

Diskrete Strukturen

— Skript zur Vorlesung —

Ulrik Brandes

Sommersemester 2003
(Version vom 22. Oktober 2004)

Prolog

— Di., 8.4. (V1) —

- Übungsbetrieb (Termine, Gruppen, Einteilung, Punkte)
- Schein (Klausur, Zulassung, Prüfungsschienen)
- Sprechstunden
- Inhalte
- Literatur

Inhaltsverzeichnis

1	Kombinatorik	1
1.1	Auswahlen	1
1.2	Kombinatorische Beweisprinzipien	5
1.3	Anzahlbestimmungen	13
2	Diskrete Wahrscheinlichkeitsrechnung	24
2.1	Wahrscheinlichkeitsräume	25
2.2	Bedingung und Unabhängigkeit	33
2.3	Zufallsvariablen	39
3	Analyse von Algorithmen	44
3.1	Standardanalysen	46
3.2	Rekursionen	49
4	Graphentheorie	58
4.1	Bäume und Wälder	63
4.2	Durchläufe	66
4.3	Matchings und Färbungen	75

Kapitel 1

Kombinatorik

Hauptfragen der Kombinatorik:

„Kombinationen“

1. *Existenz* eines Objekts mit gewissen Eigenschaften
2. *Anzahl* der Objekte mit gewissen Eigenschaften
3. *Konstruktion* eines oder aller Objekte mit gewissen Eigenschaften

Die Objekte sind meist Mengen und wir beschränken uns hier auf *endliche* Mengen, d.h. Mengen, für die es keine bijektive Abbildung auf eine ihrer echten Teilmengen gibt. vgl. unendliches Hotel

Ausserdem behandeln wir vorwiegend Anzahlprobleme. Diese bilden die Grundlage für die in den Kapiteln 2 und 3 behandelten Themen.

1.1 Auswahlen

Zentrale Frage:

Wieviele Möglichkeiten gibt es, aus n Objekten k mal auszuwählen?

Hängt davon ab: ($M = \{1, 2\}$, $|M| = n = 2$, $k = 2$)

Reihenfolge	relevant	unerheblich
Wiederholungen		
möglich	4: (1, 1), (1, 2), (2, 1), (2, 2)	3: [1, 1], [1, 2], [2, 2]
ausgeschlossen	2: (1, 2), (2, 1)	1: {1, 2}

Häufig spricht man auch vom *Ziehen* von k Elementen aus einer Menge von n Elementen, und zwar mit oder ohne *Zurücklegen* (je nachdem, ob Wiederholungen erlaubt sind) und mit oder ohne *Berücksichtigung der Reihenfolge*.

1.1 Definition (Multimenge)

Eine Menge M zusammen mit einer Vielfachheit $\#_M : M \rightarrow \mathbb{N}_0$ ihrer Elemente heißt Multimenge. Wir schreiben kurz $\#a = \#_M(a)$ und $a \in_k M$, falls $\#a = k$, sowie $a \in M$ bzw. $a \notin M$, falls $a \in_k M$ für ein $k \in \mathbb{N}$ bzw. $k = 0$.

$\mathbb{N} := \{1, 2, 3, \dots\}$
 $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$

Die Kardinalität (auch: Mächtigkeit) $|M| = \sum_{a \in M} \#a$.

Für Multimengen M, N gilt $M \subseteq N$, falls $a \in_k M \implies a \in_l N$ mit $k \leq l$. Ist N jedoch eine gewöhnliche Menge, so gilt $M \subseteq N$, falls $a \in M \implies a \in N$ (unabhängig von $\#a$).

— Do., 10.4. (V2) —

1.2 Beispiel (Auswahlprobleme)

1. PINs

($n = 10$ Ziffern, $k = 4$ Länge)

→ Wiederholungen möglich, Reihenfolge wird berücksichtigt

2. Wahlausgänge

(n Kandidaten, k Wähler)

→ Wiederholungen möglich, Reihenfolge wird nicht berücksichtigt

3. Wettkampfausgänge

(n Teilnehmer, k Medaillen)

→ keine Wiederholungen, Reihenfolge wird berücksichtigt

4. Lotto 6-aus-49 (ohne Zusatzzahl)

($n = 49$, $k = 6$)

→ keine Wiederholungen, Reihenfolge wird nicht berücksichtigt

Wiederholungen zugelassen, Reihenfolge berücksichtigt

Da die Reihenfolge berücksichtigt wird, können wir auch bei der Bestimmung der Anzahlen der Reihe nach vorgehen. Bei der ersten Auswahl stehen uns alle n Elemente zur Verfügung. Da Wiederholungen erlaubt sind, kann wieder jedes der n Elemente gewählt und mit der ersten Auswahl kombiniert werden.

Genauso bei der dritten, vierten, usw., sodass es insgesamt

$$\underbrace{n \cdot n \cdot \dots \cdot n}_{k \text{ mal}} = n^k$$

verschiedene Möglichkeiten gibt.

1.3 Folgerung

Für eine Menge M gilt $|M^k| = \underbrace{|M \times \dots \times M|}_{k \text{ mal}} = |M|^k$.

Wiederholungen ausgeschlossen, Reihenfolge berücksichtigt

Wieder gibt es für die erste Auswahl n Möglichkeiten. Bei der zweiten ist das zuerst gewählte Element aber ausgeschlossen, sodass noch $n-1$ Möglichkeiten bleiben. Bei der dritten Auswahl bleiben noch $n-2$, weil die beiden zuerst gewählten Elemente ausgeschlossen sind, usw., sodass es insgesamt

$$n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1) = \prod_{i=0}^{k-1} (n-i) =: n^{\underline{k}}$$

verschiedene Möglichkeiten gibt.

1.4 Bemerkung

Der Ausdruck $n^{\underline{k}}$ heißt fallende Faktorielle (von n der Länge k). Für $k = n$ erhalten wir

$$n^{\underline{n}} = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 =: n!$$

die Fakultät (von n ; auch: n -Fakultät). Werden aus n Elementen n ohne Wiederholungen ausgewählt, kommt jedes Element genau einmal vor. Es gibt daher $n!$ Möglichkeiten, n Elemente anzuordnen (Permutationen). $n^{\underline{0}} := 1$
 $0! := 1$

Wiederholungen ausgeschlossen, Reihenfolge unberücksichtigt

Alle ausgewählten Elemente sind verschieden und ihre Reihenfolge ist egal. Also kommt es nur darauf an, *welche* k Elemente ausgewählt werden, nicht *wie* sie ausgewählt werden. Wir suchen also die Anzahl aller k -elementigen Teilmengen einer Menge mit n Elementen.

Von den n^k Möglichkeiten, k Elemente ohne Wiederholung aber mit Berücksichtigung der Reihenfolge auszuwählen, liefern alle Auswahlen, die sich nur in der Reihenfolge unterscheiden, die gleiche Teilmenge. Wir haben aber gerade gesehen, dass es $k!$ Möglichkeiten gibt, k Elemente anzuordnen, sodass es für $0 \leq k \leq n$ gerade

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

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

verschiedene k -elementige Teilmengen einer n -elementigen Menge gibt. Die Zahl $\binom{n}{k}$ heißt auch Binomialkoeffizient (von n über k).

1.5 Folgerung

Für alle $n, k \in \mathbb{N}_0$ gilt

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

$$\binom{n}{k} = \binom{n}{n-k}.$$

Wiederholungen zugelassen, Reihenfolge unberücksichtigt

Da Wiederholungen zugelassen sind, suchen wir jetzt also nach der Anzahl der *Multimengen* mit Kardinalität k , die Teilmenge einer n -elementigen Menge sind. Dabei ist folgende Darstellung einer Multimenge hilfreich (für die wir eine beliebige, aber feste Nummerierung der n möglichen Elemente annehmen): Für das erste Element schreiben wir entsprechend seiner Vielfachheit oft $*$, dann (als Trennzeichen) ein $|$, dann für das zweite Element entsprechend seiner Vielfachheit oft $*$ und wieder ein $|$, usw. Insgesamt erhalten wir also eine Zeichenkette aus $n + k - 1$ Zeichen (k mal $*$ und $n - 1$ mal $|$).

Beispiel: $[2, 2, 5, 5, 5, 7] \subseteq \{1, \dots, 7\}$ wird dargestellt durch $|**|||***||*$.

Jede solche Zeichenkette entspricht genau einer der gesuchten Multimengen und umgekehrt. Die Zeichenketten sind aber leichter zu zählen, denn eine Zeichenkette ist eindeutig durch die Position der k Elementzeichen $*$ bestimmt. Wieviele Möglichkeiten es gibt, aus den $n + k - 1$ Positionen k auszuwählen, haben wir aber gerade erst festgestellt:

$$\binom{n+k-1}{k}.$$

Überblick: aus n Objekten k mal wählen

Reihenfolge Wiederholungen	berücksichtigt	unberücksichtigt
zugelassen	n^k <i>k-Variationen</i> <i>k-Stichproben</i>	$\binom{n+k-1}{k}$ <i>k-Repetitionen</i> <i>k-Multiteilmengen</i>
ausgeschlossen	$n^{\underline{k}}$ <i>k-Permutationen</i> <i>n = k: Permutationen</i>	$\binom{n}{k}$ <i>k-Kombinationen</i> <i>k-Teilmengen</i>

1.2 Kombinatorische Beweisprinzipien

Im vorigen Abschnitt haben wir die Auswahlmengen in leichter abzuzählende zerlegt und deren Anzahlen kombiniert. Wird eine Gleichheit auf Anzahlüberlegungen wie diese zurück geführt, so spricht man auch von einem *kombinatorischen Beweis*.

In diesem Abschnitt sollen die oben implizit angewandten Regeln in allgemeiner Form festgehalten werden. Sie werden hier nicht bewiesen, sondern als wahr angenommen (in einer formalen Begründung der Kombinatorik sprächen wir von Axiomen).

1.6 Prinzip (Summenregel)

Sind S_1, \dots, S_k disjunkte Mengen, dann gilt

$$|S_1 \uplus \dots \uplus S_k| = |S_1| + \dots + |S_k| .$$

Die Summenregel wird meist in der Form angewandt, dass die Elemente einer Menge nach sich gegenseitig ausschliessenden Eigenschaften klassifiziert werden. Viele Rekursionen lassen sich so herleiten.

1.7 Beispiel (Rekursionsformel für Binomialkoeffizienten)

Sei M eine Menge mit $|M| = n$ und $S = \binom{M}{k}$ die Menge der k -elementigen Teilmengen von M . Wir haben gezeigt, dass $|S| = \binom{n}{k}$.

Andererseits können wir die Teilmengen in S danach unterscheiden, ob sie ein festes Element $a \in M$ enthalten. Sei also $S_a \subseteq S$ die Menge der k -elementigen Teilmengen von M , die a enthalten, und $\overline{S}_a = S \setminus S_a$ die Menge der k -elementigen Teilmengen von M , die a nicht enthalten.

Es gilt $|S_a| = \left| \binom{M \setminus \{a\}}{k-1} \right| = \binom{n-1}{k-1}$, denn wenn jede Menge in S_a das Element a enthält, dann können jeweils nur noch $k-1$ Elemente aus $M \setminus \{a\}$ gewählt werden. Entsprechend gilt $|\overline{S}_a| = \left| \binom{M \setminus \{a\}}{k} \right| = \binom{n-1}{k}$ und mit der Summenregel folgt für alle $n \geq 1$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Wird die Summenregel in der obigen Form angewandt, so spricht man auch von einem *Pascal-Argument* („ein Element isolieren, dann Fallunterscheidung“).

Die nächste Regel ist geeignet für Mengen, deren Elemente aus frei kombinierbaren Bausteinen zusammengesetzt sind. An die Stelle der disjunkten Vereinigung tritt das kartesische Produkt.

1.8 Prinzip (Produktregel)

Sind S_1, \dots, S_k Mengen, dann gilt

$$|S_1 \times \dots \times S_k| = |S_1| \cdot \dots \cdot |S_k|.$$

1.9 Beispiel (Telefonnummern)

In den USA bestehen Telefonnummern aus einer 3-stelligen Vorwahl und einer 7-stelligen Rufnummer, die folgenden Bedingungen genügen müssen:

1. Die Vorwahl darf weder mit 0 noch mit 1 beginnen, muss aber an zweiter Stelle eine 0 oder 1 haben.
2. Die Rufnummer darf an den ersten beiden Stellen weder eine 0 noch eine 1 haben.

Bezeichnen wir die Menge der zulässigen Ziffern an der i -ten Stelle mit S_i , dann gilt also $S_1 = S_4 = S_5 = \{2, \dots, 9\}$, $S_2 = \{0, 1\}$ und $S_3 = S_6 = S_7 = S_8 = S_9 = S_{10} = \{0, \dots, 9\}$. Somit gibt es in den USA genau

$$|S_1| \cdot \dots \cdot |S_{10}| = 8 \cdot 2 \cdot 10 \cdot 8^2 \cdot 10^5 = 1.024.000.000$$

zulässige Telefonnummern.

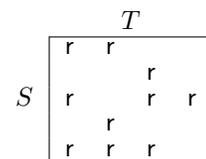
Relationen sind Teilmengen kartesischer Produkte. Die Richtigkeit mancher Gleichungen lässt sich dadurch zeigen, dass eine geeignete binäre Relationen auf verschiedene Weise abgezählt wird. Dies ist eine spezielle Verwendung der Summenregel.

