

Wahrscheinlichkeitstheorie und stochastische Prozesse für  
Informatik  
Skriptum

Karl Grill  
Institut für Stochastik und Wirtschaftsmathematik  
TU Wien

17. Januar 2018  
Version 0.2018.1

©2013–2018 Karl Grill CC-BY-SA 3.0 or later

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>2</b>
<b>2</b>	<b>Grundlagen der Wahrscheinlichkeitstheorie</b>	<b>4</b>
2.1	Die Axiome von Kolmogorov . . . . .	4
2.2	Bedingte Wahrscheinlichkeiten . . . . .	9
2.3	Zufallsvariable . . . . .	13
2.4	Transformationen . . . . .	21
2.5	Erwartungswert und Varianz . . . . .	26
2.6	Momente . . . . .	30
2.7	Folgen von Zufallsvariablen . . . . .	30
2.8	Spezielle Verteilungen . . . . .	33
2.8.1	Diskrete Verteilungen . . . . .	33
2.8.2	Stetige Verteilungen . . . . .	34
<b>3</b>	<b>Stochastische Prozesse</b>	<b>36</b>
3.1	Stationäre Prozesse . . . . .	36
3.2	Markovprozesse . . . . .	37
3.3	Markovketten in diskreter Zeit . . . . .	38
3.3.1	Übergangswahrscheinlichkeiten . . . . .	38
3.3.2	Klasseneigenschaften . . . . .	40
3.3.3	Markov Chain Monte Carlo . . . . .	45
3.3.4	Markovketten in stetiger Zeit . . . . .	45
<b>4</b>	<b>Informationstheorie</b>	<b>50</b>
4.1	Entropie und Information . . . . .	50
4.2	Codes . . . . .	56
4.3	Informationsquellen . . . . .	58
4.4	Blockcodes . . . . .	59
4.5	Kanalcodierung . . . . .	59
4.6	Natürliche Sprachen als Informationsquellen . . . . .	59
<b>5</b>	<b>Statistik</b>	<b>60</b>
5.1	Schätztheorie . . . . .	60
5.1.1	Punktschätzung . . . . .	60
5.1.2	Intervallschätzung . . . . .	62
5.2	Tests . . . . .	63
5.2.1	Grundlagen . . . . .	63
5.2.2	Spezielle Tests . . . . .	64
5.2.3	Der Chi-Quadrat-Anpassungstest . . . . .	64
5.2.4	Tests und Konfidenzintervalle . . . . .	65
<b>A</b>	<b>Tabellen</b>	<b>66</b>
<b>B</b>	<b>Mathematische Hintergründe</b>	<b>71</b>
B.1	Wahrscheinlichkeitsräume . . . . .	71

# Kapitel 1

## Einleitung

Als um das Jahr 2011 herum davon die Rede war, dass im Bachelorstudium “Technische Informatik” eine Einführungsvorlesung in Wahrscheinlichkeitstheorie und die Theorie der stochastischen Prozesse geschaffen werden soll, ist für mich ein lang gehegter Wunsch in Erfüllung gegangen — ich hatte schon lange davon geträumt, die Grundideen der Theorie der stochastischen Prozesse auf elementarem Niveau und mit einer Verbindung zur Anwendung zu unterrichten. Ich bedanke mich hier bei allen, die das möglich gemacht haben, ganz besonders bei dem Studienplankoordinator für die Technische Informatik, Ulrich Schmid, und bei meinem Kollegen Norbert Kusolitsch, die auch die ersten Überlegungen dazu angestellt haben, für ihre Unterstützung.

Ich selbst bin nun (Anfang 2018, im sechsten Jahr dieser Vorlesung) immer noch dabei, zu lernen und an der Gewichtung der Inhalte zu arbeiten. Ich danke allen meinen Studentinnen und Studenten für ihre Mitarbeit und für das hilfreiche Feedback, und bei meinen Kollegen, allen voran Zsolt Saffer, für die inhaltlichen und methodischen Diskussionen.

Dieses Skriptum und die Lehrveranstaltung dazu haben eine recht ambitionierte Inhaltsangabe: jedes der vier Kapitel Wahrscheinlichkeitstheorie, stochastische Prozesse, Informationstheorie und Statistik wäre für eine eigene Vorlesung und in einem Ausmaß, das über diese hinausgeht. Es ist also hier notwendig, eine sehr selektive Auswahl des Stoffes zu treffen, und an einigen Stellen habe ich mich gezwungen gesehen, auf eine mathematisch strenge Herleitung der Ergebnisse zu verzichten, um mich mehr mit der Anwendung der jeweiligen Resultate beschäftigen zu können, etwa bei den Gesetzen der großen Zahlen oder beim zentralen Grenzwertsatz. Zu meiner eigenen Beruhigung und für interessierte Leserinnen und Leser werden nach und nach im Anhang über mathematische Hintergründe zumindest skizzenhaft die Details ergänzt werden. Einstweilen (Jänner 2018) ist das noch Zukunftsmusik, momentan kämpfe ich noch damit, dieses Skriptum aus einer Sammlung von Überschriften und Schlagwörtern für diejenigen, die die Vorlesung besucht haben, in einen einigermaßen selbst stehenden Einführungstext zu verwandeln.

Dieses Skriptum versteht sich als freie Software. Die Creative Commons Attribution Share-Alike Lizenz erlaubt fast alles, auch eine kommerzielle Nutzung. Es sind nur zwei Bedingungen zu erfüllen: abgeleitete Werke müssen meinen Namen nennen (etwa: “dieses Werk basiert auf dem Skriptum ‘Wahrscheinlichkeitstheorie und stochastische Prozesse für Informatik’ von Karl Grill”), und sie müssen unter derselben Lizenz veröffentlicht werden, es dürfen also die Rechte, die hier gewährt werden, nicht eingeschränkt werden.

Zur Genderfrage: eigentlich habe ich das Glück, in der Mathematik zu arbeiten, die geradezu der Inbegriff von Körper- und damit Geschlechtslosigkeit ist (was manchmal zu recht interessanten Assoziationen führt, wie etwa in Wilhelm Reichs “Charakteranalyse” nachzulesen ist). Dennoch sind in manchen Beispielen, die Bezug auf die reale Welt nehmen, die handelnden Personen eben handelnde Personen, und gelegentlich möchte ich mich auch an Sie, liebe Leserinnen und Leser, wenden. Da bin ich nun hin- und hergerissen zwischen der Überzeugung, dass nur ein konsequenter Gebrauch von weiblicher und männlicher Form nebeneinander einen korrekten Umgang mit dem Problem darstellt (und nicht irgendwelche “I-” und “/”-Konstruktionen; der oft angepriesene Ausweg, nur geschlechtsneutrale Formulierungen zu verwenden, ist für mich nichts anderes als eine Flucht), und dem ästhetisch-pragmatischen Problem, dass Sätze mit vielen “sie und er”-Kombinationen holprig und schwer lesbar sind. Deswegen möchte ich es so halten, dass

grundsätzlich Formulierungen à la “Studentinnen und Studenten” oder “Studentin oder Student” verwendet werden, aber in Beispielen, die sonst zu mühsam zu lesen wären, die Rollen zur Hälfte weiblich und zur Hälfte männlich besetzt werden (wobei im Zweifelsfall die Frauen die besseren Rollen bekommen).

## Kapitel 2

# Grundlagen der Wahrscheinlichkeitstheorie

### 2.1 Die Axiome von Kolmogorov

Wir beginnen unsere Erkundung der Welt der Wahrscheinlichkeitstheorie mit einem einfachen Beispiel, dem Werfen von zwei Würfeln. Dabei gibt es insgesamt 36 mögliche Ausgänge — 6 Möglichkeiten für die Augenzahl des ersten Würfels, 6 für die des zweiten. Wenn wir diesen Versuch sehr oft wiederholen, etwa 36000 mal, werden wir feststellen, dass die Häufigkeiten der einzelnen Ausgänge sich nicht allzu sehr von 1000 unterscheiden (mit dem Wissen, das wir in dieser Vorlesung erwerben, würde es uns sehr verwundern, wenn die Abweichung größer als 100 wäre). Die relative Häufigkeit der einzelnen Ausgänge liegt also ungefähr bei  $1/36$ . Die Feststellung, dass sich die relativen Häufigkeiten der einzelnen Versuchsausgänge in einer großen Anzahl von Versuchen bei gewissen Werten, den Wahrscheinlichkeiten, “einpendeln”, ist als das “empirische Gesetz der großen Zahlen” bekannt. Dabei handelt es sich zwar nicht um einen mathematischen Satz, und deshalb hat es in einer strengen Behandlung des Themas eigentlich nichts verloren, wir werden es aber gelegentlich benutzen, um gewisse Begriffe zu motivieren oder zu veranschaulichen.

Was wir aus dem empirischen Gesetz der großen Zahlen mitnehmen können, ist, dass Wahrscheinlichkeiten etwas sind, mit dem man rechnen kann wie mit relativen Häufigkeiten. Dazu fassen wir zunächst die möglichen Versuchsausgänge zu einer Menge  $\Omega$  zusammen, die wir die Grundmenge nennen. In unserem Beispiel ist

$$\Omega = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\} = \{(1, 1), (1, 2), \dots, (6, 6)\}.$$

Die Elemente von  $\Omega$  heißen Elementarereignisse. Wir können nun beliebige Ereignisse definieren, etwa “die Summe der Augenzahlen ist 9” oder “der erste Würfel zeigt Augenzahl 5”. Wir können solche Ereignisse festlegen, indem wir die Menge der Elementarereignisse angeben, bei denen sie eintreten. Aus diesem Grund werden für uns in Hinkunft Ereignisse einfach Teilmengen der Grundmenge  $\Omega$  sein.

Die beiden Ereignisse, die wir genannt haben, sind dann

$$A = \{(3, 6), (4, 5), (5, 4), (6, 3)\}$$

und

$$B = \{(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6)\}.$$

Da wir unsere Ereignisse als Mengen definieren, können wir sie auch mit den Mengenoperationen verknüpfen. Wir können also von den Ereignissen  $A^C$  (“ $A$  tritt nicht ein”),  $A \cap B$  (“ $A$  und  $B$  treten ein”) und  $A \cup B$  (“ $A$  oder  $B$  tritt ein”) sprechen — wie es in der Mathematik üblich ist, verstehen wir das “oder” inklusiv. Ein “exklusives Oder” für Ereignisse gibt es allerdings auch, als Mengenoperation heißt es “symmetrische Differenz”:

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Die leere Menge heißt auch das unmögliche Ereignis, die Grundmenge  $\Omega$  das sichere Ereignis.

Diesen Ereignissen wollen wir Zahlenwerte — Wahrscheinlichkeiten — zuordnen. Diese sollen sich verhalten wie relative Häufigkeiten, insbesondere zwischen 0 und 1 liegen und additiv sein — die Wahrscheinlichkeit der Vereinigung von disjunkten Ereignissen ist die Summe der einzelnen Wahrscheinlichkeiten. Wir verlangen zusätzlich, dass diese Additivität auch für abzählbar unendlich viele Ereignisse gilt:

### Definition 2.1: Axiome von Kolmogorov

$\Omega$  sei eine beliebige (nichtleere) Menge. Eine Funktion  $\mathbb{P}$ , die Mengen  $A \subseteq \Omega$  reelle Zahlen zuordnet, heißt Wahrscheinlichkeit (oder Wahrscheinlichkeitsmaß), wenn die folgenden Axiome gelten:

1.  $0 \leq \mathbb{P}(A) \leq 1$ ,
2.  $\mathbb{P}(\emptyset) = 0$ ,
3.  $\mathbb{P}(\Omega) = 1$ ,
4. wenn  $A_n, n \in \mathbb{N}$  disjunkte Ereignisse sind (d.h.,  $A_i \cap A_j = \emptyset, i \neq j$ ), dann gilt

$$\mathbb{P}\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \sum_{n \in \mathbb{N}} \mathbb{P}(A_n).$$

Wir fassen noch einmal zusammen:

### Definition 2.2: Wahrscheinlichkeitsraum

Ein Wahrscheinlichkeitsraum besteht aus einer Menge  $\Omega$ , der *Grundmenge*. Die Elemente  $\omega \in \Omega$  heißen *Elementarereignisse*, die Teilmengen  $A \subseteq \Omega$  *Ereignisse*. Auf der Menge der Ereignisse ist ein Wahrscheinlichkeitsmaß  $\mathbb{P}$  definiert.

Anmerkungen:

1. In dieser Definition haben wir keine genauen Angaben über den Definitionsbereich von  $\mathbb{P}$  gemacht. Wir hoffen natürlich, dass wir für alle Teilmengen von  $\Omega$  eine Wahrscheinlichkeit definieren können. Wenn  $\Omega$  unendlich (überabzählbar) ist, gibt es damit allerdings Probleme. Wir werden in dieser Vorlesung darauf vertrauen, dass alle Mengen, mit denen wir es zu tun haben, brav genug sind, dass sie eine Wahrscheinlichkeit verdienen, und ansonsten nicht weiter darüber nachdenken. In der Mathematik wird das Problem so gelöst, dass der Definitionsbereich des Wahrscheinlichkeitsmaßes auf eine Teilmenge der Potenzmenge von  $\Omega$  eingeschränkt wird (siehe Anhang).
2. Ein simples Beispiel für einen Wahrscheinlichkeitsraum mit (abzählbar) unendlich vielen Elementen ist das Werfen einer Münze, bis zum ersten Mal “Kopf” erscheint. Die Anzahl der Würfe kann jede beliebige positive ganze Zahl sein, also ist  $\Omega = \mathbb{N}$  (und  $\mathbb{P}(\{n\}) = 2^{-n}$ , wenn wir annehmen, dass alle möglichen Münzwurffolgen der Länge  $n$  gleiche Wahrscheinlichkeit haben).
3. Ein Beispiel für einen überabzählbaren Wahrscheinlichkeitsraum gibt das Intervall  $[0, 1]$ , wobei wir  $\mathbb{P}([a, b]) = b - a$  setzen (die Wahrscheinlichkeit eines Intervalls ist also gleich seiner Länge). Im nächsten Beispiel werden wir einen Weg sehen, wie man dazu kommt.
4. Die Elementar-“Ereignisse” sind eigentlich keine Ereignisse, weil sie ja *Elemente* und keine *Teilmengen* von  $\Omega$  sind. So ist etwa für  $\Omega = \{1, 2, 3\}$  das Elementarereignis “1” kein Ereignis, um es zu einem Ereignis zu machen, müssen wir Mengenklammern darum setzen:  $\{1\}$  ist das Ereignis mit dem einen Element 1. In der Zukunft wird allerdings wenig Anlass bestehen, über Elementarereignisse im eigentlichen Sinn zu sprechen, wir werden uns also die Freiheit nehmen, auch die Mengen der Form  $\{\omega\}$  als “Elementarereignisse” zu bezeichnen. Diese kleine Schlamperei können wir uns erlauben, weil stets aus dem Kontext klar sein sollte, in welchem Sinn dieser Begriff zu verstehen ist (gewissermaßen als objektorientierte Überladung).

In vielen Fällen (etwa beim Würfeln) ist es aus Symmetriegründen plausibel, dass alle Elementarereignisse dieselbe Wahrscheinlichkeit haben müssen; wegen der Additivität muss dann die Wahrscheinlichkeit eines Ereignisses proportional zu seiner Mächtigkeit sein, also kommen wir zu der Definition

**Definition 2.3: Laplacescher Wahrscheinlichkeitsraum**

Wenn  $\Omega$  endlich ist und

$$\mathbb{P}(A) = \frac{|A|}{|\Omega|}$$

(d.h. alle Elementarereignisse haben dieselbe Wahrscheinlichkeit), dann heißt der Wahrscheinlichkeitsraum ein Laplace'scher Wahrscheinlichkeitsraum.

Diese Annahme liegt den meisten "Spielzeugen" der Wahrscheinlichkeitstheoretiker zugrunde: wir werden meist annehmen, dass die Seiten eines Würfels, die Seiten einer Münze, die Kugeln in einer Urne... alle dieselbe Wahrscheinlichkeit haben, geworfen bzw. gezogen zu werden. Gelegentlich werden wir diese Eigenschaft hervorheben, indem wir von einem "fairen" Würfel oder einer "fairen" Münze sprechen. Im Beispiel am Anfang unseres Kapitels würden wir also dem Ereignis  $A$  ("Augensumme 9") die Wahrscheinlichkeit  $4/36 = 1/9$  und dem Ereignis  $B$  ("erster Würfel 5") die Wahrscheinlichkeit  $6/36 = 1/6$  zuordnen.

Die Definition eines Laplace'schen Wahrscheinlichkeitsraumes ist nur für endliche Mengen  $\Omega$  sinnvoll. Die Wahrscheinlichkeiten in Anmerkung 3 kann man zwar auch als "gleichmäßig verteilt" ansehen, aber die Analogie zum endlichen Fall ist nicht perfekt: für endliche Laplace'sche Räume ergibt sich durch eine umkehrbar eindeutige Abbildung etwa wieder ein Laplacescher Raum, im unendlichen Beispiel stimmt das (etwa mit der Abbildung  $x \mapsto x^3$ ) nicht.

Auf der anderen Seite lässt sich das Wahrscheinlichkeitsmaß in Anmerkung 3 als Grenzfall von Laplace'schen Maßen (etwa auf  $\Omega_n = \{k2^{-n}, 1 \leq k \leq 2^n\}$ ) ansehen. Man muss dazu nur das Maß zu einem Maß auf ganz  $[0, 1]$  ergänzen, indem das Komplement von  $\Omega_n$  (und auch alle seine Teilmengen) Maß 0 erhält. Dann überzeugt man sich leicht, dass die Wahrscheinlichkeit von  $[0, x]$  tatsächlich gegen  $x$  konvergiert (für  $0 \leq x \leq 1$ ).

**Beispiel 2.1**

Man kann sich etwa vorstellen, dass ein Mann zu einem zufälligen Zeitpunkt zwischen 8 und 9 in seinem bevorzugten Bar Tabacchi eintrifft. Wenn die Ankunftszeit in Minuten gemessen wird, sollte jede der 60 Minuten gleich wahrscheinlich sein, bei immer genauerer Messung sollte auch jede Sekunde, Zehntel-, Hundertstel-, Millionstel-, ..., Abstrusillionstel-Sekunde dieselbe Wahrscheinlichkeit wie alle anderen haben (die natürlich für kleinere Einheiten auch immer kleiner werden). Im Grenzfall (wenn wir diese Zeiteinheit gegen 0 gehen lassen) ergibt sich so genau das Beispiel aus Anmerkung 3. Lassen wir nun eine Kollegin ebenfalls zufällig zwischen 8 und 9 dort ankommen, und nehmen wir weiter an, dass beide jeweils 10 Minuten bei ihrem Kaffee verbringen. Wir wollen wissen, wie groß die Wahrscheinlichkeit ist, dass beide zusammentreffen. Dazu tragen wir die beiden Ankunftszeiten in einem rechtwinkligen Koordinatensystem ein (Abb. 2.1).

Die gesuchte Wahrscheinlichkeit bestimmen wir als das Verhältnis der schraffierten Fläche ( $|x - y| \leq 10$ ) zur Gesamtfläche des Quadrats (also  $11/36$ ).

Solche "geometrischen Wahrscheinlichkeiten" sind in einfachen Fällen wie diesem eine brauchbare Veranschaulichung — die Berechnung der Wahrscheinlichkeit über die Fläche entspricht der Annahme, dass die beiden Ankunftszeiten unabhängig sind — Dieser Begriff wird uns im nächsten Abschnitt beschäftigen.

In komplizierteren Fällen ist nicht immer eindeutig klar, was unter einer "gleichmäßigen" Verteilung zu verstehen ist, und unterschiedliche Interpretationen geben unterschiedliche Resultate (Bertrand'sches Paradox).

Aus den Axiomen von Kolmogorov ergeben sich einige elementare Folgerungen:

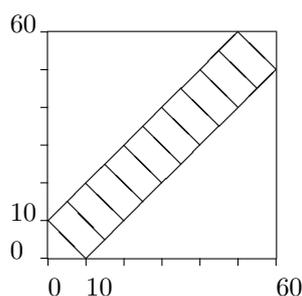


Abbildung 2.1: Geometrische Wahrscheinlichkeit

**Satz 2.1**

1.  $\mathbb{P}(A^C) = 1 - \mathbb{P}(A)$ .
2. Wenn  $A \subseteq B$ , dann gilt  $\mathbb{P}(A) \leq \mathbb{P}(B)$ .
3.  $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ .
4. Für Ereignisse  $A_n$  mit  $A_n \subseteq A_{n+1}$  gilt

$$\mathbb{P}\left(\bigcup_n A_n\right) = \lim_n \mathbb{P}(A_n).$$

5. Für Ereignisse  $A_n$  mit  $A_n \supseteq A_{n+1}$  gilt

$$\mathbb{P}\left(\bigcap_n A_n\right) = \lim_n \mathbb{P}(A_n).$$

6. Für beliebige Ereignisse  $A_n, n \in \mathbb{N}$  gilt

$$\mathbb{P}\left(\bigcup_n A_n\right) \leq \sum_n \mathbb{P}(A_n).$$

7. Borel-Cantelli Lemma: wenn  $\sum_n \mathbb{P}(A_n) < \infty$ , dann ist

$$\mathbb{P}(\text{unendlich viele Ereignisse } A_n \text{ treten ein}) = 0.$$

*Beweis:*

1. folgt aus  $\Omega = A \cup A^C$ .
2.  $\mathbb{P}(B) = \mathbb{P}(A) + \mathbb{P}(B \setminus A)$ .
3. folgt aus den Gleichungen

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

und

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

Insbesondere ist

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

4. Mit  $B_1 = A_1, B_n = A_n \setminus A_{n-1} (n \geq 2)$  ergibt sich

$$A_n = \bigcup_{i \leq n} B_i,$$

$$\bigcup_n A_n = \bigcup_i B_i,$$

und wegen 2

$$\mathbb{P}(B_n) \leq \mathbb{P}(A_n),$$

also

$$\mathbb{P}\left(\bigcup_n A_n\right) = \mathbb{P}\left(\bigcup_n B_n\right) = \sum_n \mathbb{P}(B_n) = \lim_{N \rightarrow \infty} \sum_{n \leq N} \mathbb{P}(B_n) = \lim_{N \rightarrow \infty} \mathbb{P}\left(\bigcup_{n \leq N} B_n\right) = \lim_{N \rightarrow \infty} \mathbb{P}(A_n).$$

5. folgt aus 1 und 4.

6. Wiederholte Anwendung der Folgerung zu Punkt 3 liefert

$$\mathbb{P}\left(\bigcup_{n \leq N} A_n\right) \leq \sum_{n \leq N} \mathbb{P}(A_n),$$

und wegen 4 kann man hier  $N$  gegen  $\infty$  gehen lassen.

7. Wir bezeichnen das Ereignis “unendlich viele  $A_n$  treffen ein” mit  $B$ . Für jedes  $N > 0$  gilt

$$B \subseteq \bigcup_{n \geq N} A_n,$$

und damit

$$\mathbb{P}(B) \leq \sum_{n \geq N} \mathbb{P}(A_n),$$

und für  $N \rightarrow \infty$

$$\mathbb{P}(B) \leq \lim_{N \rightarrow \infty} \sum_{n \geq N} \mathbb{P}(A_n) = 0.$$

Punkt 3 des letzten Satzes lässt sich verallgemeinern, etwa ergibt sich für die Vereinigung von 3 Ereignissen

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

Allgemein gilt

### Satz 2.2: Additionstheorem

$A_1, \dots, A_n$  seien beliebige Ereignisse. Dann gilt

$$\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n (-1)^{i-1} S_i$$

mit

$$S_i = \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} \mathbb{P}(A_{j_1} \cap \dots \cap A_{j_i}).$$

Es werden also alle Wahrscheinlichkeiten summiert, davon wird die Summe aller Wahrscheinlichkeiten von Durchschnitten von zwei Mengen abgezogen, dann kommen die dreifachen Durchschnitte dazu, die vierfachen weg, bis schließlich der Durchschnitt aller  $n$  Mengen dazugezählt ( $n$  ungerade bzw. abgezogen ( $n$  gerade) wird.

### Beispiel 2.2

Als Anwendung dieses Satzes berechnen wir die Wahrscheinlichkeit, dass eine zufällig gewählte Permutation von  $n$  Elementen keinen Fixpunkt hat. Diese Frage wird gern in der Form präsentiert, dass eine Anzahl (10) von Ehepaaren sich zu einer Tanzveranstaltung treffen, und nach einiger Zeit, in der nur die Ehepartner miteinander tanzen, beschließen, die Tanzpartner durch das Los zu bestimmen. In dieser Einkleidung wird unsere Frage zu der nach der Wahrscheinlichkeit, dass kein Ehepaar miteinander tanzt.

Wir betrachten das Gegenereignis  $A$ , dass mindestens ein Fixpunkt existiert. Dieses können wir wieder als Vereinigung der Ereignisse  $A_i$ , dass  $i$  ein Fixpunkt ist, schreiben, also

$$\mathbb{P}(A) = \mathbb{P}\left(\bigcup_{i=1}^n A_i\right).$$

Diese Wahrscheinlichkeit bestimmen wir mit dem Additionstheorem. Dazu müssen wir die Summen  $S_k$  berechnen. Das Ereignis  $A_{i_1} \cap \dots \cap A_{i_k}$  tritt ein, wenn  $i_1, \dots, i_k$  Fixpunkte sind, die anderen  $n - k$  Elemente können beliebig vertauscht werden. Das gibt  $(n - k)!$  günstige Möglichkeiten von insgesamt  $n!$  und somit eine Wahrscheinlichkeit  $(n - k)!/n!$ . Es gibt  $\binom{n}{k}$  solcher Summanden, also

$$S_k = \binom{n}{k} \frac{(n - k)!}{n!} = \frac{1}{k!}.$$

Insgesamt ist

$$\mathbb{P}(A) = \sum_{k=1}^n (-1)^{k-1} \frac{1}{k!}$$

und die Wahrscheinlichkeit, die wir suchen,

$$\mathbb{P}(A^C) = \sum_{k=0}^n (-1)^k \frac{1}{k!}.$$

Für großes  $n$  ist das näherungsweise  $1/e$ . Die Näherung ist so gut, dass sich die Anzahl der Permutationen ohne Fixpunkt (für  $n \geq 1$ ) bestimmen lässt, indem man  $n!/e$  auf die nächste ganze Zahl rundet.

## 2.2 Bedingte Wahrscheinlichkeiten

### Definition 2.4

$A$  und  $B$  seien zwei Ereignisse mit  $\mathbb{P}(B) > 0$ . Dann heißt

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

die bedingte Wahrscheinlichkeit von  $A$  unter (der Bedingung)  $B$ .

Zur Motivation dieser Definition geben wir vor, an das empirische Gesetz der großen Zahlen zu glauben. Unter  $N$  Versuchen sind dann etwa  $N\mathbb{P}(B)$  Versuche, bei denen  $B$  eintritt. Die Information, dass  $B$  eingetreten ist, sagt uns jetzt, dass unser Versuch zu diesen  $N\mathbb{P}(B)$  gehört. Von diesen sind wiederum etwa  $N\mathbb{P}(A \cap B)$  solche, bei denen auch  $A$  eintritt. Nach der Formel “günstige durch mögliche Fälle” ergibt sich unsere Formel.

Die Definition kann man ausmultiplizieren und erhält

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

Mehrfache Anwendung dieser Formel liefert den

### Satz 2.3: Multiplikationssatz

$A_1, \dots, A_n$  seien Ereignisse mit  $\mathbb{P}(A_1 \cap \dots \cap A_{n-1}) > 0$ . Dann gilt

$$\mathbb{P}(A_1 \cap \dots \cap A_n) = \mathbb{P}(A_1)\mathbb{P}(A_2|A_1)\mathbb{P}(A_3|A_1 \cap A_2) \dots \mathbb{P}(A_n|A_1 \cap \dots \cap A_{n-1}).$$

**Beispiel 2.3: Ziehen ohne Zurücklegen**

Ein typisches Beispiel ist das Ziehen ohne Zurücklegen: Es seien etwa in einer Urne zwei schwarze und drei weiße Kugeln. Es wird dreimal ohne Zurücklegen gezogen, und wir wollen die Wahrscheinlichkeit bestimmen, dass alle gezogenen Kugeln weiß sind. Wir setzen also  $A_i$  gleich dem Ereignis, dass die  $i$ -te gezogene Kugel weiß ist, und suchen  $\mathbb{P}(A_1 \cap A_2 \cap A_3)$ . Am Anfang sind in der Urne fünf Kugeln, drei davon sind weiß, also

$$\mathbb{P}(A_1) = \frac{3}{5}.$$

Nach der ersten Ziehung (mit Ergebnis  $A_1$ ) sind noch vier Kugeln in der Urne, davon sind zwei weiß, also

$$\mathbb{P}(A_2|A_1) = \frac{2}{4}.$$

Schließlich sind nach den ersten beiden Ziehungen noch eine weiße und zwei schwarze Kugeln in der Urne, und die Wahrscheinlichkeit, nochmals weiß zu ziehen, ist

$$\mathbb{P}(A_3|A_1 \cap A_2) = \frac{1}{3}.$$

Insgesamt ergibt sich

$$\mathbb{P}(A_1 \cap A_2 \cap A_3) = \frac{3 \cdot 2 \cdot 1}{5 \cdot 4 \cdot 3} = \frac{1}{10}.$$

Wenn wir nach der Wahrscheinlichkeit fragen, dass zwei weiße Kugeln unter den drei gezogenen sind, dann stellen wir zuerst fest, dass dieses Ereignis auf drei Arten eintreten kann — die schwarze Kugel kann die erste, zweite oder dritte gezogene sein. Das ergibt

$$\begin{aligned} \mathbb{P}(\text{“2 weiße”}) &= \mathbb{P}(A_1^C \cap A_2 \cap A_3) + \mathbb{P}(A_1 \cap A_2^C \cap A_3) + \mathbb{P}(A_1 \cap A_2 \cap A_3^C) = \\ &= \frac{2 \cdot 3 \cdot 2 + 3 \cdot 2 \cdot 2 + 3 \cdot 2 \cdot 2}{5 \cdot 4 \cdot 3} = \frac{3}{5}. \end{aligned}$$

Es fällt auf, dass die drei Summanden den gleichen Wert haben — die Faktoren treten nur in unterschiedlicher Reihenfolge auf.

