwischen den Ereignissen erscheint zufällig



# Woraus entsteht Zufall?

## 4. Zwei Ereignisse stehen in keinem (bekannten) kausalen Zusammenhang

Zusammenhang zwischen den Ereignissen erscheint zufällig

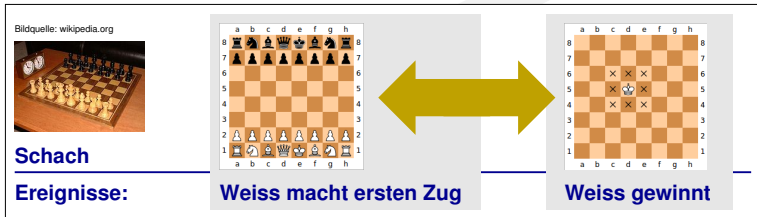


Schachspiel mit unbekanntem Spielern

# Woraus entsteht Zufall?

## 4. Zwei Ereignisse stehen in keinem (bekanntem) kausalen Zusammenhang

Zusammenhang zwischen den Ereignissen erscheint zufällig



Schachspiel mit unbekanntem Spielern

- kann in endlichen bzw. diskreten Systemen auftreten
- statistische Aussagen möglich

# Wofür benötigt man Zufall in der Informatik?

Hilfsmittel zur Entscheidungsfindung und für Algorithmenkonstruktion



# Wofür benötigt man Zufall in der Informatik?

Hilfsmittel zur Entscheidungsfindung und für Algorithmenkonstruktion

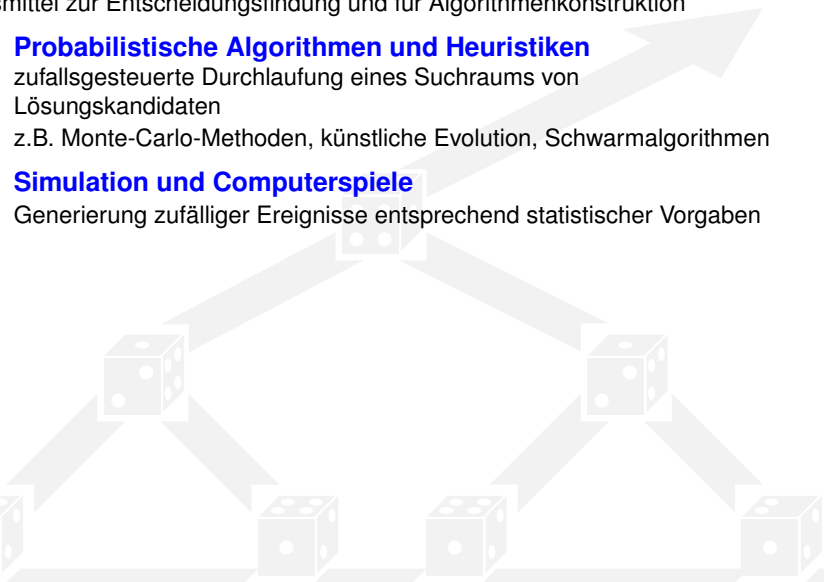
- **Probabilistische Algorithmen und Heuristiken**  
zufallsgesteuerte Durchlaufung eines Suchraums von Lösungskandidaten  
z.B. Monte-Carlo-Methoden, künstliche Evolution, Schwarmalgorithmen



# Wofür benötigt man Zufall in der Informatik?

Hilfsmittel zur Entscheidungsfindung und für Algorithmenkonstruktion

- **Probabilistische Algorithmen und Heuristiken**  
zufallsgesteuerte Durchlaufung eines Suchraums von Lösungskandidaten  
z.B. Monte-Carlo-Methoden, künstliche Evolution, Schwarmalgorithmen
- **Simulation und Computerspiele**  
Generierung zufälliger Ereignisse entsprechend statistischer Vorgaben



# Wofür benötigt man Zufall in der Informatik?

Hilfsmittel zur Entscheidungsfindung und für Algorithmenkonstruktion

- **Probabilistische Algorithmen und Heuristiken**  
zufallsgesteuerte Durchlaufung eines Suchraums von Lösungskandidaten  
z.B. Monte-Carlo-Methoden, künstliche Evolution, Schwarmalgorithmen
- **Simulation und Computerspiele**  
Generierung zufälliger Ereignisse entsprechend statistischer Vorgaben
- **Kryptographie / Kryptoanalyse**  
z.B. Schlüssel- und Parametererzeugung, Verschlüsselungsverfahren, Verfahren zur digitalen Signatur, Dummy Traffic, Angriffe auf kryptographische Verfahren



# Wofür benötigt man Zufall in der Informatik?

Hilfsmittel zur Entscheidungsfindung und für Algorithmenkonstruktion

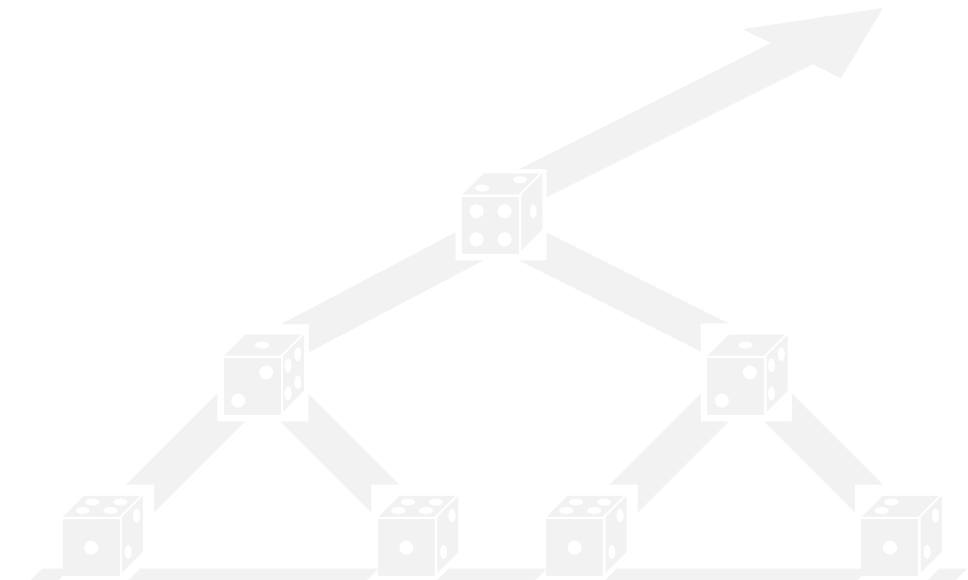
- **Probabilistische Algorithmen und Heuristiken**  
zufallsgesteuerte Durchlaufung eines Suchraums von Lösungskandidaten  
z.B. Monte-Carlo-Methoden, künstliche Evolution, Schwarmalgorithmen
- **Simulation und Computerspiele**  
Generierung zufälliger Ereignisse entsprechend statistischer Vorgaben
- **Kryptographie / Kryptoanalyse**  
z.B. Schlüssel- und Parametererzeugung, Verschlüsselungsverfahren, Verfahren zur digitalen Signatur, Dummy Traffic, Angriffe auf kryptographische Verfahren
- **Test**  
Generierung von Testsätzen für Soft- und Hardware

# Wofür benötigt man Zufall in der Informatik?

Hilfsmittel zur Entscheidungsfindung und für Algorithmenkonstruktion

- **Probabilistische Algorithmen und Heuristiken**  
zufallsgesteuerte Durchlaufung eines Suchraums von Lösungskandidaten  
z.B. Monte-Carlo-Methoden, künstliche Evolution, Schwarmalgorithmen
- **Simulation und Computerspiele**  
Generierung zufälliger Ereignisse entsprechend statistischer Vorgaben
- **Kryptographie / Kryptoanalyse**  
z.B. Schlüssel- und Parametererzeugung, Verschlüsselungsverfahren, Verfahren zur digitalen Signatur, Dummy Traffic, Angriffe auf kryptographische Verfahren
- **Test**  
Generierung von Testsätzen für Soft- und Hardware
- **Algorithmische Informationstheorie**  
theoretische Untersuchungen zu Informationsgehalt, Entropie und Komprimierbarkeit von Daten

# Grundlegende Begriffe und Zusammenhänge



# Grundlegende Begriffe und Zusammenhänge

- **zufälliges Ereignis**

**Ereignis**, dessen Eintrittszeitpunkt oder Wirkung **nicht** mit absoluter Sicherheit **vorhergesagt** werden kann

⇒ Zufall als Ausdruck von Unwissenheit



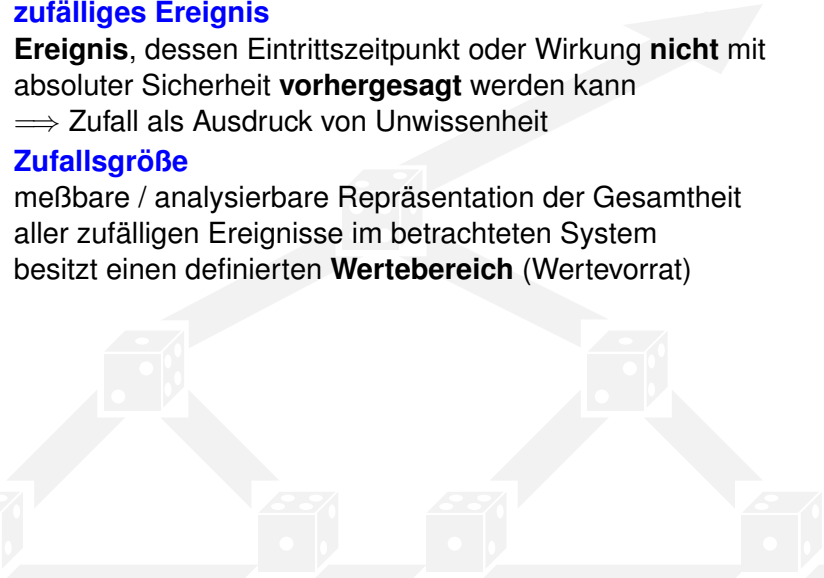
# Grundlegende Begriffe und Zusammenhänge

