Stochastik und Kryptologie im Grundkurs Mathematik

DANIEL FROHN, BIELEFELD

Zusammenfassung: *Im Zusammenhang mit der Kryptologie lassen sich auf natürliche Weise einige klassische stochastische Themen behandeln. Dies umfasst elementare Kombinatorik, Baumdiagramme und bedingte Wahrscheinlichkeiten sowie Binomialverteilungen und Hypothesentests.*

1 Einleitung

Die Kryptologie ist eine Wissenschaft, die im modernen Informationszeitalter immer mehr an Bedeutung gewinnt. Sie leistet einen wichtigen Beitrag, die Vertraulichkeit von Daten und Nachrichten sowie die Sicherheit elektronischen Geschäftsverkehrs zu gewährleisten. Es bietet sich daher an, kryptologische Lerninhalte in den Mathematikunterricht einfließen zu lassen. Interessant aus Sicht der Mathematik ist besonders, dass Erkenntnisse der elementaren Zahlentheorie Grundlage moderner Verschlüsselungsverfahren sind. Etwas überraschender mag erscheinen, dass sich im Kontext der Kryptologie auch stochastische Fragestellungen thematisieren lassen. Ansätze in diese Richtung wurden von mir in zwei Grundkursen Mathematik am Oberstufenkolleg Bielefeld in den Jahren 2008 und 2009 entwickelt und sollen in diesem Artikel vorgestellt werden.

Die hier verwendeten Grundbegriffe der Kryptologie werden jeweils kurz erläutert; für ausführlichere Erklärungen sei auf die Literatur (z. B. Beutelspacher 2005) verwiesen. Wie üblich wird folgende Konvention verwendet: Klartexte werden stets klein- und Geheimtexte stets großgeschrieben.

2 Kombinatorik: Transpositions- und Substitutionschiffren

Grundsätzlich gibt es zwei verschiedene Möglichkeiten, eine Nachricht zu verschlüsseln: Man kann die Buchstabensymbole unverändert lassen, sie aber in eine neue Reihenfolge bringen (Transposition) oder man kann die Buchstaben an ihren Plätzen lassen, sie aber durch neue Symbole ersetzen (Substitution). Beispielsweise könnte das Wort „hallo“ durch eine Transposition in „LOHLA“ und durch eine Substitution in „ALEEN“ übergehen.

Als ein erstes Maß für die Sicherheit einer Verschlüsselung könnte man zunächst die Anzahl aller möglichen Chiffren betrachten. Es ergeben sich also ganz natürlich die Fragen:

Wie viele verschiedene Transpositions- bzw. Substitutionschiffren gibt es?

Dies führt auf die gängigen Grundaufgaben der elementaren Kombinatorik, wie im Folgenden aufgezeigt wird.

Anzahl der Substitutionschiffren

Wir betrachten hier zunächst nur die sogenannten monoalphabetischen Substitutionen, d. h. es existiert eine eindeutige Zuordnung von Klartext- und Geheimtextalphabet, die während der gesamten Verschlüsselung unverändert bleibt. Die Anzahl der möglichen Substitutionschiffren hängt somit nur von der Anzahl der Buchstaben im Alphabet ab (wenn man davon ausgeht, dass alle Buchstaben des Alphabets auch in der Nachricht verwendet werden). Hier kommt nun die Fakultät ins Spiel: Bei einem Alphabet von 26 Buchstaben gibt es 26 Möglichkeiten, den ersten Buchstaben zu ersetzen. Für jede dieser Möglichkeiten hat man nun noch 25 Möglichkeiten, den zweiten Buchstaben zu ersetzen und so weiter. Es ergeben sich $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = 26!$ Substitutionschiffren für das Alphabet der deutschen Sprache (ohne Umlaute, Satz- und Sonderzeichen). Allgemein beträgt die Anzahl $n!$ bei einem Alphabet von n Buchstaben. Die Größe der Zahl $26! \approx 4 \cdot 10^{26}$ ist beeindruckend: Wenn ein Computer in jeder Sekunde eine Milliarde verschiedene Substitutionschiffren durchprobieren könnte, bräuchte er immer noch etwa 13 Milliarden Jahre, um alle möglichen Fälle durchzugehen. Dies zeigt, dass eine Substitutionschiffre durch bloßes Durchprobieren nicht zu knacken ist. Diese vermeintliche Sicherheit ist allerdings trügerisch; verwendet man nämlich die Häufigkeitsanalyse, so kann man die meisten monoalphabetisch verschlüsselten Texte relativ leicht entschlüsseln.

Anzahl der Transpositionschiffren

Im Unterschied zu den Substitutionschiffren ist die Anzahl der Transpositionschiffren auch noch ganz wesentlich von der Länge der Nachricht abhängig. Hier beginnt man am besten mit kurzen Wörtern, die aus lauter verschiedenen Buchstaben zusammengesetzt sind, und erhöht dann den Schwierigkeitsgrad durch Vorgabe von Wörtern mit mehrfach auftretenden Buchstaben. Das hier skizzierte Vorgehen ist gut für selbstständiges entdeckendes Lernen geeignet.

Schritt 1: Wörter aus paarweise verschiedenen Buchstaben

Beispiel „gut“:

- Transpositionen: GUT, GTU, UGT, UTG, TUG, TGU
- 3 Plätze für das G, noch 2 Plätze für das U, das T ist dann festgelegt, also 3! = 6 Transpositionschiffren

Für ein Wort mit n paarweise verschiedenen Buchstaben gibt es also analog $n!$ Transpositionschiffren.

Schritt 2: Wörter, die genau einen mehrfach auftretenden Buchstaben enthalten

Beispiel „nett“:

- Transpositionen: NETT, NTET, NTTE, ENTT, ETNT, ETTN, TENT, TETN, TNET, TNTE, TTEN, TTNE
- Wenn die T’s unterscheidbar wären, hätte man 4! = 24 Möglichkeiten. Da sie es nicht sind, stimmen jeweils 2 Möglichkeiten davon überein, und man erhält daher nur die Hälfte, also $\frac{4!}{2} = 12$ Möglichkeiten.

Beispiel „puppe“:

- Hier wird es schon recht mühsam, alle Transpositionen aufzulisten.
- Die 3 P’s lassen sich auf 3! viele Arten anordnen. Also ergeben sich $\frac{5!}{3!} = 20$ Transpositionschiffren.

Hat man das Prinzip einmal erkannt, so lässt es sich mühelos auf mehrere mehrfach auftretende Buchstaben übertragen.

Schritt 3: Wörter, die mehrere mehrfach auftretende Buchstaben enthalten

Beispiele:

„papa“: $\frac{4!}{2! \cdot 2!} = 6$ Transpositionen

„mississippi“: $\frac{11!}{4! \cdot 4! \cdot 2!} = 34650$ Transpositionen

Dies führt auf den allgemeinen Ausdruck des **Multinomialkoeffizienten**: Ein Wort aus insgesamt n Buchstaben besitzt genau $\frac{n!}{n_1!n_2!\cdots n_k!}$ verschiedene Transpositionschiffren, wobei die k verschiedenen auftretenden Buchstaben jeweils $n_1, n_2, \ldots, n_k$ mal auftreten. Hierbei kann auch $n_i = 1$ und $n_i = 0$ zugelassen werden; dabei wird deutlich, dass die Definition 0! = 1 sinnvoll ist.