In einer allgemeinen Formulierung — in der Urne sind  $N$  Kugeln, davon sind  $A$  weiß,  $n$  werden gezogen,  $x$  gezogene sind weiß — ist die Situation genauso. Die weißen Kugeln können auf  $\binom{n}{x}$  Arten auf die  $n$  Ziehungen verteilt werden, und in jeder dieser Wahrscheinlichkeiten treten dieselben Faktoren auf, es ergibt sich also

$$\begin{aligned} \mathbb{P}(x \text{ wei\ss e}) &= \binom{n}{x} \frac{A \cdot (A-1) \cdots (A-x+1)(N-A) \cdot (N-A-1) \cdots (N-A-n+x+1)}{N \cdot (N-1) \cdots (N-n+1)} = \\ &= \frac{\binom{A}{x} \binom{N-A}{n-x}}{\binom{N}{n}}. \end{aligned} \tag{2.1}$$

Die letzte Gleichung lässt sich etwas einfacher so ableiten: aus Symmetriegründen sind alle  $\binom{N}{n}$  Auswahlen von  $n$  gezogenen Kugeln aus den  $N$  vorhandenen gleich wahrscheinlich; günstig sind die, bei denen aus den  $A$  weißen Kugeln genau  $x$  Kugeln gezogen werden und die übrigen  $n-x$  aus den  $N-A$  schwarzen. Das geht auf  $\binom{A}{x} \binom{N-A}{n-x}$  Arten. Eigentlich müssten wir hier noch Grenzen für  $x$  vorgeben (in unserem Beispiel mit  $N=5$ ,  $A=3$  und  $n=3$  muss  $1 \leq x \leq 3$  gelten), aber wir können darauf verzichten, wenn wir

$$\binom{n}{k} = 0$$

setzen, wenn  $k < 0$  oder  $k > n$  ist.

Im Multiplikationssatz ist es nicht zwingend notwendig, dass die bedingenden Ereignisse positive Wahrscheinlichkeiten haben. Es muss dann natürlich die bedingte Wahrscheinlichkeit auf einem anderen Weg gefunden werden, etwa so wie in diesem Beispiel:

**Beispiel 2.4**

Ein Würfel wird einmal geworfen. Anschließend werden eine schwarze Kugel und so viele weiße Kugeln, wie die Augenzahl des Würfels angibt, in eine Urne gelegt. Aus dieser Urne wird dann eine Kugel zufällig gezogen. Wir definieren die Ereignisse  $A_n$ : “es wird eine  $n$  gewürfelt” und  $B$ : “die gezogene Kugel ist schwarz”. Dann ist

$$\mathbb{P}(B|A_n) = \frac{1}{n+1}$$

(es sind ja  $n$  weiße und eine schwarze Kugel in der Urne), und

$$\mathbb{P}(A_n \cap B) = \mathbb{P}(A_n)\mathbb{P}(B|A_n) = \frac{1}{6(n+1)}$$

für  $n = 1, \dots, 6$ . Wir können aber auch ein  $n > 6$  einsetzen. Dann ist nämlich  $\mathbb{P}(A_n) = 0$ , und damit auch  $\mathbb{P}(A_n \cap B) = 0$  und

$$\mathbb{P}(A_n)\mathbb{P}(B|A_n) = \mathbb{P}(A_n)\frac{1}{n+1} = 0.$$

Es gilt also auch im Fall  $\mathbb{P}(A) = 0$

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

Für die Gültigkeit dieser Gleichung ist sogar unwichtig, welchen Wert wir der bedingten Wahrscheinlichkeit geben. Das ist hier nicht besonders wichtig, im Kapitel über Markovketten werden wir diese Tatsache (meist stillschweigend) verwenden.

Wenn die bedingte Wahrscheinlichkeit  $\mathbb{P}(A|B)$  gleich der unbedingten  $\mathbb{P}(A)$  ist, wenn also das Wissen um das Eintreten von  $B$  unsere Einschätzung der Wahrscheinlichkeit von  $A$  nicht ändert, werden wir sagen, dass  $A$  von  $B$  unabhängig ist. Die entsprechende Gleichung können wir ausmultiplizieren, dadurch können wir auf die Forderung  $\mathbb{P}(B) > 0$  verzichten und sehen, dass die Rollen von  $A$  und  $B$  symmetrisch sind:

**Definition 2.5: Unabhängigkeit**

Zwei Ereignisse  $A$  und  $B$  heißen unabhängig, wenn

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

Die Ereignisse  $A_1, \dots, A_n$  heißen unabhängig, wenn für alle  $k \leq n$  und  $1 \leq i_1 < i_2 < \dots < i_k \leq n$  gilt

$$\mathbb{P}(A_{i_1} \cap \dots \cap A_{i_k}) = \mathbb{P}(A_{i_1})\mathbb{P}(A_{i_2}) \dots \mathbb{P}(A_{i_k}).$$

Die Ereignisse  $A_1, \dots, A_n$  heißen paarweise unabhängig, wenn für alle  $1 \leq i < j \leq n$

$$\mathbb{P}(A_i \cap A_j) = \mathbb{P}(A_i)\mathbb{P}(A_j).$$

Unendlich viele Ereignisse nennen wir unabhängig, wenn jede endliche Auswahl daraus unabhängig ist.

In unserem Urnenbeispiel sind die Ereignisse  $A_i$  (“die  $i$ -te Kugel ist weiß”) nicht unabhängig. Um das für  $A_1$  und  $A_2$  zu verifizieren, bestimmen wir die Wahrscheinlichkeit von  $A_2$ . Das kann mit einem Symmetrieargument geschehen (auch beim zweiten, dritten, ... Zug muss jede Kugel mit gleicher Wahrscheinlichkeit  $1/5$  gezogen werden) geschehen, andererseits können wir die Wahrscheinlichkeit von  $A_2$  auch so erhalten:

$$\begin{aligned} \mathbb{P}(A_2) &= \mathbb{P}(\Omega \cap A_2) = \mathbb{P}((A_1 \cup A_1^C) \cap A_2) = \mathbb{P}(A_1 \cap A_2) + \mathbb{P}(A_1^C \cap A_2) = \\ &= \mathbb{P}(A_1)\mathbb{P}(A_2|A_1) + \mathbb{P}(A_1^C)\mathbb{P}(A_2|A_1^C) = \frac{3 \cdot 2 + 2 \cdot 3}{5 \cdot 4} = \frac{3}{5}. \end{aligned}$$

Damit sehen wir

$$\mathbb{P}(A_1 \cap A_2) = 0.3 \neq \mathbb{P}(A_1)\mathbb{P}(A_2) = 0.36,$$

und  $A_1$  und  $A_2$  sind nicht unabhängig.

Das Vorgehen, das wir zur Berechnung von  $\mathbb{P}(A_2)$  verwendet haben, lässt sich auch in allgemeiner Form anwenden: wir nehmen an, dass (endlich oder abzählbar viele) Ereignisse  $B_i$  gegeben sind, von denen genau eines eintritt, und dass wir sowohl die Wahrscheinlichkeiten der Ereignisse  $B_i$  und die bedingten Wahrscheinlichkeiten eines weiteren Ereignisses  $A$  bezüglich jedes dieser Ereignisse kennen (oder leicht berechnen können). Dann gilt

**Satz 2.4: Satz von der vollständigen Wahrscheinlichkeit**

$B_i$  seien disjunkte Ereignisse mit  $\mathbb{P}(B_i) > 0$  und  $\bigcup_i B_i = \Omega$  und  $A$  ein beliebiges Ereignis. Dann gilt

$$\mathbb{P}(A) = \sum_i \mathbb{P}(B_i)\mathbb{P}(A|B_i).$$

Diese Berechnungen lassen sich (wenn es nicht zu viele Möglichkeiten gibt) mit einem Baumgraphisch darstellen (Abb. 2.2): An den Kanten stehen die bedingten Wahrscheinlichkeiten, an den Knoten die Wahrscheinlichkeiten der einzelnen Zweige, die sich als Produkt der Werte an den Kanten (von der Wurzel ausgehend) berechnen. Die Wahrscheinlichkeit des gesuchten Ereignisses  $A$  ergibt sich als die Summe der Wahrscheinlichkeiten aller Endknoten, die zu  $A$  gehören.

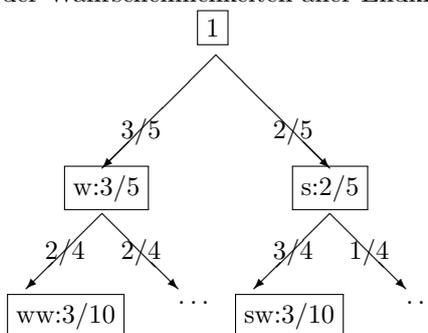


Abbildung 2.2: Vollständige Wahrscheinlichkeit

Wir können dann umgekehrt die bedingte Wahrscheinlichkeit ausrechnen, dass eines der Ereignisse  $B_i$  eingetreten ist, wenn  $A$  beobachtet wurde:

**Satz 2.5: Satz von Bayes**

Unter denselben Voraussetzungen wie im vorigen Satz gilt (wenn der Nenner positiv ist)

$$\mathbb{P}(B_j|A) = \frac{\mathbb{P}(B_j)\mathbb{P}(A|B_j)}{\sum_i \mathbb{P}(B_i)\mathbb{P}(A|B_i)}.$$

**Beispiel 2.5: Blutgruppen**

Wir wenden diesen Satz auf eine Frage an, die mich einige Zeit beschäftigt hat: ich habe lange Zeit meine Blutgruppe nicht gekannt, aber die meiner Frau ( $A$ ) und die meines Sohnes ( $0$ ). Wir wollen also nun die bedingte Wahrscheinlichkeit für die möglichen Ausprägungen meiner Blutgruppe bestimmen. Dazu müssen wir zuerst einige Informationen zu den Blutgruppen einholen: wie jede genetisch bedingte Eigenschaft wird auch die Blutgruppe durch zwei Gene (eins vom Vater, eins von der Mutter) bestimmt. Diese können die Ausprägungen  $a$ ,  $b$  und  $o$  besitzen. Bei einem zufällig gewählten Menschen nehmen die beiden Gene unabhängig voneinander die einzelnen Werte mit Wahrscheinlichkeiten  $p_a$ ,  $p_b$  und  $p_o$  an. Die Kombinationen  $aa$ ,

$ao$  und  $oa$  resultieren in Blutgruppe A,  $bb$ ,  $b0$  und  $0b$  ergeben B,  $ab$  und  $ba$  AB und schließlich  $oo$  0. Pschyrembels medizinisches Wörterbuch liefert, dass in Europa 47% der Bevölkerung Blutgruppe A haben, 9% B, 4% AB und 40% 0. Daraus ergibt sich (ungefähr, die Gleichungen sind überbestimmt und nicht exakt zu lösen)

$$p_a = 0.300, p_b = 0.067, p_0 = 0.633.$$

Aus den Informationen über die Blutgruppen meiner Frau und meines Sohnes können wir folgern, dass mein Sohn von mir ein Gen  $o$  haben muss. Meine Ausstattung muss also entweder  $oa/ao$  (wir bezeichnen dieses Ereignis mit  $A_a$ ),  $ob/bo$  (Ereignis  $A_b$ ) oder  $oo$  (Ereignis  $A_0$ ) sein. Die a-priori-Wahrscheinlichkeiten dafür sind  $2p_a p_0$ ,  $2p_b p_0$  und  $p_0^2$ . In den ersten beiden Fällen ist die bedingte Wahrscheinlichkeit für die Weitergabe einer  $o$  (Ereignis  $B$ )  $1/2$ , im letzten 1.

Jetzt haben wir alles beisammen, was in den Satz von Bayes einzusetzen ist, und erhalten

$$\mathbb{P}(A_a|B) = \frac{\frac{1}{2}2p_a p_0}{\frac{1}{2}2p_a p_0 + \frac{1}{2}2p_b p_0 + 1p_0^2} = .300$$

und analog

$$\mathbb{P}(A_b|B) = .067$$

und

$$\mathbb{P}(A_0|B) = .633.$$

Wir würden also am ehesten darauf wetten, dass ich Blutgruppe 0 habe. Inzwischen habe ich mich natürlich pieksen lassen (und für die Bestimmung geblecht), und es wäre schön zu berichten, dass unsere Analyse uns zur korrekten Vermutung geführt hat, aber solche Bilderbuchenden gibt es nicht immer — ich darf mich über Blutgruppe A freuen.

## 2.3 Zufallsvariable

Eine Zufallsvariable ist im wesentlichen eine zufälliger Zahlenwert (mit dem man rechnen kann). Formal heißt das, mit einer beliebigen Grundmenge  $\Omega$  und einem Wahrscheinlichkeitsmaß  $\mathbb{P}$  darauf:

### Definition 2.6

Eine Zufallsvariable  $X$  ist eine Abbildung von  $\Omega$  nach  $\mathbb{R}^d$ .

Bemerkungen:

1. Wenn  $\Omega$  überabzählbar ist, muss man von  $X$  eine zusätzliche Eigenschaft verlangen, die Messbarkeit (Anhang).
2. Meistens werden wir  $d = 1$  haben, also reellwertige Zufallsvariable. Im Fall  $d > 1$  haben wir  $X = (X_1, \dots, X_d)$ , also einen Vektor von reellen Zufallsvariablen. Zur Unterscheidung gegenüber dem Fall  $d = 1$  spricht man auch gerne von einem Zufallsvektor.

Ein zentraler Begriff ist die Verteilung einer Zufallsvariable:

### Definition 2.7

Die Verteilung einer Zufallsvariable ist das Wahrscheinlichkeitsmaß

$$\mathbb{P}_X(A) = \mathbb{P}(X^{-1}(A)) = \mathbb{P}(\{\omega : X(\omega) \in A\}) (A \subseteq \mathbb{R}^d).$$

### Definition 2.8

Wenn der Wertebereich von  $X$  endlich oder höchstens abzählbar ist, dann nennen wir  $X$  diskret.

In diesem Fall kann die Verteilung von  $X$  durch die Wahrscheinlichkeitsfunktion

$$p_X(x) = \mathbb{P}(X = x) = \mathbb{P}_X(\{x\})$$

angegeben werden.

Wir können etwa das Urnenbeispiel aus dem vorigen Abschnitt unter diesem Gesichtspunkt betrachten, indem wir eine Zufallsvariable  $X$  definieren, die die Anzahl der weißen Kugeln unter den 3 gezogenen ist. Wir haben schon die Wahrscheinlichkeiten

$$p_X(3) = \frac{1}{10}, p_X(2) = \frac{3}{5},$$

die wir nach der allgemeinen Formel (2.1) durch

$$p_X(1) = \frac{3}{10}, p_X(0) = 0$$

ergänzen können. Diese Wahrscheinlichkeitsfunktion ist in Abbildung 2.3 graphisch dargestellt.

Die allgemeine Form (2.1) ist die erste Verteilung, für die wir einen Namen haben:

### Definition 2.9

Die hypergeometrische Verteilung  $H(N, A, n)$  ( $n, A, N \in \mathbb{N}$ ,  $0 \leq n, A \leq N$ ) hat die Wahrscheinlichkeitsfunktion

$$p(x) = \frac{\binom{A}{x} \binom{N-A}{n-x}}{\binom{N}{n}}.$$

Diese Verteilung tritt auf, wenn aus einer Grundgesamtheit mit  $N$  Elementen, von denen  $A$  "günstig" sind,  $n$  ohne Zurücklegen gezogen werden, und  $X$  die Anzahl der "günstigen" Elemente unter den gezogenen ist.

Wird mit Zurücklegen gezogen, dann sind die einzelnen Ziehungen unabhängig voneinander mit Wahrscheinlichkeit  $p = A/N$  "günstig" ("Erfolge"); wir können etwas allgemeiner den Fall betrachten, dass  $n$  unabhängige Versuche gemacht werden, die jeweils mit Wahrscheinlichkeit  $p$  (die nicht rational sein muss) einen Erfolg ergeben, und  $X$  die Anzahl der Erfolge in diesen  $n$  Versuchen ist. Das führt zu

### Definition 2.10

Die Binomialverteilung  $B(n, p)$ :

$$p(x) = \binom{n}{x} p^x (1-p)^{n-x}.$$

Einen besonders einfachen Fall erhalten wir, wenn wir in der Binomialverteilung (oder in der hypergeometrischen Verteilung)  $n = 1$  setzen:

### Definition 2.11

$X$  heißt alternativverteilt ( $X \sim A(p)$ ) wenn

$$\mathbb{P}(X = 1) = p, \mathbb{P}(X = 0) = 1 - p.$$

Eine alternativverteilte Zufallsvariable lässt sich als *Indikatorvariable* darstellen:

### Definition 2.12

Für ein Ereignis  $A$  heißt die Funktion

$$I_A : \Omega \rightarrow \{0, 1\}$$

mit

$$I_A(\omega) = \begin{cases} 1 & \text{wenn } \omega \in A, \\ 0 & \text{wenn } \omega \notin A \end{cases}$$

Indikator von  $A$ .

Für allgemeinere Fälle (nicht diskrete Zufallsvariable) ist die Wahrscheinlichkeitsfunktion nicht brauchbar. Immer funktioniert die Verteilungsfunktion:

**Definition 2.13**

Die Verteilungsfunktion von  $X$  ist gegeben durch

$$F_X(x) = \mathbb{P}_X((-\infty, x]) = \mathbb{P}(X \leq x)$$

(wenn  $X$   $d$ -dimensional ist, ist auch  $x$   $d$ -dimensional, und die Ungleichung ist komponentenweise zu verstehen, also  $X \leq x$  wenn  $X_i \leq x_i$  für alle  $i = 1, \dots, d$  und  $(-\infty, x] = (-\infty, x_1] \times \dots \times (-\infty, x_d]$ ). Damit ist

$$F_X(x) = F_{(X_1, \dots, X_d)}(x_1, \dots, x_d) = \mathbb{P}(X_1 \leq x_1, \dots, X_d \leq x_d).$$

Für  $d = 1$  kann man die Verteilungsfunktionen einfach charakterisieren:

**Satz 2.6**

$F : \mathbb{R} \rightarrow \mathbb{R}$  ist genau dann eine Verteilungsfunktion, wenn

1.  $0 \leq F(x) \leq 1$  für alle  $x$ ,
2.  $F$  ist monoton nichtfallend,
3.  $F$  ist rechtsstetig,
4.  $\lim_{x \rightarrow -\infty} F(x) = 0$ ,
5.  $\lim_{x \rightarrow \infty} F(x) = 1$ .

Zur Veranschaulichung ist in Abbildung 2.3 neben der Wahrscheinlichkeitsfunktion die Verteilungsfunktion der hypergeometrischen Verteilung graphisch dargestellt. Sie zeigt die typische Form der Verteilungsfunktion einer diskreten Zufallsvariable: die Funktion hat im Punkt  $x$  einen Sprung der Höhe  $p(x)$  und ist zwischen den Sprungstellen konstant.

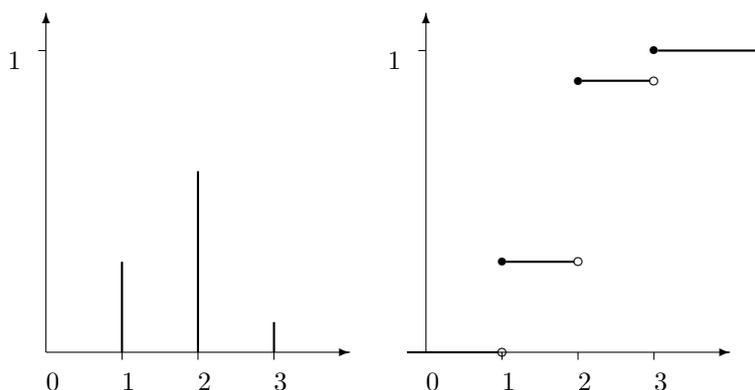


Abbildung 2.3: Wahrscheinlichkeits- und Verteilungsfunktion der hypergeometrischen Verteilung  $H_{5,3,3}$

Mithilfe der Verteilungsfunktion kann man Wahrscheinlichkeiten berechnen:

$$\mathbb{P}(X \leq a) = F_X(a),$$

$$\begin{aligned} \mathbb{P}(X < a) &= F_X(a - 0), \\ \mathbb{P}(a < X \leq b) &= F_X(b) - F_X(a), \\ \mathbb{P}(a < X < b) &= F_X(b - 0) - F_X(a), \\ \mathbb{P}(a \leq X \leq b) &= F_X(b) - F_X(a - 0), \\ \mathbb{P}(a \leq X < b) &= F_X(b - 0) - F_X(a - 0), \\ \mathbb{P}(X = a) &= F_X(a) - F_X(a - 0). \end{aligned}$$

Dabei ist  $F(x - 0) = \lim_{h \downarrow 0} F(x - h)$  der linksseitige Grenzwert von  $F$  in  $x$ .

Mehrdimensionale Verteilungsfunktionen haben zusätzliche Eigenschaften, wir betrachten hier nur den Fall  $d = 2$ :

**Satz 2.7**

$F : \mathbb{R}^2 \rightarrow \mathbb{R}$  ist genau dann eine Verteilungsfunktion, wenn

1.  $0 \leq F(x_1, x_2) \leq 1$  für alle  $x_1, x_2$ ,
2.  $F$  ist monoton nichtfallend in jeder Argumentvariable,
3.  $F$  ist rechtsstetig,
4.  $\lim_{x_1 \rightarrow -\infty} F(x_1, x_2) = \lim_{x_2 \rightarrow -\infty} F(x_1, x_2) = 0$ ,
5.  $\lim_{x_1, x_2 \rightarrow \infty} F(x_1, x_2) = 1$ ,
6. Für  $a_1 < b_1, a_2 < b_2$  gilt

$$F(b_1, b_2) - F(a_1, b_2) - F(b_1, a_2) + F(a_1, a_2) \geq 0.$$

Diese Eigenschaften sind analog zu denen von eindimensionalen Verteilungsfunktionen, nur die letzte ist neu. Der Ausdruck der dort steht, ist genau die Wahrscheinlichkeit

$$\mathbb{P}(a_1 < X_1 \leq b_1, a_2 < X_2 \leq b_2).$$

Im diskreten Fall (und für  $d = 1$ ) hat  $F_X$  Sprünge der Höhe  $p_X(x)$  an den Punkten  $x$ , die mit positiver Wahrscheinlichkeit angenommen werden, und ist dazwischen konstant. Wenn  $F$  (stückweise stetig) differenzierbar ist, dann können wir  $F$  durch die Ableitung festlegen:

**Definition 2.14**

Wenn  $F_X$  in der Form

$$F_X(x) = \int_{-\infty}^x f_X(u) du$$

bzw.

$$F_X(x) = \int_{-\infty}^{x_d} \dots \int_{-\infty}^{x_1} f_X(u_1, \dots, u_d) du_1 \dots du_d$$

(falls  $X = (X_1, \dots, X_d)$  mehrdimensional ist) darstellbar ist, dann heißt  $f_X$  die Dichte der Verteilung von  $X$ , und wir nennen  $X$  stetig (verteilt).

Wahrscheinlichkeits- und Dichtefunktionen sind leicht zu charakterisieren:

**Satz 2.8**

1. Die Funktion  $p$  ist genau dann eine Wahrscheinlichkeitsfunktion, wenn

$$p(x) \geq 0 \text{ für alle } x \in \mathbb{R}^d \text{ und } \sum_x p(x) = 1.$$

2. Die Funktion  $f$  ist genau dann eine Dichtefunktion, wenn

$$f(x) \geq 0 \text{ für alle } x \in \mathbb{R}^d \text{ und } \int f(x)dx = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f(x_1, \dots, x_d) dx_1 \dots dx_d = 1.$$

Beispiele für stetige Verteilungen:

- Die stetige Gleichverteilung  $U(a, b)$ :

$$f(x) = \begin{cases} \frac{1}{b-a} & \text{wenn } a \leq x \leq b, \\ 0 & \text{sonst.} \end{cases}$$

Diese Verteilung (mit  $a = 0, b = 1$ ) ist uns schon als Beispiel für einen Wahrscheinlichkeitsraum mit unendlich vielen Elementen begegnet. Ihre Dichte und Verteilungsfunktion sind in Abbildung 2.3 dargestellt.

- Die Exponentialverteilung  $Ex(\lambda)$ :

$$f(x) = \lambda e^{-\lambda x} [x \geq 0].$$

- Die Normalverteilung (eine der wichtigsten Verteilungen)  $N(\mu, \sigma^2)$ :

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right).$$

Der Spezialfall  $N(0, 1)$  (also  $\mu = 0, \sigma^2 = 1$ ) wird als Standardnormalverteilung bezeichnet, für ihre Dichte bzw. Verteilungsfunktion haben sich die Bezeichnungen  $\varphi$  und  $\Phi$  eingebürgert, also

$$\phi(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}, \Phi(x) = \int_{-\infty}^x \phi(u) du.$$

Die Dichte der Normalverteilung kann nicht geschlossen integriert werden. Für die Berechnung der Verteilungsfunktion werden Näherungsformeln bzw. Tabellen herangezogen. Eine Tabelle für die Verteilungsfunktion  $\Phi(x)$  der Standardnormalverteilung finden Sie (neben anderen) in Anhang A.

Durch Integrieren der Dichte erhält man für eine Zufallsvariable mit einer Normalverteilung  $N(\mu, \sigma^2)$  die Verteilungsfunktion

$$F_X(x) = \Phi\left(\frac{x-\mu}{\sigma}\right).$$

Wir berechnen als Beispiel die Wahrscheinlichkeit, dass eine Zufallsvariable  $X$  mit Verteilung  $N(4, 25)$  Werte zwischen 2 und 7 annimmt:

$$\mathbb{P}(2 \leq x \leq 7) = \Phi\left(\frac{7-4}{5}\right) - \Phi\left(\frac{2-4}{5}\right) = \Phi(0.6) - \Phi(-0.4) = 0.726 - (1 - 0.655) = 0.381.$$

Es kann sein, dass eine Zufallsvariable sowohl diskrete als auch stetige Anteile hat:

### Definition 2.15

Wenn  $F_X$  sowohl Sprünge als auch eine nichtverschwindende Ableitung hat, dann nennen wir  $X$  gemischt verteilt. In diesem Fall gibt es sowohl eine Wahrscheinlichkeitsfunktion als auch eine Dichte.

*Anmerkung:* Die Wahrscheinlichkeitsfunktion und Dichte einer gemischten Verteilung sind unvollständig; die Summe bzw. das Integral dieser Funktionen sind jeweils kleiner als 1, ihre Summe muss natürlich 1 ergeben. Manchmal werden diese unvollständigen Funktionen als modifizierte Dichte bzw. Wahrscheinlichkeitsfunktion bezeichnet.

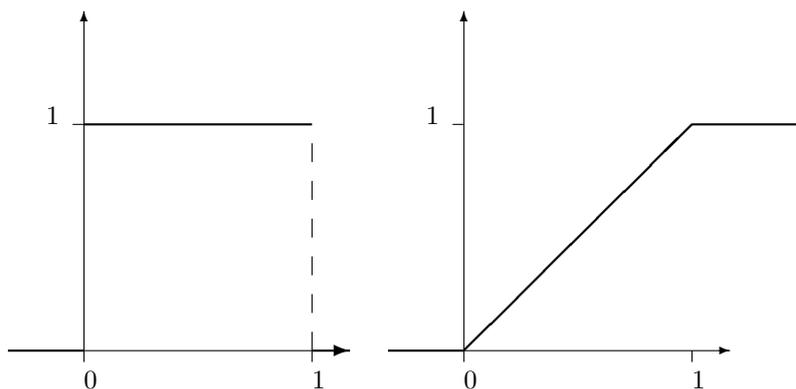


Abbildung 2.4: Dichte- und Verteilungsfunktion der stetigen Gleichverteilung  $U(0, 1)$

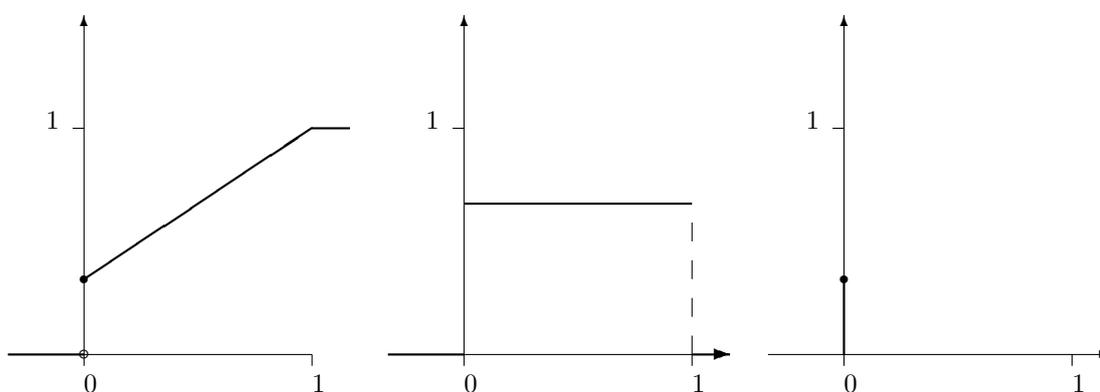


Abbildung 2.5: Verteilungs-, Dichte- und Wahrscheinlichkeitsfunktion einer gemischten Verteilung

Ein typisches Beispiel für eine gemischte Verteilung ist die Wartezeit bei einer Ampel (bei der wir zufällig eintreffen): mit positiver Wahrscheinlichkeit ist die Ampel grün und die Wartezeit 0; wenn gewartet werden muss, ist die Wartezeit stetig gleichverteilt (Abb. 2.5).