1.10 Prinzip (Doppeltes Abzählen)

Für eine Relation $R \subseteq S \times T$ gilt

$$|R| = \sum_{s \in S} |\{t \in T : (s, t) \in R\}| = \sum_{t \in T} |\{s \in S : (s, t) \in R\}| .$$

Zeilensummen
Spaltensummen



— Do., 24.4. (V2) —

1.11 Beispiel (Durchschnittliche Anzahl von Teilern)

Sei $t : \mathbb{N} \rightarrow \mathbb{N}$ die Funktion, die einer natürlichen Zahl $n \in \mathbb{N}$ die Anzahl $t(n)$ ihrer Teiler zuordnet, d.h. die Anzahl der Zahlen von $1, \dots, n$, die n teilen.

Offensichtlich gilt z.B. $t(p) = 2$ für alle Primzahlen $p \in \mathbb{N}$ und $t(2^k) = k + 1$ für alle $k \in \mathbb{N}$, die Funktion scheint also sehr unregelmässig zu verlaufen.

Wir zeigen durch doppeltes Abzählen, dass sich die „durchschnittliche“ Anzahl von Teilern, d.h. die Funktion $\langle t(n) \rangle = \frac{1}{n} \sum_{j=1}^n t(j)$, wesentlich gleichförmiger verhält.

Betrachte dazu die Teilbarkeitsrelation $| \subset \{1, \dots, n\} \times \{1, \dots, n\}$, d.h. $(i, j) \in |$ genau dann, wenn i Teiler von j . Für $n = 8$ ergibt sich z.B.:

	1	2	3	4	5	6	7	8
1	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8
2		2 2		2 4		2 6		2 8
3			3 3			3 6		
4				4 4				4 8
5					5 5			
6						6 6		
7							7 7	
8								8 8

Spaltenweise betrachtet entsprechen die Einträge gerade den Teilern einer Zahl. In der j -ten Spalte stehen daher $t(j)$ viele Einträge. Zeilenweise betrachtet entsprechen die Einträge gerade den Vielfachen einer Zahl. In der i -ten Zeile stehen daher $\lfloor \frac{n}{i} \rfloor$ viele Einträge. Mit dem Prinzip des doppelten

Abzählens erhalten wir für die durchschnittliche Teileranzahl

$$\langle t(n) \rangle = \frac{1}{n} \sum_{j=1}^n t(j) = \frac{1}{n} \sum_{i=1}^n \left\lfloor \frac{n}{i} \right\rfloor$$

Ersetzen wir $\lfloor \frac{n}{i} \rfloor$ durch $\frac{n}{i}$, so ist der Fehler für alle i höchstens 1, also auch für den Durchschnitt. Diese Abschätzung liefert schließlich

$$\langle t(n) \rangle \sim \frac{1}{n} \sum_{i=1}^n \frac{n}{i} = \sum_{i=1}^n \frac{1}{i} \sim \ln n ,$$

harmonische
Reihe

ein erstaunliches Resultat.

Statt eine Menge auf zwei Weisen abzuzählen ist es oft einfacher, eine Menge auf eine leichter zählbare abzubilden. Dieses Prinzip ist grundlegend und von uns auch schon oft verwendet worden.

1.12 Prinzip (Gleichheits- oder Identitätsprinzip)

Ist $\beta : S \rightarrow T$ eine Bijektion, dann gilt

$$|S| = |T| .$$

1.13 Beispiel

Wir haben das Identitätsprinzip bereits benutzt, um die Anzahl der k -Repetitionen von n Elementen zu bestimmen, indem wir Multimengen bijektiv auf Zeichenketten aus $*$ und $|$ abgebildet haben.

Ist die Bildmenge zu klein für eine Bijektion, lassen sich daraus trotzdem nützliche Einsichten gewinnen.

1.14 Prinzip (Schubfach- oder Taubenschlagprinzip)

Ist $\alpha : S \rightarrow T$ eine Abbildung mit $|S| > |T|$, dann gibt es ein $t \in T$ mit

$$|\alpha^{-1}(t)| \geq 2 .$$

Einfach ausgedrückt: Steckt man n Tauben in $n - 1$ Taubenschläge, dann sitzen in mindestens einem Taubenschlag mindestens zwei Tauben.

1.15 Beispiel

Von 13 Personen haben immer mindestens zwei im selben Monat Geburtstag.

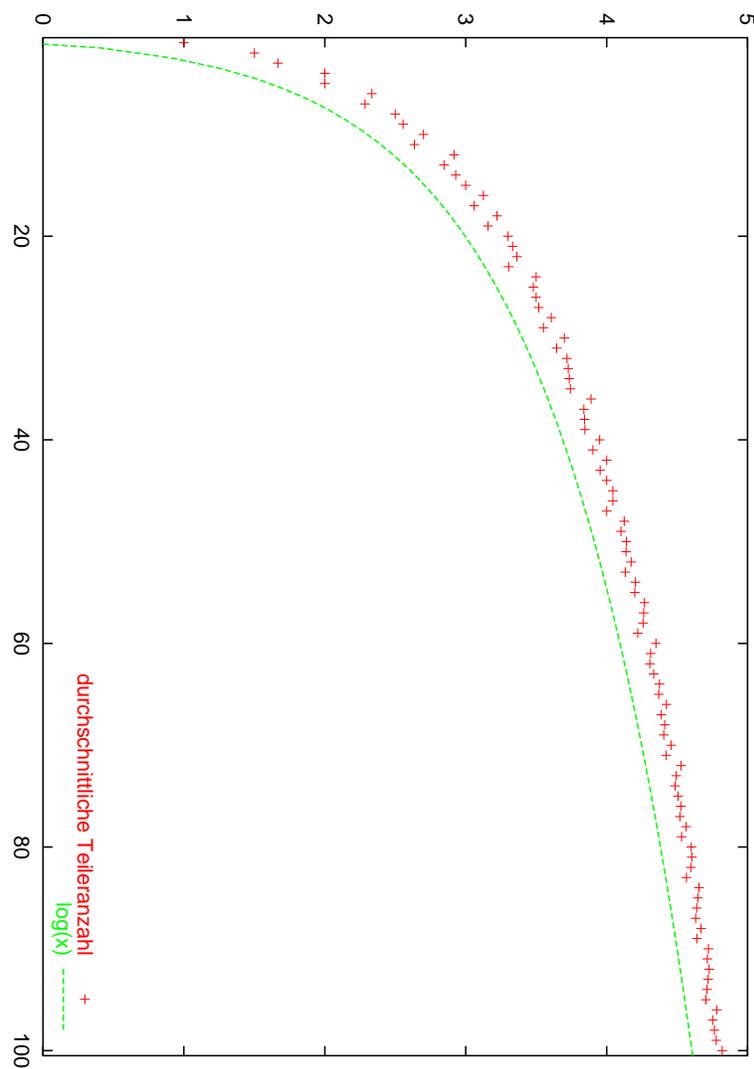


Abbildung 1.1: Vergleich der durchschnittlichen Anzahl von Teilern mit dem natürlichen Logarithmus.

1.2.1 Verallgemeinerungen

Das Taubenschlagprinzip scheint ein bisschen sehr einfach, doch es gilt auch in allgemeinerer Form.

1.16 Satz (verallgemeinertes Schubfach- oder Taubenschlagprinzip)

Ist $\alpha : S \rightarrow T$ eine Abbildung, dann gibt es ein $t \in T$ mit

$$|\alpha^{-1}(t)| \geq \left\lceil \frac{|S|}{|T|} \right\rceil .$$

■ **Beweis:** Angenommen, es gibt eine Abbildung $\alpha : S \rightarrow T$ mit $|\alpha^{-1}(t)| < \left\lceil \frac{|S|}{|T|} \right\rceil$ für alle $t \in T$. Dann gilt

$$\begin{aligned} \sum_{t \in T} |\alpha^{-1}(t)| &\leq |T| \cdot \left(\left\lceil \frac{|S|}{|T|} \right\rceil - 1 \right) \\ &\leq |T| \cdot \left(\frac{|S| + (|T| - 1)}{|T|} - 1 \right) \\ &= |T| \cdot \frac{|S| - 1}{|T|} = |S| - 1 . \end{aligned}$$

Da α eine Abbildung ist, gilt mit der Summenregel aber auch

$$|S| = \left| \bigcup_{t \in T} \alpha^{-1}(t) \right| = \sum_{t \in T} |\alpha^{-1}(t)| .$$

Zusammen genommen ergibt sich der Widerspruch $|S| \leq |S| - 1$. □

1.17 Beispiel

Wir zeigen: Auf einer Party mit mindestens sechs Personen gibt es immer drei, die sich gegenseitig die Hand schütteln, oder drei, die das nicht tun. Ramsey-Zahlen

Sei $P = \{p_1, \dots, p_6\}$ die Menge der Personen und $\sigma : P \setminus \{p_1\} \rightarrow \{0, 1\}$ ordne jeder Person außer p_1 eine 0 oder 1 zu, je nachdem, ob sie p_1 die Hand schüttelt oder nicht.

Mit dem verallgemeinerten Taubenschlagprinzip folgt, dass es mindestens $\left\lceil \frac{|P|-1}{|\{0,1\}|} \right\rceil = \left\lceil \frac{5}{2} \right\rceil = 3$ Personen gibt, die p_1 die Hand schütteln oder dieses eben nicht tun. Ohne Einschränkung nehmen wir daher an, dass p_1 sich mit

p_2, p_3, p_4 die Hand gibt (sonst umbenennen bzw. analoge Argumentation für keinen Handschlag).

Wenn sich irgendeins der Paare $(p_2, p_3), (p_2, p_4), (p_3, p_4)$ die Hand gibt, dann haben wir zusammen mit p_1 eine Gruppe von drei Personen, die sich gegenseitig die Hand geben. Andernfalls bilden p_2, p_3, p_4 eine Gruppe von drei Personen, die das nicht tun.

Zum Abschluss wollen wir auch die Summenregel verallgemeinern. Ist die Voraussetzung disjunkter Mengen nicht erfüllt, ist die Aussage falsch, denn Elemente, die in mehreren Mengen vorkommen, werden dann auch mehrfach gezählt. Beispielweise werden bei zwei Mengen S_1, S_2 die Elemente im Schnitt genau zweimal gezählt, sodass wir

Venn-Diagramm!

$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|$$

folgern können. Werden bei drei Mengen S_1, S_2, S_3 die Kardinalitäten der paarweisen Schnitte wieder abgezogen, so werden die Elemente in $S_1 \cap S_2 \cap S_3$ dreimal gezählt, aber auch dreimal wieder abgezogen, müssen letztlich also nochmal hinzugezählt werden:

Venn-Diagramm!

$$\begin{aligned} |S_1 \cup S_2 \cup S_3| &= |S_1| + |S_2| + |S_3| \\ &\quad - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| \\ &\quad + |S_1 \cap S_2 \cap S_3|. \end{aligned}$$

1.18 Satz (Inklusions-Exklusionsprinzip, Siebformel)

Für Mengen S_1, \dots, S_k gilt

$$|S_1 \cup \dots \cup S_k| = \sum_{l=1}^k (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq k} \left| \bigcap_{j=1}^l S_{i_j} \right|.$$

■ **Beweis:** Wir zeigen, dass jedes $a \in (S_1 \cup \dots \cup S_k)$ genau 1 zur Größe der Zahlen auf beiden Seiten der Gleichung beiträgt. Für die linke Seite ist das offensichtlich.

Ist a in genau r der Mengen S_1, \dots, S_k enthalten, dann trägt es immer dann eine 1 zur inneren Summe $\sum_{1 \leq i_1 < \dots < i_l \leq k} \left| \bigcap_{j=1}^l S_{i_j} \right|$ auf der rechten Seite bei, wenn alle l geschnittenen Mengen aus den r Mengen gewählt wurden, die a enthalten; insgesamt also $\binom{r}{l}$ mal.

Die Beiträge von a auf der rechten Seite summieren sich damit zu

Summenregel

$$\sum_{l=1}^r (-1)^{l-1} \binom{r}{l}$$

auf. Wegen

binomische
Formel

$$\begin{aligned} 0 &= (-1 + 1)^r = \sum_{l=0}^r \binom{r}{l} (-1)^l 1^{r-l} = 1 + \sum_{l=1}^r \binom{r}{l} (-1)^l \\ &= 1 - \sum_{l=1}^r (-1)^{l-1} \binom{r}{l} \end{aligned}$$

ist diese Summe aber ebenfalls 1. □

1.19 Beispiel (Primzahlen)

Wieviele Primzahlen gibt es unter den ersten n natürlichen Zahlen?

Sei $M = \{1, \dots, n\}$. Eine Zahl $r \in M$ ist prim, wenn sie durch keine andere Primzahl $2 \leq p \leq \sqrt{r}$ teilbar ist. Sei P die Menge der Primzahlen in $\{2, \dots, \lfloor \sqrt{n} \rfloor\}$ und zu jeder Primzahl $p \in P$ sei $S_p \subseteq M$ die Menge der Vielfachen von p in M , d.h. $S_p = \{r \in M : r = i \cdot p \text{ für ein } i \in \mathbb{N}\}$. Dann ist die Menge der Primzahlen in M gerade $(M \setminus \bigcup_{p \in P} S_p) \cup P$.