- **zufälliges Ereignis**

**Ereignis**, dessen Eintrittszeitpunkt oder Wirkung **nicht** mit absoluter Sicherheit **vorhergesagt** werden kann  
⇒ Zufall als Ausdruck von Unwissenheit

- **Zufallsgröße**

meßbare / analysierbare Repräsentation der Gesamtheit aller zufälligen Ereignisse im betrachteten System besitzt einen definierten **Wertebereich** (Wertevorrat)



# Grundlegende Begriffe und Zusammenhänge

- **zufälliges Ereignis**

**Ereignis**, dessen Eintrittszeitpunkt oder Wirkung **nicht** mit absoluter Sicherheit **vorhergesagt** werden kann  
⇒ Zufall als Ausdruck von Unwissenheit

- **Zufallsgröße**

meßbare / analysierbare Repräsentation der Gesamtheit aller zufälligen Ereignisse im betrachteten System besitzt einen definierten **Wertebereich** (Wertevorrat)

- **diskret**: **endlicher** oder **abzählbar unendlicher** Wertevorrat

# Grundlegende Begriffe und Zusammenhänge

- **zufälliges Ereignis**

**Ereignis**, dessen Eintrittszeitpunkt oder Wirkung **nicht** mit absoluter Sicherheit **vorhergesagt** werden kann  
⇒ Zufall als Ausdruck von Unwissenheit

- **Zufallsgröße**

meßbare / analysierbare Repräsentation der Gesamtheit aller zufälligen Ereignisse im betrachteten System besitzt einen definierten **Wertebereich** (Wertevorrat)

- **diskret**: **endlicher** oder **abzählbar unendlicher** Wertevorrat

- **Zufallszahl**

Wert, den eine Zufallsgröße bei ihrer Bestimmung annimmt

# Grundlegende Begriffe und Zusammenhänge

- **zufälliges Ereignis**

**Ereignis**, dessen Eintrittszeitpunkt oder Wirkung **nicht** mit absoluter Sicherheit **vorhergesagt** werden kann  
⇒ Zufall als Ausdruck von Unwissenheit

- **Zufallsgröße**

meßbare / analysierbare Repräsentation der Gesamtheit aller zufälligen Ereignisse im betrachteten System besitzt einen definierten **Wertebereich** (Wertevorrat)

- **diskret: endlicher** oder **abzählbar unendlicher** Wertevorrat

- **Zufallszahl**

Wert, den eine Zufallsgröße bei ihrer Bestimmung annimmt

- **Zufallszahlenfolge**

Folge voneinander möglichst **unabhängiger** Zufallszahlen, die einer gegebenen **statistischen Verteilung** genügen



# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:



# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:

- Gleichwahrscheinlichkeit der Ereignisse:  $P(X = a_i) = \frac{1}{n}$

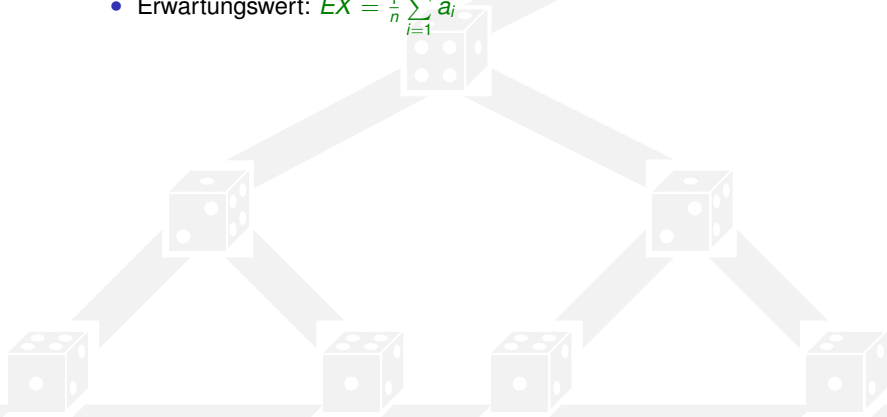


# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:

- Gleichwahrscheinlichkeit der Ereignisse:  $P(X = a_i) = \frac{1}{n}$
- Erwartungswert:  $EX = \frac{1}{n} \sum_{i=1}^n a_i$



# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:

- Gleichwahrscheinlichkeit der Ereignisse:  $P(X = a_i) = \frac{1}{n}$
- Erwartungswert:  $EX = \frac{1}{n} \sum_{i=1}^n a_i$
- Streuung:  $D^2 X = \frac{1}{n} \sum_{i=1}^n (a_i - EX)^2$

# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:

- Gleichwahrscheinlichkeit der Ereignisse:  $P(X = a_i) = \frac{1}{n}$
- Erwartungswert:  $EX = \frac{1}{n} \sum_{i=1}^n a_i$
- Streuung:  $D^2 X = \frac{1}{n} \sum_{i=1}^n (a_i - EX)^2$

- **Korrelation**

Grad des linearen Zusammenhangs zwischen Zufallsgrößen

# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:

- Gleichwahrscheinlichkeit der Ereignisse:  $P(X = a_i) = \frac{1}{n}$
- Erwartungswert:  $EX = \frac{1}{n} \sum_{i=1}^n a_i$
- Streuung:  $D^2 X = \frac{1}{n} \sum_{i=1}^n (a_i - EX)^2$

- **Korrelation**

Grad des linearen Zusammenhangs zwischen Zufallsgrößen

- **Korrelationskoeffizient**

zweier Zufallsgrößen  $X$  und  $Y$ :  $\rho(X, Y) := \frac{E(X \cdot Y) - EX \cdot EY}{\sqrt{D^2 X \cdot D^2 Y}}$

Es gilt:  $\rho(X, Y) = \begin{cases} = 0 & \rightarrow X, Y \text{ unkorreliert} \\ \neq 0 & \rightarrow X, Y \text{ korreliert} \end{cases}$

# Definitionen aus der mathematischen Statistik

- **diskret gleichverteilte Zufallsgröße**

Eine diskrete Zufallsgröße  $X$  heißt **gleichverteilt** auf den Ereignissen (Zufallszahlen)  $a_1, \dots, a_n$ , wenn für  $i = 1, \dots, n$  gilt:

- Gleichwahrscheinlichkeit der Ereignisse:  $P(X = a_i) = \frac{1}{n}$
- Erwartungswert:  $EX = \frac{1}{n} \sum_{i=1}^n a_i$
- Streuung:  $D^2 X = \frac{1}{n} \sum_{i=1}^n (a_i - EX)^2$

- **Korrelation**

Grad des linearen Zusammenhangs zwischen Zufallsgrößen

- **Korrelationskoeffizient**

zweier Zufallsgrößen  $X$  und  $Y$ :  $\rho(X, Y) := \frac{E(X \cdot Y) - EX \cdot EY}{\sqrt{D^2 X \cdot D^2 Y}}$

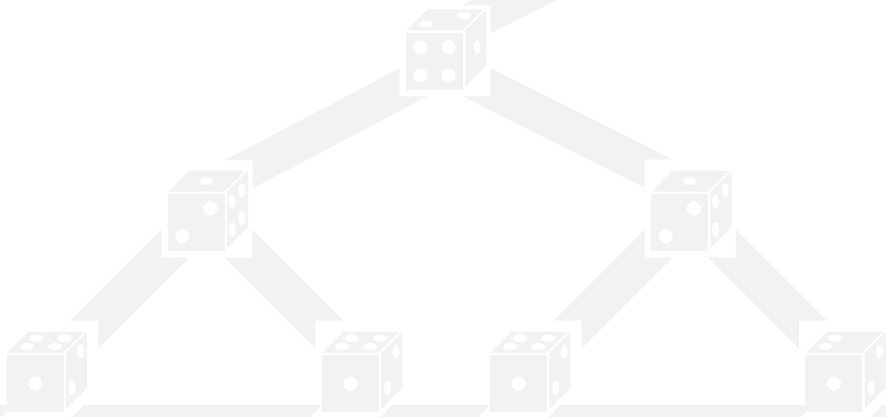
Es gilt:  $\rho(X, Y) = \begin{cases} = 0 & \rightarrow X, Y \text{ unkorreliert} \\ \neq 0 & \rightarrow X, Y \text{ korreliert} \end{cases}$

- **Autokorrelation**

Korrelation einer Zufallsgröße  $X$  mit sich selbst ( $\rho(X, X)$ )

# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern



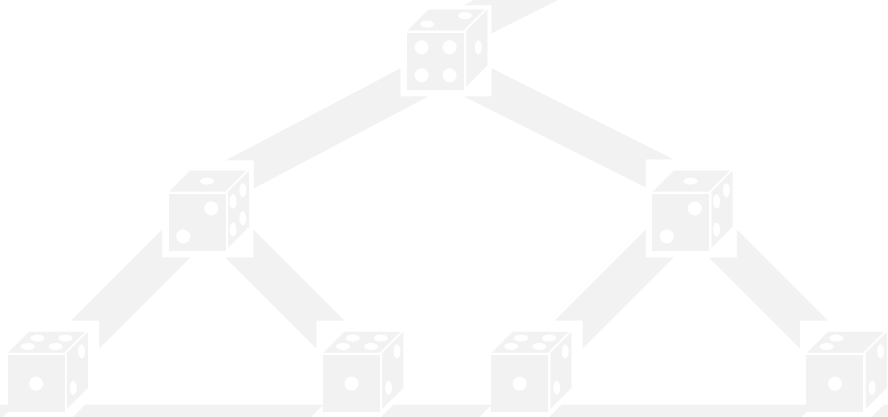


# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge



# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge
- **Unabhängigkeit:** keine Autokorrelation zwischen den erzeugten ZZ-Folgen



# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge
- **Unabhängigkeit:** keine Autokorrelation zwischen den erzeugten ZZ-Folgen

- **zusätzliche Wünsche/Erfordernisse**

- **diskrete** Zufallsgrößen

# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge
- **Unabhängigkeit:** keine Autokorrelation zwischen den erzeugten ZZ-Folgen

- **zusätzliche Wünsche/Erfordernisse**

- **diskrete** Zufallsgrößen
- anwendungsabhängig: entweder **Reproduzierbarkeit** oder **Irreproduzierbarkeit** der ZZ-Folgen

# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge
- **Unabhängigkeit:** keine Autokorrelation zwischen den erzeugten ZZ-Folgen

- **zusätzliche Wünsche/Erfordernisse**

- **diskrete** Zufallsgrößen
- anwendungsabhängig: entweder **Reproduzierbarkeit** oder **Irreproduzierbarkeit** der ZZ-Folgen
- ZZ oft im **Intervall**  $[0, 1)$ ,  $\{0, 1\}$ ,  $\{0, \dots, 9\}$

# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge
- **Unabhängigkeit:** keine Autokorrelation zwischen den erzeugten ZZ-Folgen

- **zusätzliche Wünsche/Erfordernisse**

- **diskrete** Zufallsgrößen
- anwendungsabhängig: entweder **Reproduzierbarkeit** oder **Irreproduzierbarkeit** der ZZ-Folgen
- ZZ oft im **Intervall**  $[0, 1)$ ,  $\{0, 1\}$ ,  $\{0, \dots, 9\}$
- **Schnelligkeit, Ergiebigkeit, Unvorhersagbarkeit** des Generators

# Vereinbarungen und Forderungen in der Informatik

- **Verarbeitung** der Zufallszahlen (ZZ) stets durch Computer
- **Erzeugung** der ZZ entweder durch Computer oder extern

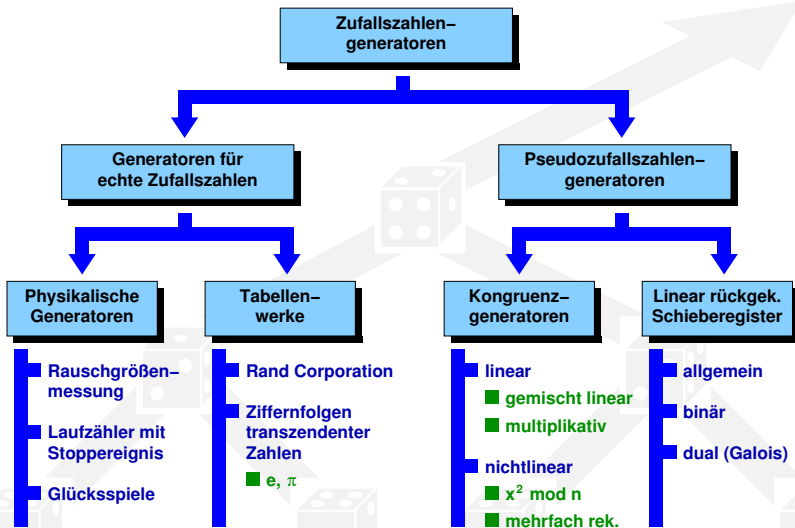
- **Grundanforderungen an Zufallszahlengeneratoren**

- **Uniformität:** Gleichvert. der ZZ in jeder erzeugten Folge
- **Unabhängigkeit:** keine Autokorrelation zwischen den erzeugten ZZ-Folgen

- **zusätzliche Wünsche/Erfordernisse**

- **diskrete** Zufallsgrößen
- anwendungsabhängig: entweder **Reproduzierbarkeit** oder **Irreproduzierbarkeit** der ZZ-Folgen
- ZZ oft im **Intervall**  $[0, 1)$ ,  $\{0, 1\}$ ,  $\{0, \dots, 9\}$
- **Schnelligkeit, Ergiebigkeit, Unvorhersagbarkeit** des Generators
- algorithmische Transformation Gleichverteilung → andere bekannte Verteilungen bei Bedarf

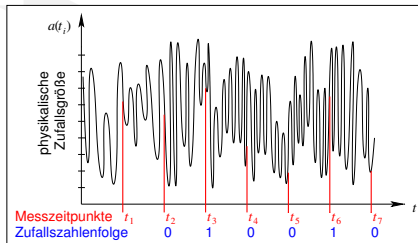
# Klassifikation der Prinzipien





# Rauschgrößenmessung

- zeitquantisierte Erfassung einer zugrundeliegenden physikalischen Zufallsgröße und Transformation in Zufallszahlenfolge
- Transformation z.B.:  
 $a(t_j) \geq a(t_{j-1}) \rightarrow \text{Ausgabe } y(t_j) = 1$   
 $a(t_j) < a(t_{j-1}) \rightarrow \text{Ausgabe } y(t_j) = 0$

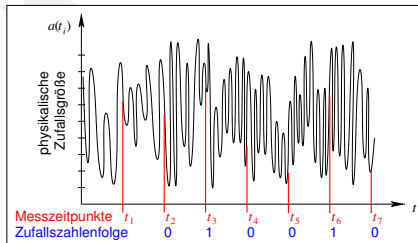


# Rauschgrößenmessung

- zeitquantisierte Erfassung einer zugrundeliegenden physikalischen Zufallsgröße und Transformation in Zufallszahlenfolge
- Transformation z.B.:  
 $a(t_j) \geq a(t_{j-1}) \rightarrow \text{Ausgabe } y(t_j) = 1$   
 $a(t_j) < a(t_{j-1}) \rightarrow \text{Ausgabe } y(t_j) = 0$

## Vorteile

- gute statistische Eigenschaften
- keine inhärente Reproduzierbarkeit



# Rauschgrößenmessung

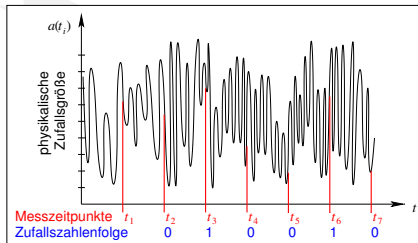
- zeitquantisierte Erfassung einer zugrundeliegenden physikalischen Zufallsgröße und Transformation in Zufallszahlenfolge
- Transformation z.B.:  
 $a(t_j) \geq a(t_{j-1}) \rightarrow \text{Ausgabe } y(t_j) = 1$   
 $a(t_j) < a(t_{j-1}) \rightarrow \text{Ausgabe } y(t_j) = 0$

## Vorteile

- gute statistische Eigenschaften
- keine inhärente Reproduzierbarkeit

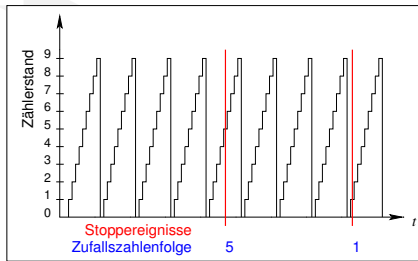
## Nachteile

- Auswirkungen von Messfehlern
- Verfügbarkeit und maximale Abtastrate abhängig von physikalischer Zufallsgröße



# Laufzähler mit Stoppereignis

- Zähler modulo  $n$ , der in schneller Folge fortlaufend von  $0$  bis  $n - 1$  zählt und jeweils bei Eintreten des zufälligen zählerunabhängigen Stoppereignisses sofort den aktuellen Zählerwert als Zufallszahl bereitstellt

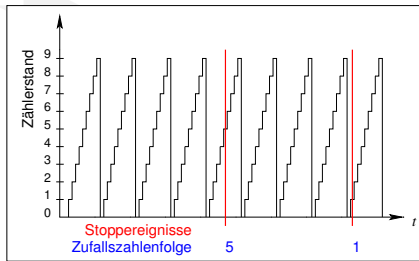


# Laufzähler mit Stoppereignis

- Zähler modulo  $n$ , der in schneller Folge fortlaufend von  $0$  bis  $n - 1$  zählt und jeweils bei Eintreten des zufälligen zählerunabhängigen Stoppereignisses sofort den aktuellen Zählerwert als Zufallszahl bereitstellt

## Vorteile

- gute statistische Eigenschaften
- keine inhärente Reproduzierbarkeit



# Laufzähler mit Stoppereignis

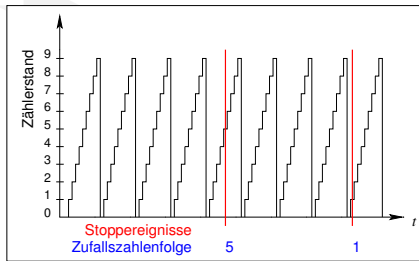
- Zähler modulo  $n$ , der in schneller Folge fortlaufend von  $0$  bis  $n - 1$  zählt und jeweils bei Eintreten des zufälligen zählerunabhängigen Stoppereignisses sofort den aktuellen Zählerwert als Zufallszahl bereitstellt

## Vorteile

- gute statistische Eigenschaften
- keine inhärente Reproduzierbarkeit

## Nachteile

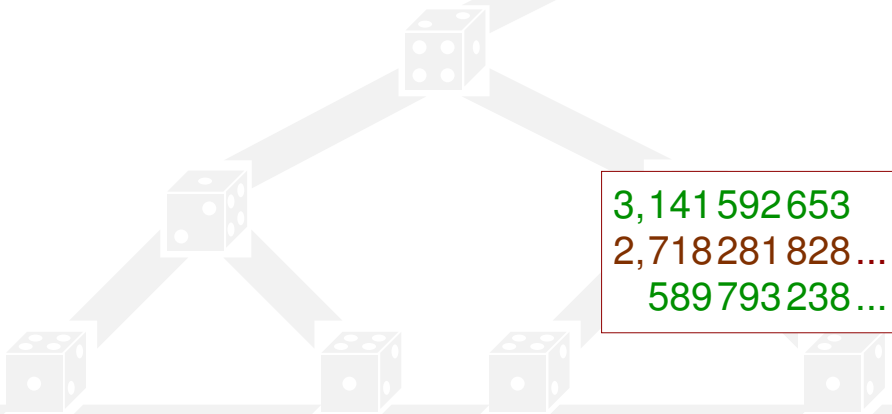
- Organisation der Stoppereignisse
- Stoppereignisse nicht zeitlich äquidistant
- mehrfaches vollständiges Durchzählen zwischen aufeinanderfolgenden Stoppereignissen sicherzustellen



# Ziffernfolgen transzendenter Zahlen

- Definition transzendente Zahlen**

Zahlen, die nicht algebraisch sind, d.h. die nicht als Nullstellen beliebiger Polynome  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  mit  $a_i \in \mathbb{Q}$  und  $i \in \{0, \dots, n\}$ ,  $n \in \mathbb{N} \setminus \{0\}$  vorkommen können. (z.B.  $e$ ,  $\pi$ )



3,141 592 653  
2,718 281 828 ...  
589 793 238 ...