Mithilfe der Wahrscheinlichkeits- bzw. Dichtefunktion kann die Wahrscheinlichkeit, dass eine Zufallsvariable  $X$  Werte in der Menge  $A$  annimmt, als Summe bzw. Integral dargestellt werden:

Für diskretes  $X$ :

$$\mathbb{P}(X \in A) = \sum_{x \in A} p_X(x),$$

für stetiges  $X$ :

$$\mathbb{P}(X \in A) = \int_A f_X(x) dx,$$

bzw. im mehrdimensionalen Fall

$$\mathbb{P}(X \in A) = \int_A f_X(x_1, \dots, x_d) dx_1 \dots dx_d,$$

und für gemischte Verteilungen

$$\mathbb{P}(X \in A) = \sum_{x \in A} p_X(x) + \int_A f_X(x) dx.$$

Wenn  $X$  und  $Y$  eine gemeinsame Verteilung mit der Dichte  $f_{X,Y}(x, y)$  haben, dann können wir die Verteilungsfunktion von  $X$  wie folgt berechnen:

$$F_X(x) = \mathbb{P}(X \leq x, -\infty < Y < \infty) = \int_{-\infty}^x \int_{-\infty}^{\infty} f_{X,Y}(x, y) dy dx,$$

und durch Differenzieren ergibt sich die Dichte von  $X$  (und analog für  $Y$ ) als

$$f_X(x) = \int_{-\infty}^{\infty} f_{X,Y}(x,y)dy, f_Y(y) = \int_{-\infty}^{\infty} f_{X,Y}(x,y)dx.$$

Für diskrete Verteilungen gilt

$$p_X(x) = \sum_y p_{X,Y}(x,y), p_Y(y) = \sum_x p_{X,Y}(x,y).$$

Wenn die Verteilung von  $X$  (oder  $Y$ ) in dieser Weise aus der gemeinsamen Verteilung erhalten wird, nennt man sie auch die Randverteilung (im stetigen Fall heißt die Dichte dieser Verteilung Randdichte). Diese Bezeichnung kommt daher, dass man für diskrete Variable die gemeinsame Verteilung in Form einer Tabelle aufschreiben kann, die man durch eine zusätzliche Zeile und Spalte für die Summen ergänzt.

Als Beispiel würfeln wir dreimal,  $X$  soll die Anzahl der Einsen sein,  $Y$  die Anzahl der Sechsen (Abb.2.6).

	Y				
X	0	1	2	3	$p_X$
0	$\frac{64}{216}$	$\frac{48}{216}$	$\frac{12}{216}$	$\frac{1}{216}$	$\frac{125}{216}$
1	$\frac{48}{216}$	$\frac{24}{216}$	$\frac{3}{216}$	0	$\frac{75}{216}$
2	$\frac{12}{216}$	$\frac{3}{216}$	0	0	$\frac{15}{216}$
3	$\frac{1}{216}$	0	0	0	$\frac{1}{216}$
$p_Y$	$\frac{125}{216}$	$\frac{75}{216}$	$\frac{15}{216}$	$\frac{1}{216}$	1

Abbildung 2.6: Eine mehrdimensionale diskrete Verteilung, rechts und unten die beiden Randverteilungen

Diese Verteilung ist ein Spezialfall der einzigen mehrdimensionalen diskreten Verteilung, für die wir einen Namen haben:

**Definition 2.16: Multinomialverteilung**

Die Multinomialverteilung  $M(n, p_1, \dots, p_k)$  ( $k \geq 2, p_i \geq 0, \sum_{i=1}^k p_i = 1$ ) ist die  $k$ -dimensionale Verteilung mit der Wahrscheinlichkeitsfunktion

$$p_{(X_1, \dots, X_k)}(x_1, \dots, x_k) = \mathbb{P}(X_1 = x_1, \dots, X_k = x_k) = \begin{cases} \frac{n!}{x_1!x_2!\dots x_k!} p_1^{x_1} \dots p_k^{x_k} & \text{wenn } x_i \geq 0, \sum_{i=1}^k x_i = n, \\ 0 & \text{sonst.} \end{cases}$$

Diese Verteilung tritt auf, wenn  $n$  unabhängige Versuche angestellt werden, die jeweils mit Wahrscheinlichkeit  $p_i$  den Ausgang  $i$  ( $i = 1, \dots, k$ ) liefern, und  $X_i$  die Anzahl der Ausgänge  $i$  in diesen  $n$  Versuchen ist. Die eindimensionalen Randverteilungen dieser Verteilung sind natürlich Binomialverteilungen.

Ein wichtiger Begriff ist die Unabhängigkeit von Zufallsvariablen:

**Definition 2.17**

Die Zufallsvariablen  $(X_1, \dots, X_n)$  heißen unabhängig, wenn für alle  $x_1, \dots, x_n$

$$F_{X_1, \dots, X_n}(x_1, \dots, x_n) = \prod_{i=1}^n F_{X_i}(x_i).$$

Die unendliche Folge  $(X_n, n \in \mathbb{N})$  heißt unabhängig, wenn jede endliche Teilfolge unabhängig ist.

Wenn die gemeinsame Verteilung diskret bzw. stetig ist, kann man in dieser Definition die Verteilungsfunktion durch die Wahrscheinlichkeits- bzw. Dichtefunktion ersetzen.

Wenn wir von Unabhängigkeit sprechen, können wir auch über bedingte Wahrscheinlichkeiten nachdenken, die wir in diesem Fall als “bedingte Verteilung” bezeichnen. Im diskreten Fall kann man etwa die bedingte Wahrscheinlichkeit

$$\mathbb{P}(X \leq a | Y = y)$$

nach der üblichen Formel berechnen. Für stetige Verteilungen macht dieser Ausdruck vordergründig keinen Sinn, weil das bedingende Ereignis Wahrscheinlichkeit 0 hat. Wir können aber versuchen, diese Wahrscheinlichkeit als Grenzwert von

$$\mathbb{P}(X \leq a | y - \epsilon \leq Y \leq y + \epsilon)$$

für  $\epsilon \rightarrow 0$  zu berechnen. Das funktioniert auch, und führt uns zu

### Definition 2.18

$X, Y$  seien stetig verteilt mit Dichte  $f_{X,Y}$ . Die bedingte Dichte von  $X$  unter  $Y = y$  ist

$$f_X(x|Y = y) = \frac{f_{X,Y}(x, y)}{f_Y(y)}.$$

Damit erhalten wir die bedingte Wahrscheinlichkeit als

$$\mathbb{P}(X \leq a | Y = y) = \int_{-\infty}^a f_X(x|Y = y) dx.$$

Ein Beispiel:

### Beispiel 2.6: Zweidimensionale Dichte

$X$  und  $Y$  haben eine gemeinsame Verteilung mit der Dichte

$$cxy[0 \leq x \leq y \leq 1].$$

Wir wollen  $c$ , die beiden Randdichten und die Wahrscheinlichkeiten

$$\mathbb{P}(X + Y < 1)$$

und

$$\mathbb{P}(0.2 < X < 0.4 | Y = 0.6)$$

bestimmen.

Für die Bestimmung von  $c$  verwenden wir, dass das Integral der Dichte 1 sein muss:

$$1 = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) dx dy = \int_0^1 \int_0^y cxy dx dy = \int_0^1 \frac{cy^3}{2} dy = \frac{1}{8},$$

also  $c = 1$ .

Randdichte von  $Y$ :

$$f_Y(y) = \int_{-\infty}^{\infty} f(x, y) dx = \int_0^y 8cxy dx = 4y^3$$

(das haben wir eigentlich schon in der Zeile darüber als inneres Integral berechnet).

Randdichte von  $X$ :

$$f_X(x) = \int_{-\infty}^{\infty} f(x, y) dy = \int_x^1 8cxy dy = 4x(1 - x^2).$$

Die Wahrscheinlichkeit von  $[X + Y < 1]$  ergibt sich als

$$\mathbb{P}(X + Y < 1) = \int \int_{[x+y < 1]} f(x, y) dx dy = \int_{-\infty}^{\infty} \int_{-\infty}^{1-y} f(x, y) dx dy.$$

$f(x, y)$  ist nur für  $0 \leq x \leq y \leq 1$  von 0 verschieden. Also

$$\begin{aligned} \mathbb{P}(X + Y < 1) &= \int_0^1 \int_0^{\min(y, 1-y)} 8xy dx dy = \int_0^{1/2} \int_0^y 8xy dx dy + \int_{1/2}^1 \int_0^{1-y} 8xy dx dy = \\ &= \frac{1}{16} + \frac{5}{48} = \frac{1}{6}. \end{aligned}$$

Die bedingte Dichte macht nur für  $0 < y \leq 1$  Sinn und ist dort

$$f_X(x|Y = y) = \frac{f(x, y)}{f_Y(y)} = \frac{8xy[0 \leq x \leq y]}{4y^3} = \frac{2x[0 \leq x \leq y]}{y^2}.$$

Damit ist

$$\mathbb{P}(0.2 \leq X \leq 0.4|Y = 0.6) = \int_{0.2}^{0.4} f_X(x|Y = 0.6) dx = \int_{0.2}^{0.4} \frac{2x}{0.36} dx = \frac{1}{3}.$$

## 2.4 Transformationen

Wir betrachten jetzt den Fall, dass die Verteilung einer Zufallsvariable  $X$  bekannt ist und wir die Verteilung der transformierten Zufallsvariable

$$Y = g(X)$$

bestimmen wollen, wobei  $g$  irgendeine Funktion (im einfachsten Fall  $g: \mathbb{R} \rightarrow \mathbb{R}$  ist. Falls  $X$  diskret ist, dann hat auch  $Y$  eine diskrete Verteilung. In diesem Fall gilt klarerweise

### Satz 2.9

Wenn  $X$  eine diskrete Verteilung mit Wahrscheinlichkeitsfunktion  $p_X$  hat und  $Y = g(X)$  gilt, dann ist

$$p_Y(y) = \mathbb{P}(Y = y) = \mathbb{P}(g(X) = y) = \sum_{x:g(x)=y} p_X(x).$$

Wenn  $X$  stetig verteilt ist, dann kann  $Y = g(X)$  immer noch diskret verteilt sein (wenn  $g$  nur endlich viele Werte annimmt, etwa falls  $g$  die Vorzeichenfunktion ist). Wir sind allerdings besonders an dem Fall interessiert, dass  $Y$  ebenfalls eine stetige Verteilung besitzt. In einfachen Fällen können wir diese Verteilung direkt erhalten:

### Beispiel 2.7: Quadrat einer Normalverteilung

Wir nehmen an, dass  $X$  eine Standardnormalverteilung hat, und wollen die Verteilung von  $Y = X^2$  bestimmen. Wir beginnen mit der Verteilungsfunktion von  $Y$ . Für  $y \geq 0$  gilt

$$F_Y(y) = \mathbb{P}(Y \leq y) = \mathbb{P}(X^2 \leq y) = \mathbb{P}(-\sqrt{y} \leq X \leq \sqrt{y}) = \Phi(\sqrt{y}) - \Phi(-\sqrt{y}) = 2\Phi(\sqrt{y}) - 1.$$

Klarerweise ist  $F_Y(y) = 0$  für  $y < 0$ .

Durch Ableiten der Verteilungsfunktion erhalten wir die Dichte

$$f_Y(y) = \begin{cases} \frac{1}{\sqrt{2\pi y}} e^{-y/2} & \text{für } y > 0. \\ 0 & \text{sonst.} \end{cases}$$

Diese Verteilung ist ein Spezialfall der Gammaverteilung  $\Gamma(\alpha, \lambda)$  mit der Dichte

$$f(x) = \frac{x^{\alpha-1} \lambda^\alpha}{\Gamma(\alpha)} e^{-\lambda x} [x > 0],$$

wobei  $\Gamma$  die Gammafunktion

$$\Gamma(\alpha) = \int_0^\infty x^{\alpha-1} e^{-x} dx$$

ist. Diese erfüllt die Gleichung

$$\Gamma(\alpha + 1) = \alpha \Gamma(\alpha)$$

und insbesondere

$$\Gamma(n) = (n - 1)! (n \in \mathbb{N}).$$

Die Verteilung von  $Y$  ist eine Gammaverteilung mit  $\alpha = \lambda = 1/2$ .

In diesem Fall konnten wir unser Wissen über die spezielle Funktion  $g(x) = x^2$  ausnützen. Für allgemeine Funktionen  $g$  kann die Bestimmung der Verteilung von  $Y = g(X)$  kompliziert sein, weil die Menge aller  $x$  mit  $g(x) \leq y$  bestimmt werden muss. Dies ist relativ einfach, wenn wir annehmen, dass  $g$  stetig differenzierbar und eindeutig umkehrbar, also streng monoton ist. Dann gibt es die beiden Möglichkeiten, dass  $g$  entweder steigend oder fallend sein kann. Wir führen die Rechnung für den etwas komplizierteren zweiten Fall durch.

Das Bild der reellen Zahlen unter  $g$  ist

$$g(\mathbb{R}) = \{g(x) : x \in \mathbb{R}\} = (a, b)$$

mit

$$a = \lim_{x \rightarrow \infty} g(x)$$

und

$$b = \lim_{x \rightarrow -\infty} g(x).$$

Für  $a < y < b$  gilt

$$F_Y(y) = \mathbb{P}(g(X) \leq y) = \mathbb{P}(X \geq g^{-1}(y)) = 1 - F_X(g^{-1}(y)).$$

Ableiten gibt die Dichte:

$$f_Y(y) = \begin{cases} -(g^{-1})'(y) f_X(g^{-1}(y)) = |(g^{-1})'(y)| f_X(g^{-1}(y)) = \frac{f_X(g^{-1}(y))}{|g'(g^{-1}(y))|} & \text{wenn } x \in g(\mathbb{R}) \\ 0 & \text{sonst.} \end{cases}$$

Falls  $g$  steigend ist, dann ergibt sich dieselbe Darstellung.

Dieses Ergebnis gilt auch in mehreren Dimensionen:

**Satz 2.10: Transformationssatz für Dichten**

$X = (X_1, \dots, X_n)$  sei stetig verteilt mit der Dichte  $f_X$ .  $g : \mathbb{R}^n \rightarrow \mathbb{R}^n$  sei stetig differenzierbar und eindeutig umkehrbar.  $Y = g(X)$  (d.h.  $Y_i = g_i(X_1, \dots, X_n)$ ) ist dann ebenfalls stetig verteilt mit der Dichte

$$f_Y(y) = \begin{cases} f_X(g^{-1}(y)) \left| \frac{\partial g^{-1}}{\partial y} \right| = f_X(g^{-1}(y)) \frac{1}{\left| \frac{\partial g}{\partial x}(g^{-1}(y)) \right|} & \text{wenn } y \in g(\mathbb{R}^n), \\ 0 & \text{sonst.} \end{cases}$$

Dabei ist

$$\frac{\partial g}{\partial x} = \det\left(\left(\frac{\partial g_i}{\partial x_j}\right)_{n \times n}\right)$$

die Funktionaldeterminante.

Damit können wir die Verteilung einer Summe von zwei unabhängigen Zufallsvariablen  $X$  und  $Y$  bestimmen: mit dem Transformationssatz kann die gemeinsame Dichte von  $X$  und  $X+Y$  bestimmt werden, und die Verteilung von  $X+Y$  als Randverteilung davon:

Wir setzen also

$$g(x, y) = (g_1(x, y), g_2(x, y)) = (x, x + y).$$

Diese Transformation hat die Funktionaldeterminante

$$\begin{vmatrix} \frac{\partial g_1}{\partial x} & \frac{\partial g_1}{\partial y} \\ \frac{\partial g_2}{\partial x} & \frac{\partial g_2}{\partial y} \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1$$

und die Umkehrfunktion

$$g^{-1}(u, v) = (u, v - u).$$

Weil  $X$  und  $Y$  unabhängig sind, ergibt sich ihre gemeinsame Dichte als Produkt:

$$f_{X,Y}(x, y) = f_X(x)f_Y(y),$$

also ergibt sich die gemeinsame Dichte von  $U = X, Z = X + Y$  als

$$f_{Z,U}(z, u) = f_X(u)f_Y(z - u),$$

und durch Integrieren ergibt sich die Randdichte von  $Z$ :

#### Satz 2.11

$X$  und  $Y$  seien unabhängig mit Dichte  $f_X$  und  $f_Y$ . Dann ist die Dichte von  $X + Y$

$$f_{X+Y}(z) = f_X * f_Y(z) = \int_{-\infty}^{\infty} f_X(x)f_Y(z - x)dx.$$

#### Definition 2.19

$f$  und  $g$  seien zwei Dichten. Die Dichte  $f * g$  mit

$$f * g(z) = \int_{-\infty}^{\infty} f(x)g(z - x)dx.$$

heißt die Faltung von  $f$  und  $g$ .

Die Dichte der Summe von zwei stetigen Zufallsvariablen ist also die Faltung der Dichten der beiden Summanden.

Als Beispiel wollen wir die Faltung zweier Exponentialdichten mit Parameter  $\lambda$  ( $f(x) = \lambda e^{-\lambda x} [x \geq 0]$ ) bestimmen. Für  $z < 0$  ist  $f * f(z) = 0$ , für  $z \geq 0$  erhalten wir

$$f * f(z) = \int_{-\infty}^{\infty} f(z - x)f(x)dx = \int_0^z \lambda e^{-\lambda(z-x)} \lambda e^{-\lambda x} dx = \int_0^z \lambda^2 e^{-\lambda z} dx = z \lambda^2 e^{-\lambda z}.$$

Auch diese Verteilung ist eine Gammaverteilung (mit  $\alpha = 2$ ); auch die Exponentialverteilung ist ein Spezialfall der Gammaverteilung für  $\alpha = 1$ . In ähnlicher Weise ergibt sich die Dichte von  $X/Y$ : wir setzen  $u = y, z = x/y$ . Die Umkehrfunktion  $y = u, x = zu$  hat die Funktionaldeterminante  $-u$ , und wir erhalten

#### Satz 2.12

$X$  und  $Y$  seien unabhängig mit Dichte  $f_X$  und  $f_Y$ . Dann hat  $Z = X/Y$  die Dichte

$$f_Z(z) = \int_{-\infty}^{\infty} f_Y(y)f_X(zy)|y|dy.$$

Setzen wir wieder für  $X$  und  $Y$  Exponentialverteilungen ein, dann ergibt sich (für  $z \geq 0$ )

$$f_{X/Y}(z) = \int_0^\infty \lambda^2 y e^{-y(1+z)} dy = \frac{1}{(1+z)^2}.$$

Wir können auch die gemeinsame Verteilung von  $Q = X/Y$  und  $S = X + Y$  bestimmen. Die Umkehrfunktion zu

$$q = x/y, s = x + y$$

ist

$$x = \frac{qs}{1+q}, y = \frac{s}{1+q}.$$

Die Funktionaldeterminante dazu ist

$$\frac{\partial(x, y)}{\partial(q, s)} = \begin{vmatrix} \frac{s}{(1+q)^2} & \frac{q}{1+q} \\ -\frac{s}{(1+q)^2} & \frac{1}{1+q} \end{vmatrix} = \frac{s}{(1+q)^2}.$$

Insgesamt ist

$$f_{Q,S}(q, s) = \frac{\lambda^2 s e^{-\lambda s}}{(1+q)^2} [s \geq 0][q \geq 0].$$

$S$  und  $Q$  sind also unabhängig.

Es gilt allgemeiner: wenn  $X \sim \Gamma(\alpha, \lambda)$  und  $Y \sim \Gamma(\beta, \lambda)$  unabhängig sind, dann sind  $S = X + Y$  und  $Q = X/Y$  unabhängig,  $S \sim \Gamma(\alpha + \beta, \lambda)$ , und  $Q$  hat eine Beta-Verteilung 2. Art ( $B_2(\alpha, \beta)$ ) mit der Dichte

$$f_{\alpha, \beta}(x) = \frac{x^{\alpha-1}}{B(\alpha, \beta)(1+x)^{\alpha+\beta}} [x > 0].$$

Wird statt durch  $Y$  durch die Summe  $X + Y$  dividiert, dann ergibt sich für  $X/(X + Y)$  eine Beta-Verteilung 1. Art ( $B_1(\alpha, \beta)$ ) mit der Dichte

$$f_{\alpha, \beta}(x) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha, \beta)} [0 < x < 1].$$

In den letzten beiden Gleichungen ist  $B$  die Betafunktion

$$B(\alpha, \beta) = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha + \beta)}.$$

Eine ähnliche Formel wie die Faltung zweier Dichten gibt es auch für die Summe von zwei diskreten Zufallsvariablen:

**Satz 2.13**

$X$  und  $Y$  seien unabhängig mit Wahrscheinlichkeitsfunktion  $p_X$  und  $p_Y$ . Dann ist die Wahrscheinlichkeitsfunktion von  $X + Y$  die (diskrete) Faltung von  $p_X$  und  $p_Y$ :

$$p_{X+Y}(z) = p_X * p_Y(z) = \sum_x p_X(x)p_Y(z-x)dx.$$

Wir nehmen jetzt an, dass die Verteilungsfunktion  $F$  von  $X$  stetig und streng monoton ist (und daher umkehrbar), und betrachten

$$Y = F(X).$$

Die Verteilungsfunktion von  $Y$  berechnet sich als

$$\mathbb{P}(Y \leq y) = \mathbb{P}(F(X) \leq y) = \mathbb{P}(X \leq F^{-1}(y)) = F(F^{-1}(y)) = y,$$

$Y$  ist also gleichverteilt auf  $[0, 1]$ . Umgekehrt ist  $F^{-1}(Y)$  nach  $F$  verteilt, wenn  $Y$  auf  $[0, 1]$  gleichverteilt ist. Dieses Ergebnis gilt auch für allgemeine Verteilungen, allerdings muss man dazu die Inverse neu definieren: es kann ja einerseits die Gleichung

$$F(x) = y$$

gar keine Lösung  $x$  haben, und andererseits kann es mehrere Lösungen  $x$  geben. Der erste Fall tritt auf, wenn  $F$  unstetig ist, also Sprünge hat, und wenn  $y$  innerhalb eines Sprunges liegt. Mit anderen Worten, es gibt einen Punkt  $x$ , für den der linksseitige Grenzwert  $F(x - 0)$  kleiner als  $y$  ist und der Funktionswert  $F(x)$  größer als  $y$ . In diesem Fall ist dieses  $x$  die natürliche Wahl für  $F^{-1}(y)$ . Wenn es mehrere  $x$  mit  $F(x) = y$  gibt, dann bilden alle diese  $x$  ein Intervall. Ein möglicher Zugang besteht darin, alle diese  $x$  gleichberechtigt zu behandeln. Das führt zur Definition der *Quantile*.

**Definition 2.20: Quantil**

$x$  heißt  $p$ -Quantil ( $0 > p > 1$ ) der Verteilung mit der Verteilungsfunktion  $F$ , wenn

$$F(x - 0) \leq p \leq F(x)$$

(d.h., wenn  $X \sim F$ , dann ist  $\mathbb{P}(X < x) \leq p \leq \mathbb{P}(X \leq x)$ ).

Für das  $p$ -Quantil wird gerne die Notation  $x_p$  verwendet. Dass dieses nicht eindeutig bestimmt ist, stört oft nicht. Muss man die Definition eindeutig machen, gibt es im wesentlichen drei Möglichkeiten, das  $p$ -Quantil zu definieren: der Mittelpunkt des Intervalls, in dem  $F(x) = p$  gilt, oder einer der Endpunkte. Die erste Wahl hat etwas Salomonisches und wird gelegentlich in der beschreibenden Statistik verwendet. Mathematisch ergiebiger sind die Endpunkte, und zu unserer Definition der Verteilungsfunktion ( $F_X(x) = \mathbb{P}(X \leq x)$ , man könnte auch  $\mathbb{P}(X < x)$  verwenden) passt am besten der linke Endpunkt. Formal gibt das

**Definition 2.21**

Die verallgemeinerte Inverse der Verteilungsfunktion  $F$  ist gegeben durch

$$F^{-1}(y) = \inf\{x : F(x) \geq y\}.$$

**Satz 2.14**

Wenn  $U$  auf  $[0, 1]$  gleichverteilt ist, dann hat

$$X = F^{-1}(U)$$

die Verteilungsfunktion  $F$ .

Dieser Satz gibt uns die wichtigste Methode zur Erzeugung von Zufallszahlen mit beliebiger Verteilung, vorausgesetzt, dass wir einen Zufallsgenerator haben, der unabhängig gleichverteilte Zufallszahlen liefert. Wenn wir etwa exponentialverteilte Zufallszahlen erzeugen wollen, dann können wir die Verteilungsfunktion

$$F(x) = 1 - e^{-\lambda x}$$

invertieren

$$F^{-1}(y) = -\frac{1}{\lambda} \log(1 - y).$$

Wir haben also mit

$$X = -\frac{1}{\lambda} \log(1 - U)$$

die gesuchte exponentialverteilte Zufallszahl. Diese Formel lässt sich noch etwas vereinfachen, wenn man bedenkt, dass  $1 - U$  so wie  $U$  auf  $[0, 1]$  gleichverteilt ist, also funktioniert auch

$$X = -\frac{1}{\lambda} \log(U).$$

Die Subtraktion, die man sich dabei erspart, fällt zwar vom Aufwand her gegenüber dem Logarithmus und der Division nicht wirklich ins Gewicht, aber es gibt halt Prinzipien. . .

Etwas, das man bei der Anwendung der Inversenmethode beachten sollte, ist, dass zwar die theoretische Gleichverteilung einzelne Werte mit Wahrscheinlichkeit 0 annimmt, die (eigentlich

diskreten, aber mit sehr vielen möglichen Werten) Zufallszahlen aus dem Generator aber nicht, und es kann sein, dass die Werte 0 und/oder 1 tatsächlich auftreten, was bei der Inversion zu unliebsamen Reaktionen der Laufzeitbibliothek führen kann. Weil so etwas nur etwa ein Mal in  $10^9$  Versuchen auftritt ist das einer der Fehler, die oft erst beim ‘‘Gammatesten’’ erkannt werden.

## 2.5 Erwartungswert und Varianz

Auch hier wollen wir uns zur Motivation den frequentistischen Standpunkt zu eigen machen: stellen wir uns vor, dass wir 6000000 mal würfeln und den Mittelwert

$$\bar{X} = \frac{1}{6000000} \sum_{i=1}^{6000000} X_i$$

der Augenzahlen berechnen. In dieser ‘‘Stichprobe’’ wird jede Augenzahl etwa 1000000 mal vorkommen, also gilt

$$\bar{X} \approx \frac{1}{6000000} (1000000 \cdot 1 + \dots + 1000000 \cdot 6) = \frac{1}{6} \cdot 1 + \dots + \frac{1}{6} \cdot 6 = 3.5.$$

Die rechte Seite ist unschwer als die Summe aus den Produkten der einzelnen Werte mit ihren Wahrscheinlichkeiten zu erkennen. Als Frequentisten glauben wir natürlich daran, dass diese Gleichung für  $n \rightarrow \infty$  exakt wird. Wenn wir wieder zu Sinnen kommen, können wir das als Definition niederschreiben (und dezent verschweigen, wie wir dazu gekommen sind):

### Definition 2.22

Der Erwartungswert einer Zufallsvariable  $X$  ist

$$\mathbb{E}(X) = \sum_x x p_X(x)$$

für diskrete Zufallsvariable, und

$$\mathbb{E}(X) = \int_{-\infty}^{\infty} x f_X(x) dx$$

für stetige Zufallsvariable. Falls  $X$  gemischt verteilt ist, gilt

$$\mathbb{E}(X) = \sum_x x p_X(x) + \int_{-\infty}^{\infty} x f_X(x) dx.$$

Die Summen und Integrale in dieser Definition sind so zu verstehen, dass sie zuerst in die Teile  $x > 0$  und  $x < 0$  zerlegt werden; jeder Teil kann einen endlichen oder unendlichen Wert ergeben, und das Endergebnis ist die Summe dieser beiden; wenn beide Summanden unendlich sind, also eine unbestimmte Form  $\infty - \infty$  auftritt, dann ist das Ergebnis nicht definiert, und der Erwartungswert existiert nicht. In allen anderen Fällen hat der Erwartungswert einen bestimmten Wert, der auch  $+\infty$  oder  $-\infty$  sein kann.

### Beispiel 2.8

Wir berechnen als Beispiel den Erwartungswert der Binomialverteilung:

$$\begin{aligned} \mathbb{E}(X) &= \sum_{i=0}^n i \binom{n}{i} p^i (1-p)^{n-i} = \sum_{i=1}^n i \binom{n}{i} p^i (1-p)^{n-i} = \\ &= \sum_{i=1}^n n \binom{n-1}{i-1} p^i (1-p)^{n-i} \Big|_{i=j+1} = \sum_{j=0}^{n-1} n \binom{n-1}{j} p^{j+1} (1-p)^{n-1-j} = \end{aligned}$$

$$np \sum_{j=0}^{n-1} \binom{n-1}{j} p^j (1-p)^{n-1-j} = np.$$

**Beispiel 2.9**

Die stetige Gleichverteilung  $U(a, b)$  hat Erwartungswert

$$\int_a^b \frac{x}{b-a} dx = \frac{a+b}{2}.$$

**Beispiel 2.10**

Für die Cauchyverteilung mit der Dichte

$$f(x) = \frac{1}{\pi(1+x^2)}$$

existiert der Erwartungswert nicht, weil

$$\int_0^{\infty} x f(x) dx = \infty$$

und

$$\int_{-\infty}^0 x f(x) dx = -\infty$$

gilt.

**Satz 2.15: Eigenschaften des Erwartungswerts**

1. Linearität:  $\mathbb{E}(aX + b) = a\mathbb{E}(X) + b$ ,
2. Additivität:  $\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y)$ ,
3. Monotonie: wenn  $X \leq Y$ , dann ist auch  $\mathbb{E}(X) \leq \mathbb{E}(Y)$ ,
4. wenn  $X$  und  $Y$  unabhängig sind, dann gilt  $\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$ .