Als Beispiel berechnen wir die Anzahl der Primzahlen unter den ersten einhundert Zahlen und haben daher $M = \{1, \dots, 100\}$ und $P = \{2, 3, 5, 7\}$. Die gesuchte Anzahl ist also

$$100 - |S_2 \cup S_3 \cup S_5 \cup S_7| + 4 .$$

Mit der Siebformel erhalten wir

$$\begin{aligned}
 & |S_2 \cup S_3 \cup S_5 \cup S_7| \\
 &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{7} \right\rfloor \\
 &\quad - \left\lfloor \frac{100}{2 \cdot 3} \right\rfloor - \left\lfloor \frac{100}{2 \cdot 5} \right\rfloor - \left\lfloor \frac{100}{2 \cdot 7} \right\rfloor - \left\lfloor \frac{100}{3 \cdot 5} \right\rfloor - \left\lfloor \frac{100}{3 \cdot 7} \right\rfloor - \left\lfloor \frac{100}{5 \cdot 7} \right\rfloor \\
 &\quad + \left\lfloor \frac{100}{2 \cdot 3 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 3 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 5 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 5 \cdot 7} \right\rfloor \\
 &\quad - \left\lfloor \frac{100}{2 \cdot 3 \cdot 5 \cdot 7} \right\rfloor \\
 &= 50 + 33 + 20 + 14 - 16 - 10 - 7 - 6 - 4 - 2 \\
 &\quad + 3 + 2 + 1 + 0 - 0 \\
 &= 78
 \end{aligned}$$

und damit insgesamt $100 - 78 + 4 = 26$ Primzahlen (einschliesslich der 1).

1.3 Anzahlbestimmungen

— Di., 29.4. (V1) —

Die Prinzipien aus beiden vorangegangenen Abschnitten werden wir jetzt benutzen, um typische Anzahlprobleme zu lösen, bei denen

- aus den Elementen einer Menge Teilmengen gebildet
- die Elemente einer Menge in Klassen eingeteilt
- Elemente einer Menge angeordnet

werden, und diese dann auf Anzahlen von Abbildungen verallgemeinern.

1.3.1 Teilmengen

Die Menge aller Teilmengen einer Menge M heisst deren Potenzmenge, $\mathcal{P}(M)$.

1.20 Satz

Für jede Menge M mit $|M| = n \in \mathbb{N}_0$ Elementen gilt

$$|\mathcal{P}(M)| = 2^n .$$

■ **Beweis:** Sei $M = \{a_1, \dots, a_n\}$, also $|M| = n$. Wir wenden zunächst das Identitätsprinzip an und definieren dazu die Bijektion $\chi : \mathcal{P}(M) \rightarrow \{0, 1\}^n$, die jede Teilmenge $S \subseteq M$ auf eine Folge von Nullen und Einsen (den so genannten *charakteristischen Vektor*) abbildet:

$$\chi(S) = (b_1, \dots, b_n) \quad \Leftrightarrow \quad b_i = \begin{cases} 1 & \text{falls } a_i \in S \\ 0 & \text{falls } a_i \notin S \end{cases} \quad \text{für alle } i = 1, \dots, n.$$

Mit der Produktregel sehen wir sofort, dass $|\{0, 1\}^n| = 2^n$. □

Die Potenzmenge wird daher auch oft mit 2^M bezeichnet.

1.21 Satz

Für alle $n \in \mathbb{N}_0$ gilt

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$

■ **Beweis:** Für $M = \{1, \dots, n\}$ gilt nach obigem Satz $|\mathcal{P}(M)| = 2^n$. Andererseits sind die Mengen S_k , $k = 0, \dots, n$, der k -elementigen Teilmengen von M offensichtlich disjunkt, sodass mit der Summenregel

$$|\mathcal{P}(M)| = \left| \biguplus_{k=0}^n S_k \right| = \sum_{k=0}^n |S_k| = \sum_{k=0}^n \binom{n}{k}$$

gilt. □

Wir haben in Beispiel 1.7 bereits bewiesen, dass Binomialkoeffizienten als Summe solcher mit kleineren Parametern ausgedrückt werden können:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Da für die Randfälle $k = 0$ und $k = n$ die Binomialkoeffizienten konstant gleich 1 sind, können wir mit dieser Rekursionsformel alle Binomialkoeffizienten nach folgendem Schema (dem *Pascalschen Dreieck*) auch ohne Fakultäten

berechnen:

$n :$	0	1	2	3	4	5	6	\dots
$k = 0$	1	1	1	1	1	1	1	\dots
1		1	2	3	4	5	6	\dots
2			1	3	6	10	15	\dots
3				1	4	10	20	\dots
4					1	5	15	\dots
5						1	6	\dots
6							1	\dots
\vdots								\ddots
Σ	1	2	4	8	16	32	64	\dots

Wir werden darauf in Kapitel 3 zurück kommen und beweisen hier noch eine Rekursion mit größeren Schritten.

1.22 Satz (Vandermonde-Identität)

$$\binom{n+m}{k} = \sum_{l=0}^k \binom{n}{l} \binom{m}{k-l}.$$

■ **Beweis:** Betrachte zwei disjunkte Mengen N und M mit $|N| = n$ und $|M| = m$. Für die Menge S der k -Teilmengen von $N \uplus M$ gilt $|S| = \binom{n+m}{k}$.

Um die Summenregel anwenden zu können, zerlegen wir S entsprechend der Anzahl von Elementen aus N , die in den in S enthaltenen Mengen vorkommen. Für $l = 0, \dots, k$ sei also $S_l \subseteq S$ die Menge der k -Teilmengen von $N \cup M$, die genau l Elemente aus N (und damit genau $k-l$ Elemente aus M) enthalten.

Es gibt damit $\binom{n}{l}$ viele Möglichkeiten, die l Elemente aus N zu wählen, und $\binom{m}{k-l}$ viele Möglichkeiten, die $k-l$ Elemente aus M zu wählen. Jede Kombination dieser Möglichkeiten liefert eine k -elementige Teilmenge von $N \uplus M$, und es gilt daher $|S_l| = \binom{n}{l} \binom{m}{k-l}$ für alle $l = 0, \dots, k$ (man überlege sich diesen Schritt als Anwendung der Summen- oder Produktregel!). Insgesamt gilt also

$$\binom{n+m}{k} = |S| = |S_0 \uplus \dots \uplus S_k| = \sum_{l=0}^k |S_l| = \sum_{l=0}^k \binom{n}{l} \binom{m}{k-l}.$$

□

1.3.2 Zerlegungen

— Di., 6.5. (V1) —

Mengenpartitionen

Wir haben nun schon mehrfach Mengen in disjunkte Teilmengen zerlegt, um die Summenregel anwenden zu können. Hier fragen wir danach, wieviele solcher Zerlegungen es überhaupt gibt, d.h. nach der Anzahl von möglichen Äquivalenzrelationen.

Wieviele Möglichkeiten gibt es, n Objekte in k Klassen einzuteilen?

Die gesuchten Anzahlen werden Stirlingzahlen 2. Art genannt und mit $S_{n,k}$ bezeichnet.

1.23 Beispiel

Wieviele Möglichkeiten gibt es, aus vier Personen zwei Gruppen zu bilden?

Für $M = \{1, 2, 3, 4\}$ ist

$$\begin{aligned} M &= \{1\} \uplus \{2, 3, 4\} = \{2\} \uplus \{1, 3, 4\} = \{3\} \uplus \{1, 2, 4\} = \{4\} \uplus \{1, 2, 3\} \\ &= \{1, 2\} \uplus \{3, 4\} = \{1, 3\} \uplus \{2, 4\} = \{1, 4\} \uplus \{2, 3\}, \end{aligned}$$

und es gibt keine weiteren Möglichkeiten, d.h. $S_{4,2} = 7$.

Zwar sind alle Randfälle $k = 1$ und $k = n$ wieder klar, denn dann sind entweder alle Elemente in der selben Klasse, oder jedes in einer Klasse für sich. Im allgemeinen Fall scheint die Anzahlbestimmung nicht so ganz einfach zu sein. Wir zeigen, dass wie bei den Binomialkoeffizienten eine rekursive Berechnung möglich ist.

1.24 Satz (Rekursionsformel für Stirlingzahlen 2. Art)

Für alle $n, k \in \mathbb{N}$ gilt

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$$

$$\begin{aligned} S_{0,0} &:= 1 \\ S_{n,0} &:= 0 \text{ für } n > 0 \\ S_{n,k} &:= 0 \text{ für } n < k \end{aligned}$$

■ **Beweis:** Wir verwenden wieder ein Pascal-Argument: Betrachte ein M mit $|M| = n$ und ein Element $a \in M$. Die Klasse, in die a eingeteilt wird, besteht entweder nur aus a , oder sie enthält auch andere Elemente. Im ersten Fall werden die anderen $n - 1$ Elemente in $k - 1$ Klassen eingeteilt, wofür es $S_{n-1,k-1}$ Möglichkeiten gibt. Im zweiten Fall sind die anderen $n - 1$ Elemente in k Klassen eingeteilt worden (wofür es $S_{n-1,k}$ Möglichkeiten gibt) und a kann in jeder dieser k Klassen liegen. \square

Mit dieser Rekursionsformel erhalten wir auch für die Stirlingzahlen 2. Art ein Dreiecks-Schema

$n :$	0	1	2	3	4	5	6	\dots
$k = 0$	1	0	0	0	0	0	0	\dots
1		1	1	1	1	1	1	\dots
2			1	3	7	15	31	\dots
3				1	6	25	90	\dots
4					1	10	65	\dots
5						1	15	\dots
6							1	\dots
\vdots								\ddots
Σ	1	1	2	5	15	52	203	\dots

dessen Spaltensummen

$$B_n = \sum_{k=0}^n S_{n,k}$$

die Anzahl aller *Partitionen* (Zerlegungen in disjunkte Klassen) einer n -elementigen Menge angeben und Bellzahlen genannt werden. Auch für diese gilt eine Rekursionsformel.

1.25 Satz (Rekursionsformel für Bellzahlen)

Für alle $n \in \mathbb{N}_0$ gilt

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} \cdot B_k .$$

■ **Beweis:** Für eine Menge M mit $|M| = n + 1$ ist die Anzahl aller Partitionen nach Definition B_{n+1} . Für die rechte Seite verwenden wieder ein Pascal-Argument und betrachten dazu ein festes Element $a \in M$.

Die Partitionen von M unterscheiden wir zunächst danach, wieviele Elemente *nicht* mit a zusammen in einer Klasse sind. Diese $k \in \{0, \dots, n\}$ Elemente können auf $\binom{n}{k}$ verschiedene Weisen gewählt und auf jeweils B_k Weisen partitioniert werden. □

Zahlpartitionen

— Do., 8.5. (V2) —

Sind wir nur an den Kardinalitäten der gebildeten Klassen interessiert, ist das Abzählproblem identisch mit den Zerlegungen einer Zahl in ihre Summanden

(Identitätsregel).

Wieviele Möglichkeiten gibt es, die Zahl n als Summe von k Zahlen zu schreiben?

Wie bei den Mengen sprechen wir von den *Partitionen* einer Zahl $n \in \mathbb{N}_0$ in k Summanden, aber wie bei den Auswahlen unterscheiden wir zwischen geordneten und ungeordneten Partitionen.

1.26 Beispiel

Die Zahl $n = 4$ lässt sich auf drei Weisen als geordnete Summe zweier Zahlen schreiben,

$$4 = 1 + 3 = 3 + 1 = 2 + 2 ,$$

von denen zwei auch ungeordnet (d.h. wenn die Reihenfolge nicht berücksichtigt wird) verschieden.

Wieder ist der geordnete Fall einfacher als der ungeordnete.

1.27 Satz

Für alle $n, k \in \mathbb{N}$ gibt es

$$\binom{n-1}{k-1}$$

geordnete Partitionen von n mit k Summanden.

■ **Beweis:** Da sich jede Zahl n als Summe von n Einsen darstellen lässt, kann jede geordnete k -Partition $n = n_1 + \dots + n_k$ als Zusammenfassung dieser Einsen zu k Summanden n_i aufgefasst werden:

$$n = \underbrace{1 + 1 + 1}_{n_1} + \underbrace{1}_{n_2} + \underbrace{1 + 1 + 1 + 1 + 1}_{n_3} + \dots + \underbrace{1 + 1}_{n_k} .$$

Jede k -Partition ist dadurch die Wahl der $k - 1$ von $n - 1$ Additionen, die nicht zusammengefasst werden, eindeutig bestimmt. □ analog zu k -Multimengen

1.28 Folgerung

Eine Zahl $n \in \mathbb{N}$ lässt sich auf

Summenregel
(Anzahl Summanden)

$$\sum_{k=1}^n \binom{n-1}{k-1} = 2^{n-1}$$

verschiedene Weisen als geordnete Summe schreiben.

Für die ungeordneten Partitionen können wir hier nur eine Rekursion zeigen. Dazu bezeichne $P_{n,k}$ die Anzahl der ungeordneten k -Partitionen von n , von denen es für die Randfälle $k = 1$ und $k = n$ wieder genau eine gibt.