# Ziffernfolgen transzendenter Zahlen

- **Definition transzendente Zahlen**

Zahlen, die nicht algebraisch sind, d.h. die nicht als Nullstellen beliebiger Polynome  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  mit  $a_i \in \mathbb{Q}$  und  $i \in \{0, \dots, n\}$ ,  $n \in \mathbb{N} \setminus \{0\}$  vorkommen können. (z.B.  $e$ ,  $\pi$ )

- **Prinzip**

- Berechnung und Tabellierung der gewünschten transzendenten Zahl auf hinreichend viele zuverlässige Nachkommastellen (z.B. mittels Spigotalgorithmus)
- zufällige Auswahl einer Ziffernfolge, Nutzung als Zufallszahlenfolge und Kennzeichnung als bereits genutzt



3,141 592 653  
2,718 281 828 ...  
589 793 238 ...



# Ziffernfolgen transzendenter Zahlen

- **Definition transzendente Zahlen**

Zahlen, die nicht algebraisch sind, d.h. die nicht als Nullstellen beliebiger Polynome  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  mit  $a_i \in \mathbb{Q}$  und  $i \in \{0, \dots, n\}$ ,  $n \in \mathbb{N} \setminus \{0\}$  vorkommen können. (z.B.  $e$ ,  $\pi$ )

- **Prinzip**

- Berechnung und Tabellierung der gewünschten transzendenten Zahl auf hinreichend viele zuverlässige Nachkommastellen (z.B. mittels Spigotalgorithmen)
- zufällige Auswahl einer Ziffernfolge, Nutzung als Zufallszahlenfolge und Kennzeichnung als bereits genutzt

## Vorteile

- leichte rechnergestützte Realisierbarkeit
- leichte Vorabgenerierung für spätere Nutzung

3,141 592 653  
2,718 281 828 ...  
589 793 238 ...

# Ziffernfolgen transzendenter Zahlen

- **Definition transzendente Zahlen**

Zahlen, die nicht algebraisch sind, d.h. die nicht als Nullstellen beliebiger Polynome  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  mit  $a_i \in \mathbb{Q}$  und  $i \in \{0, \dots, n\}$ ,  $n \in \mathbb{N} \setminus \{0\}$  vorkommen können. (z.B.  $e$ ,  $\pi$ )

- **Prinzip**

- Berechnung und Tabellierung der gewünschten transzendenten Zahl auf hinreichend viele zuverlässige Nachkommastellen (z.B. mittels Spigotalgorithm)en)
- zufällige Auswahl einer Ziffernfolge, Nutzung als Zufallszahlenfolge und Kennzeichnung als bereits genutzt

## Vorteile

- leichte rechnergestützte Realisierbarkeit
- leichte Vorabgenerierung für spätere Nutzung

## Nachteile

- keine gesicherten statistischen Eigenschaften, nur Annahmen
- hoher Bekanntheitsgrad der Ziffernfolgen

3,141 592 653  
2,718 281 828 ...  
589 793 238 ...

# Pseudozufallszahlengeneratoren

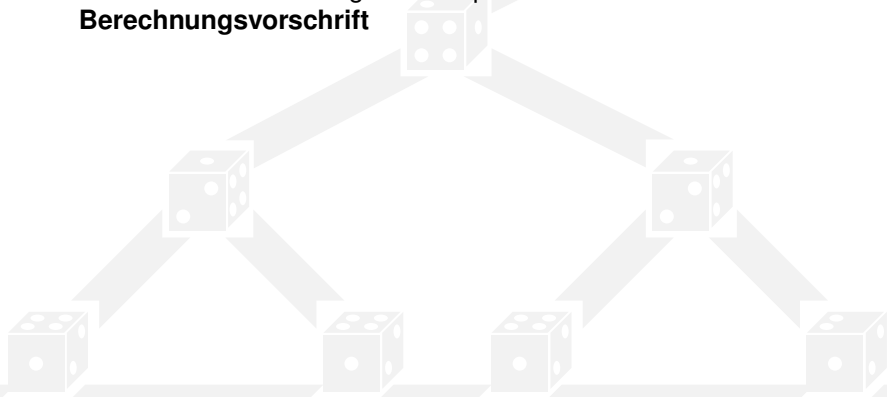
Gewinnung der Zahlenfolgen durch **deterministische Berechnung**  
Zufall → Pseudozufall: Wegfall der generellen Unvorhersagbarkeit



# Pseudozufallszahlengeneratoren

Gewinnung der Zahlenfolgen durch **deterministische Berechnung**  
Zufall → Pseudozufall: Wegfall der generellen Unvorhersagbarkeit

- **gemeinsames Prinzip**  
ausgehend von einem gewählten **Startwert** und **geeigneten Parameterbelegungen** erfolgt Bestimmung der Pseudozufallszahlenfolge durch spezifische **rekursive Berechnungsvorschrift**



# Pseudozufallszahlengeneratoren

Gewinnung der Zahlenfolgen durch **deterministische Berechnung**  
Zufall → Pseudozufall: Wegfall der generellen Unvorhersagbarkeit

- **gemeinsames Prinzip**  
ausgehend von einem gewählten **Startwert** und **geeigneten Parameterbelegungen** erfolgt Bestimmung der Pseudozufallszahlenfolge durch spezifische **rekursive Berechnungsvorschrift**
- **Forderung für perfekten Pseudozufallszahlengenerator**  
Es soll **keinen effizienten** (polynomiellen) **Algorithmus** geben, der eine **Pseudozufallszahlenfolge** ohne Kenntnis der Berechnungsvorschrift, des Startwertes und der Parameterbelegungen signifikant von einer **echten Zufallszahlenfolge unterscheiden** kann.

# Pseudozufallszahlengeneratoren

Gewinnung der Zahlenfolgen durch **deterministische Berechnung**  
Zufall → Pseudozufall: Wegfall der generellen Unvorhersagbarkeit

- **gemeinsames Prinzip**  
ausgehend von einem gewählten **Startwert** und **geeigneten Parameterbelegungen** erfolgt Bestimmung der Pseudozufallszahlenfolge durch spezifische **rekursive Berechnungsvorschrift**
- **Forderung für perfekten Pseudozufallszahlengenerator**  
Es soll **keinen effizienten** (polynomiellen) **Algorithmus** geben, der eine **Pseudozufallszahlenfolge** ohne Kenntnis der Berechnungsvorschrift, des Startwertes und der Parameterbelegungen signifikant von einer **echten Zufallszahlenfolge unterscheiden** kann.
- **gemeinsame Eigenschaft**
  - **Periodizität:** zyklische Wiederholung der Pseudozufallszahlenfolge (PZZ-Folge) nach endlicher Länge
  - **Ziel:** Maximierung der Periodenlänge

# Multiplikativer Kongruenzgenerator

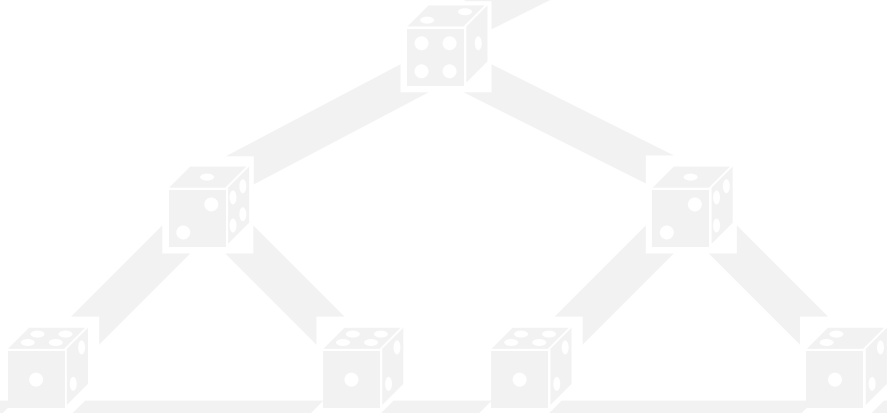
- Prinzip

**Parameter:**  $a, m \in \mathbb{N}$  mit  $a \geq 2, a < m, m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1}) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$



# Multiplikativer Kongruenzgenerator

- **Prinzip**

**Parameter:**  $a, m \in \mathbb{N}$  mit  $a \geq 2$ ,  $a < m$ ,  $m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1}) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

- **maximale Periodenlänge**

$m$  unter folgenden Bedingungen (Kobayashi):

- $m = p^k$  oder  $m = 2p^k$  mit  $p$  ungerade Primzahl,  $k \in \mathbb{N} \setminus \{0\}$
- $a^{m-1} \equiv 1 \pmod m$
- $\text{ggT}(z_0, m) = 1$

Minimierung der Autokorrelation:  $a \approx \sqrt{m}$



# Multiplikativer Kongruenzgenerator

- **Prinzip**

**Parameter:**  $a, m \in \mathbb{N}$  mit  $a \geq 2$ ,  $a < m$ ,  $m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1}) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

- **maximale Periodenlänge**

$m$  unter folgenden Bedingungen (Kobayashi):

- $m = p^k$  oder  $m = 2p^k$  mit  $p$  ungerade Primzahl,  $k \in \mathbb{N} \setminus \{0\}$
- $a^{m-1} \equiv 1 \pmod m$
- $\text{ggT}(z_0, m) = 1$

Minimierung der Autokorrelation:  $a \approx \sqrt{m}$

## Vorteile

- Schnelligkeit des Verfahrens und leichte Implementierbarkeit

# Multiplikativer Kongruenzgenerator

- **Prinzip**

**Parameter:**  $a, m \in \mathbb{N}$  mit  $a \geq 2, a < m, m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1}) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

- **maximale Periodenlänge**

$m$  unter folgenden Bedingungen (Kobayashi):

- $m = p^k$  oder  $m = 2p^k$  mit  $p$  ungerade Primzahl,  $k \in \mathbb{N} \setminus \{0\}$
- $a^{m-1} \equiv 1 \pmod m$
- $\text{ggT}(z_0, m) = 1$