Die Beweise für diese Behauptungen werden sehr viel einfacher, wenn wir zuerst die folgende Aussage für den Erwartungswert einer Funktion von  $X$ :

**Satz 2.16: Satz vom unachtsamen Statistiker**

$X$  sei eine Zufallsvariable,  $g: \mathbb{R} \rightarrow \mathbb{R}$  eine Funktion und  $Y = g(X)$ . Dann ist

1. Wenn  $X$  diskret verteilt ist mit Wahrscheinlichkeitsfunktion  $p_X$ ,

$$\mathbb{E}(Y) = \sum_x g(x) p_X(x).$$

2. Wenn  $X$  stetig verteilt ist mit Dichte  $f_X$ ,

$$\mathbb{E}(Y) = \int g(x) f_X(x) dx.$$

Diese Formel gilt sinngemäß auch für mehrdimensionales  $X \in \mathbb{R}^k$  und  $g : \mathbb{R}^k \rightarrow \mathbb{R}$ :

$$\mathbb{E}(Y) = \int g(x) f_X(x) dx = \int \dots \int g(x_1, \dots, x_k) f_{X_1, \dots, X_k}(x_1, \dots, x_k) dx_1 \dots dx_k.$$

3. Wenn  $X$  gemischt verteilt ist mit Wahrscheinlichkeitsfunktion  $p_X$  und Dichte  $f_X$ ,

$$\mathbb{E}(Y) = \sum_x g(x) p_X(x) + \int g(x) f_X(x) dx.$$

Wir müssen also nicht erst die Verteilung von  $Y$  bestimmen, um den Erwartungswert zu berechnen, sondern können in der Formel für  $\mathbb{E}(X)$  einfach  $x$  durch  $g(x)$  ersetzen.

Wir beweisen diesen Satz für den Fall, dass  $X$  diskret ist. Offensichtlich gilt

$$p_Y(y) = \mathbb{P}(Y = y) = \sum_{x: f(x)=y} p_X(x),$$

damit ist

$$\mathbb{E}(Y) = \sum_y y p_Y(y) = \sum_y \sum_{x: f(x)=y} y p_X(x) = \sum_y \sum_{x: f(x)=y} f(x) p_X(x) = \sum_x f(x) p_X(x).$$

Dieser Satz ist hilfreich beim Beweis der Eigenschaften des Erwartungswerts. Die Additivität ergibt sich etwa so (wieder für diskrete Verteilungen):

$$\begin{aligned} \mathbb{E}(X + Y) &= \sum_{x,y} (x + y) p_{X,Y}(x, y) = \sum_x x \sum_y p_{X,Y}(x, y) + \sum_y y \sum_x p_{X,Y}(x, y) = \\ &= \sum_x x p_X(x) + \sum_y y p_Y(y) = \mathbb{E}(X) + \mathbb{E}(Y). \end{aligned}$$

### Definition 2.23

Die Varianz von  $X$  ist

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

### Satz 2.17: Steinerscher Verschiebungssatz

Für beliebiges reelles  $x$  gilt

$$\mathbb{E}((X - a)^2) = \mathbb{V}(X) + (\mathbb{E}(X) - a)^2.$$

### Satz 2.18: Eigenschaften der Varianz

1.  $\mathbb{V}(X) \geq 0$ ,
2.  $\mathbb{V}(X) = 0$  genau dann, wenn  $\mathbb{P}(X = \mathbb{E}(X)) = 1$ ,
3.  $\mathbb{V}(aX + b) = a^2 \mathbb{V}(X)$ ,
4. wenn  $X$  und  $Y$  unabhängig sind, dann ist  $\mathbb{V}(X + Y) = \mathbb{V}(X) + \mathbb{V}(Y)$ .

### Definition 2.24

$X$  und  $Y$  seien Zufallsvariable mit endlicher Varianz. Dann heißt

$$\mathbf{Cov}(X, Y) = \mathbb{E}((X - \mathbb{E}(X))(Y - \mathbb{E}(Y))) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)$$

die Kovarianz von  $X$  und  $Y$ .

Damit erhalten wir

$$\mathbb{V}(X + Y) = \mathbb{V}(X) + \mathbb{V}(Y) + 2\mathbf{Cov}(X, Y).$$

Wenn die Kovarianz von zwei Zufallsvariablen gleich 0 ist, dann nennen wir sie unkorreliert. Aus der Unabhängigkeit folgt die Unkorreliertheit, die umgekehrte Aussage gilt nicht, wie das Beispiel  $X \sim N(0, 1), Y = X^2$  zeigt.

### Beispiel 2.11

Wir berechnen die Varianz der Binomialverteilung  $B(n, p)$ . Wir wissen bereits, dass

$$\mathbb{E}(X) = np.$$

Wir berechnen also

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

$$np \sum_{k=1}^n k \binom{n-1}{k-1} p^{k-1} (1-p)^{n-k} = np \sum_{l=0}^{n-1} (l+1) \binom{n-1}{l} p^l (1-p)^{n-1-l} = np((n-1)p+1) = n(n-1)p^2 + np.$$

Damit ergibt sich

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

### Satz 2.19: Ungleichung von Markov

$X$  sei eine nichtnegative Zufallsvariable,  $\lambda > 0$ . Dann ist

$$\mathbb{P}(X \geq \lambda) \leq \frac{1}{\lambda} \mathbb{E}(X).$$

Zum Beweis definieren wir die Zufallsvariable

$$Y = \begin{cases} \lambda & \text{wenn } X \geq \lambda, \\ 0 & \text{sonst.} \end{cases}$$

Es gilt  $Y \leq X$  und daher

$$\mathbb{E}(X) \geq \mathbb{E}(Y) = \lambda \mathbb{P}(Y = \lambda) = \lambda \mathbb{P}(X \geq \lambda).$$

### Satz 2.20: Ungleichung von Chebychev

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \lambda) \leq \frac{\mathbb{V}(X)}{\lambda^2}.$$

Wir wenden die Ungleichung von Markov auf die Zufallsvariable

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

an:

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \lambda) = \mathbb{P}(Y \geq \lambda^2) \leq \frac{\mathbb{E}(Y)}{\lambda^2} = \frac{\mathbb{V}(X)}{\lambda^2}.$$

**Satz 2.21: Ungleichung von Kolmogorov**

$X_1, \dots, X_n$  seien unabhängig mit Erwartungswert 0,  $S_0 = 0$ ,  $S_n = X_1 + \dots + X_n$ . Dann ist

$$\mathbb{P}(\max_{k \leq n} |S_k| \geq \lambda) \leq \frac{\mathbb{V}(S_n)}{\lambda^2}.$$

Für  $i = 1, \dots, n$  setzen wir

$$Y_i = \begin{cases} 1 & \text{wenn } |S_i| \geq \lambda \text{ und } |S_j| < \lambda \text{ für } j < i, \\ 0 & \text{sonst,} \end{cases}$$

und

$$Y = \sum_{i=1}^n Y_i.$$

$Y$  ist genau dann 1, wenn  $\max_{0 \leq k \leq n} |S_k| \geq \lambda$ , und sonst 0.

Weil  $\mathbb{E}(S_n) = 0$  ist, gilt

$$\mathbb{V}(S_n) = \mathbb{E}(S_n^2) \geq \mathbb{E}(Y S_n^2) = \sum_{i=1}^n \mathbb{E}(Y_i S_n^2).$$

Für die Summanden ergibt sich

$$\mathbb{E}(Y_i S_n^2) = \mathbb{E}(Y_i (S_i + (S_n - S_i))^2) = \mathbb{E}(Y_i S_i^2) + 2\mathbb{E}(Y_i S_i (S_n - S_i)) + \mathbb{E}(Y_i (S_n - S_i)^2).$$

Im ersten Summanden ist  $Y_i S_i^2 \geq Y_i \lambda^2$ , im zweiten sind  $Y_i S_i$  und  $S_n - S_i$  unabhängig, und daher ist der Erwartungswert 0, und der letzte Summand kann einfach mit 0 nach unten abgeschätzt werden. Das ergibt

$$\mathbb{V}(S_n) \geq \sum_{i=1}^n \lambda^2 \mathbb{E}(Y_i) = \lambda^2 \mathbb{E}(Y) = \lambda^2 \mathbb{P}(\max_{0 \leq k \leq n} |S_k| \geq \lambda).$$

## 2.6 Momente

Neben den Erwartungswerten von  $X$  und  $X^2$  kann man auch die von höheren Potenzen betrachten:

**Definition 2.25**

$$M_n(X) = \mathbb{E}(X^n)$$

heißt das  $n$ -te Moment von  $X$ ,

$$m_n(X) = \mathbb{E}((X - \mathbb{E}(X))^n)$$

das  $n$ -te zentrale Moment von  $X$ .

## 2.7 Folgen von Zufallsvariablen

**Satz 2.22: schwaches Gesetz der großen Zahlen**

$(X_n, n \in \mathbb{N})$  sei eine Folge von unabhängigen, identisch verteilten Zufallsvariablen mit endlicher Varianz,  $S_n = X_1 + \dots + X_n$ . Dann gilt

$$\mathbb{P}\left(\left|\frac{S_n}{n} - \mathbb{E}(X_1)\right| \geq \epsilon\right) \rightarrow 0$$

für jedes  $\epsilon > 0$ .

Der Beweis dieses Satzes ist nicht schwer, wir verwenden einfach die Ungleichung von Chebychev:

$$\mathbb{P}\left(\left|\frac{S_n}{n} - \mathbb{E}(X_1)\right| \geq \epsilon\right) = \mathbb{P}(|S_n - n\mathbb{E}(X_1)| \geq n\epsilon) = \mathbb{P}(|S_n - \mathbb{E}(S_n)| \geq n\epsilon) \leq \frac{\mathbb{V}(S_n)}{(n\epsilon)^2} = \frac{\mathbb{V}(X_1)}{n\epsilon^2},$$

und das geht natürlich gegen 0.

### Satz 2.23: Starkes Gesetz der großen Zahlen

$(X_n, n \in \mathbb{N})$  sei eine Folge von unabhängigen, identisch verteilten Zufallsvariablen mit endlichem Erwartungswert,  $S_n = X_1 + \dots + X_n$ . Dann konvergiert  $\frac{S_n}{n}$  mit Wahrscheinlichkeit 1 gegen  $\mathbb{E}(X_1)$ .

Dieser Satz liefert einerseits eine mathematisch strenge Version des “empirischen Gesetzes der großen Zahlen”, andererseits bildet er auch die Grundlage zur Berechnung von Erwartungswerten und Integralen durch Simulation. Wenn wir den Erwartungswert einer Verteilung bestimmen wollen, erzeugen wir einfach  $n$  unabhängige Zufallszahlen mit dieser Verteilung. Das Stichprobenmittel  $\bar{X}_n$  sollte dann für hinreichend großes  $n$  nahe beim gesuchten Erwartungswert liegen. Integrale der Form

$$I = \int_0^1 \int f(x) dx$$

kann man als Erwartungswert

$$I = \mathbb{E}(f(X))$$

betrachten, wobei  $X$  auf  $[0, 1]$  gleichverteilt ist. Diese Idee ist natürlich nur dann brauchbar, wenn wir auch die Genauigkeit dieser Näherung angeben können. Wie bei allen wahrscheinlichkeitstheoretischen Verfahren ist das auch hier nur mit einer gewissen Wahrscheinlichkeit möglich. Eine grobe Abschätzung dieser Genauigkeit liefert die Ungleichung von Chebychev. Etwas besser geht das mit dem nächsten Satz. Es wird sich herausstellen, dass sich mit  $n$  eine Genauigkeit in der Größenordnung  $1/\sqrt{n}$  erreichen lässt. Das ist auf den ersten Blick nicht gar so berauschend, die Trapez- oder Simpsonregel garantieren bessere Raten. Allerdings macht die Simulation keine Voraussetzungen über die Funktion  $f$ , während die deterministischen Verfahren Annahmen über die Ableitungen von  $f$  benötigen. Theoretisch müsste für die Simulation  $f$  nicht einmal stetig sein, in der Praxis sind die Verteilungen der “gleichverteilten” Zufallszahlen, die wir für die Simulation verwenden, allerdings nur diskrete Approximationen der stetigen Gleichverteilung, also ist doch etwas Stetigkeit notwendig. Die wahre Stärke der Simulationsmethode zeigt sich aber bei mehrdimensionalen Integralen: um ein Integral wie

$$J = \int_0^1 \dots \int_0^1 f(x_1, \dots, x_{20}) dx_1 \dots dx_{20}$$

mit der Trapezmethode zu bestimmen, müssen wir ein 20-dimensionales Gitter verwenden. Bei auch nur zwei Stützwerten in jeder Dimension sind das schon  $2^{20} = 1048576$  Punkte. Von der anderen Seite her betrachtet: wenn wir  $n$  Punkte verwenden, sind das  $n^{1/d}$  Stützwerte pro Dimension, und etwa mit der Simpsonregel erhalten wir einen Fehler in der Größenordnung  $n^{-4/d}$ . Mit der Simulationsmethode können wir das Integral durch

$$\hat{J}_n = \frac{1}{n} \sum_{i=0}^{n-1} f(X_{id+1}, \dots, X_{id+d})$$

annähern, und es gilt immer noch die Fehlerabschätzung in der Größenordnung  $n^{-1/2}$ .

### Satz 2.24: Zentraler Grenzwertsatz

$(X_n, n \in \mathbb{N})$  sei eine Folge von unabhängigen, identisch verteilten Zufallsvariablen mit  $\mathbb{E}(X) =$

$\mu$ ,  $\mathbb{V}(X) = \sigma^2$ . Dann gilt

$$\mathbb{P}\left(\frac{S_n - n\mu}{\sqrt{n\sigma^2}} \leq x\right) \rightarrow \Phi(x) = \int_{-\infty}^x \frac{1}{\sqrt{2\pi}} e^{-x^2/2}.$$

Eine Summe von unabhängigen identisch verteilten Zufallsvariablen ist also näherungsweise normalverteilt.

Damit lassen sich Wahrscheinlichkeiten, in denen die Summen von unabhängigen Zufallsvariablen vorkommen, näherungsweise berechnen. Dazu muss die Anzahl der Summanden hinreichend groß sein — für die Binomialverteilung und die Poissonverteilung gibt es die Faustregel, dass die Varianz mindestens 9 sein soll, die Regel  $n \geq 30$ , die oft für den allgemeinen Fall kolportiert wird, ist eher mit Vorsicht zu genießen.

### Beispiel 2.12

Als Beispiel berechnen wir die Wahrscheinlichkeit, dass in 1000 Würfeln eines fairen Würfels mehr als 200 mal eine Sechs erscheint:

$$\mathbb{P}(X > 200) \approx 1 - \Phi\left(\frac{200 - 1000/6}{\sqrt{1000 * 5/36}}\right) = 1 - \Phi(2.83) = 0.002.$$

### Beispiel 2.13

Nehmen wir an, wir wollen das Integral

$$I = \int_0^\pi \sin(x) dx$$

durch Simulation bestimmen. Wir möchten wissen, wie groß wir  $n$  wählen müssen, um mit 99% Wahrscheinlichkeit eine Genauigkeit von zwei Nachkommastellen (also  $\pm 0.005$ ) zu garantieren. Zuerst transformieren wir das Integral auf das Intervall  $[0, 1]$ :

$$I = \int_0^1 \pi \sin(\pi x) dx.$$

Unsere Näherung ist

$$\hat{I}_n = \frac{1}{n} \sum_{i=1}^n Y_i$$

mit

$$Y_i = f(X_i) = \pi \sin(\pi X_i),$$

und  $X_i$  sind die unabhängigen  $U(0, 1)$ -Zufallszahlen aus unserem Generator.

Für unsere Fehlerabschätzung wollen wir den zentralen Grenzwertsatz verwenden. Dazu benötigen wir die Varianz von  $Y_i$ . Diese berechnet sich als

$$\sigma^2 = \mathbb{E}(Y^2) = \mathbb{E}(Y)^2 = \int_0^1 f(x)^2 dx - I^2.$$

Da wir das Integral  $I$  erst berechnen wollen, können wir im allgemeinen nicht annehmen, dass wir  $\sigma^2$  kennen. Eine Möglichkeit wäre eine grobe Abschätzung: hier wissen wir etwa, dass  $|f| \leq \pi$  gilt, was die Abschätzung  $\sigma \leq \pi$  liefert, wenn man auch noch bemerkt, dass  $f \geq 0$  gilt, dann lässt sich diese Abschätzung auf  $\sigma \leq \pi/2$  verbessern. Wir werden hier schummeln und die exakten Werte einsetzen. In der Praxis geht man meist so vor, dass auch für die Varianz ein Näherungswert aus der Simulation berechnet und damit der Fehler abgeschätzt wird. Das lässt sich sehr schön iterativ bewerkstelligen.

Wir wollen (mit  $\delta = 0.005$ )

$$\mathbb{P}(I - \delta \leq \hat{I}_n \leq I + \delta) \geq 0.99$$

Mit der Normalapproximation erhalten wir

$$\begin{aligned} \mathbb{P}(-\delta \leq \hat{I}_n - I \leq \delta) &= \mathbb{P}\left(-\frac{\delta}{\sigma/\sqrt{n}} \leq \frac{\hat{I}_n - I}{\sigma/\sqrt{n}} \leq \frac{\delta}{\sigma/\sqrt{n}}\right) \approx \Phi\left(\frac{\delta}{\sigma/\sqrt{n}}\right) - \Phi\left(-\frac{\delta}{\sigma/\sqrt{n}}\right) = \\ &= 2\Phi\left(\frac{\delta}{\sigma/\sqrt{n}}\right) - 1. \end{aligned}$$

Das soll 0.99 sein, also

$$\Phi\left(\frac{\delta}{\sigma/\sqrt{n}}\right) = 0.995,$$

und

$$\frac{\delta}{\sigma/\sqrt{n}} = \Phi^{-1}(0.995) = 2.576,$$

also

$$n = \frac{2.576^2 \sigma^2}{\delta^2}.$$

Wir verwenden unser Wissen, dass  $\sigma^2 = \frac{\pi^2}{2} - 4 = 0.935$  gilt:

$$n = \frac{2.576^2 \cdot 0.935}{0.005^2} = 248178.$$

Eine schnelle Berechnung mit dem Statistikpaket R ergab als Ergebnis einer Simulation mit diesem  $n$

$$\hat{I}_n = 2.002622,$$

drei weitere Versuche die Werte 2.000864, 1.999885 und 2.001498.

## 2.8 Spezielle Verteilungen

In diesem Abschnitt sammeln wir einige wichtige Beispiele für Verteilungen, die oft gebraucht werden. Bei den Verteilungen, die nicht schon im Kapitel erwähnt worden sind, geben wir auch an, wie man dazu kommt.

### 2.8.1 Diskrete Verteilungen

Die Binomialverteilung und die Hypergeometrische Verteilung wurden schon besprochen.

Die Geometrische Verteilung tritt auf, wenn ein Experiment mit Erfolgswahrscheinlichkeit  $p$  so lange wiederholt wird, bis der erste Erfolg eintritt. Wird dabei  $X$  als die Anzahl der Versuche definiert, dann hat  $X$  die Verteilung  $G^*(p)$ . Man kann aber auch die Anzahl der *Misserfolge* zählen, die man in Kauf nehmen muss, bis der erste Erfolg eintritt. Diese Anzahl ist dann nach  $G(p)$  verteilt. Auf den ersten Blick erscheint die erste Betrachtungsweise natürlicher, aber die Verteilung, die bei 0 anfängt, tritt öfter auf als die, die bei 1 anfängt, deshalb ist für uns  $G(p)$  die Standardversion der geometrischen Verteilung, und  $G^*(p)$  die alternative Form (weil sie aus  $G(p)$  durch eine Verschiebung um eins nach rechts entsteht, heißt sie auch die "verschobene geometrische Verteilung". Dasselbe gilt für die negative Binomialverteilung:  $NB^*$  zählt die Anzahl der Versuche bis zum  $n$ -ten Erfolg,  $NB$  die Anzahl der Misserfolge, die man in Kauf nehmen muss, bis der  $n$ -te Erfolg eintritt. In der negativen Binomialverteilung  $NB$  kann man auch nicht ganzzahliges  $n$  verwenden, wenn man den Binomialkoeffizienten für beliebiges  $x$  als

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

definiert.

Die Poissonverteilung ergibt sich als Grenzfall der Binomialverteilung für  $n \rightarrow \infty$  und  $np \rightarrow \lambda$ . Das wird in den Übungen nachgewiesen.

Name	Symbol	$p(x)$	$\mathbb{E}(X)$	$\mathbb{V}(X)$
Binomial $n \in \mathbb{N}, 0 \leq p \leq 1$	$B(n, p)$	$\binom{n}{x} p^x (1-p)^{n-x} (0 \leq x \leq n)$	$np$	$np(1-p)$
Gleichverteilung (diskret) $a \leq b, a, b \in \mathbb{Z}$	$D(a, b)$	$\frac{1}{b-a+1} (a \leq x \leq b)$	$\frac{a+b}{2}$	$\frac{(b-a+1)^2-1}{12}$
Geometrisch $0 < p < 1$	$G(p)$	$p(1-p)^x, (x \geq 0)$	$\frac{1-p}{p}$	$\frac{1-p}{p^2}$
Geometrisch (alternativ) $0 < p < 1$	$G^*(p)$	$p(1-p)^{x-1}, (x \geq 1)$	$\frac{1}{p}$	$\frac{1-p}{p^2}$
Negativ Binomial $n > 0, 0 < p < 1$	$NB(n, p)$	$\binom{n+x-1}{n} p^n (1-p)^x, (x \geq 0)$	$\frac{n(1-p)}{p}$	$\frac{n(1-p)}{p^2}$
Negativ Binomial (alternativ) $n \in \mathbb{N}, 0 < p < 1$	$NB^*(n, p)$	$\binom{x-1}{n-1} p^{n-x} (1-p)^x, (x \geq n)$	$\frac{n}{p}$	$\frac{n(1-p)}{p^2}$
Poisson $\lambda > 0$	$P(\lambda)$	$\frac{\lambda^x e^{-\lambda}}{x!}$	$\lambda$	$\lambda$
Hypergeometrisch $N, A, n \in \mathbb{N}, n, A \leq N$	$H(N, A, n)$	$\frac{\binom{A}{x} \binom{N-A}{n-x}}{\binom{N}{n}} (0 \leq x \leq n)$	$\frac{nA}{N}$	$\frac{nA(N-A)(N-n)}{N^2(N-1)}$

## 2.8.2 Stetige Verteilungen

Die stetige Gleichverteilung ist ein Konzept, das uns schon in unseren ersten Überlegungen begegnet ist — eine Zahl wird zufällig aus dem Intervall  $[a, b]$  gewählt, und alle diese Zahlen sind “gleichberechtigt”. Eine alternative Betrachtungsweise ist, diese Verteilung als Grenzfall von diskreten Gleichverteilungen auf einem immer feineren Gitter anzusehen, so, wie wir es in Beispiel 2.1 getan haben.

Auch über die Normalverteilung haben wir schon gesprochen; der zentrale Grenzwertsatz gibt uns Anlass, viele Größen, die als Summe von vielen kleinen und unabhängigen Einflüssen zustandekommen, als zumindest näherungsweise normalverteilt anzusehen. Das und auch die Tatsache, dass sie in der Statistik sehr angenehm zu behandeln ist, machen sie zur wichtigsten Verteilung von allen.

Einige der anderen Verteilungsfunktionen in der folgenden Tabelle sind von der Normalverteilung abgeleitet: Die Chi-Quadratverteilung ergibt sich als die Verteilung der Summe

$$X_1^2 + \dots + X_n^2,$$

wobei  $(X_1, \dots, X_n)$  unabhängig standardnormalverteilt ( $N(0, 1)$ ) sind.

Die  $t$ -Verteilung ist die Verteilung von  $X/\sqrt{Y/n}$  mit  $X, Y$  unabhängig  $X \sim N(0, 1), Y \sim \chi_n^2$ .

Die  $F$ -Verteilung ist die Verteilung von  $\frac{X/n}{Y/m}$ ,  $X, Y$  unabhängig,  $X \sim \chi_n^2, Y \sim \chi_m^2$ .

Diese Verteilungen sind in der Statistik von großer Bedeutung. Ihre Parameter ( $n$  bei  $\chi^2$  und  $t$ ,  $n$  und  $m$  bei  $F$ ) werden gemeinhin als “Freiheitsgrade” bezeichnet.

Die Erlangverteilung  $Er(n, \lambda)$  ist die Verteilung einer Summe von  $n$  unabhängigen exponentialverteilten Zufallsvariablen mit Parameter  $\lambda$ .

Für die Gammaverteilung gibt es ein Additionstheorem: sind  $X \sim \Gamma(\alpha, \lambda)$  und  $Y \sim \Gamma(\beta, \lambda)$  unabhängig, dann gilt  $X + Y \sim \Gamma(\alpha + \beta, \lambda)$ . Unter denselben Voraussetzungen sind die Beta-Verteilungen als die Verteilungen von Quotienten zu erhalten:  $X/(X + Y) \sim B_1(\alpha, \beta), X/Y \sim B_1(\alpha, \beta)$ .

Die Exponentialverteilung kann als Grenzfall aus der geometrischen Verteilung erhalten werden und steht in enger Verbindung mit der geometrischen Verteilung; die Details dazu werden im nächsten Kapitel erörtert. Dort, speziell in der Theorie der Markovketten, hat die Exponentialverteilung eine zentrale Rolle.

Name	Symbol	$f(x)$	$\mathbb{E}(X)$	$\mathbb{V}(X)$
Gleichverteilung (diskret) (stetig) $a < b$	$U(a, b)$	$\frac{1}{b-a} (a \leq x \leq b)$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$
Exponential $\lambda > 0$	$E(\lambda)$	$\lambda e^{-\lambda x} (x \geq 0)$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$
Gamma $\alpha, \lambda > 0$	$\Gamma(\alpha, \lambda)$	$\frac{\lambda^\alpha x^{\alpha-1}}{\Gamma(\alpha)} e^{-\lambda x} (x \geq 0)$	$\frac{\alpha}{\lambda}$	$\frac{\alpha}{\lambda^2}$
Cauchy $a > 0$	$C(a)$	$\frac{a}{\pi(x^2+a^2)}$	N.A.	N.A.
Normal $\mu \in \mathbb{R}, \sigma^2 > 0$	$N(\mu, \sigma^2)$	$\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$	$\mu$	$\sigma^2$
Beta 1. Art $\alpha, \beta > 0$	$B_1(\alpha, \beta)$	$\frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha, \beta)} (0 \leq x \leq 1)$	$\frac{\alpha}{\alpha+\beta}$	$\frac{\alpha\beta}{(\alpha+\beta+1)(\alpha+\beta)^2}$
Beta 2. Art $\alpha, \beta > 0$	$B_1(\alpha, \beta)$	$\frac{x^{\alpha-1}(1+x)^{-\alpha-\beta}}{B(\alpha, \beta)} (0 \leq x)$	$\frac{\alpha}{\beta-1} (\beta > 1)$	$\frac{\alpha(\alpha+\beta-1)}{(\beta-2)(\beta-1)^2} (\beta > 2)$
Chiquadrat $n \in \mathbb{N}$	$\chi_n^2$	$= \Gamma(n/2, 1/2)$		
Erlang $n \in \mathbb{N}, \lambda > 0$	$Er(n, \lambda)$	$= \Gamma(n, \lambda)$		
$t$ -Verteilung $n \in \mathbb{N}$	$t_n$	$\frac{2}{\sqrt{n}B(n/2, 1/2)(1+x^2/n)^{(n+1)/2}}$	$0 (n > 1)$	$\frac{n}{n-2} (n > 2)$
$F$ -Verteilung $m, n \in \mathbb{N}$	$F_{n,m}$	$\frac{x^{n/2-1} n^{n/2} (1+nx/m)^{-(m+n)/2}}{m^{n/2} B(n/2, m/2)} (0 \leq x)$	$\frac{m}{m-2} (m > 2)$	$\frac{m^2(m+n-2)}{n(m-4)(m-2)^2} (m > 4)$

# Kapitel 3

## Stochastische Prozesse

### Definition 3.1

Ein stochastischer Prozess ist eine Familie  $(X_t, t \in T)$  von Zufallsvariablen. Die Indexmenge  $T$  wird Parameterraum genannt und soll eine Teilmenge der reellen Zahlen sein. Der Wertebereich  $\Omega_X$  von  $X_t$  heißt Zustandsraum oder Phasenraum. Wenn  $T$  endlich oder abzählbar (etwa  $\mathbb{N}$ ) ist, sprechen wir von einem Prozess in diskreter Zeit, wenn  $T$  ein ganzes (endliches oder unendliches) Intervall ist, von einem Prozess in stetiger Zeit,

Stochastische Prozesse in diskreter Zeit sind einfach Folgen von Zufallsvariablen. Der Unterschied zu unseren früheren Überlegungen besteht darin, dass wir nicht mehr annehmen, dass die einzelnen Zufallsvariablen voneinander unabhängig sind. Wir müssen also die Abhängigkeiten zwischen den einzelnen Zufallsvariablen festlegen, das heißt, wir müssen gewisse Annahmen über die gemeinsame Verteilung von  $(X_{t_1}, \dots, X_{t_n})$  mit  $t_1 < \dots < t_n$  treffen.

Die meisten Eigenschaften, die unsere Klassen von stochastischen Prozessen definieren, sind von Eigenschaften einer Folge  $X_n$  von unabhängigen Zufallsvariablen oder der Folge ihrer Partialsummen  $S_n = X_1 + \dots + X_n$  abgeleitet.