1.29 Satz

Für alle $n, k \in \mathbb{N}$ gilt

$$P_{n,k} = P_{n-k,k} + P_{n-1,k-1} .$$

$$\begin{aligned} P_{0,0} &:= 1 \\ P_{n,0} &:= 0 \text{ für } n > 0 \\ P_{n,k} &:= 0 \text{ für } n < k \end{aligned}$$

■ **Beweis:** Da die Reihenfolge der Summanden nicht berücksichtigt wird, können wir annehmen, dass sie nicht-aufsteigend sortiert sind. Eine solchermaßen sortierte Partition von n in k Summanden stellen wir durch ein *Ferrers-Diagramm* dar, d.h. durch k linksbündige Zeilen mit insgesamt n Punkten, von denen die i -te gerade so viele Punkte enthält wie der i -te Summand groß ist. Für Beispiel 1.26 erhalten wir

$$\begin{array}{c} 4 = 3 + 1 = 2 + 2 \\ \bullet \bullet \bullet \quad \bullet \bullet \\ \bullet \quad \bullet \bullet \end{array}$$

Für die k -Partitionen von n können wir dann zwei Fälle unterscheiden:

1. *Alle Summanden sind größer als 1:*
Streich man die k Punkte in der linkensten Spalte des Ferrers-Diagramms, so bleibt in jeder Zeile mindestens ein Punkt übrig.



Die verbleibenden $n - k$ Punkte entsprechen daher einer k -Partition von $n - k$, von denen es $P_{n-k,k}$ gibt.

2. *Mindestens ein Summand ist 1:*
Streichen wir die letzte Zeile des Ferrers-Diagramms (in der genau ein Punkt steht), dann erhalten wir das Ferrers-Diagramm einer $k - 1$ -Partition von $n - 1$.



Davon gibt es $P_{n-1,k-1}$ viele.

Die Behauptung folgt mit der Summenregel. □

Auch aus dieser Rekursionsformel erhalten wir ein Dreiecks-Schema

$n :$	0	1	2	3	4	5	6	\dots
$k = 0$	1	0	0	0	0	0	0	\dots
1		1	1	1	1	1	1	\dots
2			1	1	2	2	3	\dots
3				1	1	2	3	\dots
4					1	1	2	\dots
5						1	1	\dots
6							1	\dots
\vdots								\ddots
Σ	1	1	2	3	5	7	11	\dots

dessen Spaltensummen

$$P_n = \sum_{k=0}^n P_{n,k}$$

die Anzahl aller Summendarstellungen der Zahl n angeben und Partitionszahlen genannt werden. Der langsame Beginn täuscht, auch die Partitionszahlen werden schnell größer.

$$P_{500} > 2 \cdot 10^{21}$$

1.3.3 Abbildungen

Durch die Identitätsregel können alle bisher behandelten Anzahlprobleme als Spezialfälle der folgenden Frage betrachtet werden:

Wieviele Abbildungen von einer k -Menge in eine n -Menge gibt es?

Wir betrachten also Abbildungen $\alpha : D \rightarrow R$ mit $|D| = k$ und $|R| = n$. Die Spezialfälle ergeben sich einerseits aus der Forderung, dass die Abbildungen injektiv, surjektiv oder sogar bijektiv sein sollen, und andererseits aus der Unterscheidung der Elemente in D , in R oder in D und R (d.h. wir zählen z.B. Abbildungen, die sich nur durch Permutation der Mengen von einander unterscheiden, nicht mehrfach).

D : domain
 R : range

$\alpha : D \rightarrow R$ $ D = d, R = r$		alles unterschieden	nur D permutierbar	nur R permutierbar	D und R permutierbar
		A	B	C	D
beliebig $r, d \in \mathbb{N}$	1	r^d	$\binom{r+d-1}{d}$	$\sum_{i=1}^r S_{d,i}$ $= B_d, \text{ falls } r \geq d$	$\sum_{i=1}^r P_{d,i}$ $= P_d, \text{ falls } r \geq d$
injektiv $r \geq d \in \mathbb{N}$	2	$r^{\underline{d}}$	$\binom{r}{d}$	1	1
surjektiv $d \geq r \in \mathbb{N}$	3	$r! S_{d,r}$	$\binom{d-1}{r-1}$	$S_{d,r}$	$P_{d,r}$
bijektiv $d = r \in \mathbb{N}$	4	$r! = d!$	1	1	1

Deutet man D als Menge von Zeitpunkten und die Bilder von α als Auswahlen, bedeutet die Permutierbarkeit von D , dass Reihenfolgen unterschieden werden, und die Injektivität von α , dass Wiederholungen ausgeschlossen werden. Die vier Felder links oben sind daher wie in Abschnitt 1.1.

Die vier Einsen in (C2), (C4), (D2) und (D4) erklären sich daraus, dass injektive Abbildungen durch Permutation der Bilder in einander überführt werden können, und (A4) und (B4) sind gerade die Permutationen.

Die Felder (C1) und (D1) ergeben sich aus der Zusammenfassung derjenigen Elemente von D (bzw. ihrer Anzahl), die ein gemeinsames Bild haben.

Feld (C3) ergibt sich ebenfalls aus der Zusammenfassung der Elemente von D mit gleichem Bild, da α surjektiv sein muss, sind dies aber gerade R viele Klassen. In Spalte A wird noch unterschieden, welches Element in R das Bild ist, und in den den Spalten B und D kommt es nur darauf an, wieviele Elemente von D jeweils ein gemeinsames Bild haben.

1.3.4 Permutationen

Wir betrachten noch eine spezielle Einteilung in Äquivalenzklassen, die sich aus den Eigenschaften einer Permutation ergibt.

Formal ist eine Permutation eine bijektive Abbildung $\pi : M \rightarrow M$ in sich selbst. Wegen des Identitätsprinzips können wir für Anzahlprobleme wieder $M = \{1, \dots, n\}$ annehmen. Jede Permutation von $\{1, \dots, n\}$ lässt sich in der

Form

$$\begin{array}{c|cccccc} i \in M & 1 & 2 & 3 & \cdots & n \\ \hline \pi(i) & \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{array}$$

notieren und, da die erste Zeile immer gleich ist, reicht auch die Angabe der Bilder in dieser Reihenfolge. (Erinnerung: Wir hatten Permutationen gerade als die Anordnungen einer n -elementige Menge eingeführt.)

Es gibt noch eine andere Schreibweise, für die wir zunächst betrachten was passiert, wenn π mehrmals angewendet wird. Sei $1 \leq i \leq n$ beliebig. Spätestens nach n -maliger Anwendung kommt unter den Werten

$$i, \pi(i), \underbrace{\pi(\pi(i))}_{\pi^2(i)}, \underbrace{\pi(\pi(\pi(i)))}_{\pi^3(i)}, \dots, \underbrace{\pi(\cdots \pi(\pi(i)) \cdots)}_{\pi^n(i)},$$

ein Wert doppelt vor (Taubenschlagprinzip). Sei $1 \leq j \leq n$ ein solcher Wert mit $\pi^k(j) = j$, wobei $k \in 1, \dots, n$ minimal gewählt sei. Das heißt aber, dass sich die Folge $(j, \pi(j), \dots, \pi^{k-1}(j))$ bei weiterer Anwendung von π periodisch wiederholt (auch das Element i) und aus lauter verschiedenen Werte besteht (andernfalls gäbe es darunter ein Element mit kürzerer Periode). Wir nennen eine solche Folge *Zykel* der Länge k , und im Fall $k = 1$ sprechen wir von einem *Fixpunkt*.

Da wir von einem beliebigen i gestartet sind, ist jede Zahl in einem Zykel enthalten, die Menge der Zykel bildet damit eine Zerlegung von $\{1, \dots, n\}$. Eine Permutation π können wir daher statt durch die resultierende Anordnung der Zahlen $1, \dots, n$ nach einmaliger Anwendung von π auch durch Angabe der Zykelfolgen beschreiben.

1.30 Beispiel

Wir betrachten die Permutation $\pi : \{1, \dots, 11\} \rightarrow \{1, \dots, 11\}$ mit

$$\begin{array}{c|cccccccccccc} i \in M & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \hline \pi(i) & 5 & 8 & 3 & 6 & 2 & 6 & 4 & 1 & 9 & 11 & 10 \end{array} .$$

Die Permutation hat offensichtlich die Fixpunkte 3 und 9. Ausserdem bilden 10 und 11 einen Zykel, denn $\pi(10) = 11$ und $\pi(11) = 10$. Man prüft leicht nach, dass auch die Folgen $(4 \ 6 \ 7)$ und $(1 \ 5 \ 2 \ 8)$ Zyklen bilden. Stellen wir π durch seine Zykelfolgen dar, erhalten wir also zunächst

$$\pi = (3)(9)(10 \ 11)(4 \ 6 \ 7)(1 \ 5 \ 2 \ 8) .$$

Da die Reihenfolge der Zykel keine Rolle spielt und jeder Zykel zyklisch durchgetauscht werden kann, gilt aber z.B. auch

$$\pi = (11\ 10)(3)(6\ 7\ 4)(9)(2\ 8\ 1\ 5) \neq (11\ 10)(3)(6\ 7\ 4)(9)(8\ 2\ 1\ 5) .$$

Wenn wir nach der Anzahl der Permutationen von $\{1, \dots, n\}$ mit genau k -Zykeln fragen, erhalten wir (weil die Elemente eines Zykel eine Äquivalenzklasse bilden) eine Variante der Frage nach k -Partitionen einer n -Menge.

Die gesuchten Anzahlen heißen Stirlingzahlen der 1. Art und werden mit $s_{n,k}$ bezeichnet. Hier gibt es für die Randfälle $k = 0$ keine (jedes Element ist in einem Zykel) und für $k = n$ genau eine Permutation (die Identität).

1.31 Satz (Rekursionsformel für Stirlingzahlen der 1. Art)

Für alle $n, k \in \mathbb{N}$ gilt

$$s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k} .$$

$$\begin{aligned} s_{0,0} &:= 1 \\ s_{n,0} &:= 0 \text{ für } n > 0 \\ s_{n,k} &:= 0 \text{ für } n < k \end{aligned}$$

■ **Beweis:** Nach Definition ist $s_{n,k}$ die Zahl der Permutationen von $M = \{1, \dots, n\}$ mit genau k Zykeln. Wir verwenden wieder ein Pascal-Argument und betrachten dazu ein $i \in M$.

Entweder a ist ein Fixpunkt, dann gibt es $s_{n-1,k-1}$ Permutationen der $n-1$ übrigen Elemente mit genau $k-1$ Zykeln, oder wir können a in jeder der $s_{n-1,k}$ Permutationen mit k Zykeln vor irgendeinem der $n-1$ anderen Elemente in dessen Zykel eintragen. □

Auch aus dieser Rekursionsformel erhalten wir ein Dreiecks-Schema

$n :$	0	1	2	3	4	5	6	...
$k = 0$	1	0	0	0	0	0	0	...
1		1	1	2	6	24	120	...
2			1	3	11	50	274	...
3				1	6	35	225	...
4					1	10	85	...
5						1	15	...
6							1	...
⋮								⋱
Σ	1	1	2	6	24	120	720	...

für dessen Spaltensummen

$$\sum_{k=0}^n s_{n,k} = n!$$

gilt, weil es sie die Zahl aller Permutation von $\{1, \dots, n\}$ angeben.

Kapitel 2

Diskrete Wahrscheinlichkeitsrechnung

— Di., 13.5. (V1) —

Wahrscheinlichkeiten modellieren Vorgänge, die „zufällig“ erscheinen, weil ihr Ablauf (nach jeweils aktuellem Stand des Wissens) undurchschaubar ist. Sie dienen also dem Umgang mit „Unsicherheit“.

2.1 Beispiel (Würfelspiel)

Zwei Spieler setzen je 1 Euro ein und würfeln nach einander: den Einsatz beider erhält, wer die höhere Zahl hat; bei Gleichstand wird das Geld für einen guten Zweck gespendet.

Aus der Perspektive beider Spieler besteht zunächst größere Unsicherheit über den Ausgang des Spiels. Das Siegesgefühl ändert sich jedoch (auf beiden Seiten) nach dem ersten Wurf. Abhängig davon, wie hoch oder niedrig er ausfällt, verringert sich die Unsicherheit mehr oder weniger stark.

Lässt sich diese Änderung quantifizieren? Ist sie für beide Spieler gleich, d.h. spielt die Reihenfolge des Würfeln eine Rolle? Was ändert sich, wenn der zweite Spieler nach dem ersten Wurf eine Verdopplung des Einsatzes verlangen kann? Oder bei Zuzahlung eines weiteren Euros zwei Würfel benutzen darf, von denen das höhere Ergebnis gewertet wird? Oder der erste Spieler gegen Zahlung von 50 Cent aussteigen darf? Wie oft wird gespendet?

Bei vielen anscheinend „zufälligen“ Vorgängen lassen sich aber zumindest Aussagen darüber machen, wie oft ein Ausgang auftritt, wenn der Vorgang sehr oft wiederholt wird. Die *relative Häufigkeit* eines möglichen Ergebnisses

ist definiert durch das Verhältnis

$$\frac{\text{absolute H\u00e4ufigkeit des Auftretens}}{\text{Anzahl der Versuche}} .$$

Stabilisiert sich dieser Wert bei wachsender Zahl der Versuche, so macht es Sinn, bei dem untersuchten Vorgang davon zu sprechen, dass ein bestimmtes Ergebnis eine bestimmte *Auftrittswahrscheinlichkeit* hat.