Nun kann der **Binomialkoeffizient** als Spezialfall des Multinomialkoeffizienten eingeführt werden. Arbeitet man – wie in der Computerhardware – mit einem Alphabet aus 2 Buchstaben (den Bits 0 und 1), so ist $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ die Anzahl der Transpositionschiffren einer Folge von n Bits mit genau k Einsen. Dies ist eine Grundvorstellung, die in den verschiedenen Zusammenhängen, in denen der Binomialkoeffizient auftritt, tragfähig sein kann.

Beispiel: Betrachtet man die allgemeine binomische Formel

$$(a+b)^n = a^n + \ldots + \binom{n}{k} a^{n-k}b^k + \ldots + b^n$$

in diesem Kontext, so kann man $\binom{n}{k}$ deuten als Anzahl der möglichen „Wörter“ aus (n–k) a’s und k b’s, die jeweils zu den Produkten $a^{n-k}b^k$ führen.

Letztlich kann die Grundvorstellung der Binomialkoeffizienten als Anzahlen von Wörtern der Länge n über einem Alphabet von 2 Buchstaben in jeder Auswahlsituation ein tragfähiges mentales Modell darstellen: Die Anzahl der Möglichkeiten, aus n Objekten k Objekte ohne Berücksichtigung der Reihenfolge auszuwählen, ist immer durch Wörter der Länge n modellierbar, indem einem ausgewählten Objekt eine 1 und einem nicht ausgewählten Objekt eine 0 zugeordnet wird.

Weitere elementare kombinatorische Grundaufgaben

Im Zusammenhang der Anzahlen von Substitutions- und Transpositionschiffren sind weitere elementare kombinatorische Fragestellungen interessant, die hier noch kurz aufgezeigt werden sollen.

Zunächst kann die Frage nach der Anzahl aller Nachrichten der Länge k gestellt werden. Bei einem Alphabet von n Zeichen sind dies n^k, da an jeder Stelle der Nachricht jedes Zeichen des Alphabets stehen kann. Es handelt sich also um die Anzahl $\overline{P}(n, k)$ der Permutationen mit Wiederholung.

Bei vielen klassischen Verschlüsselungen wird der Schlüssel aus einem Schlüsselwort erzeugt, indem die mehrfach auftretenden Buchstaben gestrichen werden, so dass ein evtl. verkürztes Wort aus lauter verschiedenen Buchstaben entsteht. Hierbei wird z. B. aus dem Schlüsselwort „MATHEMATIK“ der Schlüssel „MATHEIK“. Wie viele solcher Schlüssel der Länge k gibt es nun? Für den ersten Buchstaben hat man n Möglichkeiten, für den zweiten nur noch $n – 1$ usw.; man erhält also insgesamt

$$n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

mögliche Schlüssel. Dies ist die Anzahl $P(n, k)$ der Permutationen ohne Wiederholung.

Der Vollständigkeit halber sei hier noch eingefügt, dass man auch die Anzahl $\overline{C}(n, k) = \binom{n+k-1}{k}$ der Kombinationen mit Wiederholung im Kontext der Transpositionschiffren deuten kann: Fasst man alle Nachrichten der Länge k, die durch eine Transposition ineinander überführt werden können, in einer „Transpositionsklasse“ zusammen, so gibt $\binom{n+k-1}{k}$ die Anzahl dieser Transpositionsklassen an.

Wie über den Multinomialkoeffizienten hinaus die elementaren kombinatorischen Grundaufgaben auf natürliche Weise im Kontext der Substitutions- und Transpositionschiffren auftreten, ist in Tabelle 1 zusammengefasst.

Kombinatorische Grundaufgabe	**Deutung im klassischen Urnenmodell** (Ziehung von k Kugeln aus einer Urne mit n Kugeln)	**Deutung im Kontext von Substitutions- und Transpositionschiffren**
Anzahl der Permutationen ohne Wiederholung $P(n, k) = \frac{n!}{(n-k)!}$	Anzahl der möglichen Ziehungen ohne Zurücklegen mit Berücksichtigung der Reihenfolge	Anzahl der Schlüssel der Länge k ohne mehrfache Buchstaben bei einem Alphabet von n Zeichen
Spezialfall $k = n$: $P(n, n) = n!$		Spezialfall $k = n$: Anzahl der Substitutionschiffren bei einem Alphabet von n Zeichen
Anzahl der Permutationen mit Wiederholung $\overline{P}(n, k) = n^k$	Anzahl der möglichen Ziehungen mit Zurücklegen mit Berücksichtigung der Reihenfolge	Anzahl der Nachrichten der Länge k bei einem Alphabet von n Zeichen
Anzahl der Kombinationen ohne Wiederholung $C(n, k) = \binom{n}{k}$	Anzahl der möglichen Ziehungen ohne Zurücklegen ohne Berücksichtigung der Reihenfolge	Anzahl der Transpositionschiffren einer binären Nachricht der Länge n mit genau k Einsen
Anzahl der Kombinationen mit Wiederholung $\overline{C}(n, k) = \binom{n+k-1}{k}$	Anzahl der möglichen Ziehungen mit Zurücklegen ohne Berücksichtigung der Reihenfolge	Anzahl der Transpositionsklassen aller Nachrichten der Länge k bei einem Alphabet von n Zeichen

Tab. 1: Überblick über kombinatorische Grundaufgaben

3 Wahrscheinlichkeitsbäume: Koinzidenzindex/Friedman-Test

Im Unterschied zu den monoalphabetischen ist es bei den polyalphabetischen Substitutionschiffren so, dass die Zuordnung von Klar- und Geheimtextalphabet veränderlich ist, d. h. der selbe Klartextbuchstabe kann innerhalb der Verschlüsselung durch verschiedene Geheimtextbuchstaben ersetzt werden. Dies geschieht mit dem Ziel, die für eine Sprache charakteristische Häufigkeitsverteilung der Buchstaben, die unter einer monoalphabetischen Substitution erhalten bleibt, zu „glätten“

Bei der nach dem französischen Diplomaten Blaise de Vigenère (1523–1596) benannten de-Vigenère-Verschlüsselung wird das jeweils zu verwendende Geheimtextalphabet durch ein Schlüsselwort festgelegt. Dieses wird Buchstabe für Buchstabe über den Klartext geschrieben (falls nötig mehrfach) und gibt an, um wie viele Stellen das Geheimtextalphabet gegenüber dem Klartextalphabet verschoben wird: A bedeutet keine Verschiebung, B eine Verschiebung um eine Stelle usw., Z eine Verschiebung um 25 Stellen. Das Schlüsselwort legt also fest, welche dieser 26 verschiedenen Verschiebechiffren für einen Klartextbuchstaben jeweils verwendet wird (siehe Tabelle 2).