### 3.1 Stationäre Prozesse

Wir betrachten eine Folge  $(X_1, X_2, \dots)$  von unabhängigen identisch verteilten Zufallsvariablen. Wenn wir vom Anfang dieser Folge ein paar Glieder entfernen, dann ist etwa  $(X_n, X_{n+1}, \dots)$  ebenfalls eine Folge von unabhängig identisch verteilten Zufallsvariablen mit derselben gemeinsamen Verteilung. Durch diese Verschiebung ändert sich also die Verteilung der Folge nicht. Diese Eigenschaft können wir für sich betrachten:

### Definition 3.2

Der Prozess  $X_t, t \in T$  heißt stationär, wenn für  $t_1 < t_2 < \dots < t_n$  und  $h > 0$  die gemeinsame Verteilung von  $(X(t_1), \dots, X(t_n))$  mit der von  $(X(t_1 + h), \dots, X(t_n + h))$  übereinstimmt.

Diese simple Forderung hat weitreichende Konsequenzen: sie genügt, um einen Satz im Geiste des Gesetzes der großen Zahlen zu beweisen:

### Satz 3.1: Ergodensatz von Birkhoff

Wenn die Folge  $(X_n)$  stationär ist und endlichen Erwartungswert hat, dann existiert

$$X_\infty = \lim_{n \rightarrow \infty} \bar{X}_n$$

mit Wahrscheinlichkeit 1 und

$$\mathbb{E}(X_\infty) = \mathbb{E}(X_1).$$

Es gilt also eine ähnliche Aussage wie im Gesetz der großen Zahlen, allerdings ist der Grenzwert im allgemeinen eine Zufallsvariable. Wenn er deterministisch ist, muss er natürlich gleich  $\mathbb{E}(X_1)$  sein. Stationäre Folgen, in denen dieser Grenzwert deterministisch ist (nicht nur für  $X_n$  selbst, sondern auch für alle beschränkten Funktionen  $f(X_n, \dots, X_{n+k})$ ), heißen ergodisch.

Wir werden uns hier nicht weiter mit der Theorie der stationären Prozesse auseinandersetzen, gelegentlich werden sie in den folgenden Kapiteln (speziell bei der Informationstheorie) wieder auftauchen.

### 3.2 Markovprozesse

Die nächste Definition leitet sich nicht direkt von der Folge  $(X_n)$  von unabhängigen Zufallsvariablen ab, sondern von der Folge der Partialsummen  $S_n = X_1 + \dots + X_n$ . Wenn wir für  $m > n$  die Differenz  $S_m - S_n$  betrachten, dann hängt diese nur von den Zufallsvariablen  $X_{n+1}, \dots, X_m$  ab, und die sind unabhängig von den Variablen  $X_1, \dots, X_n$ , die in  $S_n$  stecken.  $S_n$  und  $S_m - S_n$  sind also unabhängig. Genauso kann man sich überlegen, dass für  $n_1 < n_2 < \dots < n_k$  die Zufallsvariablen

$$S_{n_1}, S_{n_2} - S_{n_1}, \dots, S_{n_k} - S_{n_{k-1}}$$

unabhängig sind. Diese Eigenschaft kann man fast wörtlich übertragen:

**Definition 3.3**

Der Prozess  $(X_t, t \in T)$  heißt Prozess mit unabhängigen Zuwächsen, wenn für  $t_1 < t_2 < \dots < t_n$  die Zufallsvariablen

$$X(t_1), X(t_2) - X(t_1), X(t_3) - X(t_2), \dots, X(t_n) - X(t_{n-1})$$

unabhängig sind.

Hier und auch später verwenden wir die Notation  $X(t)$  für  $X_t$ , weil komplexe Ausdrücke im Index schlecht lesbar sind. Beide sollen natürlich dieselbe Bedeutung haben.

Etwas allgemeiner kann man sagen, dass die Verteilung von

$$S_m = S_n + S_m - S_n$$

von den Werten von  $S_i$  mit  $i \leq n$  nur durch den Wert von  $S_n$  abhängt. Diese Eigenschaft heißt die Markoveigenschaft:

**Definition 3.4**

Der Prozess  $X(t)$  heißt Markovprozess, wenn für  $t_1 < t_2 < \dots < t_n$

$$\mathbb{P}(X(t_n) \leq x_n | X(t_1) = x_1, \dots, X(t_{n-1}) = x_{n-1}) = \mathbb{P}(X(t_n) \leq x_n | X(t_{n-1}) = x_{n-1}).$$

Die Zukunft hängt also von der Vergangenheit nur über den letzten Wert  $X(t_{n-1})$  ab. Ein Beispiel für Markovprozesse sind Prozesse mit unabhängigen Zuwächsen.

Wir sehen uns ein einfaches Beispiel für einen Prozess in stetiger Zeit an. So wie schon bei anderer Gelegenheit beginnen wir mit einem diskreten Modell und machen es immer feiner (wir erhöhen schrittweise die Auflösung): Wir teilen das unendliche Intervall  $[0, \infty[$  in Teilintervalle der Länge  $2^{-N}$ , also  $[0, 2^{-N}[, [2^{-N}, 2 \cdot 2^{-N}[, \dots$ . Jedes Intervall markieren wir mit Wahrscheinlichkeit  $\lambda 2^{-N}$  unabhängig von allen anderen (wir müssen natürlich  $N$  so groß wählen, dass diese Wahrscheinlichkeit kleiner als 1 ist). Für jedes  $N$  ist die mittlere Anzahl von Markierungen (ihr Erwartungswert) im Intervall  $[0, 1]$  gleich  $\lambda$ . Dasselbe gilt zumindest näherungsweise für jedes Intervall der Länge 1; es stimmt für ein bestimmtes  $N$  genau, wenn die Endpunkte des Intervalls ganzzahlige Vielfache

von  $2^{-N}$  sind. Wir müssen uns aber nicht mit Erwartungswerten begnügen, wir wissen ja, dass die Anzahl der Markierungen im Intervall  $[0, 1[$  binomialverteilt ist mit Parametern  $2^N$  und  $\lambda 2^{-N}$ . Für  $N \rightarrow \infty$  konvergiert das gegen eine Poissonverteilung mit Parameter  $\lambda$ , wie wir in den Übungen gezeigt haben. Genauso kann man erhalten, dass für irgendein Intervall der Länge  $t$  die Anzahl der Markierungen darin für großes  $N$  näherungsweise Poissonverteilt ist mit Parameter  $t\lambda$ . Klarerweise sind die Anzahlen in disjunkten Intervallen unabhängig (zumindest wenn sie positiven Abstand voneinander haben; wenn nicht, dann gibt es nur eines der kleinen Intervalle, dessen Markierung bei beiden zählt, also ist die Abhängigkeit zwischen beiden Anzahlen nur schwach). Für  $N \rightarrow \infty$  ergibt sich für  $X(t)$ , die Anzahl der Markierungen zwischen 0 und  $t$ , dass die Anzahl  $X(t) - X(s)$  von Markierungen zwischen  $s$  und  $t$ , von allem unabhängig ist, was vor  $s$  passiert. Wir haben also einen Prozess mit unabhängigen Zuwächsen, bei dem  $X(t) - X(s)$  mit der Poissonverteilung  $P(\lambda(t - s))$  verteilt ist. Diesen Prozess nennen wir den Poissonprozess:

**Definition 3.5**

Der Poissonprozess mit Rate  $\lambda > 0$  ist ein Prozess mit unabhängigen Zuwächsen, mit  $X(0) = 0$  und  $X(t) - X(s) \sim P(\lambda(t - s)) (s < t)$ .

Wir können diesen Prozess auch anders ansehen: Wir zählen die Anzahl  $Y_1$  von kleinen Intervallen, die wir durchlaufen müssen, bis wir die erste Markierung finden, danach zählen wir die Anzahl  $Y_2$ , die zwischen der ersten und der zweiten Markierung liegen, usw. Die Position der ersten Markierung ist dann  $T_1 = 2^{-N} Y_1$ , der Abstand zwischen erster und zweiter  $T_2 = 2^{-N} Y_2$ , etc.  $Y_1, Y_2, \dots$  sind unabhängig und geometrisch verteilt mit Erfolgswahrscheinlichkeit  $\lambda 2^{-N}$ , also

$$\mathbb{P}(Y_i > k) = \left(1 - \frac{\lambda}{2^N}\right)^k$$

und daher

$$\mathbb{P}(T_i > x) = \left(1 - \frac{\lambda}{2^N}\right)^{x 2^N},$$

und das konvergiert für  $N \rightarrow \infty$  gegen  $e^{-\lambda x}$ . Wir kommen so zu einer Folge  $T_1, T_2, \dots$  von unabhängigen exponentialverteilten Zufallsvariablen, und  $X(t) = 0$  für  $t < T_1$ ,  $X(t) = 1$  für  $T_1 \leq t < T_1 + T_2$ ,  $X(t) = k$  für  $T_1 + \dots + T_k \leq t < T_1 + \dots + T_{k+1}$ . Dieses Modell lässt sich auch verallgemeinern:

**Definition 3.6**

$(T_n)$  sei eine Folge von unabhängigen identisch verteilten Zufallsvariablen mit  $T_n > 0$ . Wir setzen  $S_0 = 0$ ,  $S_n = T_1 + \dots + T_n$ , und für  $n = 0, \dots$

$$X(t) = n \text{ für } S_n \leq t < S_{n+1}.$$

Wir nennen  $X$  einen Erneuerungsprozess.

### 3.3 Markovketten in diskreter Zeit

#### 3.3.1 Übergangswahrscheinlichkeiten

Markovprozesse mit diskretem Zustandsraum nennen wir Markovketten. Wir können noch zwischen Markovketten in diskreter und in stetiger Zeit unterscheiden. In beiden Fällen kann man die diskrete Verteilung der einzelnen Zufallsvariablen durch ihre Wahrscheinlichkeitsfunktion beschreiben, deshalb erhält die Markoveigenschaft die besonders einfache Form

$$\mathbb{P}(X_n = x_n | X_1 = x_1, \dots, X_{n-1} = x_{n-1}) = \mathbb{P}(X_n = x_n | X_{n-1} = x_{n-1}).$$

Die Wahrscheinlichkeiten

$$\mathbb{P}(X_{n+1} = j | X_n = i)$$

nennen wir die Übergangswahrscheinlichkeiten der Markovkette. Wenn diese nicht von  $n$  abhängen, sprechen wir von einer homogenen Markovkette und setzen

$$p_{ij}\mathbb{P}(X_{n+1} = j|X_n = i)$$

Die Wahrscheinlichkeiten

$$p_{ij}(t) = \mathbb{P}(X_{n+t} = j|X_n = i)$$

nennen wir die  $t$ -stufigen Übergangswahrscheinlichkeiten. Aus dem Satz von der vollständigen Wahrscheinlichkeit erhalten wir die Chapman-Kolmogorov Gleichungen

$$p_{ij}(s+t) = \sum_{k \in \Omega_X} p_{ik}(s)p_{kj}(t).$$

in Matrixnotation mit

$$P(t) = (p_{ij}(t))_{\Omega_X \times \Omega_X}$$

lauten die Chapman-Kolmogorov Gleichungen

$$P(t+s) = P(t)P(s),$$

und mit  $P = P(1)$

$$P(t) = P^t.$$

Wir nennen  $P$  die Übergangsmatrix und  $P(t)$  die  $t$ -stufige Übergangsmatrix.

Wir setzen zusätzlich  $p_i(t) = \mathbb{P}(X_t = i)$  und  $p(t) = (p_i(t), i \in \Omega_X)$  (als Zeilenvektor). Wieder mit dem Satz von der vollständigen Wahrscheinlichkeit erhalten wir

$$p(t) = p(0)P^t.$$

Durch  $p(0)$  und  $P$  werden alle endlichdimensionalen Verteilungen festgelegt.

Der einfachste nichttriviale Fall ist eine Markovkette mit zwei Zuständen. Ihre Übergangsmatrix hat die allgemeine Form

$$P = \begin{pmatrix} 1-a & a \\ b & 1-b \end{pmatrix}.$$

Die Potenzen dieser Matrix berechnen wir mithilfe der Eigenwertzerlegung: Wenn  $A$  diagonalisierbar ist, als so viele Eigenvektoren hat wie Zeilen/Spalten, dann gilt die Darstellung

$$A = X\Lambda X^{-1},$$

wobei  $X$  die Matrix aus den (Spalten-) Eigenvektoren und  $\Lambda$  die Diagonalmatrix der Eigenwerte ist. Die Matrix  $P$  hat einen Eigenwert 1, den es bei jeder Übergangsmatrix gibt, der zweite ist  $1 - (a + b)$ . Die Eigenvektoren dazu sind  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  und  $\begin{pmatrix} a \\ -b \end{pmatrix}$ . Insgesamt ergibt sich

$$P^t = \frac{1}{a+b} \left( \begin{pmatrix} b & a \\ b & a \end{pmatrix} + (1-a-b)^t \begin{pmatrix} a & -a \\ -b & b \end{pmatrix} \right).$$

Diese Darstellung gilt natürlich nur, wenn  $a + b > 0$ . Der verbleibende Fall  $a = b = 0$  ist der Leserin/dem Leser überlassen.

Ein einfaches Beispiel für eine Markovkette mit unendlichem Zustandsraum bietet der Random Walk:

**Definition 3.7**

Der einfache Random Walk (auch: einfache Irrfahrt) ist der Partialsummenprozess

$$X(t) = X(0) + \sum_{i=1}^t Y_i,$$

wobei  $(Y_1, Y_2, \dots)$  unabhängige Zufallsvariable mit

$$\mathbb{P}(Y_i = 1) = p, \mathbb{P}(Y_i = -1) = 1 - p$$

sind. Der Spezialfall  $p = 1/2$  heißt einfacher symmetrischer Random Walk.

Wird die spezielle Annahme an die Verteilung von  $Y_i$  fallengelassen (wenn also nur angenommen wird, dass  $(Y_n)$  eine Folge von unabhängigen, identisch verteilten Zufallsvariablen mit ganzzahligen Werten ist), dann ist  $(X(t))$  ein allgemeiner Random Walk.

Die einstufigen Übergangswahrscheinlichkeiten sind

$$p_{ij} = \begin{cases} p & \text{wenn } j = i + 1, \\ 1 - p & \text{wenn } j = i - 1, \\ 0 & \text{sonst.} \end{cases}$$

In Hinkunft verwenden wir zur Abkürzung die Notationen

$$\mathbb{P}_i(A) = \mathbb{P}(A|X_0 = i)$$

und

$$\mathbb{E}_i(Y) = \mathbb{E}(Y|X_0 = i).$$

### 3.3.2 Klasseneigenschaften

Wir definieren

#### Definition 3.8

Der Zustand  $j$  heißt Nachfolger von  $i$  ( $i \rightarrow j$ ), wenn es ein  $t \geq 0$  gibt, sodass  $p_{ij}(t) > 0$ .

Wenn sowohl  $i \rightarrow j$  als auch  $j \rightarrow i$  gilt, dann heißen  $i$  und  $j$  verbunden oder kommunizierend.

Das Kommunizieren ist eine Äquivalenzrelation, wir können daher den Phasenraum in die Äquivalenzklassen zerlegen, die wir Rekurrenzklassen oder kurz Klassen nennen. Gibt es nur eine Klasse (wenn also alle Zustände miteinander kommunizieren), heißt die Markovkette irreduzibel. Ein Zustand mit  $p_{ii} = 1$  heißt absorbierender Zustand. Ein solcher Zustand ist offensichtlich eine Klasse für sich.

#### Definition 3.9

Eine Eigenschaft heißt Klasseneigenschaft, wenn sie entweder für alle Zustände einer Klasse oder für keinen gilt.

Ein einfaches Beispiel einer Klasseneigenschaft ist die Periode:

#### Definition 3.10

Die Periode eines Zustandes ist

$$d(i) = \text{ggT}\{t \geq 0 : p_{ii}(t) > 0\}.$$

Wenn  $d(i) = 1$  gilt, dann heißt der Zustand  $i$  aperiodisch, sonst periodisch.

Dass die Periode eine Klasseneigenschaft ist, ist einfach zu beweisen: wenn  $i$  und  $j$  verbunden sind, dann gibt es  $t_1$  und  $t_2$  mit  $p_{ij}(t_1) > 0$  und  $p_{ji}(t_2) > 0$ . Weiters sei  $t$  eine Zahl mit  $p_{jj}(t) > 0$ . Es gilt

$$p_{ii}(t_1 + t_2) \geq p_{ij}(t_1)p_{ji}(t_2) > 0$$

und

$$p_{ii}(t_1 + t + t_2) \geq p_{ij}(t_1)p_{jj}(t)p_{ji}(t_2) > 0,$$

deshalb gilt

$$d(i) \mid t_1 + t_2$$

und

$$d(i) | t_1 + t + t_2,$$

deshalb auch  $d(i) | t$ . Weil das für jedes  $t$  mit  $p_{jj}(t) > 0$  gilt, ergibt sich  $d(i) | d(j)$ . Weil auch umgekehrt  $d(j) | d(i)$  ergibt sich  $d(i) = d(j)$ .

Etwas spannender ist die Rekurrenz: wir fragen uns nach dem Rückkehrverhalten unserer Markovkette. Ansatzweise ist das schon geschehen, bei der Nachfolger- und Verbundenheitsrelation geht es ja darum, ob man einen Zustand  $j$  von einem Zustand  $i$  aus erreichen kann (oder ob man wieder nach  $i$  zurückkehren kann). Jetzt fragen wir uns, ob der Prozess zurückkehren *muß*, oder ob es eine positive Wahrscheinlichkeit gibt, dass der Prozess nicht zurückkehrt. Dazu definieren wir zuerst

$$\tau_i = \inf\{t > 0 : X_t = i\},$$

die Übergangs- bzw. Rückkehrzeit (je nachdem, ob  $X_0 \neq i$  ist oder nicht) nach  $i$ , und

$$\nu_i = \#\{t > 0 : X_t = i\},$$

die Anzahl der Besuche in  $i$ .

**Satz 3.2**

Die folgenden Bedingungen sind äquivalent:

1.  $\mathbb{P}_i(\tau_i < \infty) = 1$ ,
2.  $\mathbb{P}_i(\nu_i = \infty) = 1$ ,
3.  $\mathbb{E}_i(\nu_i) = \infty$ ,
4.  $\sum_t p_{ii}(t) = \infty$ .

Wenn diese Bedingungen erfüllt sind, dann heißt  $i$  rekurrent, sonst transient. Rekurrenz und Transienz sind Klasseigenschaften.

Bei der Rekurrenz kann man weiter unterscheiden:

**Definition 3.11**

$i$  sei ein rekurrenter Zustand. Wenn

$$\mathbb{E}_i(\tau_i) < \infty$$

gilt, dann heißt  $i$  positiv rekurrent, sonst nullrekurrent.

**Definition 3.12**

$(\pi_i, i \in \Omega_X)$  heißt stationäre Verteilung, wenn

$$\pi_i \geq 0,$$

$$\sum_i \pi_i = 1$$

und

$$\sum_i \pi_i p_{ij} = \pi_j.$$

**Satz 3.3**

Wenn  $(X_n)$  irreduzibel und aperiodisch ist, dann existieren die Grenzwerte

$$\lim_{n \rightarrow \infty} p_{ij}(t) = \pi_j = \frac{1}{\mathbb{E}_j(\tau_j)}.$$

Im periodischen Fall gilt

$$\pi_j = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{t=1}^n p_{ij}(t).$$

Wenn  $(\pi_i)$  nicht identisch verschwindet (also wenn die Kette positiv rekurrent ist), dann ist es eine stationäre Verteilung. Umgekehrt folgt aus der Existenz einer stationären Verteilung die positive Rekurrenz. Die positive Rekurrenz bzw. Nullrekurrenz ist ebenfalls eine Klasseeigenschaft.

Für einen absorbierenden Zustand  $i_0$  definieren wir die Absorptionswahrscheinlichkeit  $a_i$  als

$$\mathbb{P}_i(\tau_{i_0} < \infty) = \mathbb{P}_i(X \text{ wird in } i_0 \text{ absorbiert}).$$

**Satz 3.4**

Die Absorptionswahrscheinlichkeiten sind die kleinste nichtnegative Lösung des Gleichungssystems

$$\begin{aligned} a_{i_0} &= 1, \\ a_i &= \sum_j p_{ij} a_j, i \neq i_0. \end{aligned}$$

Das gibt uns eine Möglichkeit, die Transienz oder Rekurrenz einer irreduziblen Markovkette zu entscheiden. Wir wählen einen Zustand und machen ihn zu einem absorbierenden Zustand und bestimmen für die modifizierte Übergangsmatrix die Absorptionswahrscheinlichkeiten. Sind diese gleich 1, ist die Kette rekurrent.

Wir nehmen an, dass  $i_0$  der einzige absorbierende Zustand ist und alle anderen Zustände kommunizieren und die Absorptionswahrscheinlichkeiten 1 sind. Dann erhalten wir für die mittlere Zeit bis zur Absorption

$$m_i = \mathbb{E}_i(\tau_{i_0})$$

eine ähnliche Gleichung:

$$\begin{aligned} m_{i_0} &= 0, \\ m_i &= 1 + \sum_j p_{ij} m_j, i \neq i_0. \end{aligned}$$

Allgemeiner kann man eine Zufallsvariable  $S = \sum_{t=1}^{\tau-1} x_{t,t+1}$  betrachten (d.h., wir "sammeln" auf unserem Weg zur Absorption Beträge  $x_{ij}$ , die von dem jeweiligen Übergang abhängen dürfen).

Wir setzen

$$m_i = \mathbb{E}_i(S)$$

und

$$v_i = \mathbb{V}_i(S).$$

Dann sind  $m_i$  und  $v_i$  die Lösungen der Gleichungen

$$\begin{aligned} m_{i_0} &= 0, v_{i_0} = 0, \\ m_i &= \sum_j p_{ij} x_{ij} + \sum_j p_{ij} m_j, i \neq i_0. \\ v_i &= \sum_j p_{ij} (x_{ij} + m_j - m_i)^2 + \sum_j p_{ij} v_j, i \neq i_0. \end{aligned}$$

Wenn es mehrere absorbierende Zustände gibt,  $A = \{i_1, \dots, i_k\}$ , dann kann man die Wahrscheinlichkeiten der Absorption  $a_i(i_j)$  in dem absorbierenden Zustand  $i_j$  oder allgemeiner in einem der Zustände in der Menge  $B \subseteq A$  (wenn wir auf die konkrete Menge  $B$  hinweisen wollen, schreiben wir für  $a_i$   $a_i(B)$ ). Das gibt die Gleichungen

$$a_i = \sum_j p_{ij} a_j, i \notin A$$

$$a_i = 1, i \in B$$

$$a_i = 0, i \in A \setminus B.$$

Manchmal ist es interessant (wieviel Geld werde ich haben, wenn ich nicht bankrott gehe?), den Erwartungswert von  $S$  unter der Bedingung, dass die Absorption in einem bestimmten Zustand oder in einer bestimmten Teilmenge der Menge der absorbierenden Zustände erfolgt. Da hilft es, dass  $X(t)$  unter der Bedingung der Absorption in  $B$  wieder eine Markovkette bildet, mit den Übergangswahrscheinlichkeiten

$$p_{ij}^B = \frac{p_{ij}a_j(B)}{a_i(B)}.$$

Mit diesen modifizierten Übergangswahrscheinlichkeiten (wobei die absorbierenden Zustände  $\notin B$  weggelassen werden) kann man die Gleichungen für  $m_i$  und  $v_i$  lösen und erhält so die bedingte Erwartung bzw. Varianz.

### Beispiel 3.1

Ein Münzwurfspiel: Angelina und Brad werfen eine Münze. Zeigt diese ‘‘Kopf’’, dann erhält Angelina einen Euro von Brad, bei Kopf gibt sie ihm einen Euro. Am Anfang hat Angelina  $a$  Euro, Brad  $b$  Euro. Das Spiel wird so lange wiederholt, bis Angelina oder Brad kein Geld mehr hat.

Bei diesem Spiel bildet das Kapital  $X_n$  von Angelina nach der  $n$ -ten Runde eine Markovkette: es verändert sich ja aufgrund eines Münzwurfes, der von der Vorgeschichte unabhängig ist. Die Übergangswahrscheinlichkeiten sind leicht bestimmt: aus einem der Zustände  $1, \dots, a + b - 1$  wird mit Wahrscheinlichkeit  $1/2$  in einen der Nachbarzustände gesprungen, die Zustände  $0$  und  $a + b$  sind absorbierend, weil bei ihrem Erreichen das Spiel endet, also

$$p_{i,i+1} = p_{i,i-1} = 1/2 \quad (1 \leq i \leq a + b - 1),$$

$$p_{00} = p_{a+b,a+b} = 1,$$

alle anderen Übergangswahrscheinlichkeiten sind  $0$ .

Als erstes bestimmen wir die Wahrscheinlichkeit, dass Angelina gewinnt: das ist die Absorptionswahrscheinlichkeit in  $a + b$ . Also setzen wir

$$a_0 = 0, a_{a+b} = 1,$$

$$a_i = \frac{a_{i+1} + a_{i-1}}{2} \quad (i = 1, \dots, a + b - 1).$$

Wir lösen die Rekursionsgleichung wieder mit dem Ansatz  $a_i = z^i$ . Die charakteristische Gleichung hat die doppelte Lösung  $z = 1$ , also ist  $a_i = ci + d$ . Die Koeffizienten  $c$  und  $d$  ergeben sich aus den Randbedingungen  $a_0 = 0$  und  $a_{a+b} = 1$ , also

$$a_i = \frac{i}{a + b}.$$

Am Anfang hat Angelina  $a$  Euro, also ist ihre Gewinnwahrscheinlichkeit

$$a_a = \frac{a}{a + b}.$$

Als nächstes interessiert uns der Erwartungswert der Spieldauer, also die mittlere Absorptionszeit. Wir haben die Gleichungen

$$m_0 = m_{a+b} = 0,$$

$$m_i = \frac{m_{i+1} + m_{i-1}}{2} + 1 \quad (1 \leq i \leq a + b - 1).$$

Wir kennen schon die allgemeine Lösung der  $\tilde{m}_n = cn + d$  homogenen Gleichung (in der der Störterm  $+1$  nicht vorhanden ist). Wenn wir eine Lösung der inhomogenen Gleichung kennen, dann kann man alle Lösungen erhalten, indem man zu dieser einen Lösung eine beliebige Lösung der homogenen Gleichung addiert. Im allgemeinen lässt sich eine Lösung des inhomogenen Problems für Störterme der Form  $P(n)z^n$  mit einem Polynom  $P$  in der Form  $Q(n)z^n$  finden, wobei  $Q$  vom gleichen Grad wie  $P$ . Wenn  $z$  aber eine Nullstelle des charakteristischen Polynoms ist, muss der Grad von  $Q$  um die Vielfachheit dieser Nullstelle erhöht werden. In unserem Fall ist  $z = 1$  (der Störterm  $1$  ist ja  $1 \cdot 1^n$ ) zweifache Nullstelle des charakteristischen Polynoms, also Versuchen wir eine Lösung der Form  $\bar{m}_n = kn^2$ . Einsetzen ergibt  $k = -1$ . Diese Lösung erfüllt noch nicht alle Randbedingungen, aber weil alle Lösungen von der Form

$$m_n = \bar{m}_n + \tilde{m}_n = -n^2 + c_n + d$$

sein müssen, bleiben nur noch  $c$  und  $d$  zu bestimmen, und es ergibt sich

$$m_i = i(a + b - i),$$

und die gesuchte mittlere Spieldauer ist

$$m_a = ab.$$

Für die Varianz der Spieldauer erhalten wir (nach einigen Rechnungen)

$$v_i = \frac{v_{i-1} + v_{i+1}}{2} + (a + b - 2i)^2, 1 \leq i \leq a + b - 1,$$

$$v_0 = v_{a+b} = 0.$$

Diesmal ist der Störterm quadratisch, also müssen wir die Lösung als Polynom vierten Grades ansetzen. Nach einigem Rechnen ist

$$v_i = \frac{1}{3}i(a + b - i)(4i^2 + (a + b)^2 - 2).$$

Die letzte Frage lautet: wie lange dauert das Spiel im Durchschnitt, wenn Angelina gewinnt? Wir fragen also nach dem bedingten Erwartungswert der Absorptionszeit unter der Bedingung der Absorption in  $a + b$ . Dazu berechnen wir die Übergangswahrscheinlichkeiten für die "bedingte Markovkette"

$$p_{ij}^{\{a+b\}} = \frac{p_{ij}a_j}{a_i}, \quad i, j = 1, \dots, a + b$$

(den "falschen" absorbierenden Zustand  $0$  haben wir entfernen müssen), und wir lösen damit die Gleichungen

$$m_{a+b} = 0,$$

$$m_i = 1 + \sum_{j=1}^{a+b} p_{ij}m_j, \quad i = 1, \dots, a + b - 1.$$

In vielen Fällen (und auch hier) ist es günstig, statt  $m_i$  die Variablen  $y_i = a_i x_i$  zu verwenden. Dann kann man nämlich die ursprünglichen  $p_{ij}$  verwenden, und wir müssen auch die "schlechten" absorbierenden Zustände nicht entfernen (weil sie automatisch  $y_i = 0$  bekommen). Das gibt im allgemeinen Fall die Gleichungen

$$y_i = \begin{cases} 0 & \text{wenn } i \text{ absorbierend ist,} \\ \sum_j p_{ij}y_j + a_i x_{ij} & \text{sonst.} \end{cases}$$

In unserem Fall ist das

$$y_0 = y_{a+b} = 0,$$

$$y_i = \frac{y_{i+1} + y_{i-1}}{2} + a_i = \frac{y_{i+1} + y_{i-1}}{2} + \frac{i}{a+b}, \quad i = 1, \dots, a+b.$$

Diemal müssen wir  $y$  als Polynom dritten Grades ansetzen und erhalten

$$y_i = \frac{i((a+b)^2 - i^2)}{3(a+b)}$$

und

$$m_i^{\{a+b\}} = \frac{y_i}{a_i} = \frac{(a+b)^2 - i^2}{3},$$

und wieder speziell für  $i = a$

$$m_a^{\{a+b\}} = \frac{b(2a+b)}{3}.$$

### 3.3.3 Markov Chain Monte Carlo

### 3.3.4 Markovketten in stetiger Zeit

Wir betrachten jetzt Markovketten, bei denen die Zeit nicht mehr nur ganzzahlige, sondern beliebige reelle (nichtnegative) Werte annehmen darf. Wir bleiben bei unserer Annahme, dass es sich um einen homogenen Prozess handelt, also dass die Übergangswahrscheinlichkeiten

$$\mathbb{P}(X_t = j | X_s = i)$$

nur von der Differenz  $t - s$  abhängen, und setzen wieder

$$p_{ij}(t) = \mathbb{P}(X_{s+t} = j | X(s) = i)$$

und setzen die Übergangswahrscheinlichkeiten zu den Übergangsmatrizen

$$P(t) = (p_{ij}(t))_{\Omega_X \times \Omega_X}$$

zusammen.