2.1 Wahrscheinlichkeitsr\u00e4ume

Nach obiger Diskussion besteht eine geeignete Modellierung f\u00fcr Vorg\u00e4nge mit unsicherem Ausgang darin, die grunds\u00e4tzlich m\u00f6glichen Ausg\u00e4nge zu identifizieren und ihnen als Wahrscheinlichkeit die (vermutete) relative H\u00e4ufigkeit ihres Auftretens zuzuordnen.

2.2 Definition (Wahrscheinlichkeitsraum)

Ein (endlicher) Wahrscheinlichkeitsraum ist ein Paar (Ω, P) bestehend aus einer Menge $\Omega = \{\omega_1, \dots, \omega_n\}$ von Elementarereignissen und einer (Wahrscheinlichkeits)Verteilung $P : \Omega \rightarrow [0, 1]$ mit

$$\sum_{\omega \in \Omega} P(\omega) = 1 .$$

Ein Wahrscheinlichkeitsraum hei\u00dft uniform (auch: Laplacescher Wahrscheinlichkeitsraum), falls $P(\omega) = \frac{1}{|\Omega|}$ f\u00fcr alle $\omega \in \Omega$. Wir setzen die Verteilung auf $\mathcal{P}(\Omega)$ fort durch die Definition

$$P(A) = \sum_{\omega \in A} P(\omega) \quad \text{f\u00fcr alle } A \subseteq \Omega$$

$$\begin{aligned} P(\emptyset) &= 0 \\ P(\{\omega\}) &= P(\omega) \\ P(\Omega) &= 1 \end{aligned}$$

und nennen jedes $A \subseteq \Omega$ ein Ereignis und $P(A)$ seine Wahrscheinlichkeit. Die Menge $T = \{\omega \in \Omega : P(\omega) > 0\}$ der Elementarereignisse mit positiver Wahrscheinlichkeit hei\u00dft Tr\u00e4ger von Ω .

In einem uniformen Wahrscheinlichkeitsraum ist die Bestimmung der Wahrscheinlichkeit eines Ereignisses $A \subseteq \Omega$ im Kern ein Abz\u00e4hlproblem, denn

$$P(A) = \sum_{\omega \in A} P(\omega) = \sum_{\omega \in A} \frac{1}{|\Omega|} = \frac{|A|}{|\Omega|} .$$

2.3 Beispiel (Lotto)

Beim Samstagslotto ist jede mögliche Ziehung (ohne Berücksichtigung der Zusatzzahl) eine Auswahl von 6 Zahlen aus $\{1, \dots, 49\}$ (ohne Wiederholungen und ohne Berücksichtigung der Ziehungsreihenfolge). Wir setzen daher $\Omega = \{Z \subseteq \{1, \dots, 49\} : |Z| = 6\}$.

Bei ordnungsgemäßem Zustand des Ziehungsgeräts ist jede Ziehung gleich wahrscheinlich, wir können daher von einem uniformen Wahrscheinlichkeitsraum (Ω, P) ausgehen. Jede Ziehung $Z \in \Omega$ ist somit ein Elementarereignis mit Wahrscheinlichkeit

$$P(Z) = \frac{|Z|}{|\Omega|} = \frac{1}{\binom{49}{6}} = \frac{1}{13.983.816}.$$

Dies ist daher auch die Wahrscheinlichkeit, mit einem Tipp $T = \{t_1, \dots, t_6\}$ sechs Richtige zu haben. Mit T genau drei Richtige zu haben entspricht dem Ereignis $\{Z \in \Omega : |T \cap Z| = 3\}$, das die Wahrscheinlichkeit

$$\frac{|\{Z \in \Omega : |T \cap Z| = 3\}|}{|\Omega|} = \frac{\binom{6}{3} \binom{43}{3}}{\binom{49}{6}} \in \left[\frac{1}{56}, \frac{1}{57} \right]$$

hat. Wie groß ist die Wahrscheinlichkeit für mindestens drei Richtige? Warum gewinnt man nicht auch schon mit zwei Richtigen etwas?

Die Fragen können wir bald beantworten. Es ist jedoch nicht immer so einfach, den „richtigen“ Wahrscheinlichkeitsraum zu bestimmen.

2.4 Beispiel (Paradoxon von de Meré)

In einem weiteren Würfelspiel mit zwei Spielern werden die Augenzahlen dreier Würfel addiert: Der eine Spieler gewinnt bei Summe 11, der andere bei Summe 12. Wer gewinnt öfter?

3-Würfel-Partitionen von 11	3-Würfel-Partitionen von 12
6 4 1	6 5 1
6 3 2	6 4 2
5 5 1	6 3 3
5 4 2	5 5 2
5 3 3	5 4 3
4 4 3	4 4 4
$P_{11,3} = 6$ Möglichkeiten	$P_{12,3} = 6$ Möglichkeiten

Also kein Vorteil für einen der Spieler? Was für ein Wahrscheinlichkeitsraum — Do., 15.5. (V1) — wurde hier verwendet? Ist das angemessen?

Setze $\Omega = \{1, \dots, 6\}^3$ (Vorstellung: Würfel haben verschiedene Farben). Die beiden Ereignisse

$$\begin{aligned} S_{11} &= \{(w_1, w_2, w_3) \in \Omega : w_1 + w_2 + w_3 = 11\} \\ S_{12} &= \{(w_1, w_2, w_3) \in \Omega : w_1 + w_2 + w_3 = 12\} \end{aligned}$$

modellieren dann, dass die Summe 11 bzw. 12 ergibt. Wenn alle Würfel fair sind, können wir einen uniformen Wahrscheinlichkeitsraum annehmen. In diesem gilt

$$P(S_{11}) = \frac{|S_{11}|}{|\Omega|} \quad \text{und} \quad P(S_{12}) = \frac{|S_{12}|}{|\Omega|} .$$

Da nur die Zahlen $1, \dots, 6$ als Summanden infrage kommen, können wir die Anzahlen nicht über die geordneten Partitionen von 11 bzw. 12 mit drei Summanden bestimmen. Stattdessen können wir z.B. die Permutationen der obigen Partitionen aufsummieren oder mit Summenregel nach der Augenzahl des ersten Würfels und der des zweiten Würfels unterscheiden. Daraus ergibt sich

$$P(S_{11}) = \frac{|S_{11}|}{|\Omega|} = \frac{27}{216} \quad \text{und} \quad P(S_{12}) = \frac{|S_{12}|}{|\Omega|} = \frac{25}{216} ,$$

der erste Spieler hat also größere Gewinnchancen. Für den in den Anfangsüberlegungen impliziten Wahrscheinlichkeitsraum folgt, dass den Elementarereignissen (den ungeordneten Partitionen) nicht die gleiche Wahrscheinlichkeit zugeordnet werden darf.

2.5 Beispiel (Hashing)

Gegeben seien k Daten, die in einem Array der Länge $n \geq k$ abgelegt werden sollen. Wie wahrscheinlich ist bei zufälliger Auswahl der Positionen das Auftreten einer Kollision?

Die Menge $\Omega = \{1, \dots, n\}^k$ beschreibt die möglichen Zuweisungen der k Daten an die n Positionen. Das Ereignis A der kollisionsfreien Ablagen entspricht der Menge der k -Permutationen (geordnete Auswahl ohne Wiederholungen).

Es gilt daher

$$\begin{aligned}
 P(A) &= \frac{|A|}{|\Omega|} = \frac{n^k}{n^k} = \frac{n}{n} \cdot \frac{n-1}{n} \cdot \dots \cdot \frac{n-k+1}{n} = \prod_{i=0}^{k-1} \left(1 - \frac{i}{n}\right) \\
 &= \exp\left(\sum_{i=0}^{k-1} \ln\left(1 - \frac{i}{n}\right)\right) \stackrel{\substack{\text{für } x < 1 \text{ gilt} \\ \ln(1-x) \leq -x}}{\leq} \exp\left(-\sum_{i=0}^{k-1} \frac{i}{n}\right) \\
 &= \exp\left(-\frac{k(k-1)}{2n}\right).
 \end{aligned}$$

Will man mit einer vorgegebenen Wahrscheinlichkeit $p \in (0, 1)$ Kollisionen vermeiden, sollte daher gelten $k < \sqrt{2n|\ln p|}$.

Für $n = 365$ ist die Frage auch als „Geburtstagsparadoxon“ bekannt: Nimmt man gleichverteilte Geburtstage bei konstant 365 Tagen pro Jahr an, dann haben unter 23 zufällig gewählten Personen nur mit Wahrscheinlichkeit kleiner $\frac{1}{2}$ keine zwei am gleichen Tag Geburtstag. (Die Näherung liefert hierfür die Schranke $\sqrt{2 \cdot 365 \cdot |\ln \frac{1}{2}|} \sim 22,49$).

2.6 Satz

Ist (Ω, P) ein Wahrscheinlichkeitsraum, dann gilt

- (i) $P(\Omega \setminus A) = 1 - P(A)$ für alle Ereignisse $A \subseteq \Omega$.
- (ii) $P(A) \leq P(B)$ für alle Ereignisse $A \subseteq B \subseteq \Omega$.
- (iii) $P(A_1 \uplus \dots \uplus A_k) = \sum_{i=1}^k P(A_i)$ für disjunkte Ereignisse $A_1, \dots, A_k \subseteq \Omega$.

■ **Beweis:** Zunächst gilt (iii), denn

$$P(A_1 \uplus \dots \uplus A_k) = \sum_{\omega \in \uplus_{i=1}^k A_i} P(\omega) = \sum_{i=1}^k \sum_{\omega \in A_i} P(\omega) = \sum_{i=1}^k P(A_i).$$

(Für uniforme Wahrscheinlichkeitsräume folgt die Aussage sofort aus der Summenregel). Damit folgt (i) aus

$$1 = P(\Omega) = P(A \uplus (\Omega \setminus A)) = P(A) + P(\Omega \setminus A)$$

und (ii) gilt wegen

$$P(B) = P(A \uplus (B \cap (\Omega \setminus A))) = P(A) + P(B \cap (\Omega \setminus A)) \geq P(A).$$

□

2.7 Beispiel (Binäre Suche)

In einem Array M mit Indizes $\{1, \dots, 2^k - 1\}$ seien Zahlen nicht-absteigend sortiert gespeichert. Um festzustellen, ob und bei welchem Index eine Zahl $x \in \mathbb{N}_0$ in M vorkommt, vergleicht man x mit dem mittleren Element und unterscheidet drei Fälle:

$$\begin{aligned} x < M[2^{k-1}] & \quad \text{suche weiter in } M[1, \dots, 2^{k-1} - 1] \\ x = M[2^{k-1}] & \quad x \text{ gefunden} \\ x > M[2^{k-1}] & \quad \text{suche weiter in } M[2^{k-1} + 1, \dots, \underbrace{2^{k-1} + (2^{k-1} - 1)}_{=2^k - 1}] \end{aligned}$$

Ist der verbleibende Indexbereich leer, ist $x \notin M$. Wie groß ist die Wahrscheinlichkeit, dass die Suche nach genau i Schritten beendet ist?

Bezeichne $\Omega = \{\star, 1, \dots, 2^k - 1\}$ die Menge der Elementarereignisse, dass x bei Index $\omega \in \Omega$ gefunden wird, wobei $\omega = \star$ den Fall $x \notin M$ kennzeichne. Ferner sei A_i das Ereignis, dass das Element nach genau i Schritten gefunden wird. Dann ist

$$\begin{aligned} A_1 &= \{2^{k-1}\} \\ A_2 &= \{2^{k-2}, 2^{k-1} + 2^{k-2}\} \\ A_3 &= \{2^{k-3}, 2^{k-2} + 2^{k-3}, 2^{k-1} + 2^{k-3}, 2^{k-1} + 2^{k-2} + 2^{k-3}\} \\ &\vdots \end{aligned}$$

also $|A_i| = 2^{i-1}$ für alle $i = 1, \dots, k$. Unterstellen wir einen Laplaceschen Wahrscheinlichkeitsraum (d.h. x kommt an jedem Index bzw. gar nicht mit gleicher Wahrscheinlichkeit vor), dann gilt

$$P(A_i) = \frac{|A_i|}{|\Omega|} = \frac{2^{i-1}}{2^k} = \frac{1}{2^{k-i+1}} \quad \text{für alle } i = 1, \dots, k.$$

Das Ereignis $A_{\leq i}$, das Element nach höchstens i Schritten zu finden, tritt mit Wahrscheinlichkeit

$$P(A_{\leq i}) = P\left(\biguplus_{j=1}^i A_j\right) = \sum_{j=1}^i P(A_j) = \sum_{j=1}^i \frac{2^{j-1}}{2^k} = \frac{1}{2^k} \sum_{j=1}^i 2^{j-1} = \frac{2^i - 1}{2^k}$$

ein. Beachte, dass der ungünstigste Fall $A_k \uplus \{\star\} = \Omega \setminus A_{\leq k-1}$ folglich mit Wahrscheinlichkeit $1 - P(A_{\leq k-1}) = 1 - \frac{2^{k-1} - 1}{2^k} > \frac{1}{2}$ eintritt!

Die Fragen am Ende von Beispiel 2.3 (Lotto) dürften nun kein Problem mehr darstellen.

Wie bei der Summenregel können wir auch für die Wahrscheinlichkeiten der Vereinigung nicht-disjunkter Ereignisse eine Verallgemeinerung angeben.