Schlüsselwort:	M	A	T	H	E	M	A	T	H	E	M	A	T	H	E	M
Klartext:	g	e	h	e	i	m	e	b	o	t	s	c	h	a	f	t
Geheimtext:	S	E	A	L	M	Y	E	U	V	X	E	C	A	H	J	F

Tab. 2: Beispiel für eine de-Vigenère-Verschlüsselung

Bei der Kryptoanalyse der de-Vigenère-Verschlüsselung, also dem Versuch der Entschlüsselung ohne Kenntnis des Schlüsselwortes, besteht die Hauptschwierigkeit darin, die Länge des Schlüsselwortes herauszufinden. Ist diese Länge nämlich bekannt und beträgt z. B. 5, so kann der Geheimtext in 5 Teile aufgeteilt werden, die jeweils durch dieselbe Verschiebechiffre entstanden sind. In obigem Beispiel wäre etwa der 1., 6., 11. und 16. Buchstabe durch die gleiche Verschiebung (um M, also 12 Stellen) hervorgegangen. Bei längeren Texten kann dann jeder der Teile leicht durch die Häufigkeitsanalyse entschlüsselt werden.

Für die Bestimmung der Schlüsselwortlänge gibt es zwei wichtige Verfahren, den Kasiski-Test, der mathematisch auf einfachen Primfaktorzerlegungen beruht, und den Friedman-Test. Im Folgenden soll nun gezeigt werden, wie der Grundgedanke des Friedman-Tests und der damit zusammenhängende Koinzidenzindex mit Hilfe von Wahrscheinlichkeitsbäumen erschlossen werden kann.

Der Koinzidenzindex

Der Koinzidenzindex I eines beliebigen Textes ist definiert als die Wahrscheinlichkeit, dass ein zufällig aus dem Text ausgewähltes Buchstabenpaar aus gleichen Buchstaben besteht. Die betrachteten Buchstabenpaare müssen dabei nicht aus aufeinanderfolgenden Buchstaben bestehen.

Beginnend bei einfachen Beispielen können die Schüler nun zu einer allgemeinen Formel für I geführt werden. Dazu ist nur die Kenntnis von Baumdiagrammen samt Pfadregeln erforderlich. Dies kann aber gegebenenfalls auch an dieser Stelle eingeführt werden. Tabelle 3 zeigt, wie von einfachen Beispielen ausgehend schrittweise der allgemeine Ausdruck für den Koinzidenzindex eines Textes erarbeitet werden kann.

Die allgemeine Formel

$$I = \frac{n_a(n_a - 1) + \ldots + n_z(n_z - 1)}{n(n-1)}$$

für den Koinzidenzindex kann nun noch übertragen werden auf den Fall eines Textes unbekannter Länge, von dem aber die Wahrscheinlichkeiten für das Auftreten der einzelnen Buchstaben bekannt sind. Man geht also von den relativen Häufigkeiten zu Wahrscheinlichkeiten über und erhält

$$I = p_a{}^2 + p_b{}^2 + \ldots + p_z{}^2$$

für den Koinzidenzindex. So kann (näherungsweise) der Koinzidenzindex der deutschen Sprache bestimmt werden ($I = 0{,}0762$) oder der Koinzidenzindex bei Gleichverteilung der Buchstaben

$$\left(I = 26 \cdot \left(\frac{1}{26}\right)^2 = \frac{1}{26} \approx 0{,}0385\right).$$

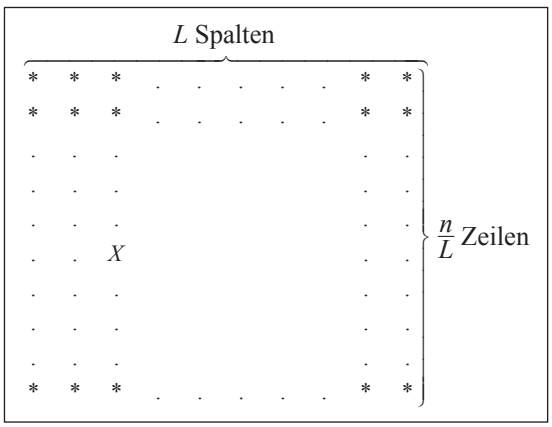
Die vereinfachte Annahme, dass die Wahrscheinlichkeit sich nach der Auswahl des ersten Buchstabens nicht ändert, ist für manchen Schüler sicherlich ein Stolperstein. Dies kann aber durch einen Vergleich der Ausdrücke $\frac{n_i}{n}$ und $\frac{n_i - 1}{n - 1}$ für große Werte von n_i und n plausibel gemacht werden.

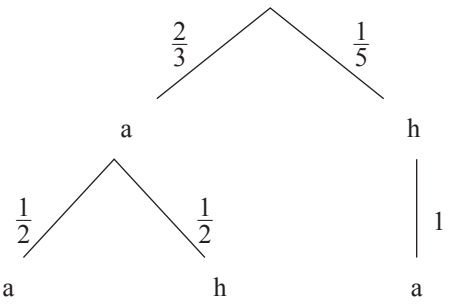
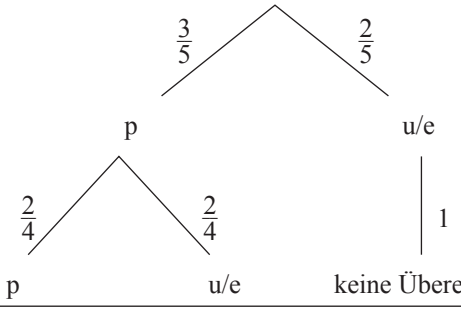
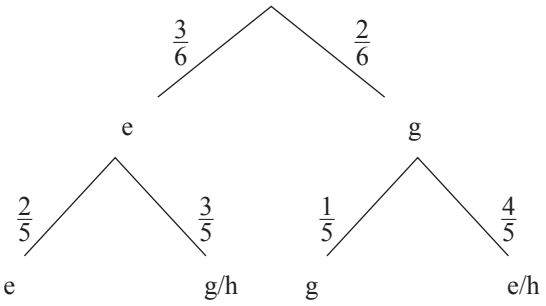
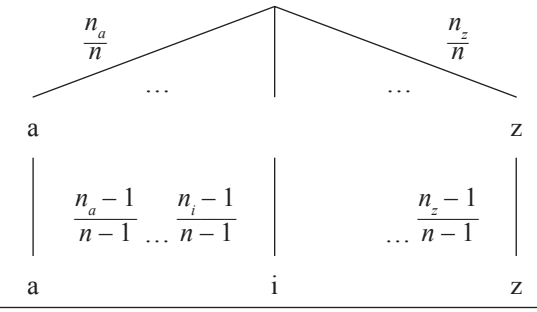
Bis hierhin scheint der Koinzidenzindex lediglich eine stochastische Spielerei zu sein. Wozu aber braucht man ihn im Rahmen der Kryptoanalyse? Eine wichtige Beobachtung hierzu ist die folgende: Der Koinzidenzindex ändert sich nicht unter einer monoalphabetischen Substitutionschiffre, da die Übereinstimmung zweier Buchstaben ja unabhängig von dem verwendeten Symbol ist. Andererseits nähern sich die Buchstabenhäufigkeiten bei polyalphabetischen Chiffrierungen der Gleichverteilung an, so dass der Koinzidenzindex eines verschlüsselten Textes als ein Maß dafür angesehen werden kann, wie gut die Verschlüsselung die charakteristische Häufigkeitsverteilung der Buchstaben einer Sprache „glättet“: Liegt der Koinzidenzindex in der Nähe von 0,0762, deutet alles auf eine monoalphabetische Substitution hin; ist er aber deutlich kleiner, so ist von einer polyalphabetischen Chiffrierung auszugehen. Je länger das Schlüsselwort bei der de-Vigenère-Verschlüsselung ist, desto mehr wird sich der Koinzidenzindex also dem Wert 0,0385 annähern.