Wie im diskreten Fall gelten die Chapman-Kolmogorov Gleichungen

$$P(s+t) = P(s)P(t).$$

Leider gibt es im stetigen Fall nicht so wie in diskreter Zeit die Möglichkeit, alle Übergangsmatrizen als Potenzen einer einzigen Matrix zu erhalten. Wir nehmen daher Zuflucht zur Differentialrechnung. Zuerst verlangen wir die Stetigkeit der Übergangswahrscheinlichkeiten bei 0, also dass

$$\lim_{t \rightarrow 0} p_{ij}(t) = p_{ij}(0) = \begin{cases} 1 & \text{wenn } i = j, \\ 0 & \text{sonst.} \end{cases}$$

Diese Annahme genügt schon für die Existenz der Ableitungen:

#### Satz 3.5

Wenn die Übergangswahrscheinlichkeiten bei 0 stetig sind, dann existieren die Grenzwerte

$$q_{ij} = \lim_{t \rightarrow 0} \frac{p_{ij}(t) - p_{ij}(0)}{t}.$$

Die Zahlen  $q_{ij}$  heißen die infinitesimalen Parameter, die Matrix

$$Q = (q_{ij})_{\Omega_X \times \Omega_X}$$

die infinitesimale Matrix oder der infinitesimale Erzeuger der Markovkette.

Offensichtlich gilt  $q_{ii} \leq 0$  und  $q_{ij} \geq 0$  für  $i \neq j$ . Wenn der Wertebereich  $\Omega_X$  endlich ist, dann können wir in den Gleichungen

$$\sum_j \frac{p_{ij}(t) - p_{ij}(0)}{t} = 0$$

und

$$\frac{P(t+s) - P(t)}{s} = P(t) \frac{P(s) - I}{s} = \frac{P(s) - I}{s} P(t).$$

und erhalten so

$$\sum_j q_{ij} = 0$$

und

**Definition 3.13: Kolmogorovsche Differentialgleichungen**

Die Gleichung

$$P'(t) = QP(t)$$

heißt die Rückwärtsgleichung,

$$P'(t) = P(t)Q$$

die Vorwärtsgleichung von Kolmogorov.

Wenn  $\Omega_X$  endlich ist, ist  $Q$  eine gewöhnliche Matrix, und die Lösung der Kolmogorov-Gleichungen ist

$$P(t) = e^{Qt} = \sum_{n=0}^{\infty} \frac{Q^n t^n}{n!}.$$

Wenn  $Q$  diagonalisierbar ist, also

$$Q = E\Lambda E^{-1}$$

mit der Diagonalmatrix  $\Lambda$  der Eigenwerte und der Matrix  $E$ , der Spalten die zugehörigen Eigenvektoren sind, dann ist

$$P(t) = e^{Qt} = E\Lambda^t E^{-1} = E \begin{pmatrix} e^{t\lambda_1} & & \\ & \ddots & \\ & & e^{t\lambda_d} \end{pmatrix} E^{-1}.$$

Für  $d = 2$ , also eine Kette mit zwei Zuständen, hat  $Q$  die allgemeine Form

$$Q = \begin{pmatrix} -a & a \\ b & -b \end{pmatrix} (a, b \geq 0).$$

Diese hat die Eigenwerte 0 und  $-(a+b)$ . Für  $a = b = 0$  ergibt sich  $P(t) = I$ , sonst

$$P(t) = \frac{1}{a+b} \begin{pmatrix} b + ae^{-(a+b)t} & a(1 - e^{-(a+b)t}) \\ b(1 - e^{-(a+b)t}) & a + be^{-(a+b)t} \end{pmatrix}.$$

Wenn  $\Omega_X$  unendlich ist, gibt es in diesen Gleichungen einen zweifachen Grenzübergang (durch die Ableitung und eine Summation), deren Vertauschbarkeit nicht garantiert ist. Man kann jedenfalls zeigen, dass für  $i \neq j$   $q_{ij} < \infty$  sein muss. Für die Diagonalelemente können unendliche Werte auftreten, also  $q_{ii} = -\infty$ . Auch wenn  $q_{ii}$  endlich Wert, kann es sein, dass die Zeilensumme echt kleiner als 0 ist. Diese Komplikationen wollen wir vermeiden und definieren

**Definition 3.14**

Die Markovkette  $X_t$  bzw. ihr Erzeuger  $Q$  heißt konservativ, wenn für alle  $i$

$$q_{ii} > -\infty$$

und

$$\sum_j q_{ij} = 0$$

gilt.

Auch die Kolmogorov-Gleichungen sind nicht immer gültig. Wir haben:

**Satz 3.6**

Wenn die Markovkette  $X_t$  konservativ ist, dann erfüllen die Übergangswahrscheinlichkeiten  $P(t)$  die Rückwärtsgleichung.

Wenn die infinitesimalen Parameter beschränkt sind, dann erfüllen die Übergangswahrscheinlichkeiten  $P(t)$  die Vorwärtsgleichung.

Im letzten Fall gilt auch bei unendlichem Zustandsraum die Gleichung

$$P(t) = e^{Qt} = \sum_{n=0}^{\infty} \frac{Q^n t^n}{n!}.$$

Wenn  $X(t)$  eine Markovkette in stetiger Zeit ist, dann ist

$$Y(n) = X(an)$$

für jedes  $a > 0$  eine Markovkette in diskreter Zeit. Wir können die Eigenschaften, die wir von den Markovketten in diskreter Zeit kennen, auf den stetigen Fall übertragen, indem wir etwa den Zustand  $i$  rekurrent nennen, wenn er für  $Y$  rekurrent ist. Wegen

$$p_{ii}(t) \geq p_{ii}\left(\frac{t}{n}\right)^n$$

ist für alle  $t$   $p_{ii}(t) > 0$ , also ist  $Y$  immer aperiodisch. Bei den anderen Eigenschaften ist eigentlich noch zu zeigen, dass ihre Definition nicht von der konkreten Diskretisierung abhängt, also dass sich für jedes  $a > 0$  dasselbe ergibt. Wir werden versuchen, diese Eigenschaften mit Hilfe von  $Q$  auszudrücken. Zuerst sehen wir uns an, wie wir den Prozess  $X_t$  simulieren können, also einen typischen Pfad erzeugen. Da wir die Übergangswahrscheinlichkeiten stetig angesetzt haben, ist es plausibel, anzunehmen, dass der Prozess eine gewisse Zeit in dem Zustand verbringt und dann in einen anderen Zustand springt. Wir beginnen mit der Wahrscheinlichkeit, dass für alle  $s \leq t$   $X(s) = i$  gilt. Dazu bestimmen wir zuerst

$$\mathbb{P}_i\left(X\left(\frac{kt}{2^n}\right) = i, k = 1, \dots, 2^n\right) = p_{ii}\left(\frac{t}{2^n}\right)^{2^n}.$$

Für  $n \rightarrow \infty$  konvergiert das wegen  $p_{ii}(t/2^n) \approx 1 + q_{ii}t/2^n$  gegen  $e^{q_{ii}t}$ . Die Zeit, die der Prozess in  $i$  verbringt, ist also exponentialverteilt mit Parameter  $-q_{ii}$ , wenn  $q_{ii}$  negativ ist. Wenn  $q_{ii} = 0$  gilt, dann gilt  $p_{ii}(t) = 1$ , also ist  $i$  absorbierend. Im anderen Fall können wir die Wahrscheinlichkeit

$$\mathbb{P}_i(X(t) = j | X(s) = i, s < t, X(t) \neq i)$$

als

$$\lim_{n \rightarrow \infty} \frac{\mathbb{P}_i(X(kt/2^n) = i, k = 1, \dots, 2^n - 1, X(t) = j)}{\mathbb{P}_i(X(kt/2^n) = i, k = 1, \dots, 2^n - 1, X(t) \neq i)} = \frac{q_{ij}}{-q_{ii}}$$

bestimmen. Wir definieren eine Übergangsmatrix  $R$  durch

$$r_{ij} = \begin{cases} \frac{q_{ij}}{-q_{ii}} & \text{wenn } q_{ii} < 0, j \neq i, \\ 1 & \text{wenn } q_{ii} = 0, j = i, \\ 0 & \text{sonst.} \end{cases}$$

Insgesamt sieht unsere Vorschrift für die Simulation einer Markovkette so aus: in einem nicht absorbierenden Zustand  $i$  bleibt der Prozess eine Zeit, die exponentialverteilt ist mit Parameter  $-q_{ii}$ , dann wird mit Wahrscheinlichkeit  $r_{ij}$  in den Zustand  $j$  gesprungen.

Die diskrete Markovkette mit  $R$ , die die Sprünge von  $X$  beschreibt, heißt die *eingebettete Markovkette*.

Diese Beschreibung funktioniert natürlich nur für konservative Markovketten. Wir können hier kurz darüber nachdenken, was geschieht, wenn die Konservativität nicht gilt: wenn  $q_{ii} = -\infty$ , dann ist für jedes  $t$  die Wahrscheinlichkeit, dass  $X(s) = i$  für alle  $s < t$  gilt, gleich 0. Der Prozess verlässt also den Zustand  $i$  sofort nach dem Betreten. Wir nennen einen solchen Zustand instabil. Ist  $q_{ii}$  endlich aber die Zeilensumme nicht 0, dann ist die Zeit, die  $X$  in  $i$  verbringt, exponentialverteilt, aber die Summe der Übergangswahrscheinlichkeiten  $r_{ij}$  ist kleiner als 1, also springt der Prozess mit positiver Wahrscheinlichkeit in keinen der anderen Zustände; er verschwindet also im Nirgendwo, von wo er allerdings sofort wieder zurückkommen muss.

Besonders schön ist der Fall, dass die eingebettete Markovkette sehr einfache Form hat, etwa, dass die Übergänge nur in Nachbarzustände erfolgen können. Ein solcher Prozess heißt Geburts- und Todesprozess.

Die allgemeine Definition ist

**Definition 3.15**

Ein Geburts- und Todesprozess ist eine Markovkette mit Zustandsraum  $\{0, 1, \dots\}$  und infinitesimalen Parametern

$$q_{00} = -\lambda_0, q_{01} = \lambda_0,$$

$$q_{i,i-1} = \mu_i, q_{ii} = -(\lambda_i + \mu_i), q_{i,i+1} = \lambda_i.$$

Die Zahlen  $\lambda_i$  heißen die Geburtsraten,  $\mu_i$  die Todesraten. Sind alle  $\mu_i = 0$ , dann sprechen wir von einem reinen Geburtsprozess, sind alle  $\lambda_i = 0$ , von einem reinen Todesprozess.

Reine Geburtsprozesse sind besonders einfach zu analysieren, weil jeweils nach einer exponentialverteilten Zeit  $\tau_i$  mit Parameter  $\lambda_i$  in den nächsthöheren Zustand  $i + 1$  gesprungen wird. Bis zum Erreichen des Zustands  $n$  (wenn in 0 gestartet wird), vergeht die Zeit

$$\tau_0 + \dots + \tau_{n-1}$$

mit Erwartungswert

$$\frac{1}{\lambda_0} + \dots + \frac{1}{\lambda_{n-1}}.$$

Wenn die Summe

$$\sum_{i=0}^{\infty} \frac{1}{\lambda_i}$$

endlich ist, dann hat die Zeit

$$\sum_{n=0}^{\infty} \tau_n$$

die benötigt wird, bis alle Zustände durchlaufen sind, endlichen Erwartungswert und ist daher endlich. Die Markovkette macht also in endlicher Zeit unendlich viele Sprünge, eine Erscheinung, die als "Explosion" bezeichnet wird. Nach diesen unendlich vielen Sprüngen ist unser Geburtsprozess erst einmal in der Unendlichkeit verschwunden. Von dort muss er natürlich sofort ins Endliche zurückkehren, das allerdings kann auf unterschiedliche Weise geschehen: wir können uns einen bestimmten Zustand aussuchen, in den gesprungen wird, oder aus mehreren nach einer Verteilung auswählen. Kurz gesagt: solange der Prozess nur endliche viele Sprünge absolviert hat, ist alles eindeutig, gibt es unendlich viele Sprünge, dann nicht mehr. Das führt uns zu der Definition

**Definition 3.16**

Eine Markovkette in stetiger Zeit heißt regulär, wenn sie in endlicher Zeit nur endlich viele Sprünge ausführt, im anderen Fall singulär..

Unser Beispiel eines singulären Geburtsprozesses (bei dem wir aus der Unendlichkeit nach 0 zurückspringen) verläuft also so, dass er immer wieder von 0 nach oben durch alle Zustände läuft.

Wenn wir diesen Prozess rückwärts laufen lassen, dann haben wir ein Beispiel für einen nicht konservativen Prozess: jetzt laufen die Zyklen aus dem Unendlichen‘ durch alle Zustände von oben nach unten und springen dann aus dem Zustand 0 nach unendlich und so weiter. Es wird immer in 0 eine exponentialverteilte Zeit verbracht, was  $q_{00} = -\lambda_0$  gibt, aber um von 0 nach  $j$  zu kommen, müssen die Zeiten  $\tau_j$  und  $\tau_{j+1}$  vergehen. Die Wahrscheinlichkeit, dass sich das in Zeit  $\leq t$  ausgeht, ist durch  $\lambda_j \lambda_{j+1} t^2$  beschränkt, und daher gilt  $q_{0j} = 0$  (und wir sehen unsere frühere Beschreibung dessen, was in einem nicht konservativen Markovkette passiert: “springt nach unendlich und läuft von dort zurück”, bestätigt).

In der Zukunft werden wir uns auf reguläre Ketten beschränken. Diese sind recht angenehm:

**Satz 3.7**

Ist  $X$  regulär, dann gelten die Vorwärts- und die Rückwärtsgleichung, und sie sind eindeutig lösbar.

Für reguläre Markovketten lassen sich alle Eigenschaften der Kette aus denen der eingebetteten Markovkette ablesen. Die Markovkette  $X$  ist etwa genau dann rekurrent, wenn die eingebettete Markovkette rekurrent ist (eine Richtung funktioniert immer: wenn die eingebettete Kette rekurrent ist, dann auch  $X$ , und  $X$  ist regulär: bis zur Explosion muss ja ein Zustand  $i$  unendlich oft besucht werden, und das braucht jedesmal im Mittel  $-1/q_i i$  Zeiteinheiten, also insgesamt unendlich lange). Für die positive Rekurrenz gilt das nicht — es ist nicht schwer, Beispiele zu konstruieren, in denen jeweils eine der beiden Ketten positiv rekurrent ist, die andere nullrekurrent. Absorptionswahrscheinlichkeiten stimmen bei beiden Ketten überein, die mittleren Absorptionszeiten haben unterschiedliche Werte.

Jedenfalls ist in regulären Ketten der Zustand  $j$  genau dann Nachfolger von  $i$ , wenn er es in der eingebetteten Kette ist. Das ist für  $j \neq i$ , dass es Zustände  $i_0 = i, \dots, i_n = j$  gibt mit  $q_{i_{l-1}i_l} \neq 0, i = 1, \dots, n$ .

Entweder über die eingebettete Markovkette, oder aus der Gleichung für die diskretisierte Kette, deren Schrittweite wir gegen 0 gehen lassen, erhalten wir die Formeln

Für die stationäre Verteilung:

$$\pi Q = 0.$$

Für die Absorptionswahrscheinlichkeiten: es wird wieder  $a_i = 1$  gesetzt, wenn  $i$  ein “guter” absorbierender Zustand ist,  $a_i = 0$  für “schlechte”, und wenn  $i$  nicht absorbierend ist, dann

$$\sum_j q_{ij} a_j = 0.$$

Wie im diskreten Fall kann es sein, dass diese Gleichung nicht eindeutig lösbar ist. Dann ist wieder die kleinste mit  $a_i \geq 0$  die richtige.

Mittlere Absorptionszeiten:  $m_i$  ist wieder 0, wenn  $i$  absorbierend ist, sonst gilt

$$\sum_j q_{ij} m_j = 0.$$

# Kapitel 4

## Informationstheorie

Was sind das für Zeiten, wo  
Ein Gespräch über Bäume fast ein  
Verbrechen ist  
Weil es ein Schweigen über so viele  
Untaten einschließt!

---

B. Brecht, "An die Nachgeborenen"

### 4.1 Entropie und Information

Das Bar Kochba Spiel: Spieler A wählt einen aus einer Menge  $M$  von  $m$  Gegenständen. Spieler B muss herausfinden, welcher es ist, und darf dazu nur Fragen stellen, die A mit ja oder nein beantworten kann. Wenn A betrügen kann und sich nur nicht widersprechen darf, dann sieht man leicht, dass mit optimaler Strategie ein Spiel genau

$$H^*(m) = \lceil \log_2(m) \rceil$$

Runden dauert: einerseits gibt es bei  $k$  Fragen  $2^k$  mögliche Kombinationen von "ja"- und "nein"-Antworten. Für jedes der  $m$  zu wählenden Elemente muss es eine solche Kombination geben, die es definiert, also ergibt sich  $2^k \geq m$ . Auf der anderen Seite können wir mit jeder Frage die Anzahl der noch in Frage kommenden Gegenstände (ungefähr) halbieren: wenn  $2^{k-1} < m \leq 2^k$  ist, dann wäre die erste Frage beispielsweise "ist die Nummer (wir müssen die Gegenstände zuerst von 0 bis  $m-1$  durchnummerieren)  $< 2^{k-1}$ ?", je nach Ausgang dieser Frage ist die nächste Frage "ist die Nummer  $< 2^{k-2}$ ?" oder "ist die Nummer  $< 3^{k-2}$ ?" und so weiter — das ist äquivalent dazu, dass man die  $k$  Binärziffern der Nummer der Reihe nach abfragt.

Durch einen Trick können wir das Aufrunden loswerden: statt nur nach einem Element der Menge  $M$  zu fragen, fragen wir nach  $n$  Elementen gleichzeitig, als nach einer Folge  $(x_1, \dots, x_n) \in M^n$ . Es gibt  $m^n$  solche Folgen. Um eine davon zu identifizieren, benötigen wir  $H^*(m^n)$  Fragen. Das liegt zwischen  $\log_2(m^n) = n \log_2(m)$  und  $n \log_2(m) + 1$ . Pro einzeltem Element sind das  $H^*(m^n)/n$  Fragen, und das konvergiert für  $n \rightarrow \infty$  gegen  $\log_2(m)$ . Das führt uns zu der Definition

#### Definition 4.1

$$H^*(m) = \lceil \log_2(m) \rceil$$

heißt die maximale Unbestimmtheit,

$$M(m) = \log_2(m)$$

die Entropie von  $m$ .

Diese Situation wird uns in der Informationstheorie öfter begegnen: es gibt einen optimalen Wert, der nicht in allen Fällen direkt erreicht werden kann, an den man aber mit großen Blöcken beliebig nahe herankommen kann (zumindest mit einer Wahrscheinlichkeit, die beliebig nahe an 1 gewählt werden kann).

Von nun an werden wir die Elemente von  $M$  durchnummerieren und durch ihre Nummern ersetzen, wir setzen also  $M = \{1, \dots, m\}$ . Die Fragen, die wir stellen, können wir durch die Teilmenge von  $M$  darstellen, für die die Frage mit “ja” beantwortet wird. Wenn die Sprache, die wir verwenden, um unsere Fragen zu formulieren, hinreichend aussagekräftig ist, können wir auch zu jeder Menge eine Frage finden, die genau dieser Menge entspricht (die langweiligste Idee ist wohl: “ist  $x$  in  $A$  enthalten?”).

Fragestrategien können wir durch Binärbäume darstellen:

#### Definition 4.2

Ein Binärbaum ist ein gerichteter zyklusfreier Graph, bei dem aus jedem Knoten höchstens zwei Kanten entspringen. Es gibt einen ausgezeichneten Knoten, die Wurzel, in der keine Kante endet. In jedem anderen Knoten endet genau eine Kante. Ein Knoten, aus dem keine Kante entspringt, heißt Endknoten oder Blatt, alle anderen heißen innere Knoten. Wenn aus jedem inneren Knoten genau zwei Kanten entspringen, dann nennen wir den Baum vollständig. Der Abstand eines Blattes von der Wurzel heißt die Blattlänge dieses Blattes, das Maximum aller Blattlängen ist die Höhe des Baums.

Unsere Fragebäume werden nun so konstruiert: an die inneren Knoten, ausgehend Wurzel des Baumes setzen wir die jeweilige Frage, ist die Antwort “ja”, dann gehen wir zum linken Nachfolger, sonst zum rechten. An die Endknoten setzen wir die Elemente, die wir dort eindeutig bestimmt haben. In Abbildung 4.1 ist der Fragebaum für eine optimale Strategie für  $m = 5$  dargestellt.

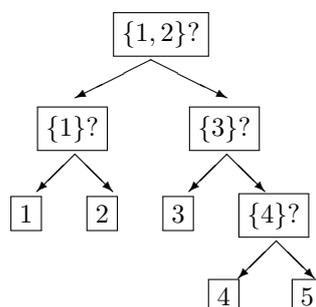


Abbildung 4.1: Ein Fragebaum

Wir ändern die Regeln des Spiels jetzt so ab, dass A nicht mehr betrügen darf und seine Auswahl zufällig mit Verteilung  $P = (p_1, \dots, p_m)$  wählt. Wir wollen die Strategie finden, bei der der Erwartungswert der Anzahl der Fragen minimal wird. Diesen Minimalwert nennen wir die mittlere Unbestimmtheit  $H^*(P)$ . Um ihn zu bestimmen, müssen wir die optimale Strategie finden. Das geht mit dem Huffman-Algorithmus: zuerst stellen wir fest, dass wir jede Fragestrategie durch einen Binärbaum repräsentieren können, und dass umgekehrt jedem solchen Baum eine Fragestrategie entspricht. Ist nämlich ein Baum gegeben, dessen Blätter von 1 bis  $m$  numeriert sind, können wir in zu einem Fragebaum machen, indem wir an jeden inneren Knoten als Frage die Menge aller Blätter setzen, die zum linken Teilbaum unter diesem Knoten gehören.

Die Blattlänge  $l_i$  des Blattes, das dem Element  $i$  entspricht, ist genau die Anzahl der Fragen, die benötigt werden, um dieses Element zu identifizieren. Die mittlere Anzahl von Fragen ist also gleich der mittleren Blattlänge

$$\sum_{i=1}^m p_i l_i.$$

Wir suchen also einen Binärbaum mit  $m$  Blättern, für den die mittlere Blattlänge minimal ist. Wir könnten versuchen, die Idee zu kopieren, die bei der maximalen Unbestimmtheit erfolgreich war, nur wollen wir jetzt statt der Anzahlen die Wahrscheinlichkeiten aufteilen. Versuchen wir das an der Verteilung  $P = (0.1, 0.2, 0.3, 0.4)$ : wir können hier sogar perfekt halbieren, indem wir 1 und 4 bzw. 2 und 3 zusammenfassen. Der komplette Baum sieht dann so aus wie in Abbildung 4.2.

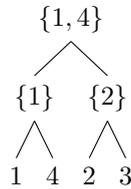


Abbildung 4.2: Halbieren: leider nicht optimal

Dieser Baum ist offensichtlich nicht optimal: die mittlere Blattlänge ist 2 und damit größer als für die Strategie in Abbildung 4.3, in der wir einfach der Reihe nach fragen ob es sich um 4, 3 oder 2 handelt, was uns eine mittlere Fragenanzahl von  $0.4 \cdot 1 + 0.3 \cdot 2 + (0.2 + 0.1) \cdot 3 = 1.9$  liefert.

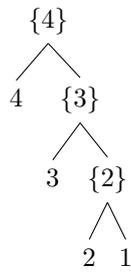


Abbildung 4.3: Eine bessere Strategie

Wir denken also darüber nach, wie ein optimaler Baum aussehen muss. Zuerst kann man ohne weitere Veränderungen am Baum versuchen, die Zuordnung der Zahlen 1 bis  $m$  zu den Endknoten zu optimieren: es ist recht offensichtlich, dass die kleinste mittlere Blattlänge dann erreicht wird, wenn die Wahrscheinlichkeiten in umgekehrter Reihenfolge geordnet werden wie die Blattlängen. Wenn die Numerierung so vorgenommen wird, dass  $p_1 \geq p_2 \geq \dots \geq p_m$  gilt, dann muss die Zuordnung zu den Blättern so vorgenommen werden, dass  $l_1 \geq l_2 \geq \dots \geq l_m$  gelten. Als nächstes geht es an die Struktur des Baumes. Ein optimaler Baum muss vollständig sein: ein innerer Knoten, von dem nur eine Kante ausgeht, entspricht einer Frage, deren Antwort man schon kennt, und kann daher weggelassen werden. Dann betrachten wir die Blätter  $m$  und  $m - 1$ . Diese haben die kleinsten Wahrscheinlichkeiten  $p_m$  und  $p_{m-1}$  und damit die beiden größten Blattlängen  $l_m$  und  $l_{m-1}$ . Weil der Baum vollständig ist, muss  $l_m = l_{m-1}$  gelten. Wir können ohne Beschränkung der Allgemeinheit annehmen, dass die Knoten  $m$  und  $m - 1$  am selben (direkten) Vorgänger hängen. Wenn wir jetzt diese beiden Knoten entfernen, erhalten wir eine Baum mit  $m - 1$  Blättern, in dem der gemeinsame Vorgänger von  $m$  und  $m - 1$  zu einem neuen Blatt (mit Gewicht  $p_m + p_{m-1}$  geworden ist. Man kann also den (einen) optimalen Baum rekursiv mit dem Huffman-Algorithmus konstruieren:

**Satz 4.1: Huffman**

Einen optimalen Baum für die Verteilung  $P = (p_1, \dots, p_m)$  kann man folgendermaßen konstruieren:

1. Wenn  $m = 1$ , dann besteht der Baum nur aus der Wurzel, Ende.
2. Ordne die Wahrscheinlichkeiten:  $p_1 \geq \dots \geq p_m$ .

3. Fasse die kleinsten Wahrscheinlichkeiten zusammen:  $p_{m-1}^* = p_{m-1} + p_m$ ,
4. Konstruiere den optimalen Baum für  $P^* = (p_1, \dots, p_{m-2}, p_{m-1}^*)$
5. Ersetze Blatt  $m - 1$  durch einen inneren Knoten mit den Blättern  $m - 1$  und  $m$ .

Wenn wir dieses Verfahren auf unser Beispiel  $P = (0.1, 0.2, 0.3, 0.4)$  anwenden, dann müssen wir zuerst die Knoten 1 und 2 zusammenfassen. Das ergibt jetzt drei Knoten mit den Wahrscheinlichkeiten  $(0.3, 0.3, 0.4)$ . Im nächsten Schritt werden wieder die beiden ersten Knoten zusammengefasst. Im Endeffekt ergibt sich genau der Baum aus Abbildung 4.3, der sich also jetzt als optimal herausstellt.

Die Bestimmung des Huffman-Baums erfordert zumindest eine Sortierung, die relativ kostspielig ist, was den Zeitaufwand betrifft (das Sortieren in jedem Schritt, das in unserer Beschreibung steht, lässt sich leicht vermeiden), also wäre es schön, wenn wir zumindest eine gute Abschätzung hätten, die sich mit weniger Aufwand berechnen lässt. Wir kehren also wieder zurück zu dem Problem, dass wir unter allen Binärbäumen denjenigen suchen, für den

$$\sum p_i l_i$$

minimal wird, wobei  $l_i$  die Blattlänge des Blatts mit dem Index  $i$  ist. Für diese Aufgabe ist es nützlich zu wissen, wann ein Binärbaum mit den Blattlängen  $l_1, \dots, l_m$  existiert:

**Satz 4.2: Ungleichung von Kraft**

Ein Binärbaum mit den Blattlängen  $l_1, \dots, l_m$  existiert genau dann, wenn

$$\sum_{i=1}^m 2^{-l_i} \leq 1.$$

Gleichheit gilt genau dann, wenn der Baum vollständig ist.

In jeder Richtung erfolgt der Beweis durch Induktion nach der Höhe des Baumes. Die eine Richtung (jeder Baum erfüllt die Ungleichung mit Gleichheit, wenn der Baum vollständig ist) ist für Höhe 0 offensichtlich: dann gibt es einen Knoten, die Wurzel, die gleichzeitig das einzige Blatt ist und Höhe 0 hat. Dieser Baum ist auch vollständig, und die Kraftsche Ungleichung gilt mit Gleichheit. Ist die Höhe positiv, dann ist die Wurzel ein innerer Knoten, an dem ein oder zwei Teilbäume hängen. Der linke davon soll  $m'$  Blätter mit den Längen  $l'_1, \dots, l'_{m'}$ , der rechte  $m''$  Blätter mit den Längen  $l''_1, \dots, l''_{m''}$ . Nach der Induktionsvoraussetzung gilt in jedem dieser Teilbäume die Kraftsche Ungleichung; für den Ursprünglichen Baum gilt  $m = m' + m''$  und  $l_i = 1 + l'_i$  für  $i \leq m'$  und  $l_i = 1 + l''_{i-m'}$  für  $m' < i \leq m' + m''$ . Das ergibt

$$\sum_{i=1}^m 2^{-l_i} = \frac{1}{2} \left( \sum_{i=1}^{m'} 2^{-l'_i} + \sum_{i=1}^{m''} 2^{-l''_i} \right) \leq 1.$$

Ist der Baum vollständig, dann sind das auch die Teilbäume, und es gilt Gleichheit.