2.8 Satz (Siebformel, Satz von Poincaré/Sylvester)

Ist (Ω, P) ein Wahrscheinlichkeitsraum, dann gilt

$$P\left(\bigcup_{i=1}^k A_i\right) = \sum_{l=1}^k (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq k} P\left(\bigcap_{j=1}^l A_{i_j}\right)$$

für alle $A_1, \dots, A_k \subseteq \Omega$.

■ **Beweis:** Vollständige Induktion über die Anzahl k der Ereignisse:

$k \leq 2$: Für $k = 1$ ist nichts zu zeigen. Weil sich daraus eine für den Induktionsschluss nützliche Beziehung ablesen lässt, rechnen wir für $k = 2$ aus:

$$\begin{aligned} P(A_1 \cup A_2) &= P(((A_1 \cup A_2) \setminus (A_1 \cap A_2)) \uplus (A_1 \cap A_2)) \\ &= P((A_1 \cup A_2) \setminus (A_1 \cap A_2)) + P(A_1 \cap A_2) \\ &= P((A_1 \setminus (A_1 \cap A_2)) \uplus (A_2 \setminus (A_1 \cap A_2))) + P(A_1 \cap A_2) \\ &= (P(A_1) - P(A_1 \cap A_2)) + (P(A_2) - P(A_1 \cap A_2)) + P(A_1 \cap A_2) \\ &= P(A_1) + P(A_2) - P(A_1 \cap A_2). \end{aligned} \tag{2.1}$$

vgl.
Flächen
im Venn-
Diagramm

$k + 1 > 2$:

$$\begin{aligned}
 P\left(\bigcup_{i=1}^{k+1} A_i\right) & \stackrel{(2.1)}{=} P(A_{k+1}) + P\left(\bigcup_{i=1}^k A_i\right) - P\left(A_{k+1} \cap \bigcup_{i=1}^k A_i\right) \\
 & \stackrel{2 \times \text{Induktions-}}{\text{voraussetzung}}{=} P(A_{k+1}) \\
 & \quad + \sum_{l=1}^k (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq k} P\left(\bigcap_{j=1}^l A_{i_j}\right) \\
 & \quad - \sum_{l=1}^k (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq k} P\left(\bigcap_{j=1}^l (A_{i_j} \cap A_{k+1})\right) \\
 & = P(A_{k+1}) \\
 & \quad + \sum_{l=1}^k (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq k} P\left(\bigcap_{j=1}^l A_{i_j}\right) \\
 & \quad + \sum_{l=2}^{k+1} (-1)^{l-1} \sum_{\substack{1 \leq i_1 < \dots < i_{l-1} \leq k \\ i_l = k+1}} P\left(\bigcap_{j=1}^l A_{i_j}\right) \\
 & = \sum_{l=1}^k (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq k} P\left(\bigcap_{j=1}^l A_{i_j}\right).
 \end{aligned}$$

□

— Di., 20.5. (V1) —

2.9 Beispiel (Vorsortierung)

Wir betrachten ein Array der Länge n mit verschiedenen vergleichbaren Elementen, o.E. $\{1, \dots, n\}$. Es sei Ω die Menge aller Permutationen von $\{1, \dots, n\}$. Annahme: $P(\omega) = \frac{1}{n!}$ für alle $\omega \in \Omega$ (Laplacescher Wahrscheinlichkeitsraum).

Wie groß ist die Wahrscheinlichkeit, dass mindestens k Elemente schon an der richtigen Stelle stehen? (Interessant für manche Sortieralgorithmen).

$k = 1$: Definiere Ereignisse $A_i = \{\omega = (w_1, \dots, w_n) \in \Omega : w_i = i\}$ („das i -te Element steht an der richtigen Stelle“). Wahrscheinlichkeit, dass mindestens ein Element richtig steht, ist dann $P(\bigcup_{i=1}^n A_i)$.

Wir betrachten zunächst eine beliebige Auswahl $1 \leq i_1 < \dots < i_l \leq n$ von $l \in \{1, \dots, n\}$ vorsortierten Elementen. Dann ist $\bigcap_{j=1}^l A_{i_j} = \{(w_1, \dots, w_n) \in$

$\Omega : w_{i_j} = i_j, j = 1, \dots, l$. Es können also nur noch $n - l$ Elemente frei permutiert werden, sodass

$$P\left(\bigcap_{j=1}^l A_{i_j}\right) = \frac{\left|\bigcap_{j=1}^l A_{i_j}\right|}{|\Omega|} = \frac{(n-l)!}{n!} = \frac{1}{\binom{n}{l}l!}.$$

Nach dieser Vorbereitung können wir die Siebformel anwenden und erhalten

$$\begin{aligned} P\left(\bigcup_{i=1}^n A_i\right) &= \sum_{l=1}^n (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq n} P\left(\bigcap_{j=1}^l A_{i_j}\right) \\ &= \sum_{l=1}^n (-1)^{l-1} \sum_{1 \leq i_1 < \dots < i_l \leq n} \frac{1}{\binom{n}{l}l!} \\ &= \sum_{l=1}^n (-1)^{l-1} \binom{n}{l} \cdot \frac{1}{\binom{n}{l}l!} \\ &= 1 - \frac{1}{2!} + \frac{1}{3!} - + \dots + \frac{(-1)^{n-1}}{n!} \\ &= 1 - \underbrace{\left(1 - \frac{1}{1!} + \frac{1}{2!} - + \dots + \frac{(-1)^n}{n!}\right)}_{\xrightarrow{n \rightarrow \infty} e^{-1}} \\ &\xrightarrow{n \rightarrow \infty} 1 - \frac{1}{e} \sim 0,6321. \end{aligned}$$

$k > 1$: Wahrscheinlichkeit für mindestens k vorsortierte Elemente ist

$$\begin{aligned} P\left(\bigcup_{1 \leq i_1 < \dots < i_k \leq n} \bigcap_{j=1}^k A_{i_j}\right) &\stackrel{\text{ÜBUNG}}{\leq} \sum_{1 \leq i_1 < \dots < i_k \leq n} P\left(\bigcap_{j=1}^k A_{i_j}\right) \\ &= \binom{n}{k} \cdot \frac{1}{\binom{n}{k}k!} = \frac{1}{k!} \end{aligned}$$

Die Wahrscheinlichkeiten fallen also mit wachsender Anzahl vorsortierter Elemente sehr schnell. Man beachte, dass die Schranke unabhängig von n ist.

2.2 Bedingung und Unabhängigkeit

Vorwissen schränkt die Zahl der möglichen Ereignisse ein, kann also die Unsicherheit über den Ausgang eines Vorgangs reduzieren.

2.10 Beispiel

Das einleitende Würfelbeispiel können wir durch einen uniformen Wahrscheinlichkeitsraum (Ω, P) mit $\Omega = \{1, \dots, 6\}^2$ modellieren. Die Gewinnwahrscheinlichkeit des zweiten Spielers ist die Wahrscheinlichkeit des Ereignisses $G = \{(w_1, w_2) \in \Omega : w_1 < w_2\}$, also $P(G) = \frac{|G|}{|\Omega|} = \frac{15}{36}$.

Wenn der erste Spieler nun aber schon eine 4 gewürfelt hat? Dann passt das Modell nicht mehr, da es unmögliche Fälle mit positiven Wahrscheinlichkeiten enthält. In einem neuen, ebenfalls uniformen Modell über $\Omega' = \{1, \dots, 6\}$ (mögliche Augenzahlen des zweiten Wurfs) reduziert sich die Gewinnwahrscheinlichkeit des zweiten Spielers auf $P'(G') = P'(\{5, 6\}) = \frac{1}{3}$.

Durch die folgende Definition kann Vorwissen in bestehenden Modellen ausgedrückt werden.

2.11 Definition

Sind (Ω, P) ein Wahrscheinlichkeitsraum und B ein Ereignis mit $P(B) > 0$, dann heißt die Abbildung $P_B : \mathcal{P}(\Omega) \rightarrow [0, 1]$ definiert durch

$$P_B(A) = P(A|B) = \frac{P(A \cap B)}{P(B)} \quad \text{für alle } A \subseteq \Omega$$

bedingte Verteilung unter der Annahme (Hypothese, Bedingung) B und $P(A|B)$ die bedingte Wahrscheinlichkeit von A (auch: A gegeben B).

Im obigen Beispiel ist die Annahme $B = \{4\} \times \{1, \dots, 6\}$ und wir erhalten wie gewünscht

$$P(G|B) = \frac{P(G \cap B)}{P(B)} = \frac{\frac{|G \cap B|}{|\Omega|}}{\frac{|B|}{|\Omega|}} = \frac{|G \cap B|}{|B|} = \frac{1}{3}.$$

2.12 Bemerkung

Man prüft leicht nach, dass die bedingte Verteilung $P_B = P(\cdot|B)$ selbst eine Wahrscheinlichkeitsverteilung (über einem geeigneten definierten Wahrscheinlichkeitsraum) ist.

Auch bei bedingten Verteilungen ist Vorsicht geboten.

2.13 Beispiel

Annahme: Jungen und Mädchen werden mit gleicher Wahrscheinlichkeit geboren. Von einer Familie mit zwei Kindern wissen wir, dass sie eine Tochter hat. Mit welcher Wahrscheinlichkeit ist das andere Kind auch ein Mädchen?

Spontane Antwort: $\frac{1}{2}$, denn das Geschlecht eines Kindes hängt nicht von dem seiner Schwester ab.

Modell: $\Omega = \{\text{Junge, Mädchen}\}^2$ (uniform). Annahme „Eines der Kinder ist ein Mädchen“: $B = \Omega \setminus \{(\text{Junge, Junge})\}$. Dann ist die bedingte Wahrscheinlichkeit für das Ereignis M , dass das andere Kind auch ein Mädchen ist, $P(M|B) = \frac{|\{(Mädchen, Mädchen)\}|}{|B|} = \frac{1}{3}$.

Die spontane Antwort hat nicht berücksichtigt, dass keine Annahme darüber gemacht wurde, welches Kind ein Mädchen ist. Besteht das Vorwissen z.B. darin, dass das ältere Kind ein Mädchen ist, wäre die Antwort richtig gewesen.

— Do., 22.5. (V2) —

2.14 Satz

Sind (Ω, P) ein Wahrscheinlichkeitsraum und $B_1 \uplus \dots \uplus B_k = B$ eine disjunkte Zerlegung eines Ereignisses $B \subseteq \Omega$, dann gilt für alle $A \subseteq B$

(a) (Satz von der totalen Wahrscheinlichkeit)

$$P(A) = \sum_{i=1}^k P(A|B_i) \cdot P(B_i) .$$

(b) (Satz von Bayes)

Falls $P(A) > 0$, gilt außerdem

$$P(B_i|A) = \frac{P(A|B_i) \cdot P(B_i)}{\sum_{j=1}^k P(A|B_j) \cdot P(B_j)}$$

für alle $i = 1, \dots, k$.

■ Beweis:

(a) Da B disjunkt zerlegt ist, gilt $A = (A \cap B_1) \uplus \dots \uplus (A \cap B_k)$. Außerdem ist nach Definition der bedingten Wahrscheinlichkeit $P(A \cap B_i) = P(A|B_i) \cdot P(B_i)$.

$P(B_i)$ (dies gilt auch, falls $P(B_i) = 0$). Zusammen genommen ergibt sich

$$P(A) = P\left(\biguplus_{i=1}^k (A \cap B_i)\right) = \sum_{i=1}^k P(A \cap B_i) = \sum_{i=1}^k P(A|B_i) \cdot P(B_i).$$

(b) Nach Definition der bedingten Wahrscheinlichkeit ist

$$P(B_i|A) = \frac{P(B_i \cap A)}{P(A)} = \frac{P(A|B_i) \cdot P(B_i)}{P(A)} \stackrel{(a)}{=} \frac{P(A|B_i) \cdot P(B_i)}{\sum_{j=1}^k P(A|B_j) \cdot P(B_j)}.$$

□

2.15 Beispiel (Expertensystem für Krankheitsdiagnose)

Es sei bekannt, dass die Symptome S_1, S_2 (genau) bei den (niemals zusammen vorkommenden) Krankheiten K_1, K_2, K_3 auftreten. Die bedingten Auftretenswahrscheinlichkeiten seien

$$D = (d_{ij})_{\substack{i=1,2,3 \\ j=1,2}} = \begin{pmatrix} P(S_1|K_1) & P(S_2|K_1) \\ P(S_1|K_2) & P(S_2|K_2) \\ P(S_1|K_3) & P(S_2|K_3) \end{pmatrix} = \begin{pmatrix} 0.8 & 0.3 \\ 0.2 & 0.9 \\ 0.4 & 0.6 \end{pmatrix}$$

und ferner, dass die Krankheiten mit den Wahrscheinlichkeiten

$$\mathbf{p} = (P(K_1), P(K_2), P(K_3)) = (0.3, 0.6, 0.1)$$

vorkommen. Der Satz von der totalen Wahrscheinlichkeit liefert die Wahrscheinlichkeiten $\mathbf{q} = (P(S_1) \ P(S_2))$, mit denen die Symptome beobachtet werden:

$$\mathbf{q} = \mathbf{p} \cdot D = (0.3, 0.6, 0.1) \cdot \begin{pmatrix} 0.8 & 0.3 \\ 0.2 & 0.9 \\ 0.4 & 0.6 \end{pmatrix} = (0.40, 0.69).$$

Aber mit welcher Wahrscheinlichkeit leidet ein Patient mit Symptom S_j an der Krankheit K_i ? Gesucht sind also die $P(K_i|S_j)$. Der Satz von Bayes ergibt

$$\begin{pmatrix} P(K_1|S_1) & P(K_2|S_1) & P(K_3|S_1) \\ P(K_1|S_2) & P(K_2|S_2) & P(K_3|S_2) \end{pmatrix} = \begin{pmatrix} 0.6 & 0.3 & 0.1 \\ 0.1\bar{6} & 0.75 & 0.08\bar{3} \end{pmatrix}$$

Bei Auftreten von S_1 leidet ein Patient (wie erwartet) am wahrscheinlichsten an K_1 , und bei S_2 an K_2 . Obwohl $P(S_1|K_3) > P(S_1|K_2)$ ist (also S_1 bei K_3

wahrscheinlicher auftritt als bei K_2), ergibt sich aber auch, dass ein Patient mit S_1 , der nicht K_1 hat, häufiger an K_2 als an K_3 leidet (weil K_2 insgesamt viel öfter vorkommt als K_3).