Der Friedman-Test

Die im letzten Abschnitt dargestellte qualitative Beobachtung kann nun durch den Friedman-Test mit Hilfe einer Formel genauer beschrieben werden. Dies geschieht auf folgende Weise:

Gegeben ist ein de-Vigenère-verschlüsselter Text, bei dem das Schlüsselwort die (noch unbekannte) Länge L hat. Nun wird der verschlüsselte Text in L Spalten angeordnet. Das bedeutet, dass alle Buchstaben einer Spalte aus derselben Verschiebechiffre hervorgehen.

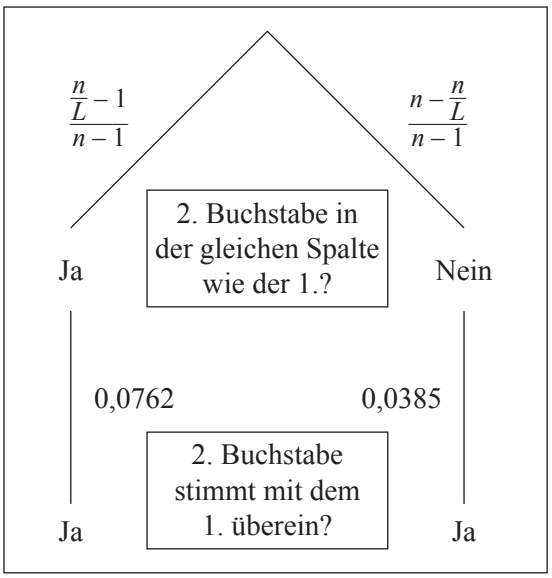


Beispiel	Baumdiagramm	Koinzidenzindex
schade	Nicht nötig	$I = 0$, da kein Buchstabe mehrfach vorkommt
aha		$I = \frac{2}{3} \cdot \frac{1}{2} = \frac{1}{3}$
puppe		$I = \frac{3}{5} \cdot \frac{2}{4} = \frac{3}{10}$
gehege		$I = \frac{3}{6} \cdot \frac{2}{5} + \frac{2}{6} \cdot \frac{1}{5} = \frac{4}{15}$
Allgemein: Text mit n Buchstaben, wobei n_a, …, n_z die entsprechenden Häufigkeiten der Buchstaben bezeichnen		$I = \frac{n_a}{n} \cdot \frac{n_a - 1}{n - 1} + \ldots + \frac{n_z}{n} \cdot \frac{n_z - 1}{n - 1}$ $= \frac{n_a(n_a - 1) + \ldots + n_z(n_z - 1)}{n(n - 1)}$

Tab. 3: Hinführung zur Formel für den Koinzidenzindex

Bei insgesamt n Buchstaben gibt es also $\frac{n}{L}$ Zeilen, d. h. $\frac{n}{L}$ Buchstaben pro Spalte (dabei wird auf die Betrachtung von Rundungsfehlern verzichtet).

Zur näherungsweisen Berechnung von I mit Hilfe dieses Schemas stellen wir uns nun vor, dass bereits der erste Buchstabe zufällig ausgewählt wurde. Er liegt in irgendeiner Spalte; es könnte z. B. ein X irgendwo in der dritten Spalte sein. Nun suchen wir ja die Wahrscheinlichkeit, dass ein zufällig ausgewählter zweiter Buchstabe mit dem ersten übereinstimmt. Dazu wird den Schülern das folgende (zunächst unausgefüllte) Baumdiagramm vorgelegt, das sie zuerst noch mit den passenden Wahrscheinlichkeiten vervollständigen sollen:



Hierbei wird der Koinzidenzindex der deutschen Sprache als Wahrscheinlichkeit gedeutet, dass zwei Buchstaben in der gleichen Spalte übereinstimmen, da es sich in den Spalten ja lediglich um eine monoalphabetische Chiffrierung handelt. Bei Buchstaben aus unterschiedlichen Spalten kann man aufgrund der unterschiedlichen verwendeten Verschiebechiffren näherungsweise von einer Gleichverteilung der Buchstaben ausgehen, also einer Wahrscheinlichkeit von etwa 0,0385 für die Übereinstimmung. Mit Hilfe des vervollständigten Baumdiagramms erhält man also die näherungsweise gültige Formel

$$I = \frac{\frac{n}{L}-1}{n-1} \cdot 0{,}0762 + \frac{n-\frac{n}{L}}{n-1} \cdot 0{,}0385 \qquad (1)$$

für den Koinzidenzindex des de-Vigenère-verschlüsselten Textes. Eine etwas mühsame algebraische Umformung nach L liefert dann schließlich die dem Friedman-Test zu Grunde liegende Formel für die Länge des Schlüsselwortes:

$$L = \frac{0{,}0377n}{I \cdot (n-1) - 0{,}0385n + 0{,}0762} \qquad (2)$$

Für einen vorliegenden de-Vigenère-verschlüsselten Geheimtext kann nun aus den Häufigkeiten der Buchstaben leicht n und I bestimmt und mit der erhaltenen Formel (2) daraus eine Näherung für L berechnet werden. Im Zusammenspiel mit dem Kasiski-Test, der die Schlüsselwortlänge mit Hilfe von Teilbarkeitsüberlegungen angibt, ist die Schlüsselwortlänge L recht zuverlässig bestimmbar, wenn sie kurz im Vergleich zur Textlänge n ist.

Didaktische Einordnung

Ausgehend von einfachen Beispielen können die Schüler selbstständig eine allgemeine Vorgehensweise für die Berechnung des Koinzidenzindex finden. Die Pfadregeln für Wahrscheinlichkeitsbäume werden hierbei wiederholend vertieft, können aber auch simultan eingeführt werden. Die Problemstellung ist gerade bei den einfachen Beispielen anschaulich und lässt einen spielerischen Zugang zu. Beispielsweise könnte das zu Grunde liegende zweistufige Zufallsexperiment durch das Ziehen von mit Buchstaben beschrifteten Zetteln aus einem Beutel veranschaulicht werden. Das Vorgehen kann auch auf andere Zusammenhänge übertragen werden: Wie wahrscheinlich ist es, dass zwei zufällig ausgewählte Schüler des Kurses das gleiche Geschlecht haben? Eine Verallgemeinerung auf mehrstufige Zufallsexperimente (mehr als 2 Stufen) ist ebenfalls möglich.

Der Übergang von den relativen Häufigkeiten zu den abstrakteren Wahrscheinlichkeiten bei unbekannter Textlänge ist paradigmatisch für stochastisches Arbeiten: Sind die konkreten relativen Häufigkeiten nicht bekannt (hier die der Gesamtheit aller deutschen Texte), so postuliert man Wahrscheinlichkeiten, entnimmt diese aber wiederum den relativen Häufigkeiten einer vergleichbaren Stichprobe (hier die der für eine Häufigkeitstabelle ausgewerteten Texte).