Minimierung der Autokorrelation:  $a \approx \sqrt{m}$

## Vorteile

- Schnelligkeit des Verfahrens und leichte Implementierbarkeit

## Nachteile

- keine optimalen statistischen Eigenschaften, kleine Periodenlänge
- leichte Vorhersagbarkeit der PZZ-Folge (nicht perfekt)

# Gemischt linearer Kongruenzgenerator

- Prinzip

**Parameter:**  $a, c, m \in \mathbb{N}$  mit  $a < m$ ,  $a \geq 2$ ,  $c < m$ ,  $c > 0$ ,  $m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1} + c) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$



# Gemischt linearer Kongruenzgenerator

- **Prinzip**

**Parameter:**  $a, c, m \in \mathbb{N}$  mit  $a < m$ ,  $a \geq 2$ ,  $c < m$ ,  $c > 0$ ,  $m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1} + c) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

- **maximale Periodenlänge**

$m$  unter folgenden Bedingungen (Lehmer):

- $\text{ggT}(c, m) = 1$
- $a \equiv 1 \pmod q$  für jeden Elementarteiler  $q$  von  $m$
- $a \equiv 1 \pmod 4$  falls 4 Teiler von  $m$  ist

Minimierung der Autokorr. (Fishman/Greenb.):  $a \approx \sqrt{m - \frac{6c}{m}(1 - \frac{c}{m})}$

# Gemischt linearer Kongruenzgenerator

## • Prinzip

**Parameter:**  $a, c, m \in \mathbb{N}$  mit  $a < m$ ,  $a \geq 2$ ,  $c < m$ ,  $c > 0$ ,  $m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1} + c) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

## • maximale Periodenlänge

$m$  unter folgenden Bedingungen (Lehmer):

- $\text{ggT}(c, m) = 1$
- $a \equiv 1 \pmod q$  für jeden Elementarteiler  $q$  von  $m$
- $a \equiv 1 \pmod 4$  falls 4 Teiler von  $m$  ist

Minimierung der Autokorr. (Fishman/Greenb.):  $a \approx \sqrt{m - \frac{6c}{m}(1 - \frac{c}{m})}$

## Vorteile

- Schnelligkeit des Verfahrens und leichte Implementierbarkeit

# Gemischt linearer Kongruenzgenerator

## • Prinzip

**Parameter:**  $a, c, m \in \mathbb{N}$  mit  $a < m$ ,  $a \geq 2$ ,  $c < m$ ,  $c > 0$ ,  $m > 1$

**Startwert:**  $z_0 \in \{1, \dots, m-1\}$

**Rekursion:**  $z_i = (a \cdot z_{i-1} + c) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

## • maximale Periodenlänge

$m$  unter folgenden Bedingungen (Lehmer):

- $\text{ggT}(c, m) = 1$
- $a \equiv 1 \pmod q$  für jeden Elementarteiler  $q$  von  $m$
- $a \equiv 1 \pmod 4$  falls 4 Teiler von  $m$  ist

Minimierung der Autokorr. (Fishman/Greenb.):  $a \approx \sqrt{m - \frac{6c}{m}(1 - \frac{c}{m})}$

## Vorteile

- Schnelligkeit des Verfahrens und leichte Implementierbarkeit

## Nachteile

- keine optimalen statistischen Eigenschaften, kleine Periodenlänge
- leichte Vorhersagbarkeit der PZZ-Folge (nicht perfekt)

# Mehrfach rekursiver Kongruenzgenerator

- Prinzip

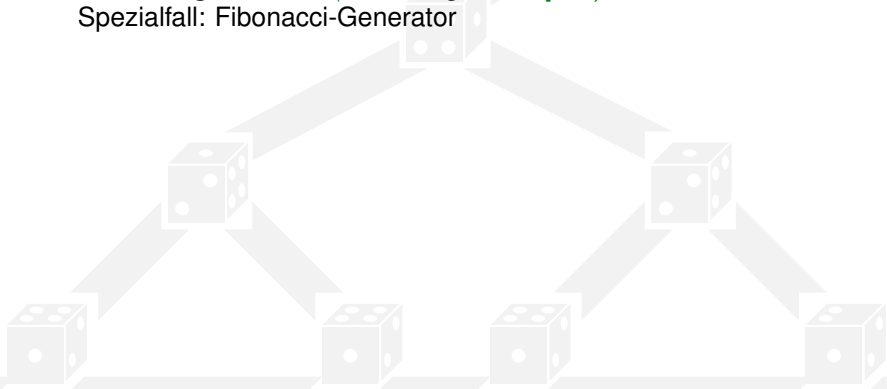
**Parameter:**  $r, m, a_1, \dots, a_r \in \mathbb{N}$  mit  $r \geq 1, a_i \in \{0, \dots, m-1\}, m > 1$

**Startwert:**  $z_1, \dots, z_r \in \{0, \dots, m-1\}$  mit  $\exists j \in \{1, \dots, r\} \cdot z_j \neq 0$

**Rekursion:**  $z_i = \left( \sum_{k=1}^r a_k \cdot z_{i-k} \right) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

Spezialfall: Fibonacci-Generator



# Mehrfach rekursiver Kongruenzgenerator

- Prinzip

**Parameter:**  $r, m, a_1, \dots, a_r \in \mathbb{N}$  mit  $r \geq 1, a_i \in \{0, \dots, m-1\}, m > 1$

**Startwert:**  $z_1, \dots, z_r \in \{0, \dots, m-1\}$  mit  $\exists j \in \{1, \dots, r\} \cdot z_j \neq 0$

**Rekursion:**  $z_i = \left( \sum_{k=1}^r a_k \cdot z_{i-k} \right) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

Spezialfall: Fibonacci-Generator

- maximale Periodenlänge

$m^r - 1$

Belegungsvorschrift der Parameter für max. Periodenlänge ändert sich mit jedem Vorgabewert für  $r$ , keine geschl. Darst.



# Mehrfach rekursiver Kongruenzgenerator

- **Prinzip**

**Parameter:**  $r, m, a_1, \dots, a_r \in \mathbb{N}$  mit  $r \geq 1$ ,  $a_i \in \{0, \dots, m-1\}$ ,  $m > 1$

**Startwert:**  $z_1, \dots, z_r \in \{0, \dots, m-1\}$  mit  $\exists j \in \{1, \dots, r\} \cdot z_j \neq 0$

**Rekursion:**  $z_i = \left( \sum_{k=1}^r a_k \cdot z_{i-k} \right) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

Spezialfall: Fibonacci-Generator

- **maximale Periodenlänge**

$$m^r - 1$$

Belegungsvorschrift der Parameter für max. Periodenlänge ändert sich mit jedem Vorgabewert für  $r$ , keine geschl. Darst.

## Vorteile

- größere maximale Periodenlänge, schwierigere Vorhersagbarkeit
- Schnelligkeit des Verfahrens und leichte Implementierbarkeit

# Mehrfach rekursiver Kongruenzgenerator

- **Prinzip**

**Parameter:**  $r, m, a_1, \dots, a_r \in \mathbb{N}$  mit  $r \geq 1$ ,  $a_i \in \{0, \dots, m-1\}$ ,  $m > 1$

**Startwert:**  $z_1, \dots, z_r \in \{0, \dots, m-1\}$  mit  $\exists j \in \{1, \dots, r\} \cdot z_j \neq 0$

**Rekursion:**  $z_i = \left( \sum_{k=1}^r a_k \cdot z_{i-k} \right) \bmod m$

**PZZ-Folge:**  $r_i = z_i/m$  Es gilt:  $r_i \in [0, 1)$

Spezialfall: Fibonacci-Generator

- **maximale Periodenlänge**

$$m^r - 1$$

Belegungs Vorschrift der Parameter für max. Periodenlänge ändert sich mit jedem Vorgabewert für  $r$ , keine geschl. Darst.

## Vorteile

- größere maximale Periodenlänge, schwierigere Vorhersagbarkeit
- Schnelligkeit des Verfahrens und leichte Implementierbarkeit

## Nachteile

- keine optimalen statistischen Eigenschaften, nicht perfekt
- hoher Aufwand zum Finden geeigneter Parameterbelegungen

# $x^2 \bmod n$ Generator nach Blum/Shub

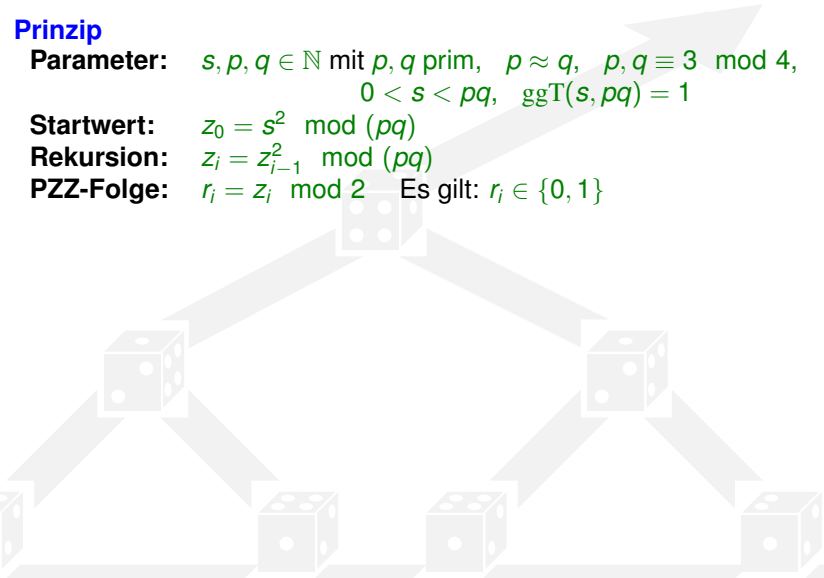
- Prinzip

**Parameter:**  $s, p, q \in \mathbb{N}$  mit  $p, q$  prim,  $p \approx q$ ,  $p, q \equiv 3 \pmod{4}$ ,  
 $0 < s < pq$ ,  $\text{ggT}(s, pq) = 1$