Wird die Diagnosesicherheit bei Berücksichtigung von mehr als einem Symptom größer? Betrachte den Fall, dass ein Patient an S_1 , aber nicht an S_2 aufweist. Wir erhalten zunächst die Ausbleibewahrscheinlichkeiten

$$\begin{aligned} (P(\overline{S_2}|K_1), P(\overline{S_2}|K_2), P(\overline{S_2}|K_3)) \\ &= (1 - P(S_2|K_1), 1 - P(S_2|K_2), 1 - P(S_2|K_3)) \\ &= (0.7, 0.1, 0.4) \end{aligned}$$

und wieder mit dem Satz von Bayes

$$(P(K_1|\overline{S_2}), P(K_2|\overline{S_2}), P(K_3|\overline{S_2})) = (0.677\dots, 0.193\dots, 0.129\dots)$$

Zusammen mit $P(K_1|S_1) = 0.6$ könnte man also vermuten, dass der Patient an K_1 leidet. Wir können die beiden Wahrscheinlichkeiten aber nicht ohne weiteres kombinieren. Dazu müssten z.B. die gemeinsamen Auftretswahrscheinlichkeiten $P(S_1 \cap S_2|K_i)$ für $i = 1, 2, 3$ bekannt sein. Dann könnte man nämlich wegen $P(S_1 \cap \overline{S_2}|K_i) = P(S_1|K_i) - P(S_1 \cap S_2|K_i)$ wieder den Satz von Bayes anwenden, um $P(K_i|S_1 \cap \overline{S_2})$ zu erhalten. Für

$$\mathbf{s} = (P(S_1 \cap S_2|K_1), P(S_1 \cap S_2|K_2), P(S_1 \cap S_2|K_3)) = (0.2, 0.1, 0.3)$$

erhalten wir auf diese Weise

$$(P(K_1|S_1 \cap \overline{S_2}), P(K_2|S_1 \cap \overline{S_2}), P(K_3|S_1 \cap \overline{S_2})) = (0.72, 0.24, 0.04) ,$$

die Sicherheit der Diagnose ist also größer als bei Berücksichtigung nur eines Symptoms. Man prüfe allerdings, dass sie bei einer anderen Verteilung der bedingten gemeinsamen Auftretswahrscheinlichkeiten, auch kleiner werden kann; man probiere etwa $\mathbf{s}' = (0.2, 0.05, 0.05)$.

Stellt ein Ereignis B mit $P(B) > 0$ ein Vorwissen dar, mit dem sich die Wahrscheinlichkeit eines Ereignisses A nicht besser einschätzen lässt, so gilt $P(A|B) = \frac{P(A \cap B)}{P(B)} = P(A)$. Wir definieren die Unabhängigkeit zweier beliebiger Ereignisse daher wie folgt.

2.16 Definition

In einem Wahrscheinlichkeitsraum (Ω, P) heißen zwei Ereignisse $A, B \subseteq \Omega$ unabhängig, falls

$$P(A \cap B) = P(A) \cdot P(B) .$$

2.17 Beispiel

Im Würfelspiel $\Omega = \{1, \dots, 6\}^2$ sind die Würfe der beiden Spieler unabhängig: Sind nämlich $A_i = \{i\} \times \{1, \dots, 6\}$ für $i = 1, \dots, 6$ (der erste Spieler würfelt i) und $B_j = \{1, \dots, 6\} \times \{j\}$ für $j = 1, \dots, 6$ (der zweite Spieler würfelt j), dann gilt

$$P(A_i \cap B_j) = \frac{1}{36} = \frac{1}{6} \cdot \frac{1}{6} = P(A_i) \cdot P(B_j)$$

und daher $P(A_i|B_j) = P(A_i) = \frac{1}{6} = P(B_j) = P(B_j|A_i)$.

Andererseits ist das Ereignis G , dass der zweite Spieler gewinnt, von keinem der A_i unabhängig, denn

$$P(A_i \cap G) = \frac{6-i}{36} \neq \frac{5}{36} = \frac{1}{6} \cdot \frac{15}{36} = P(A_i) \cdot P(G)$$

für alle $i = 1, \dots, 6$. Tatsächlich wird die Situation für den zweiten Spieler günstiger, wenn der erste eine 1, 2 oder 3 wirft, und andernfalls ungünstiger.

In dem Beispiel sind die Ereignisse A_6 , B_6 und $Z = \{(i, i) : i = 1, \dots, 6\}$ („beide gleich \rightarrow Spende für den guten Zweck“) paarweise unabhängig, aber weder ist $P(A_6 \cap B_6 \cap Z) = P(A_6) \cdot P(B_6) \cdot P(Z)$ noch z.B. $P(B_6|A_6 \cap Z) = P(B_6)$. Die Unabhängigkeit mehrerer Ereignisse wird daher wie folgt definiert (paarweise Unabhängigkeit folgt daraus).

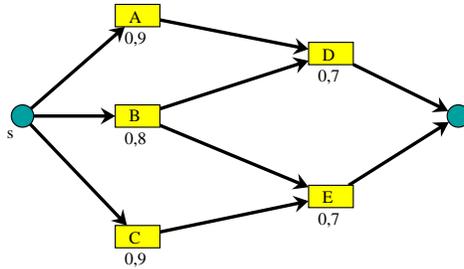
2.18 Definition

In einem Wahrscheinlichkeitsraum (Ω, P) heißen Ereignisse $A_1, \dots, A_k \subseteq \Omega$ unabhängig, falls für alle $1 \leq i_1 < \dots < i_l \leq k$, $1 \leq l \leq k$, gilt

$$P\left(\bigcap_{j=1}^l A_{i_j}\right) = \prod_{j=1}^l P(A_{i_j}) .$$

2.19 Beispiel (Ausfallsicherheit)

Betrachte das folgende Kommunikationsnetz, in dem die Beschriftungen die (unabhängigen) Funktionswahrscheinlichkeiten $P(A), \dots, P(E)$ der Bauteile angeben:



Das System S funktioniert, wenn es einen funktionierenden Weg von s nach t gibt. Damit ein Weg funktioniert, müssen alle darauf befindlichen Bauteile funktionieren (serielles System). Kommt man von einem Punkt durch zwei verschiedene Wege (ohne gemeinsame Verbindungen) zu einem anderen, reicht es, wenn einer von beiden funktioniert (paralleles System).

Die Funktionswahrscheinlichkeit des Systems ist damit

$$P(S) = P((A \cap D) \cup (B \cap D) \cup (B \cap E) \cup (C \cap E))$$

und wir könnten sie (aufwändig) mit der Siebformel bestimmen. Betrachte statt dessen zunächst die beiden Basissituationen.

serielles System: Da alle Bauteile unabhängig von einander funktionieren, gilt für ein System aus in Serie geschalteten Komponenten K_1, \dots, K_s

$$P(K_1 \cap \dots \cap K_s) = P(K_1) \cdot \dots \cdot P(K_s) .$$

paralleles System: Sind die Funktionswahrscheinlichkeiten unabhängig, dann auch die Ausfallwahrscheinlichkeiten. Für parallel geschaltete Komponenten K_1, \dots, K_p folgt daher

$$\begin{aligned} P(K_1 \cup \dots \cup K_p) &= 1 - P(\overline{K_1} \cap \dots \cap \overline{K_p}) = 1 - P(\overline{K_1} \cap \dots \cap \overline{K_p}) \\ &= 1 - P(\overline{K_1}) \cdot \dots \cdot P(\overline{K_p}) \\ &= 1 - ((1 - P(K_1)) \cdot \dots \cdot (1 - P(K_p))) \\ &= 1 - \prod_{i=1}^p (1 - P(K_i)) . \end{aligned}$$

Mit diesen beiden Regeln ergibt sich für das obige System

$$\begin{aligned}
 P(S) &= P(S|B) \cdot P(B) + P(S|\bar{B}) \cdot P(\bar{B}) \quad (\text{Satz von der totalen W'keit}) \\
 P(S|B) &= 1 - (1 - P(D))(1 - P(E)) = 1 - 0,3^2 = 0,91 \quad (D \parallel E) \\
 P(S|\bar{B}) &= 1 - (1 - P(A)P(D))(1 - P(C)P(E)) \\
 &= 1 - 0,37^2 = 1 - 0,1369 = 0,8631 \quad ((A \rightarrow D) \parallel (C \rightarrow E))
 \end{aligned}$$

und zusammen $P(S) = 0,91 \cdot 0,8 + 0,8631 \cdot 0,2 = 0,90062$.

Aus dem Satz von Bayes lassen sich bei kaputtem System Vermutungen über fehlerhafte Bauteile gewinnen.

2.3 Zufallsvariablen

Manchmal interessiert man sich nicht unmittelbar für die Ereignisse eines Wahrscheinlichkeitsraumes, sondern für (Kombinationen von) den Elementarereignissen zugeordneten Größen. In Beispiel 2.7 (binäre Suche) haben wir uns z.B. vornehmlich für die Dauer der Suche (eine dem Ereignis zugeordnete numerische Größe) interessiert. Um zufälligen Ereignissen zugeordnete Größen kombinieren zu können, führen wir den folgenden Begriff ein.

2.20 Definition (Zufallsvariable)

Eine Abbildung $X : \Omega \rightarrow \mathbb{R}$ heißt (diskrete, reelle) Zufallsvariable über dem Wahrscheinlichkeitsraum (Ω, P) . Die Verteilung P induziert eine Abbildung $P^X : \mathbb{R} \rightarrow [0, 1]$ vermöge

$$P^X(x) = P(\{\omega \in \Omega : X(\omega) = x\})$$

für alle $x \in \mathbb{R}$, die Verteilung der Zufallsvariable X . Die Menge $X(\Omega) = \bigcup_{\omega \in \Omega} X(\omega)$ der Bilder von X nennen wir Wertebereich.

2.21 Bemerkung

Für die von uns betrachteten endlichen Wahrscheinlichkeitsräume hat jede Zufallsvariable einen endlichen Wertebereich. Das Paar $(X(\Omega), P^X)$ ist daher wiederum ein (endlicher) Wahrscheinlichkeitsraum, wir können wegen des endlichen Trägers auch ganz \mathbb{R} als Menge der Elementarereignisse ansehen.

Für die Wahrscheinlichkeit von Ereignissen in Ω , die durch Werte einer Zufallsvariable X bestimmt sind, vereinbaren wir intuitivere Kurzschreibweisen — Di., 27.5. (V1) —

$$P(X = x) = P(\{\omega \in \Omega : X(\omega) = x\}) = P^X(x),$$

$$P(X < x) = P(\{\omega \in \Omega : X(\omega) < x\}),$$

usw.

Die einzelnen Werte einer Zufallsvariablen können mit sehr unterschiedlicher Wahrscheinlichkeit angenommen werden. Nicht immer ist die ganze Verteilung interessant, gelegentlich reichen auch verdichtende Kenngrößen. Die folgende Größe drückt z.B. aus, welchen Wert eine Zufallsvariable „im Mittel“ annimmt.

2.22 Definition (Erwartungswert)

Der Erwartungswert einer Zufallsvariable X über (Ω, P) ist definiert durch

$$E(X) = \sum_{x \in X(\Omega)} x \cdot P(X = x) = \sum_{\omega \in \Omega} X(\omega) \cdot P(\omega) .$$

andere
gängige Bez.:
 $\langle X \rangle = E(X)$

2.23 Beispiel (Mittlere Dauer der binären Suche)

Wir behalten die Bezeichnungen aus Beispiel 2.7 (binäre Suche) bei und definieren eine Zufallsvariable $X : \Omega \rightarrow \mathbb{R}$, welche die Dauer der Suche angibt, d.h.

$$X(\omega) = \begin{cases} i & \text{falls } \omega \in A_i, i = 1, \dots, k \\ k & \text{falls } \omega = \star . \end{cases}$$

Die erwartete Dauer der Suche ist dann

$$\begin{aligned}
 E(X) &= \sum_{i=1}^k i \cdot P(X = i) = k \cdot P(X = \star) + \sum_{i=1}^k i \cdot P(A_i) \\
 &= k \cdot \frac{1}{2^k} + \sum_{i=1}^k i \cdot 2^{(i-1)-k} = \frac{k}{2^k} + 2^{-(k+1)} \sum_{i=1}^k i \cdot 2^i \\
 &= \frac{k}{2^k} + 2^{-(k+1)} \sum_{i=1}^k \sum_{j=i}^k 2^j = \frac{k}{2^k} + 2^{-(k+1)} \sum_{i=1}^k (2^{k+1} - 2^i) \\
 &= \frac{k}{2^k} + \sum_{i=1}^k (1 - 2^{i-(k+1)}) = \frac{k}{2^k} + k + (2^{-k} - 1) \\
 &= (k - 1) + \frac{k + 1}{2^k}
 \end{aligned}$$

d.h. die erwartete Suchdauer ist kaum besser als die im schlechtesten Fall.