Beim Betrachten der Formel (2) bieten sich interessante Möglichkeiten der Interpretation. Deutet man (2) als funktionalen Zusammenhang zwischen I und L, so sind die folgenden 3 Beobachtungen einsichtig:

- *Mit kleiner werdendem I nimmt L zu.* Dies passt zur bereits gemachten Beobachtung, dass ein kleiner Koinzidenzindex auf ein langes Schlüsselwort hindeutet.
- *Für* $I = 0{,}0762$ *liefert* (2) *den Wert* $L = 1$. Der Koinzidenzindex der deutschen Sprache weist also auf eine monoalphabetische Substitution hin.
- *Für* $I = 0{,}0385$ *erhält man* $L = n$. Der Koinzidenzindex der Gleichverteilung weist auf ein Schlüsselwort hin, das genau so lang ist wie der Text.

Diese Beobachtungen machen noch einmal ganz deutlich, wie die Sicherheit der de-Vigenère-Verschlüsselung von der Länge des Schlüsselwortes abhängt. Optimale Sicherheit kann nur durch ein zufällig erstelltes Schlüsselwort, welches die gleiche Länge wie der Text hat und das nur einmal verwendet wird, erreicht werden. Dieses so genannte **One-Time-Pad** und die damit verbundenen stochastischen Fragestellungen werden in den nächsten beiden Abschnitten dargestellt.

4 Bedingte Wahrscheinlichkeiten: Perfekte Sicherheit

Dass perfekte Sicherheit in der Kryptologie möglich sein soll, klingt zunächst unglaublich. Und in der Tat ist diese Perfektion ein eher theoretisches Konstrukt, welches an Voraussetzungen gekoppelt ist, die in der Realität niemals in völliger Vollkommenheit vorliegen werden. Neben den oben genannten Eigenschaften (Zufälligkeit, Länge, einmalige Verwendung), die recht problemlos realisierbar sind, ist hierbei nämlich vor allem die völlige Geheimhaltung des Schlüssels erforderlich. Und die Erfüllung dieser Voraussetzung ist – insbesondere im Zuge der Schlüsselübermittlung – das größte praktische Problem.

Das Verfahren selbst bietet aber in der Tat perfekte Sicherheit; und dies kann mathematisch mit Hilfe von bedingten Wahrscheinlichkeiten und dem Satz von Bayes nachgewiesen werden, wie im Folgenden dargestellt wird. Es zeigt sich, dass hier ein didaktisch interessanter Kontext für die Behandlung bedingter Wahrscheinlichkeiten vorliegt.

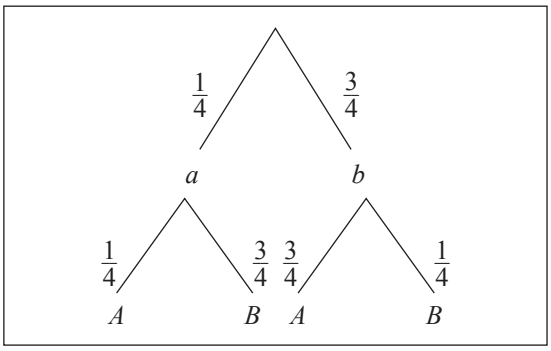
Schon durch einfache intuitive Überlegungen kann die Unmöglichkeit der Entschlüsselung von mit dem One-Time-Pad verschlüsselten Texten eingesehen werden: Erhält man beispielsweise den Geheimtext WKD, so kann dieser je nach Schlüssel ja aus *jedem* Klartext der Länge 3 hervorgegangen sein. Der Klartext könnte z. B. *elf* lauten (für den Schlüssel SBC) oder *gut* (für den Schlüssel QQK). Da keinerlei Informationen über den Schlüssel vorliegen, z. B. SBC und QQK also gleich wahrscheinlich sind, wird schon in naiver Herangehensweise deutlich, dass keine Informationen zur Kryptoanalyse verfügbar sind. Ein Durchprobieren aller möglichen Schlüssel würde ja auch alle möglichen Klartexte ergeben!

Beispiel einer binären Sprache

Wie aber kommen hier bedingte Wahrscheinlichkeiten ins Spiel? Das Prinzip wird nun am Beispiel einer „binären Sprache“ illustriert (dies ist im Hinblick auf Computerhardware ein durchaus realistisches Beispiel): Eine Sprache habe nur zwei Buchstaben *a* und *b*. Dabei sei die Buchstabenhäufigkeit von *a* ¼ und die von *b* ¾. Wir deuten diese relative Häufigkeiten nun wie gewohnt als Wahrscheinlichkeiten: $p(a) = \frac{1}{4}$ und $p(b) = \frac{3}{4}$. Bei der Schlüsselwahl treten nun auch die Schlüsselwortbuchstaben *A* bzw. *B* mit gewissen Wahrscheinlichkeiten auf. Zur Erinnerung: Der Schlüsselwortbuchstabe *A* lässt die Klartextbuchstaben *a* und *b* unverändert, der Schlüsselwortbuchstabe *B* „vertauscht“, d. h. aus *a* wird *B* und aus *b* wird *A*. Zur Verdeutlichung betrachten wir nun 2 Varianten.

Variante 1: „Natürlicher Schlüssel“

Die Wahrscheinlichkeiten beim Schlüssel entsprechen denen der Sprache, d. h. bei der Verschlüsselung bleiben die Buchstaben mit Wahrscheinlichkeit ¼ unverändert und werden mit Wahrscheinlichkeit ¾ vertauscht.



- Wahrscheinlichkeit für den Geheimtextbuchstaben *B* unter der Bedingung, dass *a* der Klartextbuchstabe ist:

  $p_a(B) = \frac{3}{4}$
- Wahrscheinlichkeit für ein *B* im Geheimtext:

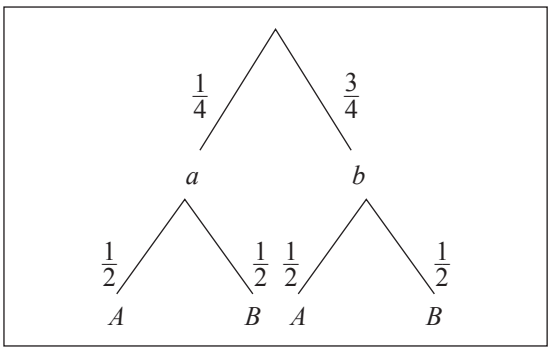
  $p(B) = \frac{1}{4} \cdot \frac{3}{4} + \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{8}$
- Wahrscheinlichkeit für den Klartextbuchstaben *a* unter der Bedingung, dass *B* der Geheimtextbuchstabe ist:

  $$p_B(a) = \frac{p(a)p_a(B)}{p(B)} = \frac{\frac{1}{4} \cdot \frac{3}{4}}{\frac{3}{8}} = \frac{1}{2} \neq p(a)$$

  (Zur Erarbeitung und Veranschaulichung der Formel von Bayes wurden im Unterricht zunächst absolute Zahlen – hier: 16 Buchstaben – verwendet)
- Fazit: Die Kenntnis des Geheimtextbuchstabens *B verändert* die Wahrscheinlichkeit für das Auftreten des Klartextbuchstabens *a*, beinhaltet also eine *wertvolle Information*!