Für die andere Richtung beginnen wir wieder mit Höhe 0; wenn die Kraftsche Ungleichung gilt, muss  $m = 1$  und  $l_1 = 0$  gelten, und wir sind wieder bei unserem einen Knoten. Wir nehmen an, dass  $l_1 \geq \dots \geq l_m$  und

$$S = \sum_{i=1}^m 2^{-l_i} \leq 1$$

gilt.  $l_m$  ist die Höhe des Baums. Es gilt

$$S = \sum_{i=1}^m 2^{l_m - l_i} \leq 2^{l_m}.$$

Auf beiden Seiten stehen ganze Zahlen, die rechte Seite ist gerade, und auf der linken Seite steht für jedes  $l_i$ , das mit  $l_m$  übereinstimmt, eine 1 und für jedes andere eine gerade Zahl. Ist die linke Seite

ungerade, dann können wir noch eine Zahl  $l_{m+1} = l_m$  hinzufügen, und die Kraftsche Ungleichung gilt mit diesem zusätzlichen Summanden immer noch. Wir dürfen also annehmen, dass es eine gerade Anzahl von Indizes  $i$  mit  $l_i = l_m$  gibt. Wir ersetzen jeweils zwei Zahlen  $l_m$  durch eine mit dem Wert  $l_m - 1$ . Dadurch behält die Summe  $S$  ihren Wert, und weil wir die Höhe um 1 kleiner gemacht haben, gibt es nach Induktionsvoraussetzung einen Baum mit diesen kürzeren Blattlängen. Wenn wir jetzt an die Blätter mit Blattlänge  $l_m - 1$  die für zwei Werte  $l_m$  stehen, zwei Nachfolger anhängen, erhalten wir einen Baum mit den ursprünglichen  $l_1, \dots, l_m$  als Blattlängen. Es folgt also aus der Gültigkeit der Kraftschen Ungleichung die Existenz eines entsprechenden Baumes. Ist  $S = 1$ , dann ist auch für den verkürzten Baum in der Kraftschen Ungleichung Gleichheit vorhanden, also ist dieser verkürzte Baum vollständig, und er bleibt es auch, wenn wir aus einigen seiner Blätter innere Knoten mit zwei Blättern als Nachfolger machen.

Die Suche nach der optimalen Strategie besteht also darin,

$$\sum p_i l_i$$

unter der Nebenbedingung

$$\sum 2^{-l_i} \leq 1$$

zu minimieren. Es ist leicht einzusehen, dass im optimalen Fall in der letzten Ungleichung Gleichheit gelten muss (sonst könnten wir einfach das größte  $l_i$  verkleinern). Wenn wir die Forderung, dass  $l_i$  ganzzahlig sein muss, beiseite lassen, lässt sich das Minimum mit der Lagrange-Methode bestimmen und hat den Wert

$$\sum p_i \log_2(1/p_i).$$

Deswegen definieren wir

**Definition 4.3**

Die Entropie der Verteilung  $P$  ist

$$H(P) = \sum_{i=1}^m p_i \log_2(1/p_i) = - \sum_{i=1}^m p_i \log_2(p_i).$$

Für eine Zufallsvariable  $X$  mit Verteilung  $P_X$  ist

$$H(X) = H(P_X).$$

**Satz 4.3**

$$H(P) \leq H^*(P) \leq H(P) + 1.$$

Die untere Abschätzung haben wir oben gezeigt, die obere folgt aus der Tatsache, dass  $l_i = \lceil \log_2(1/p_i) \rceil$  die Kraft'sche Ungleichung erfüllt.

Der Summand 1 in der oberen Abschätzung stört ein wenig; man kann diese Differenz verringern, indem man statt eines einzelnen Elements mehrere (unabhängige und identisch verteilte) errät, sagen wir  $n$ . Die Entropie der gemeinsamen Verteilung ist (wie weiter unten gezeigt wird)  $nH(P)$ , damit lässt sich die mittlere Anzahl der Fragen, um den gesamten Block zu erraten, mit  $nH(P) + 1$  abschätzen, pro Element ergibt das  $H(P) + 1/n$ , was beliebig nahe an die Entropie herankommt.

Die Formel für die Entropie legt nahe, dass in der optimalen Strategie für das erraten von  $i$  etwa  $\log_2(\frac{1}{p_i})$  Fragen nötig sind. Das ist zwar nicht ganz richtig (einerseits ist für  $m = 2$  immer  $l_i = 1$ , egal wie groß oder klein die Wahrscheinlichkeiten sind; in der anderen Richtung wird in den Übungen gezeigt, dass

$$l_i \leq \log_\tau\left(\frac{1}{p_i}\right) + 1$$

gilt. Dabei ist  $\tau = \frac{1+\sqrt{5}}{2} \approx 1.618$  der goldene Schnitt. Dieser Logarithmus ist etwa um den Faktor 1.44 größer als der Zweierlogarithmus), ist aber gelegentlich hilfreich, um Ergebnisse zu motivieren.

Wir betrachten etwa den Fall, dass wir eine Zufallsvariable  $X$  mit Verteilung  $P$  erraten müssen, aber die optimale Strategie für eine andere Verteilung  $Q$  verwenden. Wenn wir annehmen, dass die Anzahl der Fragen für Ausgang  $i$  gleich  $\log_2(1/q_i)$  ist, dann brauchen wir im Mittel

$$\sum p_i \log_2(1/q_i)$$

Fragen statt

$$\sum p_i \log_2(1/p_i),$$

also um

$$\sum p_i \log_2(p_i/q_i)$$

Fragen zuviel.

Das führt uns zu der Definition

**Definition 4.4**

$$D(P, Q) = \sum_i p_i \log_2(p_i/q_i).$$

heißt die Informationsdivergenz (I-Divergenz, Kullback-Leibler Information, relative Entropie, Strafe des Irrtums) zwischen  $P$  und  $Q$ .

Die plausible Folgerung aus unseren vorigen Überlegungen ist

**Satz 4.4**

Die I-Divergenz ist nichtnegativ

$$D(P, Q) \geq 0,$$

mit Gleichheit für  $P = Q$ .

Für den Beweis verwenden wir die Ungleichung

$$\log(x) \leq x - 1$$

(mit Gleichheit für  $x = 0$ ), die aus der bekannten Ungleichung

$$e^x \geq 1 + x$$

folgt. Damit ist

$$-D(P, Q) = \frac{1}{\log 2} \sum_i p_i \log\left(\frac{q_i}{p_i}\right) \leq \frac{1}{\log 2} \sum_i p_i \left(\frac{q_i}{p_i} - 1\right) = \frac{1}{\log 2} \sum_i (p_i - q_i) = 1 - 1 = 0.$$

Damit Gleichheit gilt, müssen alle Ungleichungen für die Logarithmen in der Summe Gleichungen sein, also  $q_i/p_i = 1$  bzw.  $p_i = q_i$ .

Wenn  $X$  und  $Y$  zwei Zufallsvariable sind, können wir  $(X, Y)$  als eine Zufallsvariable mit endlich vielen Werten ansehen und die gemeinsame Entropie  $H(X, Y) = H((X, Y))$  betrachten. Wir setzen

$$p(x|y) = \mathbb{P}(X = x|Y = y)$$

und definieren

**Definition 4.5**

$$H(X|Y = y) = - \sum_x p(x|y) \log_2(p(x|y))$$

und nennen

$$H(X|Y) = \sum_y p_Y(y) H(X|Y = y)$$

die bedingte Entropie von  $X$  unter  $Y$ .

Es gilt

**Satz 4.5**

$$\begin{aligned} H(X, Y) &= H(Y) + H(X|Y), \\ \max(H(X), H(Y)) &\leq H(X, Y) \leq H(X) + H(Y), \\ H(X|Y) &\leq H(X), \\ H(X|Y, Z) &\leq H(X|Y), \\ H(X, Y) &= H(X) + H(Y) \end{aligned}$$

gilt genau dann, wenn  $X$  und  $Y$  unabhängig sind.

$$H(X, Y) = H(X)$$

gilt genau dann, wenn es eine Funktion  $g$  gibt, sodass  $Y = g(X)$ .

**Definition 4.6**

$$I(X, Y) = H(X) + H(Y) - H(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

heißt die Information zwischen  $X$  und  $Y$ .

Der letzte Satz impliziert

**Satz 4.6**

$$0 \leq I(X, Y) \leq \min(H(X), H(Y)).$$

Die Information ist genau dann 0, wenn  $X$  und  $Y$  unabhängig sind.  $I(X, Y) = H(X)$  gilt genau dann, wenn  $X = g(Y)$  gilt, also wenn  $X$  eindeutig aus  $Y$  bestimmt werden kann.

Wenn  $X$  aus  $Y$  zwar nicht mit absoluter Sicherheit, aber mit großer Wahrscheinlichkeit bestimmt werden kann, dann unterscheidet sich die Information nur wenig von der Entropie von  $X$ :

**Satz 4.7**

Wenn  $\mathbb{P}(X \neq Y) \leq \epsilon$  ist, dann gilt

$$I(X, Y) \geq H(X) - H(\epsilon, 1 - \epsilon) - \epsilon \log_2(m).$$

## 4.2 Codes

Eine Fragestrategie kann auch unter einem anderen Gesichtspunkt gesehen werden, nämlich indem für jede Frage die Antwort "nein" mit einer 0, die Antwort "ja" mit einer 1 codiert wird. Codes, die auf diese Weise gewonnen werden, haben eine wichtige Eigenschaft — sie sind präfixfrei, d.h. kein Codewort ist Präfix (Anfangsstück) eines anderen. Diese Eigenschaft wird auch als fortlaufende Entzifferbarkeit bezeichnet, weil an jeder Stelle der codierten Nachricht festgestellt werden kann, ob dort ein Codewort endet, ohne dass die nachfolgenden Zeichen bekannt sind (man erkennt leicht, dass dies genau bei den präfixfreien Codes der Fall ist. Der Huffmancode ist damit der

optimale präfixfreie Code, also der mit der kleinsten mittleren Codewortlänge. Allerdings gibt es nicht “den” Huffmancode, weil sich durch Spiegeln des Baumes oder von Teilen davon andere Codes ergeben. Außerdem kann es mehrere äquivalente Möglichkeiten geben, Knoten zusammenzufassen, etwa für die Verteilung  $P = (0.2, 0.2, 0.2, 0.4)$ , für die  $(00, 01, 10, 11)$  und  $(000, 001, 01, 1)$  beides Huffmancodes sind. Das zweite Problem ist nicht so groß, für das erste gibt es den kanonischen Huffmancode.

**Definition 4.7**

Für einen Präfixfreien Code mit den Codewortlängen  $l_1, \dots, l_m$  wird der kanonische Code folgendermaßen konstruiert:

1. Die Wortlängen werden aufsteigend geordnet:  $l_1 \leq \dots \leq l_m$ .
2. Bei gleichen Wortlängen werden die entsprechenden Quellbuchstaben in ihrer natürlichen Reihenfolge geordnet.
3.  $c_1$  besteht aus  $l_1$  Nullen.
4.  $c_{i+1}$  wird aus  $c_i$  erhalten, indem 1 addiert wird ( $c_i$  wird als Binärzahl interpretiert), und dann werden  $l_{i+1} - l_i$  Nullen angehängt.

Das ist gleichbedeutend damit, dass  $c_i$  aus den ersten  $l_i$  Nachkommastellen von

$$\sum_{j=1}^{i-1} 2^{-l_j}$$

besteht. Der kanonische Huffmancode wird erhalten, wenn die Wortlängen mit dem Huffmanalgorithmus bestimmt werden.

Kanonische Codes haben den Vorteil, dass statt der kompletten Codewörter für jeden Quellbuchstaben nur ihre Längen übertragen werden müssen.

**Beispiel 4.1**

Es muss wieder  $P = (0.1, 0.2, 0.3, 0.4)$  erhalten:

$i$	$x_i$	$l_i$	$c_i$
1	4	1	0
2	3	2	10
3	2	3	110
4	1	3	111

Einen anderen Code mit fast optimaler Codewortlänge erhalten wir, wenn wir von unserer oberen Abschätzung für die Entropie ausgehen. Wir wollen also einen Code mit Codewortlängen  $l_i = \lceil \log_2(1/p_i) \rceil$  explizit angeben. Dazu ordnen wir die Wahrscheinlichkeiten absteigend ( $p_1 \geq \dots \geq p_m$ ) und setzen  $f_i = \sum_{j=1}^i p_j$ . Das Codewort  $c_i$  erhalten wir, indem wir  $f_{i-1}$  als Binärzahl darstellen und die ersten  $l_i$  Nachkommastellen als Code verwenden. Es ist nicht schwer einzusehen, dass dadurch ein präfixfreier Code definiert wird, der Shannon-Code. Der einzige Schönheitsfehler dabei ist, dass die Wahrscheinlichkeiten geordnet werden müssen. Diesen Schönheitsfehler behebt der Fano-Code: mit denselben Notationen wie vorhin (abgesehen davon, dass die Wahrscheinlichkeiten nicht geordnet werden müssen) codiert man  $(f_{i-1} + f_i)/2$  mit  $\lceil \log_2(1/p_i) \rceil + 1$  Bits.

**Beispiel 4.2**

Diese Codes werden wir jetzt für unser Standardbeispiel  $P = (0.1, 0.2, 0.3, 0.4)$  konstruieren. Zuerst den Shannon-Code. Für diesen müssen wir die Wahrscheinlichkeiten absteigend ordnen:

$i$	$x_i$	$p_i$	$l_i$	$f_{i-1}$		Codewort
				dezimal	binär	
1	4	0.4	2	0	0.00000000...	00
2	3	0.3	2	0.4	0.01100110...	01
3	2	0.2	3	0.7	0.10110011...	101
4	1	0.1	4	0.9	0.11100110...	1110

Für den Fanocode brauchen wir nicht zu ordnen, aber dafür sind die Codewörter einen Buchstaben länger.

$i$	$p_i$	$l_i$	$(f_i + f_{i-1})/2$		Codewort
			dezimal	binär	
1	0.1	5	0.05	0.00001101...	00001
2	0.2	4	0.2	0.00110011...	0011
3	0.3	3	0.45	0.01110011...	011
4	0.4	3	0.8	0.11001100...	110

In diesen Tabellen haben wir die Darstellung als Binärbruch aus Anschaulichkeitsgründen auf 8 Stellen ausgeschrieben. Etwas einfacher ist es, die Wahrscheinlichkeitswerte mit  $2^{l_i}$  zu multiplizieren und den ganzzahligen Anteil des Produkts als Binärzahl, eventuell mit führenden Nullen, darzustellen. Für die Codierung von "2" im Shannon-Code sieht das so aus: Der  $f$ -Wert 0.7 wird mit  $2^3 = 8$  multipliziert, und das Codewort wird erhalten, indem der ganzzahlige Anteil (5) mit drei Binärstellen geschrieben wird.

Diese Idee kann man auf das Kodieren von ganzen Blöcken anwenden, im Extremfall wird die ganze Nachricht als einzelner Block kodiert. Im Vergleich zum Huffman-Code ist das hier möglich, weil nicht der ganze Code generiert werden muss, sondern nur das eine Wort, das die Nachricht kodiert. Verfahren, die auf dieser Idee beruhen, werden als arithmetische Codes bezeichnet.

Außer den präfixfreien Codes gibt es auch noch andere, die eindeutig entziffert werden können. Wir definieren

**Definition 4.8**

1. Ein Code heißt endlich eindeutig entzifferbar, wenn jede endliche Aneinanderreihung von Codewörtern eindeutig in Codewörter zerlegt werden kann.
2. Ein Code heißt eindeutig entzifferbar (manchmal zur Unterscheidung von 1. unendlich eindeutig entzifferbar), wenn jede endliche oder unendliche Aneinanderreihung von Codewörtern eindeutig zerlegt werden kann.

Der Code  $\{0,01\}$  ist offensichtlich nicht präfixfrei, aber trotzdem eindeutig entzifferbar, für die korrekte Zerlegung muss man allerdings das nachfolgende Zeichen kennen. Der Code  $\{0,01,11\}$  ist endlich eindeutig entzifferbar, aber nicht eindeutig entzifferbar.

Wir können nun die Frage stellen, ob durch den Verzicht auf die fortlaufende Entzifferbarkeit etwas gewonnen werden kann, also ob es einen endlich eindeutig entzifferbaren Code gibt, der kleiner mittlere Codewortlänge hat als der Huffman-Code. Diese Hoffnung ist allerdings vergebens, denn es gilt

**Satz 4.8**

Die Codewortlängen in einem endlich eindeutig entzifferbaren Code erfüllen die Kraft'sche Ungleichung.

Aus diesem Satz folgt, dass es zu jedem endlich eindeutig entzifferbaren Code einen präfixfreien Code mit denselben Codewortlängen (und damit mit derselben mittleren Codewortlänge) gibt. (universelle Codes)

### 4.3 Informationsquellen

**Definition 4.9**

Eine Informationsquelle ist eine Folge  $\mathcal{X} = (X_1, \dots)$  von Zufallsvariablen.

Die verschiedenen Möglichkeiten für die Abhängigkeitsstruktur dieser Folge ergeben die Definitionen

**Definition 4.10**

Wenn die Zufallsvariablen  $X_n$  unabhängig und identisch verteilt sind, dann heißt  $\mathcal{X}$  gedächtnislos.

Wenn  $(X_n)$  eine Markovkette bilden oder stationär sind, dann heißt die Quelle Markovquelle bzw. stationäre Quelle. Eine irreduzible Markovquelle nennen wir ergodisch.

Eine wichtige Größe ist die Entropie einer Quelle. Im Sinne der Idee, die wir bei der Einführung der Entropie verwendet haben, definieren wir sie über die mittlere Codewortlänge beim optimalen Kodieren von langen Blöcken:

**Definition 4.11**

Die Entropie der Quelle  $\mathcal{X}$  ist

$$H(\mathcal{X}) = \lim_{n \rightarrow \infty} \frac{1}{n} H(X_1, \dots, X_n),$$

wenn dieser Grenzwert existiert (wenn nicht, dann hat  $\mathcal{X}$  keine Entropie).

Für eine gedächtnislose Quelle gilt

$$H(\mathcal{X}) = H(X_1).$$

Für eine (irreduzible) Markovquelle mit Übergangsmatrix  $P$  ergibt sich

$$H(\mathcal{X}) = \sum \pi_i H(P_i),$$

wobei  $P_i$  die  $i$ -te Zeile von  $P$  und  $\pi$  die stationäre Verteilung ist.

Für eine stationäre Quelle existiert die Entropie.

**Satz 4.9: Shannon-MacMillan**

Für eine stationäre Quelle gilt

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log_2 p(X_1, \dots, X_n) = -nH(\mathcal{X})$$

in Wahrscheinlichkeit.

Das kann man so sehen, dass mit hoher Wahrscheinlichkeit gilt, dass die Wahrscheinlichkeit, genau die Folge  $(X_1, \dots, X_n)$  zu ziehen  $\approx 2^{-nH(\mathcal{X})}$  ist.

**4.4 Blockcodes****4.5 Kanalcodierung****4.6 Natürliche Sprachen als Informationsquellen**

# Kapitel 5

## Statistik

Die Statistik (genauer: die schließende Statistik, mit der wir uns hier beschäftigen; es gibt auch die beschreibende Statistik mit der Aufgabe, große Datenmengen überschaubar zusammenzufassen) hat die Aufgabe, aufgrund einer Stichprobe Aussagen über die Grundgesamtheit zu treffen. Wenn aus einer endlichen Menge mit Zurücklegen gezogen wird, dann sind die einzelnen Ziehungsergebnisse unabhängig und haben als Verteilung die Häufigkeitsverteilung aus der Grundgesamtheit. Unsere Annahmen über diese zugrundeliegende Verteilung fassen wir in einem statistischen Modell zusammen:

### Definition 5.1

Ein statistisches Modell ist eine Menge  $\mathcal{P}$  von Verteilungen. Wenn diese Verteilungen durch endlich viele reelle Zahlen (die Parameter) beschrieben werden können, also

$$\mathcal{P} = \{P_\theta, \theta \in \Theta\}$$

mit  $\Theta \subseteq \mathbb{R}^d$ , dann sprechen wir von einem parametrischen Modell, sonst von einem nichtparametrischen Modell.

Eine Stichprobe ist eine Folge  $(X_1, \dots, X_n)$  von unabhängigen Zufallsvariablen mit einer (unbekannten) Verteilung aus  $\mathcal{P}$ .

### Definition 5.2

Eine Statistik  $T$  ist eine Zufallsvariable, die aus der Stichprobe berechnet werden kann:

$$T = T(X_1, \dots, X_n)$$

Insbesondere dürfen in dieser Funktion die unbekannt Parameter nicht vorkommen.

## 5.1 Schätztheorie

### 5.1.1 Punktschätzung

Die erste Aufgabe, mit der wir uns beschäftigen, besteht darin, aus einer Stichprobe Schätzwerte für den unbekannt Parameter zu bestimmen. Wir definieren

### Definition 5.3

Ein Schätzer ist eine Folge  $(\hat{\theta}_n)$  von Statistiken.

Diese Definition lässt recht dumme Schätzer zu (z.B. 42, vgl. Douglas Adams), deshalb definieren wir einige Eigenschaften, die wir von Schätzern verlangen können:

**Definition 5.4**

Ein Schätzer heißt

- schwach konsistent, wenn  $\hat{\theta}_n \rightarrow \theta$  in Wahrscheinlichkeit konvergiert (also  $\mathbb{P}_\theta(|\hat{\theta}_n - \theta| > \epsilon) \rightarrow 0$  für alle  $\epsilon > 0$ ).
- stark konsistent, wenn  $\hat{\theta}_n \rightarrow \theta$  mit Wahrscheinlichkeit 1 konvergiert (also  $\mathbb{P}_\theta(\hat{\theta}_n \rightarrow \theta) = 1$ ).
- erwartungstreu, wenn
 
$$\mathbb{E}_\theta(\hat{\theta}_n) = \theta.$$
- effizient, wenn er erwartungstreu ist und die kleinste Varianz unter allen erwartungstreuen Schätzern hat.

Eine Methode, um Schätzer zu konstruieren, ist die Momentenmethode. Ihr liegt das Gesetz der großen Zahlen zugrunde. Am einfachsten geht das, wenn es nur einen Parameter gibt. Dann können wir den Erwartungswert von  $X$  als Funktion von  $\theta$  schreiben:

$$\mathbb{E}_\theta(X) = m(\theta).$$

Wenn die Funktion  $m$  stetig umkehrbar ist, dann ist

$$\hat{\theta}_n = m^{-1}(\bar{X}_n)$$

ein (stark) konsistenter Schätzer.

Wenn es  $d > 1$  Parameter gibt, dann verwendet man zusätzlich höhere Momente:

$$\mathbb{E}_\theta(X^i) = \frac{1}{n} \sum_{j=1}^n X_j^i, \quad i = 1, \dots, d$$

und löst nach  $\theta$  auf.

Die andere Methode, die wir hier betrachten, ist die Maximum Likelihood Methode: Wenn die Wahrscheinlichkeit, die aktuelle Stichprobe zu erhalten, für einen Parameter sehr klein ist, spricht das gegen diesen Parameter. Umgekehrt heißt das, dass ein Parameterwert umso plausibler ist, je größer die Wahrscheinlichkeit der Stichprobe unter diesem Parameter ist.

**Definition 5.5**

Die Likelihoodfunktion ist

$$L(X_1, \dots, X_n; \theta) = \prod_{i=1}^n p_\theta(X_i),$$

wenn  $P_\theta$  diskret mit Wahrscheinlichkeitsfunktion  $p$  ist, und

$$L(X_1, \dots, X_n; \theta) = \prod_{i=1}^n f_\theta(X_i),$$

wenn  $P_\theta$  stetig mit Dichte  $f$  ist.

**Definition 5.6**

Der Maximum-Likelihood (ML-) Schätzer ist der Wert von  $\theta$ , der die Likelihoodfunktion maximiert.

Damit der ML-Schätzer konsistent ist, müssen die Dichten gewisse Regularitätsvoraussetzungen erfüllen. Bei der Suche nach einem effizienten Schätzer hilft der

**Satz 5.1: Cramér-Rao**

Wenn  $p_\theta$  bzw.  $f_\theta$  zweimal nach  $\theta$  differenzierbar ist und zusätzliche Regularitätsvoraussetzungen erfüllt, dann gilt für jeden Erwartungstreuen Schätzer  $\hat{\theta}_n$

$$\mathbb{V}(\hat{\theta}_n) \geq \frac{1}{I_n(\theta)} = \frac{1}{nI(\theta)}.$$

Dabei ist

$$I_n(\theta) = -\mathbb{E}_\theta\left(\frac{\partial^2}{\partial\theta^2} \log(L(X_1, \dots, X_n; \theta))\right)$$

und

$$I(\theta) = -\mathbb{E}_\theta\left(\frac{\partial^2}{\partial\theta^2} \log(f_\theta(X))\right)$$

bzw.

$$I(\theta) = -\mathbb{E}_\theta\left(\frac{\partial^2}{\partial\theta^2} \log(p_\theta(X))\right)$$

Wenn wir einen erwartungstreuen Schätzer finden können, dessen Varianz mit der Cramér-Rao Schranke übereinstimmt, dann können wir sicher sein, dass er effizient ist. Allerdings gibt es einen solchen Schätzer nicht immer, die Dichte bzw. Wahrscheinlichkeitsfunktion muss dazu von einer bestimmten Form sein. Wenn es einen solchen Schätzer gibt, dann stimmt er mit dem Maximum-Likelihood Schätzer überein (überhaupt ist der ML-Schätzer unter gewissen Regularitätsvoraussetzungen asymptotisch normalverteilt mit Mittel  $\theta$  und Varianz  $1/I_n(\theta)$ , also gewissermaßen “asymptotisch effizient”).

**5.1.2 Intervallschätzung**

Die Theorie aus dem vorigen Abschnitt gibt uns einen einzelnen Schätzwert. Manchmal möchte man auch Angaben über die Genauigkeit eines Schätzwertes machen können, also ein Intervall bestimmen, in dem der gesuchte Parameter liegt. Leider kann so etwas nicht mit absoluter Sicherheit geschehen, weil in den meisten Fällen für jeden Wert des Parameters jede Stichprobe positive (wenn auch sehr kleine) Wahrscheinlichkeit hat, gezogen zu werden.

Wir werden uns also damit begnügen müssen, ein Intervall zu bestimmen, das den gesuchten Parameter mit einer gewissen Wahrscheinlichkeit enthält.

**Definition 5.7**

$a = a(X_1, \dots, X_n) \leq b = b(X_1, \dots, X_n)$  seien zwei Statistiken. Das Intervall  $[a, b]$  heißt Konfidenzintervall für  $\theta$  mit Überdeckungswahrscheinlichkeit  $\gamma$ , wenn

$$\mathbb{P}_\theta(a \leq \theta \leq b) \geq \gamma.$$

Wenn in dieser Ungleichung Gleichheit gilt, sprechen wir von einem exakten Konfidenzintervall.

Ein möglicher Ausgangspunkt für die Konstruktion von Konfidenzintervallen ist ein Schätzer für  $\theta$ . Unter sehr günstigen Bedingungen kann die Verteilung dieses Schätzers exakt bestimmt werden, in anderen Fällen (immer noch günstig) ist er zumindest asymptotisch normalverteilt. In diesem Fall können wir ein approximatives Konfidenzintervall in der Form

$$[\hat{\theta}_n - z_{\frac{1+\gamma}{2}} \sigma_n, \hat{\theta}_n + z_{\frac{1+\gamma}{2}} \sigma_n],$$

wobei  $\sigma_n^2$  die Varianz von  $\hat{\theta}_n$  ist. Diese hängt in den meisten Fällen vom unbekanntem  $\theta$  ab, das wir durch  $\hat{\theta}_n$  ersetzen.

Für den Spezialfall einer Normalverteilung können wir exakte Konfidenzintervalle angeben:

Für  $\mu$ , wenn  $\sigma^2$  bekannt ist:

$$[\bar{X}_n - z_{\frac{1+\gamma}{2}} \sqrt{\frac{\sigma^2}{n}}, \bar{X}_n + z_{\frac{1+\gamma}{2}} \sqrt{\frac{\sigma^2}{n}}],$$

Für  $\mu$ , wenn  $\sigma^2$  unbekannt ist:

$$[\bar{X}_n - t_{n-1; \frac{1+\gamma}{2}} \sqrt{\frac{S_n^2}{n}}, \bar{X}_n + t_{n-1; \frac{1+\gamma}{2}} \sqrt{\frac{S_n^2}{n}}],$$

für  $\sigma^2$ :

$$\left[ \frac{(n-1)S_n^2}{\chi_{n-1; \frac{1+\gamma}{2}}^2}, \frac{(n-1)S_n^2}{\chi_{n-1; \frac{1-\gamma}{2}}^2} \right].$$

Für Anteilswerte verwenden wir das approximative Konfidenzintervall:

$$\left[ \hat{p} - z_{\frac{1+\gamma}{2}} \sqrt{\frac{\hat{p}(1-\hat{p})}{n}}, \hat{p} + z_{\frac{1+\gamma}{2}} \sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \right].$$

Ein anderer Weg, um Konfidenzintervalle zu erhalten, führt über die Theorie der statistischen Tests.

## 5.2 Tests

### 5.2.1 Grundlagen

Bei dieser Art von Problemen geht es nicht mehr darum, einen Näherungswert für einen unbekanntem Parameter zu bestimmen, sondern es soll eine Aussage über den Parameter überprüft werden, etwa “der Ausschussanteil ist kleiner als 1%” oder “das mittlere Gewicht ist 1kg”.

Wir definieren zuerst

#### Definition 5.8

Eine Hypothese ist eine Teilmenge des Parameterraums  $\Theta$ .