**Startwert:**  $z_0 = s^2 \bmod (pq)$

**Rekursion:**  $z_i = z_{i-1}^2 \bmod (pq)$

**PZZ-Folge:**  $r_i = z_i \bmod 2$  — Es gilt:  $r_i \in \{0, 1\}$



# $x^2 \bmod n$ Generator nach Blum/Shub

- **Prinzip**

**Parameter:**  $s, p, q \in \mathbb{N}$  mit  $p, q$  prim,  $p \approx q$ ,  $p, q \equiv 3 \pmod{4}$ ,  
 $0 < s < pq$ ,  $\text{ggT}(s, pq) = 1$

**Startwert:**  $z_0 = s^2 \bmod (pq)$

**Rekursion:**  $z_i = z_{i-1}^2 \bmod (pq)$

**PZZ-Folge:**  $r_i = z_i \bmod 2$  — Es gilt:  $r_i \in \{0, 1\}$

- **maximale Periodenlänge**

$pq$

# $x^2 \bmod n$ Generator nach Blum/Shub

- **Prinzip**

**Parameter:**  $s, p, q \in \mathbb{N}$  mit  $p, q$  prim,  $p \approx q$ ,  $p, q \equiv 3 \pmod{4}$ ,  
 $0 < s < pq$ ,  $\text{ggT}(s, pq) = 1$

**Startwert:**  $z_0 = s^2 \bmod (pq)$

**Rekursion:**  $z_i = z_{i-1}^2 \bmod (pq)$

**PZZ-Folge:**  $r_i = z_i \bmod 2$  — Es gilt:  $r_i \in \{0, 1\}$

- **maximale Periodenlänge**

$pq$

## Vorteile

- perfekter Pseudozufallszahlengenerator
- leichte Implementierbarkeit
- leichte Wahl geeigneter Parameterbelegungen

# $x^2 \bmod n$ Generator nach Blum/Shub

- **Prinzip**

**Parameter:**  $s, p, q \in \mathbb{N}$  mit  $p, q$  prim,  $p \approx q$ ,  $p, q \equiv 3 \pmod{4}$ ,  
 $0 < s < pq$ ,  $\text{ggT}(s, pq) = 1$

**Startwert:**  $z_0 = s^2 \bmod (pq)$

**Rekursion:**  $z_i = z_{i-1}^2 \bmod (pq)$

**PZZ-Folge:**  $r_i = z_i \bmod 2$  — Es gilt:  $r_i \in \{0, 1\}$

- **maximale Periodenlänge**

$pq$

## Vorteile

- perfekter Pseudozufallszahlengenerator
- leichte Implementierbarkeit
- leichte Wahl geeigneter Parameterbelegungen

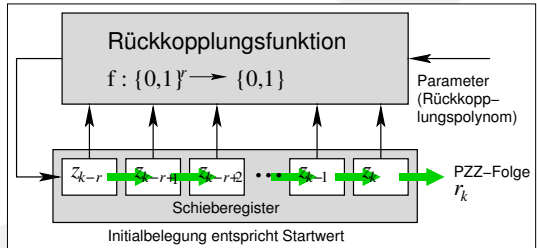
## Nachteile

- nur ein Bit pro Rekursionsschritt  $\rightarrow$  langsam
- kleine Periodenlänge

# Linear rückgekoppeltes Schieberegister

- Prinzip**

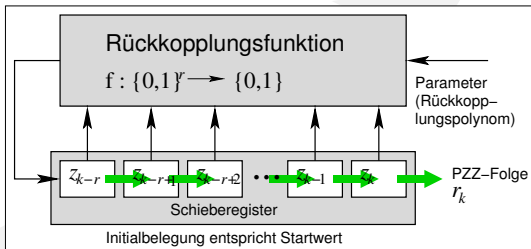
- Schieberegister mit Bitfolge  $\neq 0^r$  initialisiert



# Linear rückgekoppeltes Schieberegister

- **Prinzip**

- Schieberegister mit Bitfolge  $\neq 0^r$  initialisiert
- Bits schieben sich taktweise durch die Kaskade

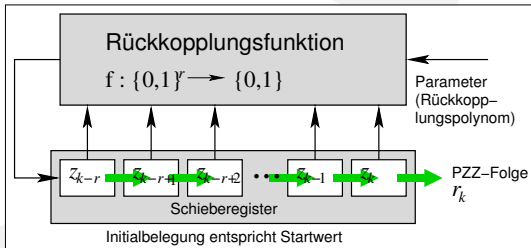




# Linear rückgekoppeltes Schieberegister

- **Prinzip**

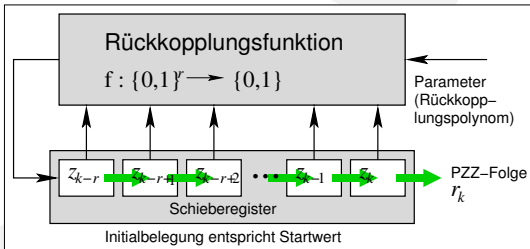
- Schieberegister mit Bitfolge  $\neq 0^r$  initialisiert
- Bits schieben sich taktweise durch die Kaskade
- Bit der letzten Zelle als Pseudozufallsbit taktweise ausgegeben



# Linear rückgekoppeltes Schieberegister

- Prinzip**

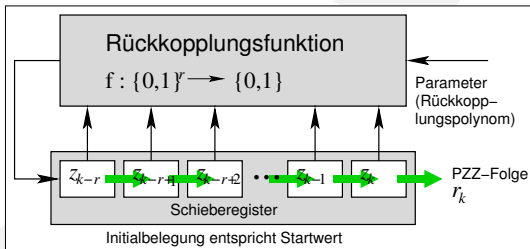
- Schieberegister mit Bitfolge  $\neq 0^r$  initialisiert
- Bits schieben sich taktweise durch die Kaskade
- Bit der letzten Zelle als Pseudozufallsbit taktweise ausgegeben
- Bit der ersten Zelle mittels Rückkopplungsfunktion berechnet



# Linear rückgekoppeltes Schieberegister

## • Prinzip

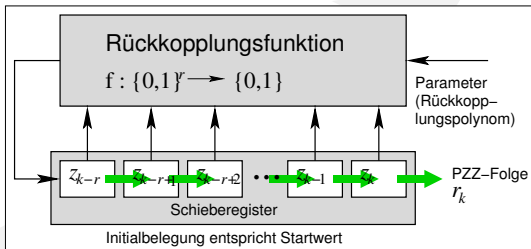
- Schieberegister mit Bitfolge  $\neq 0^r$  initialisiert
- Bits schieben sich taktweise durch die Kaskade
- Bit der letzten Zelle als Pseudozufallsbit taktweise ausgegeben
- Bit der ersten Zelle mittels Rückkopplungsfunktion berechnet
- Rückkopplungsfunktion und ihre Parameter bestimmen wesentlich die Qualität der PZZ-Folge



# Linear rückgekoppeltes Schieberegister

## • Prinzip

- Schieberegister mit Bitfolge  $\neq 0^r$  initialisiert
- Bits schieben sich taktweise durch die Kaskade
- Bit der letzten Zelle als Pseudozufallsbit taktweise ausgegeben
- Bit der ersten Zelle mittels Rückkopplungsfunktion berechnet
- Rückkopplungsfunktion und ihre Parameter bestimmen wesentlich die Qualität der PZZ-Folge



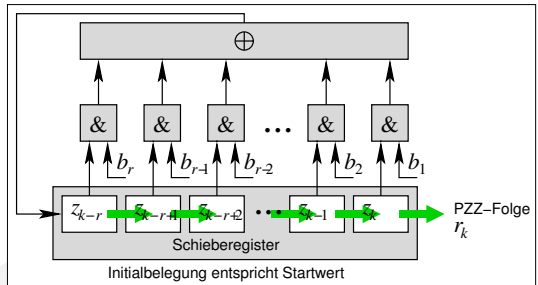
## • maximale Periodenlänge

$2^r - 1$  Bit, unabhängig von der gewählten zulässigen Initialisierung

# Binäres linear rückgekoppeltes Schieberegister

## Prinzip

- Rückkopplungsfkt. mit den Parametern  $b_i \in \{0, 1\}$  mit  $i = 1, \dots, r$  behaftet



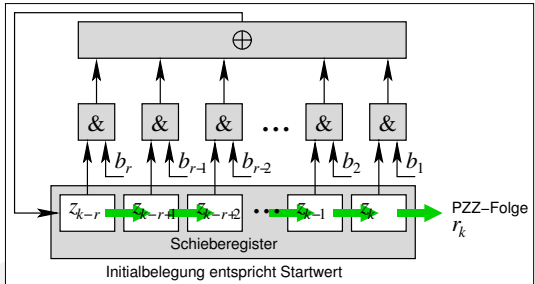
# Binäres linear rückgekoppeltes Schieberegister