Variante 2: „Zufälliger Schlüssel“

Beide Schlüsselwortbuchstaben seien gleich wahrscheinlich, demzufolge bleiben bei der Verschlüsselung die Buchstaben mit Wahrscheinlichkeit ½ unverändert und werden mit Wahrscheinlichkeit ½ vertauscht



- Wahrscheinlichkeit für den Geheimtextbuchstaben *B* unter der Bedingung, dass *a* der Klartextbuchstabe ist:

  $p_a(B) = \frac{1}{2}$

- Wahrscheinlichkeit für ein *B* im Geheimtext:

  $p(B) = \frac{1}{4} \cdot \frac{1}{2} + \frac{3}{4} \cdot \frac{1}{2} = \frac{1}{2}$

- Wahrscheinlichkeit für den Klartextbuchstaben *a* unter der Bedingung, dass *B* der Geheimtextbuchstabe ist:

  $$p_B(a) = \frac{p(a)p_a(B)}{p(B)} = \frac{\frac{1}{4} \cdot \frac{1}{2}}{\frac{1}{2}} = \frac{1}{4} = p(a)$$

  (Zur Erarbeitung und Veranschaulichung der Formel von Bayes wurden im Unterricht zunächst absolute Zahlen – hier: 8 oder 16 Buchstaben – verwendet)

- Fazit: Die Kenntnis des Geheimtextbuchstabens *B verändert* die Wahrscheinlichkeit für das Auftreten des Klartextbuchstabens *a nicht*, beinhaltet also *keine verwertbare Information*!

Perfekte Sicherheit mit dem One-Time-Pad

An diesem Beispiel wird deutlich, wie der Begriff der perfekten Sicherheit eines Kryptosystems mathematisch definiert werden kann: Für jeden Geheimtextbuchstaben Γ und jeden Klartextbuchstaben κ darf sich die Wahrscheinlichkeit für κ nicht verändern, wenn man Kenntnis über den Geheimtextbuchstaben Γ erlangt: $p(\kappa) = p_\Gamma(\kappa)$.

Dass dies bei der Verwendung eines One-Time-Pad tatsächlich der Fall ist, ist nun eine einfache Anwendung des Satzes von Bayes, auch im allgemeinen Fall von *n* Buchstaben. Bei der Behandlung in einem Grundkurs kann man sich aber auf die exemplarische Darstellung an obigem Beispiel beschränken und die Schüler analoge Überlegungen für ein Alphabet von z. B. drei Buchstaben durchführen lassen.

5 Binomialverteilung und Hypothesentest: Zufallszahlen

Die Überlegungen zur Sicherheit der de-Vigenère-Verschlüsselung machen deutlich, dass die Schlüsselerzeugung ein wichtiges Problem im Rahmen der Kryptologie darstellt. Neben der Länge eines Schlüsselwortes spielt dabei auch die Art der Erzeugung eine große Rolle. Wie im letzten Abschnitt dargestellt, haben nach dem Zufallsprinzip erstellte Schlüssel nämlich gegenüber Codewörtern bzw. -texten aus natürlichen Sprachen den Vorteil, dass die statistischen Besonderheiten natürlicher Sprachen nicht zur Rekonstruktion des Schlüssels verwendet werden können. Dies führt auf zwei Fragen:

- Wie kann man zufällige Schlüssel „erzeugen“?
- An welchen Merkmalen kann man zufällige Buchstaben- oder Zahlenfolgen von nicht zufälligen unterscheiden?

Diese beiden Fragen berühren Aspekte der Informatik und der Stochastik. Die Frage nach der Erzeugung von (Pseudo-)Zufallszahlen ist ein Problem der Informatik, während die zweite Frage stochastischer Natur ist. Sie eignet sich gut zur Motivation und Einführung von Binomialverteilung und Hypothesentest, wie im Folgenden dargestellt werden soll.

Binomialverteilung bei Zufallsfolgen

Die Leitidee bei der hier geschilderten Einführung der Binomialverteilung ist, die Frage „Was kennzeichnet eine zufällige Buchstaben- oder Zahlenfolge?“ durch die Bestimmung zugehöriger Wahrscheinlichkeiten zu beantworten. Hierbei kann man sich zu Beginn auf einen Standardkontext konzentrieren. Naheliegende Möglichkeiten sind:

- Die Wahrscheinlichkeit für das *k*-fache Auftreten eines fest gewählten Buchstabens in einer zufälligen Buchstabenfolge der Länge *n* $\left(p = \frac{1}{26}\right)$.
- Die Wahrscheinlichkeit für das *k*-fache Auftreten eines Buchstabens einer fest gewählten Buchstabenmenge in einer zufälligen Buchstabenfolge der Länge *n* $\left(\text{z. B. Vokale mit } p = \frac{5}{26}\right)$.
- Die Wahrscheinlichkeit für das *k*-fache Auftreten einer fest gewählten Ziffer in einer zufälligen Ziffernfolge der Länge *n* $\left(\text{z. B. dezimal mit } p = \frac{1}{10} \text{ oder binär mit } p = \frac{1}{2}\right)$.

Lässt man die Schüler hierbei mit kleinen Zahlenwerten für *n* und *k* mit Hilfe von Baumdiagrammen die

entsprechenden Wahrscheinlichkeiten bestimmen, so wird schnell deutlich, dass es darauf ankommt, im Baumdiagramm die Anzahl der Wege zu bestimmen, bei denen k mal Erfolg und $(n-k)$ mal Misserfolg auftritt. Bei dem hier beschriebenen Konzept zur Stochastik im Kontext der Kryptologie liegt nun bei der Lösung dieses Problems eine Anknüpfung an die Grundvorstellung des Binomialkoeffizienten als Anzahl der Transpositionschiffren eines binären Wortes nahe: Ein Weg, bei dem k mal Erfolg und $(n-k)$ mal Misserfolg auftritt, kann dann identifiziert werden mit einem Wort aus k E's und $(n-k)$ M's; und die Anzahl dieser Wege ist ja gerade $\binom{n}{k}$. So erhält man den Ausdruck $\binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}$ als Wahrscheinlichkeit für das k-fache Auftreten von „Erfolg" in einer Buchstaben- oder Zahlenfolge der Länge n.

Betrachtet man diese Vorgehensweise in der Rückschau, so fällt auf, dass der Umweg über die Baumdiagramme fast künstlich ist und ein direkter Bezug zwischen dem Binomialkoeffizienten und dem Buchstaben- bzw. Zahlenfolgenkontext hergestellt werden kann. In den Zufallsfolgen wird nämlich nur noch zwischen „richtigen" und „falschen" Buchstaben unterschieden, d. h. die Folge wird quasi „binärisiert". In dieser nun binären Folge muss bei der Frage nach der Anzahl solcher Folgen jetzt also lediglich die Anzahl der Transpositionen bestimmt werden.

Die Erkenntnis, dass die Themen „Zufallszahlen" und „Transpositionschiffren" bei der Berechnung von Wahrscheinlichkeiten im Rahmen der Binomialverteilung einen engen Bezug zueinander aufweisen, mag überraschen. Für das hier dargelegte Konzept bietet sich dadurch die Möglichkeit der Vernetzung und Vertiefung von in unterschiedlichen Kontexten eingeführten Begriffen.