Wir schreiben Hypothesen meistens nicht in Mengennotation, sondern als Aussage (meistens eine Gleichung oder Ungleichung) für den Parameter. Wir unterscheiden einseitige Hypothesen (von der Form  $\theta \leq c$  oder  $\theta > c$  etc.) und zweiseitige Hypothesen ( $\theta \neq c$ ). Enthält die Hypothese nur einen Parameterwert ( $\theta = c$ ), nennen wir sie einfach.

Ein Test wird als Entscheidung zwischen zwei Hypothesen formuliert, der Nullhypothese  $H_0$  und der Gegenhypothese oder Alternative  $H_1$ . Die Rollen der beiden Hypothesen sind nicht symmetrisch — der übliche Sprachgebrauch ist “die Nullhypothese wird angenommen” oder “die Nullhypothese wird verworfen”.

Ein Test kann durch die Menge der möglichen Stichprobenwerte angegeben werden, bei denen die Nullhypothese angenommen wird, den Annahmehereich, bzw. durch sein Komplement, den Verwerfungsbereich. Oft ist es einfacher, eine Teststatistik anzugeben, und die Nullhypothese zu verwerfen, wenn diese Statistik einen kritischen Wert überschreitet (oder unterschreitet).

Beim Testen kann man zwei Arten von Fehlern begehen: Fehler erster Art — die Nullhypothese wird verworfen, obwohl sie zutrifft, und Fehler zweiter Art — die Nullhypothese wird angenommen, obwohl sie nicht zutrifft. Man möchte natürlich die Wahrscheinlichkeit für beide Fehler möglichst klein halten. Leider geht das nicht gleichzeitig — die Wahrscheinlichkeit für einen Fehler erster Art kann (zumindest ab einem gewissen Punkt) nur Verkleinert werden, indem der Annahmehereich vergrößert wird, und dadurch wächst die Wahrscheinlichkeit für einen Fehler zweiter Art. In der Statistik wird dieses Dilemma gelöst, indem man eine Schranke für die Wahrscheinlichkeit eines Fehlers erster Art angibt:

#### Definition 5.9

Ein Test heißt vom Niveau  $\alpha$ , wenn die Wahrscheinlichkeit für einen Fehler erster Art (die bei zusammengesetzten Hypothesen eine Funktion davon  $\theta$  ist) nicht größer als  $\alpha$  ist.

Eine Möglichkeit, einen Test zu konstruieren, liefert uns die Likelihood-Methode: die Grundidee besteht darin, sich für die Hypothese zu entscheiden, für die die aktuelle Stichprobe die größere Wahrscheinlichkeit hat. Damit man das Niveau  $\alpha$  einstellen kann, wird noch ein zusätzlicher Faktor eingeführt:

**Definition 5.10**

Die Likelihoodquotientenstatistik ist

$$\ell = \frac{\sup_{\theta \in H_0} L(X_1, \dots, X_n, \theta)}{\sup_{\theta \in H_1} L(X_1, \dots, X_n, \theta)}$$

bzw.

$$\ell = \frac{\sup_{\theta \in H_0} L(X_1, \dots, X_n, \theta)}{\sup_{\theta \in \Theta} L(X_1, \dots, X_n, \theta)}$$

(die zweite Form ist oft einfacher zu berechnen, und für große Stichprobenumfänge sind die Tests identisch).

Der Likelihoodquotiententest verwirft die Nullhypothese, wenn  $\ell$  kleiner ist als ein kritischer Wert.

In einem speziellen Fall ist der Likelihoodquotiententest optimal:

**Satz 5.2: Neyman-Pearson**

Falls sowohl  $H_0$  als auch  $H_1$  einfach ist, dann ist der Likelihoodquotiententest optimal, d.h., er hat unter allen Tests mit demselben Niveau die minimale Wahrscheinlichkeit für einen Fehler zweiter Art (in diesem Fall wird der Likelihoodquotient einfach als  $L(X_1, \dots, X_n, \theta_0)/L(X_1, \dots, X_n, \theta_1)$  berechnet)

**5.2.2 Spezielle Tests**

Für den Mittelwert einer Normalverteilung, wenn  $\sigma^2$  unbekannt ist:

$$T = \frac{\bar{X}_n - \mu_0}{\sqrt{S_n^2/n}}$$

$H_0 : \mu \leq \mu_0$  gegen  $H_1 : \mu > \mu_0$ : verwerfen, wenn  $T > t_{n-1;1-\alpha}$ .

$H_0 : \mu \geq \mu_0$  gegen  $H_1 : \mu < \mu_0$ : verwerfen, wenn  $T < -t_{n-1;1-\alpha}$ .

$H_0 : \mu = \mu_0$  gegen  $H_1 : \mu \neq \mu_0$ : verwerfen, wenn  $|T| > t_{n-1;1-\alpha/2}$ .

Für die Varianz einer Normalverteilung:

$$T = \frac{(n-1)S_n^2}{\sigma_0^2}$$

$H_0 : \sigma^2 \geq \sigma_0^2$  gegen  $H_1 : \sigma^2 < \sigma_0^2$ : verwerfen, wenn  $T < \chi_{n-1;\alpha}^2$ .

$H_0 : \sigma^2 = \sigma_0^2$  gegen  $H_1 : \sigma^2 \neq \sigma_0^2$ : verwerfen, wenn  $T > \chi_{n-1;1-\alpha/2}^2$  oder  $T < \chi_{n-1;\alpha/2}^2$ .

$H_0 : \sigma^2 \leq \sigma_0^2$  gegen  $H_1 : \sigma^2 > \sigma_0^2$ : verwerfen, wenn  $T > \chi_{n-1;1-\alpha}^2$ .

Für Anteilswerte:

$$T = \frac{\hat{p} - p_0}{\sqrt{p_0(1-p_0)/n}}$$

$H_0 : p \leq p_0$  gegen  $H_1 : p > p_0$ : verwerfen, wenn  $T > z_{1-\alpha}$ .

$H_0 : p \geq p_0$  gegen  $H_1 : p < p_0$ : verwerfen, wenn  $T < -z_{1-\alpha}$ .

$H_0 : p = p_0$  gegen  $H_1 : p \neq p_0$ : verwerfen, wenn  $|T| > z_{1-\alpha/2}$ .

**5.2.3 Der Chi-Quadrat-Anpassungstest**

Die Frage, die wir hier untersuchen, ist, ob eine Stichprobe aus einer gegebenen Verteilung stammt. Das geht am einfachsten, wenn es sich bei der hypothetischen Verteilung um eine diskrete Verteilung mit endlich vielen Werten  $1, \dots, k$  handelt. Wir testen also

$$H_0 : X \sim P = (p_1, \dots, p_k)$$

gegen die Alternative  $X \not\sim P$ . Diese Frage kann man mit der Likelihoodquotientenmethode behandeln; der Test, den wir verwenden, kann man als Approximation des Likelihoodquotiententests erhalten.

Wir führen die Häufigkeiten

$$Y_i = \#\{j \leq n : X_j = i\}$$

ein. Für großes  $n$  ist  $Y_i \approx np_i$  (und approximativ normalverteilt), wenn  $H_0$  zutrifft. Wir wollen alle Differenzen zwischen  $Y_i$  und  $np_i$  gleichzeitig überprüfen. Dazu bilden wir eine gewichtete Quadratsumme:

$$T = \sum_{i=1}^k \frac{(Y_i - np_i)^2}{np_i}.$$

Diese Statistik ist asymptotisch  $\chi^2$ -verteilt mit  $k - 1$  Freiheitsgraden. Die Nullhypothese wird abgelehnt, wenn

$$T > \chi_{k-1; 1-\alpha}^2.$$

Da diese Aussagen nur asymptotisch gelten, muss  $n$  hinreichend groß sein. Die übliche Faustregel ist, dass  $np_i$  mindestens 5 sein soll.

Wenn diese Bedingung nicht erfüllt ist, oder wenn die Verteilung, die wir testen wollen, stetig ist, werden die möglichen Werte in Klassen eingeteilt. Bei stetigen Verteilungen kann man die Klassengrenzen so setzen, dass alle Klassen gleiche Wahrscheinlichkeit haben, was die Rechnung vereinfachen kann.

Wenn die Verteilung, auf die wir testen, nicht vollständig spezifiziert ist, etwa, wenn man testen will, ob eine Normalverteilung vorliegt, von der wir Mittel und Varianz nicht kennen, dann müssen die Parameter nach der Maximum-Likelihood Methode geschätzt werden. Mit diesen geschätzten Parametern können dann die Wahrscheinlichkeiten berechnet werden. Die Anzahl der Freiheitsgrade muss dann korrigiert werden, indem die Anzahl der geschätzten Parameter abgezogen wird, es sind also statt  $k - 1$   $k - 1 - d$  Freiheitsgrade, wobei  $d$  die Anzahl der geschätzten Parameter ist (im Normalverteilungsbeispiel ist  $d = 2$ ).

### 5.2.4 Tests und Konfidenzintervalle

Es gibt einen interessanten Zusammenhang zwischen Tests und Konfidenzintervallen:

#### Satz 5.3

Wenn  $I = [a(X_1, \dots, X_n), b(X_1, \dots, X_n)]$  ein Konfidenzintervall mit Überdeckungswahrscheinlichkeit  $\gamma = 1 - \alpha$  ist, dann ist für jedes  $\theta_0 \in \Theta$  durch die Regel "verwerfe, wenn  $\theta_0 \notin I$ " ein Test mit Niveau  $\alpha$  für  $H_0 : \theta = \theta_0$  gegeben.

Ist umgekehrt für jedes  $\theta_0$  ein Test mit Niveau  $\alpha$  für die Nullhypothese  $H_0 : \theta = \theta_0$  gegeben, dann ist die Menge aller  $\theta_0$ , für die  $H_0 : \theta = \theta_0$  nicht verworfen wird, ein Konfidenzintervall mit Überdeckungswahrscheinlichkeit  $\gamma = 1 - \alpha$ .

# Anhang A

## Tabellen

Die Verteilungsfunktion der Standardnormalverteilung:

$$\Phi(x) = \int_{-\infty}^x \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$$

	0	1	2	3	4	5	6	7	8	9
0.0	.500	.504	.508	.512	.516	.520	.524	.528	.532	.536
0.1	.540	.544	.548	.552	.556	.560	.564	.567	.571	.575
0.2	.579	.583	.587	.591	.595	.599	.603	.606	.610	.614
0.3	.618	.622	.626	.629	.633	.637	.641	.644	.648	.652
0.4	.655	.659	.663	.666	.670	.674	.677	.681	.684	.688
0.5	.691	.695	.698	.702	.705	.709	.712	.716	.719	.722
0.6	.726	.729	.732	.736	.739	.742	.745	.749	.752	.755
0.7	.758	.761	.764	.767	.770	.773	.776	.779	.782	.785
0.8	.788	.791	.794	.797	.800	.802	.805	.808	.811	.813
0.9	.816	.819	.821	.824	.826	.829	.831	.834	.836	.839
1.0	.841	.844	.846	.848	.851	.853	.855	.858	.860	.862
1.1	.864	.867	.869	.871	.873	.875	.877	.879	.881	.883
1.2	.885	.887	.889	.891	.893	.894	.896	.898	.900	.901
1.3	.903	.905	.907	.908	.910	.911	.913	.915	.916	.918
1.4	.919	.921	.922	.924	.925	.926	.928	.929	.931	.932
1.5	.933	.934	.936	.937	.938	.939	.941	.942	.943	.944
1.6	.945	.946	.947	.948	.949	.951	.952	.953	.954	.954
1.7	.955	.956	.957	.958	.959	.960	.961	.962	.962	.963
1.8	.964	.965	.966	.966	.967	.968	.969	.969	.970	.971
1.9	.971	.972	.973	.973	.974	.974	.975	.976	.976	.977
2.0	.977	.978	.978	.979	.979	.980	.980	.981	.981	.982
2.1	.982	.983	.983	.983	.984	.984	.985	.985	.985	.986
2.2	.986	.986	.987	.987	.987	.988	.988	.988	.989	.989
2.3	.989	.990	.990	.990	.990	.991	.991	.991	.991	.992
2.4	.992	.992	.992	.992	.993	.993	.993	.993	.993	.994
2.5	.994	.994	.994	.994	.994	.995	.995	.995	.995	.995
2.6	.995	.995	.996	.996	.996	.996	.996	.996	.996	.996
2.7	.997	.997	.997	.997	.997	.997	.997	.997	.997	.997
2.8	.997	.998	.998	.998	.998	.998	.998	.998	.998	.998
2.9	.998	.998	.998	.998	.998	.998	.998	.999	.999	.999

Quantile  $z_p$  der Standardnormalverteilung:

$p$	$z_p$	$p$	$z_p$	$p$	$z_p$
.51	.025	.71	.553	.91	1.341
.52	.050	.72	.583	.92	1.405
.53	.075	.73	.613	.93	1.476
.54	.100	.74	.643	.94	1.555
.55	.126	.75	.674	.95	1.645
.56	.151	.76	.706	.96	1.751
.57	.176	.77	.739	.97	1.881
.58	.202	.78	.772	.975	1.960
.59	.228	.79	.806	.98	2.054
.60	.253	.80	.842	.99	2.326
.61	.279	.81	.878	.991	2.366
.62	.305	.82	.915	.992	2.409
.63	.332	.83	.954	.993	2.457
.64	.358	.84	.994	.994	2.512
.65	.385	.85	1.036	.995	2.576
.66	.412	.86	1.080	.996	2.652
.67	.440	.87	1.126	.997	2.748
.68	.468	.88	1.175	.998	2.878
.69	.496	.89	1.227	.999	3.090
.70	.524	.90	1.282	.9999	3.719

Quantile  $t_{n;p}$  der  $t$ -Verteilung mit  $n$  Freiheitsgraden:

$n$	.9	.95	.975	.99	.995	$n$	.9	.95	.975	.99	.995
1	3.078	6.314	12.706	31.821	63.675	26	1.316	1.706	2.056	2.479	2.779
2	1.886	2.920	4.303	6.965	9.725	27	1.314	1.703	2.052	2.473	2.467
3	1.638	2.353	3.183	4.541	5.841	28	1.313	1.701	2.048	2.467	2.763
4	1.533	2.132	2.776	3.747	4.604	29	1.311	1.699	2.045	2.462	2.756
5	1.476	2.015	2.571	3.365	4.032	30	1.310	1.697	2.042	2.457	2.750
6	1.440	1.943	2.447	3.143	3.707	31	1.309	1.696	2.040	2.453	2.744
7	1.415	1.895	2.365	2.998	3.499	32	1.309	1.694	2.037	2.449	2.738
8	1.397	1.860	2.306	2.896	3.355	33	1.308	1.692	2.035	2.445	2.733
9	1.383	1.833	2.262	2.821	3.250	34	1.307	1.691	2.032	2.441	2.728
10	1.372	1.812	2.228	2.764	3.169	35	1.306	1.690	2.030	2.438	2.724
11	1.363	1.796	2.201	2.718	3.106	40	1.303	1.684	2.021	2.423	2.704
12	1.356	1.782	2.179	2.681	3.055	45	1.301	1.679	2.014	2.412	2.690
13	1.350	1.771	2.160	2.650	3.012	50	1.299	1.676	2.009	2.403	2.678
14	1.345	1.761	2.145	2.624	2.977	55	1.297	1.673	2.004	2.396	2.668
15	1.341	1.753	2.131	2.602	2.947	60	1.296	1.671	2.000	2.390	2.660
16	1.337	1.746	2.120	2.583	2.921	65	1.295	1.669	1.997	2.385	2.654
17	1.333	1.740	2.110	2.567	2.898	70	1.294	1.667	1.994	2.381	2.648
18	1.330	1.734	2.101	2.552	2.878	75	1.293	1.665	1.992	2.377	2.643
19	1.328	1.729	2.093	2.539	2.861	80	1.292	1.664	1.990	2.374	2.639
20	1.325	1.725	2.086	2.528	2.845	85	1.292	1.663	1.988	2.371	2.635
21	1.323	1.721	2.080	2.518	2.831	90	1.291	1.662	1.987	2.368	2.632
22	1.321	1.717	2.074	2.508	2.819	95	1.291	1.661	1.985	2.366	2.629
23	1.319	1.714	2.069	2.500	2.807	100	1.290	1.660	1.984	2.364	2.626
24	1.318	1.711	2.064	2.492	2.797	105	1.290	1.659	1.983	2.362	2.623
25	1.316	1.708	2.060	2.485	2.787	$\infty$	1.282	1.645	1.960	2.326	2.576

Quantile  $\chi^2_{n;p}$  der  $\chi^2$ -Verteilung mit  $n$  Freiheitsgraden:

$n$	.005	.01	.02	.025	.05	.1	.5	.9	.95	.975	.98	.99	.995
1	.000	.000	.001	.001	.004	.016	.455	2.706	3.841	5.024	5.412	6.635	7.879
2	.010	.020	.040	.051	.103	.211	1.386	4.605	5.991	7.378	7.824	9.210	10.597
3	.072	.115	.185	.216	.352	.584	2.366	6.251	7.815	9.348	9.837	11.345	12.838
4	.207	.297	.429	.484	.711	1.064	3.357	7.779	9.488	11.143	11.668	13.277	14.860
5	.412	.554	.752	.831	1.145	1.610	4.351	9.236	11.070	12.832	13.308	15.086	16.750
6	.676	.872	1.134	1.237	1.635	2.204	5.348	10.645	12.592	14.449	15.033	16.812	18.548
7	.989	1.239	1.564	1.690	2.167	2.833	6.346	12.017	14.067	16.013	16.622	18.475	20.278
8	1.344	1.646	2.032	2.180	2.733	3.490	7.344	13.362	15.507	17.535	18.168	20.090	21.955
9	1.735	2.088	2.532	2.700	3.325	4.168	8.343	14.684	16.919	19.023	19.679	21.666	23.589
10	2.156	2.558	3.059	3.247	3.940	4.865	9.342	15.987	18.307	20.483	21.161	23.209	25.188
11	2.603	3.053	3.609	3.816	4.575	5.578	10.341	17.275	19.675	21.920	22.618	24.725	26.757
12	3.074	3.571	4.178	4.404	5.226	6.304	11.340	18.549	21.026	23.336	24.054	26.217	28.300
13	3.565	4.107	4.765	5.009	5.892	7.042	12.340	19.812	22.362	24.736	25.472	27.688	29.819
14	4.075	4.660	5.368	5.629	6.571	7.790	13.339	21.064	23.685	26.119	26.873	29.141	31.319
15	4.601	5.229	5.985	6.262	7.261	8.547	14.339	22.307	24.996	27.488	28.259	30.578	32.801
16	5.142	5.812	6.614	6.908	7.962	9.312	15.338	23.542	26.269	28.845	29.633	32.000	34.267
17	5.697	6.408	7.255	7.564	8.672	10.085	16.338	24.769	27.587	30.191	30.995	33.409	35.718
18	6.265	7.015	7.906	8.231	9.390	10.835	17.338	25.909	28.869	31.526	32.346	34.805	37.156
19	6.844	7.633	8.567	8.907	10.117	11.651	18.338	27.204	30.144	32.852	33.687	36.191	38.582
20	7.434	8.260	9.237	9.591	10.851	12.443	19.337	28.412	31.410	34.170	35.020	37.566	39.997
21	8.034	8.897	9.915	10.283	11.591	13.240	20.337	29.615	32.671	35.479	36.343	38.932	41.401
22	8.643	9.542	10.600	10.982	12.338	14.041	21.337	30.813	33.924	36.781	37.659	40.289	42.796
23	9.260	10.196	11.293	11.689	13.091	14.848	22.337	32.007	35.172	38.076	38.968	41.638	44.181
24	9.886	10.856	11.992	12.401	13.848	15.659	23.337	33.196	36.415	39.364	40.270	42.980	45.559
25	10.520	11.524	12.697	13.120	14.611	16.473	24.337	34.382	37.652	40.646	41.566	44.324	46.928
26	11.160	12.198	13.409	13.844	15.379	17.292	25.336	35.563	38.885	41.923	42.856	45.642	48.290
27	11.808	12.879	14.125	14.573	16.151	18.114	26.336	36.741	40.113	43.194	44.140	46.963	49.645
28	12.461	13.565	14.847	15.308	16.928	18.939	27.336	37.916	41.337	44.461	45.419	48.278	50.993
29	13.121	14.256	15.574	16.047	17.708	19.768	28.336	39.087	42.557	45.722	46.693	49.588	52.336
30	13.787	14.953	16.306	16.791	18.493	20.599	29.336	40.256	43.773	46.979	47.962	50.892	53.672
31	14.458	15.655	17.042	17.539	19.281	21.434	30.336	41.422	44.985	48.232	49.226	52.191	55.003
32	15.134	16.362	17.783	18.291	20.072	22.271	31.336	42.585	46.194	49.480	50.487	53.486	56.328
33	15.815	17.074	18.527	19.047	20.867	23.110	32.336	43.745	47.400	50.725	51.743	54.776	57.648
34	16.501	17.789	19.275	19.806	21.664	23.952	33.336	44.903	48.602	51.966	52.995	56.061	58.964
35	17.192	18.509	20.027	20.569	22.465	24.797	34.336	46.059	49.802	53.203	54.244	57.342	60.275
40	20.707	22.164	23.838	24.433	26.509	29.051	39.335	51.805	55.758	59.342	60.436	63.691	66.766
45	24.311	25.901	27.720	28.366	30.612	33.350	44.335	57.505	61.656	65.410	66.555	69.957	73.166
50	27.991	29.707	31.664	32.357	34.764	37.689	49.335	63.167	67.505	71.420	72.613	76.154	79.490
55	31.735	33.570	35.659	36.398	38.958	42.060	54.335	68.796	73.311	77.380	78.619	82.292	85.749
60	35.534	37.485	39.699	40.482	43.188	46.459	59.335	74.397	79.082	83.298	84.580	88.397	91.952
65	39.383	41.444	43.779	44.603	47.450	50.883	64.335	79.973	84.821	89.177	90.501	94.422	98.105
70	43.275	45.442	47.893	48.758	51.739	55.329	69.334	85.527	90.531	95.023	96.388	100.425	104.215
75	47.206	49.475	52.039	52.942	56.054	59.795	74.334	91.061	96.217	100.839	102.243	106.393	110.286
80	51.172	53.540	56.213	57.153	60.391	64.278	79.334	96.578	101.879	106.629	108.069	112.329	116.321
85	55.170	57.634	60.412	61.389	64.749	68.777	84.334	102.079	107.522	112.393	113.871	118.236	122.325
90	59.196	61.754	64.635	65.647	69.126	73.291	89.334	107.565	113.145	118.136	119.649	124.116	128.299
95	63.250	65.898	68.879	69.925	73.520	77.818	94.334	113.038	118.752	123.858	125.405	129.973	134.247
100	67.328	70.065	73.142	74.222	77.929	82.358	99.334	118.498	124.342	129.561	131.142	135.806	140.169

# Anhang B

## Mathematische Hintergründe

### B.1 Wahrscheinlichkeitsräume

Wir haben uns bei der Definition eines Wahrscheinlichkeitsraums nicht im Detail mit dem Definitionsbereich unserer Wahrscheinlichkeitsmaße beschäftigt bzw. stillschweigend angenommen, dass wir jeder Teilmenge von  $\Omega$  eine Wahrscheinlichkeit zuordnen können. Darauf kann man sich allerdings nicht verlassen: es gibt etwa den folgenden

**Satz B.1: Ulam**

Es gibt kein Wahrscheinlichkeitsmaß  $\mathbb{P}$ , das für *alle* Teilmengen von  $[0, 1]$  und die Bedingungen

$$\mathbb{P}([0, 1]) = 1$$

und

$$\mathbb{P}(\{x\}) = 0$$

für alle  $x \in [0, 1]$  erfüllt.

Dieser Satz braucht allerdings eine zusätzliche Voraussetzung aus der Mengentheorie, die Kontinuumshypothese (oder eine Abschwächung davon).

In der Mathematik wird diese Frage so gelöst, dass eben nicht alle Teilmengen von  $\Omega$  als "Ereignisse" zugelassen werden, sondern dass  $\mathbb{P}$  auf einer Teilmenge  $\mathfrak{G}$  der Potenzmenge  $2^\Omega$  definiert wird. Es ist angenehm, wenn diese Teilmenge ein wenig Struktur mitbringt: idealerweise sollte  $\mathfrak{G}$  bezüglich der Bildung von Komplementen und abzählbaren Vereinigungen abgeschlossen sein. Ein solches System heißt Sigmaalgebra und ist auch gegenüber der Bildung von Differenzen zweier Mengen und von (endlichen oder abzählbaren) Durchschnitten abgeschlossen. Es ist allerdings nicht ganz wünschenswert, den Wert des Wahrscheinlichkeitsmaßes für alle die vielen und komplizierten Mengen aus  $\mathfrak{G}$  angeben zu müssen, besser wäre es, wenn diese Angabe nur für wenige einfache Mengen notwendig wäre. Im Spezialfall  $\Omega = \mathbb{R}$  wären etwa die Intervalle der Form  $(a, b]$  einfach genug, und ihre Wahrscheinlichkeit lässt sich mit einer Verteilungsfunktion  $F$  als

$$\mathbb{P}((a, b]) = F(b) - F(a)$$

festlegen. Es stellt sich heraus, dass damit für jede Menge in der kleinsten Sigmaalgebra  $\mathfrak{B}$ , die alle diese Intervalle enthält, die Wahrscheinlichkeit eindeutig festgelegt wird.  $\mathfrak{B}$  heißt die Borelsche Sigmaalgebra bzw. die Sigmaalgebra der Borelmengen. Sie ist sehr reichhaltig, enthält etwa alle offenen und abgeschlossenen Mengen und noch sehr viel mehr.

# Index

- absorbierender Zustand, 40
- Additionstheorem, 8
- Alternativverteilung, 14
- aperiodisch, 40
- Axiome
  - Kolmogorovsche, 5
- Bar Kochba, 50
- bedingte Dichte, 20
- bedingte Verteilung, 20
- bedingte Wahrscheinlichkeit, 9
- Binarbaum
  - vollständiger, 51
- Binärbaum, 51
- Binomialverteilung, 14
- Blatt, 51
- Blattlänge, 51
- Blutgruppe, 12
- Chapman-Kolmogorov Gleichungen, 39, 45
- Dichte, 16
  - bedingte, 20
- eingebettete Markovkette, 48
- Elementarereignis, 4
- Endknoten, 51
- Entropie, 50
  - relative, 55
- Ereignis, 4
  - sicheres, 5
  - unmögliches, 5
- Ergodensatz, 36
- ergodisch, 37
- Erneuerungsprozess, 38
- Erwartungswert, 26
- Faltung, 23
  - diskrete, 24
- Geburts- und Todesprozess, 48
- Geburtsprozess
  - reiner, 48
- geometrische Wahrscheinlichkeit, 6
- Gleichverteilung
  - stetige, 17
- Grundmenge, 4
- homogene Markovkette, 39
- hypergeometrische Verteilung, 14
- I-Divergenz, 55
- Indikator, 14
- infinitesimale Parameter, 45
- infinitesimaler Erzeuger, 45
- Informationsdivergenz, 55
- innerer Knoten, 51
- Inverse
  - verallgemeinerte, 25
- irreduzibel, 40
- Irrfahrt, 39
- Klasseneigenschaft, 40
- Knoten
  - innerer, 51
- Kolmogorov
  - Axiome, 5
- Kolmogorovsche Differentialgleichungen, 46
- kommunizierende Zustände, 40
- konservativ, 47
- Kullback-Leibler Information, 55
- Laplacescher Wahrscheinlichkeitsraum, 6
- Markovkette
  - eingebettete, 48
  - homogene, 39
  - irreduzible, 40
  - reguläre, 48
- Markovprozess, 37
- maximale Unbestimmtheit, 50
- Multinomialverteilung, 19
- Multiplikationssatz, 9
- Nachfolger, 40
- nullrekurrent, 41
- Parameterraum, 36
- Periode, 40
- periodisch, 40
- Phasenraum, 36
- Poissonprozess, 38
- positiv rekurrent, 41
- Prozess
  - in diskreter Zeit, 36
  - in stetiger Zeit, 36
  - mit unabhängigen Zuwächsen, 37

- stationärer, 36
- stochastischer, 36
- Quantil, 25
- Random Walk, 39
  - symmetrischer, 40
- Randverteilung, 19
- regulär, 48
- Rekurrenz, 41
- Rekurrenzklassen, 40
- relative Entropie, 55
- Rückkehrzeit, 41
- Rückwärtsgleichung, 46
- Satz vom unachtsamen Statistiker, 28
- Satz von Bayes, 12
- Satz von der vollständigen Wahrscheinlichkeit, 12
- sicheres
  - Ereignis, 5
- stationäre Verteilung, 41
- stationärer Prozess, 36
- stetige Gleichverteilung, 17
- stetige Verteilung, 16
- stochastischer Prozess, 36
- Todesprozess
  - reiner, 48
- Transformationssatz für Dichten, 22
- Transienz, 41
- Übergangsmatrix, 39
  - $t$ -stufige, 39
- Übergangswahrscheinlichkeiten, 39
- Übergangszeit, 41
- unabhängig, 11
- Unabhängigkeit, 20
- Unbestimmtheit
  - maximale, 50
- unmögliches Ereignis, 5
- verallgemeinerte Inverse, 25
- Verteilung, 13
  - Alternativ-, 14
  - bedingte, 20
  - Binomial-, 14
  - hypergeometrische, 14
  - stationäre, 41
  - stetige, 16
- Verteilungsfunktion, 15
  - zweidimensionale, 16
- Vorwärtsgleichung, 46
- Wahrscheinlichkeit, 5
  - bedingte, 9
  - geometrische, 6
  - Wahrscheinlichkeitsfunktion, 14
  - Wahrscheinlichkeitsmaß, 5
  - Wahrscheinlichkeitsraum, 5
    - Laplacescher, 6
  - Zufallsvariable, 13
    - diskrete, 13
    - Verteilung, 13
  - Zufallsvektor, 13
  - Zustände
    - kommunizierende, 40
  - Zustand
    - absorbierender, 40
  - Zustandsraum, 36