## Prinzip

- Rückkopplungsfkt. mit den Parametern  $b_i \in \{0, 1\}$  mit  $i = 1, \dots, r$  behaftet
- Parameter  $b_i$  bilden Koeffizienten des **charakt. Polynoms**

$$p : \{0, 1\} \rightarrow \{0, 1\}$$

$$p(x) = b_r x^{r-1} \oplus \dots \oplus b_3 x^2 \oplus b_2 x \oplus b_1$$



# Binäres linear rückgekoppeltes Schieberegister

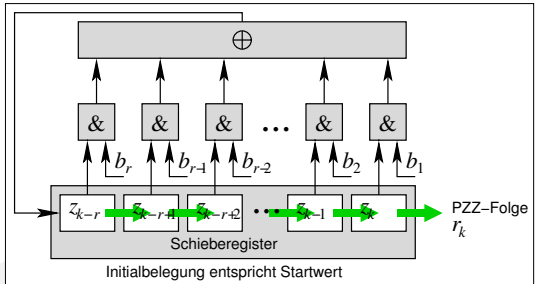
## Prinzip

- Rückkopplungsfkt. mit den Parametern  $b_i \in \{0, 1\}$  mit  $i = 1, \dots, r$  behaftet
- Parameter  $b_i$  bilden Koeffizienten des **charakt. Polynoms**

$$p : \{0, 1\} \rightarrow \{0, 1\}$$

$$p(x) = b_r x^{r-1} \oplus \dots \oplus b_3 x^2 \oplus b_2 x \oplus b_1$$

- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein



# Binäres linear rückgekoppeltes Schieberegister

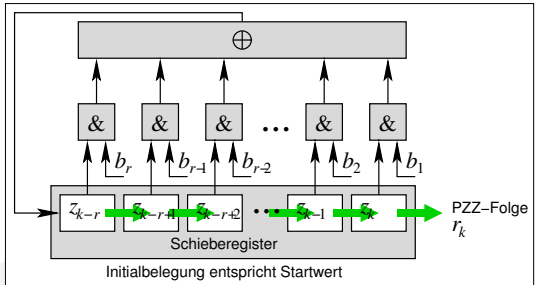
## Prinzip

- Rückkopplungsfkt. mit den Parametern  $b_i \in \{0, 1\}$  mit  $i = 1, \dots, r$  behaftet
- Parameter  $b_i$  bilden Koeffizienten des **charakt. Polynoms**

$$p : \{0, 1\} \rightarrow \{0, 1\}$$

$$p(x) = b_r x^{r-1} \oplus \dots \oplus b_3 x^2 \oplus b_2 x \oplus b_1$$

- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein



## Vorteile

- leicht in Hardware implementierbar
- sehr schnell, einfache Parameterwahl



# Binäres linear rückgekoppeltes Schieberegister

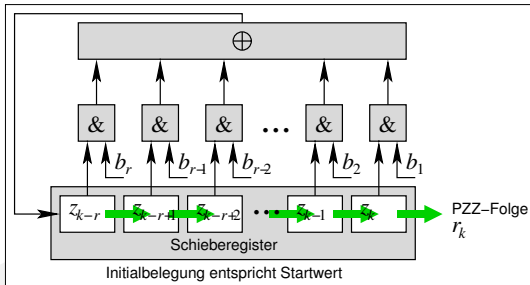
## Prinzip

- Rückkopplungsfkt. mit den Parametern  $b_i \in \{0, 1\}$  mit  $i = 1, \dots, r$  behaftet
- Parameter  $b_i$  bilden Koeffizienten des **charakt. Polynoms**

$$p : \{0, 1\} \rightarrow \{0, 1\}$$

$$p(x) = b_r x^{r-1} \oplus \dots \oplus b_3 x^2 \oplus b_2 x \oplus b_1$$

- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein



## Vorteile

- leicht in Hardware implementierbar
- sehr schnell, einfache Parameterwahl

## Nachteile

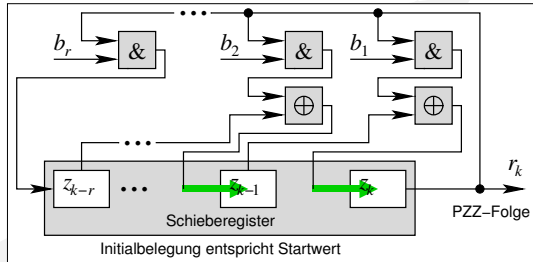
- nicht perfekt

# Duales linear rückgekoppeltes Schieberegister

## Galois-Schieberegister

### Prinzip

- entspricht dem binären linear rückgekoppelten Schieberegister

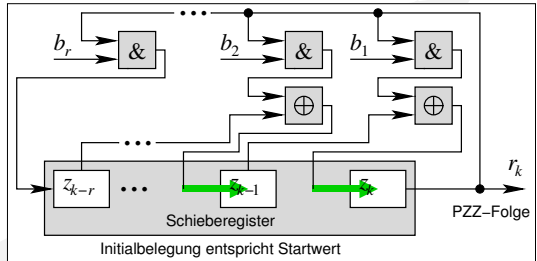


# Duales linear rückgekoppeltes Schieberegister

## Galois-Schieberegister

### Prinzip

- entspricht dem binären linear rückgekoppelten Schieberegister
- eine  $\oplus$ -Operation gespart

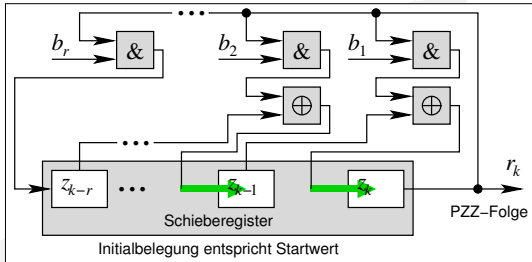


# Duales linear rückgekoppeltes Schieberegister

## Galois-Schieberegister

### Prinzip

- entspricht dem binären linear rückgekoppelten Schieberegister
- eine  $\oplus$ -Operation gespart
- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein

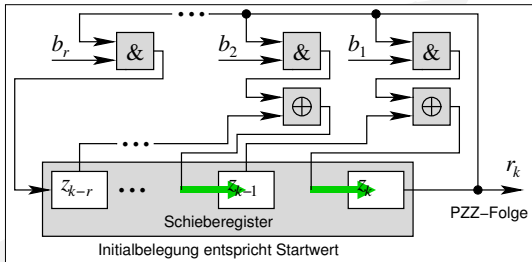


# Duales linear rückgekoppeltes Schieberegister

## Galois-Schieberegister

### Prinzip

- entspricht dem binären linear rückgekoppelten Schieberegister
- eine  $\oplus$ -Operation gespart
- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein
- Transformation duales  $\leftrightarrow$  binäres lin. rückgek. Schiebereg. möglich

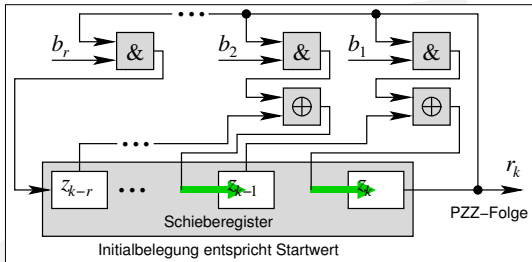


# Duales linear rückgekoppeltes Schieberegister

## Galois-Schieberegister

### Prinzip

- entspricht dem binären linear rückgekoppelten Schieberegister
- eine  $\oplus$ -Operation gespart
- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein
- Transformation duales  $\leftrightarrow$  binäres lin. rückgek. Schiebereg. möglich



### Vorteile

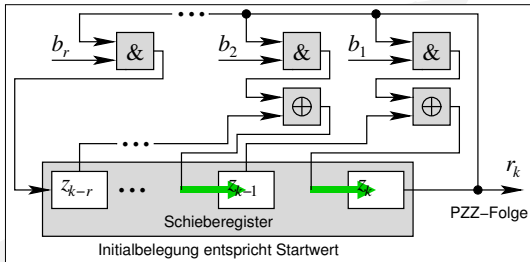
- leicht in Hardware implementierbar
- sehr schnell, einfache Parameterwahl

# Duales linear rückgekoppeltes Schieberegister

## Galois-Schieberegister

### Prinzip

- entspricht dem binären linear rückgekoppelten Schieberegister
- eine  $\oplus$ -Operation gespart
- zum Erreichen der maximalen Periodenlänge  $2^r - 1$  muss charakteristisches Polynom **irreduzibel** sein
- Transformation duales  $\leftrightarrow$  binäres lin. rückgek. Schiebereg. möglich



### Vorteile

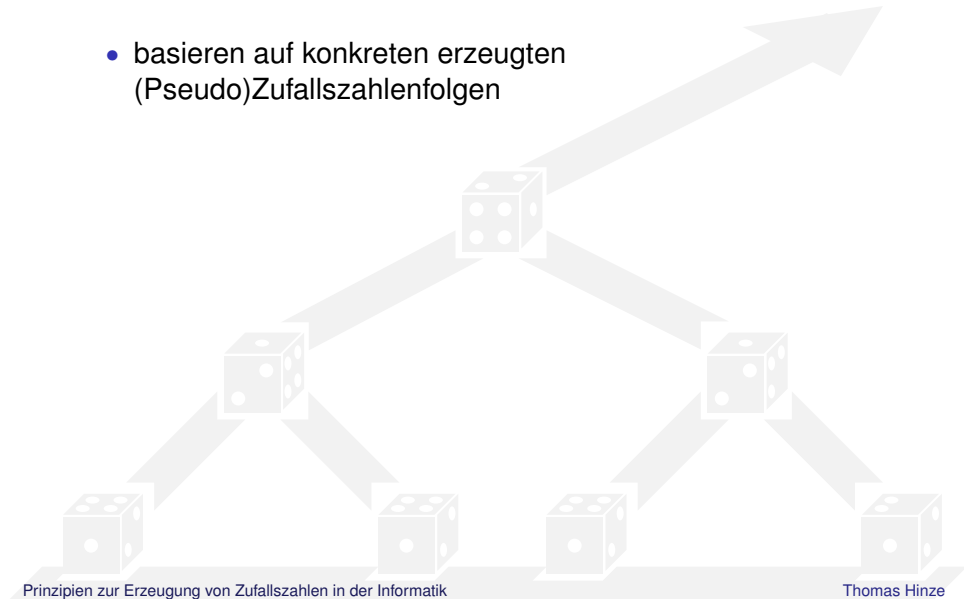
- leicht in Hardware implementierbar
- sehr schnell, einfache Parameterwahl