Beim notwendigen rechnerischen Einüben von Wahrscheinlichkeitsbestimmungen (rechnergestützt oder unter Verwendung von Tabellen) besteht erfahrungsgemäß die Gefahr, dass den Schülern das inhaltliche Verständnis für die Formel $P(X=k) = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}$ verloren geht. Es muss die Aufgabe eines verständnisorientierten Stochastikunterrichts sein, die oben beschriebenen Zusammenhänge immer wieder wiederholend und vertiefend zu thematisieren.

Hypothesentest: Wie sieht eine „gute" Zufallsfolge aus?

Das Testen der Güte von Pseudozufallszahlen bzw. Zufallsgeneratoren ist ein interessantes Problem der Stochastik und Informatik, für das eine Fülle von zum Teil sehr aufwendigen Verfahren existiert. Im Rahmen der schulischen Stochastik bietet sich hier die Behandlung von Hypothesentests mit Hilfe der Binomialverteilung an. Im Folgenden beschränken wir uns dabei auf 0/1-Folgen (also binäre Zufallszahlen) und $p = ½$, da dies einerseits der wichtigste Fall für die Anwendungen ist und andererseits gewisse didaktische Vereinfachungen bietet (so können z. B. 0/1-Zufallsfolgen schnell und einfach durch Münzwürfe von den Schülern erzeugt werden). Bei Bedarf kann das Vorgehen dann im Anschluss ohne große Schwierigkeiten auf andere Zufallsfolgen erweitert werden.

Ziel des Vorgehens ist eine genetische Entwicklung des Hypothesentestens, wie es Leuders (2005) beschreibt: *„Von einer genetischen Entwicklung des Hypothesentestens kann man sprechen, wenn das Verfahren und die mit ihm verbundenen Begriffe aus einer Problemsituation heraus von Schülerinnen und Schülern aktiv entwickelt werden."*

Beidseitiger Hypothesentest

Als Grundlage einer solchen Entwicklung muss die Wahrscheinlichkeitsverteilung einer binomialverteilten Zufallsgröße für $p = ½$ behandelt worden sein und z. B. in Form einer Tabelle für $n = 50$ vorliegen.

Ausgangspunkt des Unterrichts können dann verschiedene 0/1-Folgen der Länge 50 sein, die den Schülern mit der Bemerkung vorgelegt werden, dass es sich dabei sowohl um „zufällige" als auch um „nicht zufällige" Folgen handelt. Dabei wird hier unter einer „zufälligen" Folge das Ergebnis eines Zufallsexperiments mit binomialverteilter Zufallsgröße und $p = ½$ verstanden. Dazu wird folgende Aufgabe gestellt:

Sortiere diejenigen Folgen aus, die du für keine echten Zufallsfolgen hältst! Welche Wahrscheinlichkeitsaussage lässt sich über ein mögliches Fehlurteil treffen?

Nun ist z. B. folgender Verlauf der Diskussion im Unterricht denkbar: Eine Folge mit genau 8 Einsen bewerten die Schüler schon rein gefühlsmäßig als „unecht"; es sind einfach „zu wenige" Einsen. Hat man dagegen eine Folge mit genau 17 Einsen, so ist die Bewertung vielleicht schon umstrittener: Gefühlsmäßig ist ja 17 von 25 gar nicht mehr so weit weg; allerdings sieht man an der Tabelle auch, dass nur ca. 0,9 % der echten Zufallsfolgen genau 17 bzw. etwa 1,6 % der Folgen 17 oder weniger Einsen aufweisen.

So werden die meisten Schüler diese Folge wohl aussortieren; die Formulierung einer Wahrscheinlichkeitsaussage über ein mögliches Fehlurteil gestaltet sich allerdings als schwierig: Was ist die genaue Bedeutung der oben angegebenen Wahrscheinlichkeiten? Dass die Einzelwahrscheinlichkeit des beobachteten Merkmals keine geeignete Kennzahl zur Entscheidung ist, wird ja zum Beispiel an einer Folge mit genau 25 Einsen deutlich, die ja auch nur in etwa 11,2 % der zufälligen Folgen auftritt und somit für sich genommen noch recht unwahrscheinlich ist!

Diese Beobachtung wird noch deutlicher, wenn man jede 50stellige binäre Zahl als einzelnes Ereignis eines Zufallsexperiments betrachtet: Nun ist die Wahrscheinlichkeit für eine solche Zahl mit $\frac{1}{2^{50}}$ ja verschwindend gering, ohne dass man hieraus irgend welche Schlüsse ableiten kann!

k	$P(X \leq k)$
7	0,000000
8	0,000001
9	0,000003
10	0,000012
11	0,000045
12	0,000153
13	0,000468
14	0,001301
15	0,003300
16	0,007673
17	0,016420
18	0,032454
19	0,059460
20	0,101319
21	0,161118
22	0,239944
23	0,335906
24	0,443862
25	0,556138
26	0,664094
27	0,760056
28	0,838882
29	0,898681
30	0,940540
31	0,967546
32	0,983580
33	0,992327
34	0,996700
35	0,998699
36	0,999532
37	0,999847
38	0,999955
39	0,999988
40	0,999997
41	0,999999
42	1,000000

Somit kann zusammen mit den Schülern herausgearbeitet werden, dass vor der Entscheidung über einzelne Folgen zunächst ein ganzer Bereich für die als glaubwürdig zu betrachtenden Anzahlen von Einsen festgelegt werden muss!

Dies führt zu einer Klärung der Terminologie: Für die **Nullhypothese** „Die Folge ist zufällig“ wird ein **Annahme-** und ein **Ablehnungsbereich** bestimmt, welcher – dem betrachteten Kontext angemessen – symmetrisch um den Erwartungswert 25 gelegt wird. So nimmt ein **beidseitiger Hypothesentest** langsam Gestalt an. Erst jetzt können sinnvolle Wahrscheinlichkeitsaussagen über mögliche Fehlurteile getroffen werden. Beispielsweise könnte der Annahmebereich {18, …, 32} gewählt werden und dann die Folge mit 17 Einsen als nicht zufällig betrachtet werden, wobei dabei die Wahrscheinlichkeit, hierbei eine „echte“ Zufallsfolge als „unecht“ zu betrachten, bei etwa 3,3 % liegt (**Fehler 1. Art**). Andererseits kann keine Wahrscheinlichkeitsaussage über den Fehler gemacht werden, nicht zufällige Folgen als zufällig zu betrachten, da die wirkliche Wahrscheinlichkeitsverteilung in diesem Fall ja unbekannt ist (**Fehler 2. Art**). Nach welchen Kriterien aber werden der Annahmebereich und die daraus folgende **Entscheidungsregel** festgelegt? Dies wird durch den Begriff des **Signifikanzniveaus** festgelegt, welches die Wahrscheinlichkeit für den Fehler 1. Art begrenzt und so gewählt wird, dass dieses Risiko (die sogenannte **Irrtumswahrscheinlichkeit**) als subjektiv klein genug eingeschätzt wird.