### Nachteile

- nicht perfekt

# Statistische Tests zur Bewertung der Prinzipien

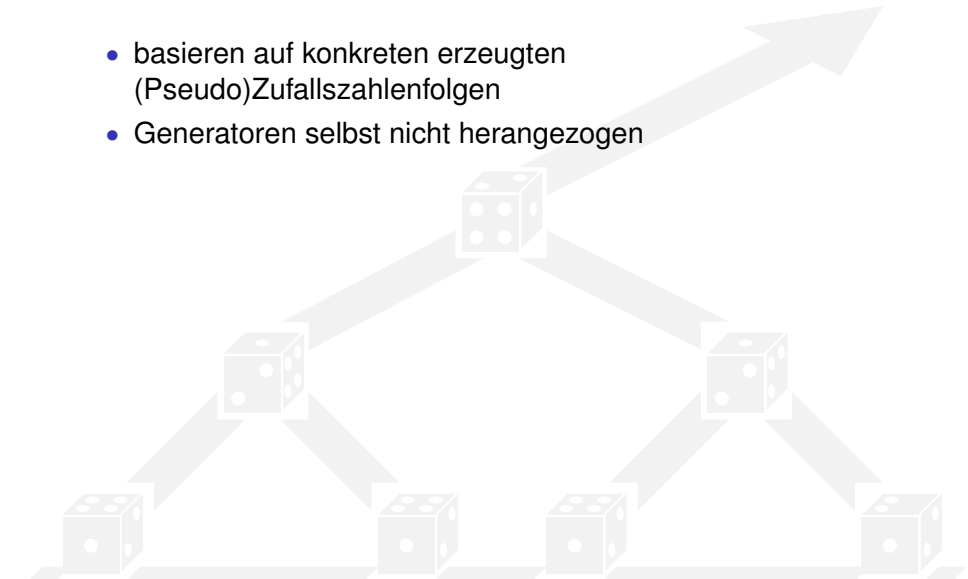
- basieren auf konkreten erzeugten (Pseudo)Zufallszahlenfolgen





# Statistische Tests zur Bewertung der Prinzipien

- basieren auf konkreten erzeugten (Pseudo)Zufallszahlenfolgen
- Generatoren selbst nicht herangezogen



# Statistische Tests zur Bewertung der Prinzipien

- basieren auf konkreten erzeugten (Pseudo)Zufallszahlenfolgen
- Generatoren selbst nicht herangezogen
- Aufschluss darüber, „**wie gut**“ Unabhängigkeit und Uniformität eingehalten werden

# Statistische Tests zur Bewertung der Prinzipien

- basieren auf konkreten erzeugten (Pseudo)Zufallszahlenfolgen
  - Generatoren selbst nicht herangezogen
  - Aufschluss darüber, „**wie gut**“ Unabhängigkeit und Uniformität eingehalten werden
  - **Hypothese**
    - Vorliegen Gleichverteilung
    - keine Autokorrelation
- auf definiertem **Signifikanzniveau** (z.B. 5%, 1% Fehlertoleranz) akzeptiert oder verworfen

# Statistische Tests zur Bewertung der Prinzipien

- basieren auf konkreten erzeugten (Pseudo)Zufallszahlenfolgen
  - Generatoren selbst nicht herangezogen
  - Aufschluss darüber, „**wie gut**“ Unabhängigkeit und Uniformität eingehalten werden
  - **Hypothese**
    - Vorliegen Gleichverteilung
    - keine Autokorrelation
- auf definiertem **Signifikanzniveau** (z.B. 5%, 1% Fehlertoleranz) akzeptiert oder verworfen
- Tests als Algorithmen der mathematischen Statistik notiert und angewendet

# Statistische Tests (Auswahl)

- $\chi^2$ -Test (u.a. auf Gleichverteilung)
  - Standardverfahren der mathematischen Statistik
  - für lange PZZ-Folgen ( $\geq 50$  Zahlen) empfohlen



# Statistische Tests (Auswahl)

- **$\chi^2$ -Test (u.a. auf Gleichverteilung)**
  - Standardverfahren der mathematischen Statistik
  - für lange PZZ-Folgen ( $\geq 50$  Zahlen) empfohlen
- **Kolmogorov-Smirnov-Test (auf Gleichverteilung)**
  - i.A. genauer als  $\chi^2$ -Test, aber aufwendiger
  - auch für kurze PZZ-Folgen



# Statistische Tests (Auswahl)

- **$\chi^2$ -Test (u.a. auf Gleichverteilung)**
  - Standardverfahren der mathematischen Statistik
  - für lange PZZ-Folgen ( $\geq 50$  Zahlen) empfohlen
- **Kolmogorov-Smirnov-Test (auf Gleichverteilung)**
  - i.A. genauer als  $\chi^2$ -Test, aber aufwendiger
  - auch für kurze PZZ-Folgen
- **Gap-Test (auf Autokorrelation)**
  - Überprüfung der Intervalllängen bis zum Wiedererscheinen der gleichen Zahl unter Anwendung des Kolmogorov-Smirnov-Tests

# Statistische Tests (Auswahl)

- **$\chi^2$ -Test (u.a. auf Gleichverteilung)**
  - Standardverfahren der mathematischen Statistik
  - für lange PZZ-Folgen ( $\geq 50$  Zahlen) empfohlen
- **Kolmogorov-Smirnov-Test (auf Gleichverteilung)**
  - i.A. genauer als  $\chi^2$ -Test, aber aufwendiger
  - auch für kurze PZZ-Folgen
- **Gap-Test (auf Autokorrelation)**
  - Überprüfung der Intervalllängen bis zum Wiedererscheinen der gleichen Zahl unter Anwendung des Kolmogorov-Smirnov-Tests
- **Poker-Test (auf Autokorrelation)**
  - analysiert die Häufigkeit, mit der sich die Ziffern in der PZZ-Folge wiederholen



# Statistische Tests (Auswahl)

- **$\chi^2$ -Test (u.a. auf Gleichverteilung)**
  - Standardverfahren der mathematischen Statistik
  - für lange PZZ-Folgen ( $\geq 50$  Zahlen) empfohlen
- **Kolmogorov-Smirnov-Test (auf Gleichverteilung)**
  - i.A. genauer als  $\chi^2$ -Test, aber aufwendiger
  - auch für kurze PZZ-Folgen
- **Gap-Test (auf Autokorrelation)**
  - Überprüfung der Intervalllängen bis zum Wiedererscheinen der gleichen Zahl unter Anwendung des Kolmogorov-Smirnov-Tests
- **Poker-Test (auf Autokorrelation)**
  - analysiert die Häufigkeit, mit der sich die Ziffern in der PZZ-Folge wiederholen
- **Mustersuche (auf Autokorrelation)**
  - graphische Darstellung und Auswertung der PZZ-Folge
  - Gibt es wiederkehrende regelmäßige Muster oder zyklische Variationen?

# Zusammenfassung

## Resümee

- vorgestellte Prinzipien i.A. seit mehreren Jahrzehnten **bekannt** und im praktischen Einsatz **bewährt**
- Prinzipien decken ein **großes Spektrum** nutzbarer und eigenständiger **Strategien** ab
- Repertoire umfasst Prinzipien, die bevorzugt **hardware-** oder **softwarebasiert** implementiert werden können
- Pseudozufallszahlengeneratoren, die üblicherweise in **Programmiersprachen** oder von **Computer-Algebra-Systemen** bereitgestellt werden, sind vorgestellt worden und spezialisieren sich durch ihre Parameterbelegungen

# Zusammenfassung

## Resümee

- vorgestellte Prinzipien i.A. seit mehreren Jahrzehnten **bekannt** und im praktischen Einsatz **bewährt**
- Prinzipien decken ein **großes Spektrum** nutzbarer und eigenständiger **Strategien** ab
- Repertoire umfasst Prinzipien, die bevorzugt **hardware-** oder **softwarebasiert** implementiert werden können
- Pseudozufallszahlengeneratoren, die üblicherweise in **Programmiersprachen** oder von **Computer-Algebra-Systemen** bereitgestellt werden, sind vorgestellt worden und spezialisieren sich durch ihre Parameterbelegungen

# Zusammenfassung

## Resümee

- vorgestellte Prinzipien i.A. seit mehreren Jahrzehnten **bekannt** und im praktischen Einsatz **bewährt**
- Prinzipien decken ein **großes Spektrum** nutzbarer und eigenständiger **Strategien** ab
- Repertoire umfasst Prinzipien, die bevorzugt **hardware-** oder **softwarebasiert** implementiert werden können
- Pseudozufallszahlengeneratoren, die üblicherweise in **Programmiersprachen** oder von **Computer-Algebra-Systemen** bereitgestellt werden, sind vorgestellt worden und spezialisieren sich durch ihre Parameterbelegungen

# Zusammenfassung

## Resümee

- vorgestellte Prinzipien i.A. seit mehreren Jahrzehnten **bekannt** und im praktischen Einsatz **bewährt**
- Prinzipien decken ein **großes Spektrum** nutzbarer und eigenständiger **Strategien** ab
- Repertoire umfasst Prinzipien, die bevorzugt **hardware-** oder **softwarebasiert** implementiert werden können
- Pseudozufallszahlengeneratoren, die üblicherweise in **Programmiersprachen** oder von **Computer-Algebra-Systemen** bereitgestellt werden, sind vorgestellt worden und spezialisieren sich durch ihre Parameterbelegungen

# Zusammenfassung

## Resümee

- vorgestellte Prinzipien i.A. seit mehreren Jahrzehnten **bekannt** und im praktischen Einsatz **bewährt**
- Prinzipien decken ein **großes Spektrum** nutzbarer und eigenständiger **Strategien** ab
- Repertoire umfasst Prinzipien, die bevorzugt **hardware-** oder **softwarebasiert** implementiert werden können
- Pseudozufallszahlengeneratoren, die üblicherweise in **Programmiersprachen** oder von **Computer-Algebra-Systemen** bereitgestellt werden, sind vorgestellt worden und spezialisieren sich durch ihre Parameterbelegungen

## Weiterführende Arbeiten

- **Zufallsfunktionen** (Orakel)
- **chaotische Systeme**

## Ausgewählte Literatur

- L. Blum, M. Blum, M. Shub.** *A Simple Unpredictable Pseudo-Random Number Generator.*  
SIAM J. on Computing **15(2)**:364–383, 1986
- A. Grube.** *Moderne Erzeugung von Zufallszahlen.*  
S.-Toeche-Mittler-Verlag Darmstadt, 1975
- D. Knuth.** *The Art of Computer Programming.* Vol. 2:  
Seminumerical Algorithms. Addison-Wesley Ontario, 1998
- N. Schmitz, F. Lehmann.** *Monte-Carlo-Methoden I.*  
Verlag Anton Hain Meisenheim, 1976
- B. Schneier.** *Applied Cryptography.*  
John Wiley and Sons Inc. New York, 1994
- R. Zielinski.** *Erzeugung von Zufallszahlen.*  
Verlag Harri Deutsch Frankfurt/M., 1978