Der hier dargestellte Aufbau der Begriffsbildung lässt sich im Kontext von Pseudozufallszahlen gut am beidseitigen Hypothesentest entwickeln. Der beidseitige birgt im Unterschied zum einseitigen Hypothesentest die Schwierigkeit, dass das Signifikanzniveau auf zwei Wahrscheinlichkeiten für den linken bzw. rechten Rand aufgeteilt werden muss. Für den hier dargestellten Fall $p = ½$ ist dies aufgrund der Symmetrie jedoch wesentlich unproblematischer als im nicht symmetrischen Fall. Weiterhin ist der beidseitige Hypothesentest im betrachteten Kontext zunächst der natürlichere Zugang, bei dem im Unterschied zum einseitigen Test auch keine Schwierigkeit bei der Wahl der Nullhypothese besteht.

Einseitiger Hypothesentest

Ein Gütetest von Pseudozufallszahlen allein auf der Basis der Ziffernanzahlen hat natürlich nur eine sehr eingeschränkte Aussagekraft. Die binären Folgen 00 00000000000000000000000111111111111111111111111 oder 01010101010101010101010101010101010101010101 wären ja auf dieser Grundlage „unverdächtig“, obwohl sie offensichtliche Besonderheiten aufweisen. Die meisten Gütetests beruhen auf komplizierteren Wahrscheinlichkeitsverteilungen und sind im schulischen Rahmen höchstens auf experimentelle Weise zu behandeln (vgl. Leuders (2005)).

Es gibt aber noch eine weitere, für die Schüler recht überraschende Möglichkeit, mit Hilfe der Binomialverteilung und einem einseitigen Hypothesentest „falsche“ Zufallszahlen zu entlarven. Die Idee hierzu geht auf Rohm (1994) zurück:

Man lässt die Schüler in Kleingruppen sowohl „ausgedachte“ als auch „echte“ Zufallszahlen produzieren. Konkret erzeugt jede Gruppe zwei 0/1-Folgen der Länge 51 (!); eine durch „Ausdenken“ und eine durch Münzwürfe. Diese beiden Folgen werden jeweils ungekennzeichnet auf eine Folie geschrieben und anschließend für alle sichtbar projiziert. Zur Überraschung der Schüler ist der Lehrer nun in den meisten Fällen in kurzer Zeit in der Lage, die ausgedachte Folge zu entlarven!

Wie funktioniert das? Der Lehrer führt im Kopf einen einseitigen Hypothesentest durch. Grundlage ist die Beobachtung, dass die meisten Menschen beim Produzieren von Zufallsfolgen dazu neigen, für übermäßig viel „Abwechslung“ zu sorgen und lange Wiederholungen zu vermeiden, da diese schnell als nicht zufällig eingeschätzt werden. Bezeichnet man bei einer Zufallszahl das Ereignis „eine Ziffer stimmt nicht mit ihrem Vorgänger überein“, als „Wechsel“, so ist die Zufallsvariable, die die Gesamtzahl der Wechsel bei einer 0/1-Folge der Länge 51 angibt, binomialverteilt mit $n = 50$ und $p = ½$. Dies kann man einfach daran erkennen, dass ab der zweiten Ziffer die beiden Möglichkeiten „Wechsel“ und „Wiederholung“ jeweils immer gleichwahrscheinlich sind. Da aufgrund obiger Beobachtung bei den ausgedachten Folgen nun mehr als 25 Wechsel erwartet werden, kann ein rechtsseitiger Hypothesentest durchgeführt werden. Ist man bei der Beurteilung einer als ausgedacht verdächtigten Folge bereit, mit einer Wahrscheinlichkeit von höchstens 6 % falsch zu liegen, so kann man die Entscheidungsregel „bei 31 oder mehr Wechseln betrachte ich die Folge als ausgedacht“ verwenden. Erfahrungsgemäß können so die meisten unvoreingenommen ausgedachten Folgen erkannt werden.

Ist den Schülern das Prinzip des beidseitigen Hypothesentests bereits bekannt, so können sie durch wenige Lehrerhinweise dahin geführt werden, den „Trick“ herauszufinden und anhand dieses Beispiels einen einseitigen Hypothesentest zu entwickeln. Als Hausaufgabe kann schließlich das oben beschriebene Experiment mit Freunden oder Familienangehörigen wiederholend durchgeführt werden, um dabei die Wirkungsweise eines solchen Hypothesentests zu vertiefen.

6 Fazit

Es wurde aufgezeigt, wie einige klassische stochastische Themen im Kontext der Kryptologie behandelt werden können:

Der erste Bereich betrifft kombinatorische Grundaufgaben, die auf natürliche Weise bei der Frage nach der Anzahl von Transpositions- und Substitutionschiffren auftreten, wodurch zum klassischen Urnenmodell alternative Grundvorstellungen für Permutationen und Kombinationen entstehen.

Zweitens kann im Rahmen des Friedman-Tests der Umgang mit Baumdiagrammen vertieft und in einem komplexeren Zusammenhang angewendet werden.

Ein drittes Themengebiet ist die Beantwortung der Frage „Was ist perfekte Sicherheit?“ durch bedingte Wahrscheinlichkeiten und den Satz von Bayes.

Und viertens wurde die Behandlung von Binomialverteilung und Hypothesentest zur Beurteilung von Pseudozufallszahlen vorgestellt, wodurch ein zentrales Gebiet der schulischen Stochastik in einen interessanten anwendungsnahen Kontext gestellt wird.

Das Konzept wurde in fächerübergreifenden Grundkursen in den Jahren 2008 und 2009 am Oberstufenkolleg in Bielefeld entwickelt und erprobt. Dabei konnten positive Erfahrungen hinsichtlich der Motivierung von Schülerinnen und Schülern für problemlösenden Mathematikunterricht mit stochastischem Schwerpunkt gemacht werden. Es scheint mir aber auch durchaus gut möglich zu sein, aus dem dargestellten Konzept einzelne Aspekte herauszugreifen und für den Unterricht in Stochastik in verschiedenen Jahrgangsstufen zu verwenden.

Aus Platzgründen konnte an dieser Stelle die konkrete unterrichtliche Umsetzung nur angedeutet werden; einzelne Unterrichtsmaterialien und ein Überblick über die zeitlichen Notwendigkeiten der Unterrichtssequenzen können auf Anfrage vom Verfasser bezogen werden.

Literatur

Beutelspacher, A. (2005): Kryptologie. Braunschweig und Wiesbaden: Vieweg.

Griesel, H.; Müller, A.; Postel, H. (2001): Geheime Nachrichten: Die Kunst des Ver- und Entschlüsselns. In: *Elemente der Mathematik – Unterrichtsmaterialien Sekundarstufe II*, Schroedel, 150–177.

Leuders, T. (2005): Darf das denn wahr sein? – Eine schüleraktive Entdeckung der Grundidee des Hypothesentestens durch Simulation mit Tabellenkalkulation. In: *Praxis der Mathematik in der Schule.* 2005 (4), 8–16.

Rohm, W. (1994): Statistik mit Zufallszahlen. Arbeitsgruppe Moderner MathematikUnterricht. http://www.ammu.at/archiv/4/ammu_4_4.pdf

Stohr, M. (2007): Unterricht in Kryptologie. Dissertation. Ludwig-Maximilian-Universität München. http://edoc.ub.uni-muenchen.de/8456/1/Stohr_Monika.pdf

Anschrift des Verfassers

Dr. Daniel Frohn
Universität Bielefeld
Institut für Didaktik der Mathematik
Postfach 10 01 31
33501 Bielefeld
daniel.frohn@uni-bielefeld.de