Mit Zufallsvariablen lässt sich wie gewohnt rechnen.

2.24 Lemma

Sind X eine Zufallsvariable über einem Wahrscheinlichkeitsraum (Ω, P) und $f : \mathbb{R} \rightarrow \mathbb{R}$, dann ist auch $f \circ X$ eine Zufallsvariable über (Ω, P) mit

$$P(f(X) = y) = \sum_{x : f(x)=y} P(X = x) = P(\{\omega \in \Omega : f(X(\omega)) = y\}) .$$

■ **Beweis:** selbst.

□

2.25 Satz (Linearität des Erwartungswerts)

Sind X eine Zufallsvariable über einem Wahrscheinlichkeitsraum (Ω, P) und $a, b \in \mathbb{R}$, dann gilt

$$E(a \cdot X + b) = a \cdot E(X) + b .$$

■ **Beweis:**

$$\begin{aligned} E(a \cdot X + b) &= \sum_{\omega \in \Omega} (a \cdot X(\omega) + b) \cdot P(\omega) \\ &= \sum_{\omega \in \Omega} a \cdot X(\omega) \cdot P(\omega) + \sum_{\omega \in \Omega} b \cdot P(\omega) \\ &= a \cdot \sum_{\omega \in \Omega} X(\omega) \cdot P(\omega) + b \cdot \sum_{\omega \in \Omega} P(\omega) \\ &= a \cdot E(X) + b . \end{aligned}$$

□

Die nächste Größe drückt aus, wie stark die Werte einer Zufallsvariable um den Erwartungswert „streu“.

2.26 Definition (Varianz)

Die Varianz einer Zufallsvariable X über (Ω, P) ist definiert durch

$$\text{Var}(X) = E((X - E(X))^2) = \sum_{x \in X(\Omega)} (x - E(X))^2 \cdot P(X = x) .$$

Die Größe $\sqrt{\text{Var}(X)}$ heißt Standardabweichung von X .

2.27 Lemma

Ist X eine Zufallsvariable über einem Wahrscheinlichkeitsraum (Ω, P) , dann gilt

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

■ **Beweis:** Aus der Definition der Varianz folgt mit der Linearität des Erwartungswerts

$$\begin{aligned} \text{Var}(X) &= E((X - E(X))^2) = E(X^2 - 2E(X)X + E(X)^2) \\ &= E(X^2) - 2E(X)E(X) + E(X)^2 = E(X^2) - E(X)^2 . \end{aligned}$$

□

2.28 Satz

Sind X eine Zufallsvariable über einem Wahrscheinlichkeitsraum (Ω, P) und $a, b \in \mathbb{R}$, dann gilt

$$\text{Var}(a \cdot X + b) = a^2 \cdot \text{Var}(X) .$$

■ **Beweis:** Mit dem vorstehenden Lemma gilt

$$\begin{aligned} \text{Var}(a \cdot X + b) &= E((aX + b)^2) - E(aX + b)^2 \\ &= E(a^2 X^2 + 2abX + b^2) - (a \cdot E(X) + b)^2 \\ &= (a^2 E(X^2) + 2abE(X) + b^2) - (a^2 E(X)^2 + 2abE(X) + b^2) \\ &= a^2 E(X^2) - a^2 E(X)^2 = a^2 \text{Var}(X) . \end{aligned}$$

□

Kapitel 3

Analyse von Algorithmen

Wir betrachten hier weniger die Korrektheit als den Ressourcenverbrauch (in erster Linie Laufzeit und Speicherplatz) von Algorithmen und zwar in Abhängigkeit von der Größe der Eingabe. Dabei sollen konstante Faktoren ignoriert werden, weil z.B. die Laufzeit eines elementaren Schrittes und die Größe eines Speicherwortes variieren können.

3.1 Definition (Asymptotisches Wachstum)

Zu einer Funktion $f : \mathbb{N}_0 \rightarrow \mathbb{R}$ wird definiert:

(i) Die Menge

$$\mathcal{O}(f(n)) = \left\{ g : \mathbb{N}_0 \rightarrow \mathbb{R} : \begin{array}{l} \text{es gibt Konstanten } c, n_0 > 0 \text{ mit} \\ |g(n)| \leq c \cdot |f(n)| \text{ für alle } n > n_0 \end{array} \right\}$$

der Funktionen, die höchstens so schnell wachsen wie f .

(ii) Die Menge

$$\Omega(f(n)) = \left\{ g : \mathbb{N}_0 \rightarrow \mathbb{R} : \begin{array}{l} \text{es gibt Konstanten } c, n_0 > 0 \text{ mit} \\ c \cdot |g(n)| \geq |f(n)| \text{ für alle } n > n_0 \end{array} \right\}$$

der Funktionen, die mindestens so schnell wachsen wie f .

(iii) Die Menge

$$\Theta(f(n)) = \left\{ g : \mathbb{N}_0 \rightarrow \mathbb{R} : \begin{array}{l} \text{es gibt Konstanten } c_1, c_2, n_0 > 0 \text{ mit} \\ c_1 \leq \frac{|g(n)|}{|f(n)|} \leq c_2 \text{ für alle } n > n_0 \end{array} \right\}$$

der Funktionen, die genauso schnell wachsen wie f .

(iv) Die Menge

$$o(f(n)) = \left\{ g : \mathbb{N}_0 \rightarrow \mathbb{R} : \begin{array}{l} \text{zu jedem } c > 0 \text{ ex. ein } n_0 > 0 \text{ mit} \\ c \cdot |g(n)| \leq |f(n)| \text{ für alle } n > n_0 \end{array} \right\}$$

der Funktionen, die gegenüber f verschwinden.

(v) Die Menge

$$\omega(f(n)) = \left\{ g : \mathbb{N}_0 \rightarrow \mathbb{R} : \begin{array}{l} \text{zu jedem } c > 0 \text{ ex. ein } n_0 > 0 \text{ mit} \\ |g(n)| \geq c \cdot |f(n)| \text{ für alle } n > n_0 \end{array} \right\}$$

der Funktionen, denen gegenüber f verschwindet.

3.2 Bemerkung

Für Funktionen mit mehreren Veränderlichen sind die Wachstumsklassen entsprechend definiert.

Die erste Aussage ist vor allem für Algorithmen interessant, in denen Teilmengen fester Größe betrachtet werden.

3.3 Satz

Für festes $k \in \mathbb{N}_0$ gilt

$$\binom{n}{k} \in \Theta(n^k).$$

■ **Beweis:** Für alle $n > k =: n_0$ gilt

$$\binom{n}{k} = \frac{n^k}{k!} = \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \dots \cdot \frac{n-(k-1)}{k-(k-1)}.$$

Wegen $\frac{n}{k} \leq \frac{n-i}{k-i} \leq n$, $i = 0, \dots, k-1$, folgt daraus

$$\left(\frac{n}{k}\right)^k = \left(\frac{1}{k}\right)^k \cdot n^k \leq \binom{n}{k} \leq n^k$$

und damit $\binom{n}{k} \in \Omega(n^k) \cap \mathcal{O}(n^k) = \Theta(n^k)$. □

In den folgenden Näherungsformeln wird statt der Funktion selbst der Fehler der Abschätzung asymptotisch angegeben, und zwar einmal additiv und einmal multiplikativ. Die Schreibweise bedeutet, dass es in der jeweiligen Wachstumsklasse eine Folge gibt, für die Gleichheit herrscht.

3.4 Satz

Für alle $n \in \mathbb{N}_0$ gilt

$$(i) \quad H_n := \sum_{k=1}^n \frac{1}{k} = \ln n + \mathcal{O}(1)$$

$$(ii) \quad n! = \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \Theta\left(\frac{1}{n}\right)\right) \quad (\text{Stirlingformel})$$

benutzt in
Beispiel 1.11
(Teileranzahlen)

3.1 Standardanalysen

Worst-, average- und best-case Analyse

Die weitaus meisten Bedarfsanalysen sind für den *worst-case*: Wie groß ist der Ressourcenbedarf im ungünstigsten Fall? Eine Analyse wird jedoch aussagekräftiger, wenn man auch den besten und mittleren Fall hinzunimmt.

3.5 Beispiel (Laufzeitanalyse der binären Suche)

Betrachte noch einmal binäre Suche nach einem Element x in einem Array $M[1, \dots, n-1]$ mit $n = 2^k$ (vgl. Beispiel 2.7).

Günstigster Fall: Steht das Element an mittlerer Position, endet die Suche nach einem Schritt. Die best-case Laufzeit ist also in $\Theta(1)$.

Ungünstigster Fall: Wie in Beispiel 2.7 festgestellt, endet die Suche nach höchstens k Schritten, und dieser Fall kann sowohl dadurch eintreten, dass $x \notin M$, als auch durch eine ungünstige Position (z.B. $x = M[1]$). Die worst-case Laufzeit ist damit in $\Theta(k) = \Theta(\log n)$.

Mittlerer Fall: Wie in Beispiel 2.23 gezeigt ist die erwartete Anzahl der Schritte um höchstens eins kleiner als die maximale. Die average-case Laufzeit ist damit ebenfalls in $\Theta(k-1) = \Theta(\log n)$.

Im allgemeinen ist die Laufzeit also irgendwo in $\Omega(1) \cap \mathcal{O}(n \log n)$, meistens jedoch nahe der oberen Schranke.

Im nächsten Abschnitt (Beispiel 3.15) werden wir sehen, dass man nicht immer mit dem Schlimmsten rechnen muss.

Trade-off zwischen Laufzeit- und Speicherplatzbedarf

— Do., 5.6. (V2) —

Gelegentlich lässt sich der Bedarf einer Ressource auf Kosten einer anderen reduzieren. Betrachte dazu die beiden folgenden Algorithmen zur Berechnung der Binomialkoeffizienten.

Algorithmus 1:
Binomialkoeffizienten
(rekursive Berechnung)

Eingabe : $n \geq k \in \mathbb{N}_0$
Ausgabe : $\binom{n}{k}$

```

binom( $n, k$ ) begin
  if  $n < k$  then return 0;
  if  $k = 0$  then return 1;
  return binom( $n - 1, k - 1$ )
         + binom( $n - 1, k$ );
end

```

Algorithmus 2:
Binomialkoeffizienten
(dynamische Programmierung)

Eingabe : $n \geq k \in \mathbb{N}_0$
Ausgabe : $\binom{n}{k}$

```

binom( $n, k$ ) begin
  if  $n < k$  then return 0;
  for  $i = 0, \dots, n$  do
     $B[i, 0] \leftarrow 1$ ;  $B[i, i] \leftarrow 1$ ;
    for  $j = 1, \dots, i - 1$  do
       $B[i, j] \leftarrow B[i - 1, j - 1]$ 
        +  $B[i - 1, j]$ ;
    end
  end
  return  $B[n, k]$ ;
end

```

Im linken (rekursiven) Algorithmus wird nur $\Theta(n)$ Speicher benötigt (für den Aufrufstack der Rekursion), die Laufzeit ist allerdings exponentiell. Das sieht man wie folgt: Ist $T(n, k)$ die Laufzeit bei Aufruf mit $n \geq k$, dann gilt im wesentlichen

$$T(n, k) = 1 + T(n - 1, k - 1) + T(n - 1, k) ,$$

und wegen der Ähnlichkeit zur Rekursionsformel für die Binomialkoeffizienten folgt $T(n, k) \geq \binom{n}{k}$. Wir wissen bereits, dass die Binomialkoeffizienten für festes k wie n^k wachsen, da wir k aber nicht als fest annehmen können, ergibt sich im ungünstigsten Fall sogar exponentielles Wachstum, denn

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad \xRightarrow[\text{Taubenschlagprinzip}]{\text{verallg.}} \quad \text{es ex. ein } k \text{ mit } \binom{n}{k} \geq \frac{2^n}{n+1} .$$

Im rechten Algorithmus werden Doppelberechnungen vermieden, indem alle bereits berechneten Werte in einem zweidimensionalen Array gespeichert werden. Der Platzbedarf steigt damit auf $\Theta(n^2)$, aber die Laufzeit verringert sich (dramatisch!) auf $\Theta(n^2)$ (zwei geschachtelte Schleifen). Wir haben also (in einem sehr vorteilhaften Verhältnis) Platz gegen Laufzeit getauscht.

3.6 Bemerkung

Tatsächlich lassen sich die Binomialkoeffizienten mit der schnelleren Laufzeit auch ohne (asymptotisch) größeren Platzbedarf berechnen (man überlege sich, dass zu jedem Zeitpunkt immer nur zwei Spalten des Pascal-Dreiecks benötigt werden).

Untere Schranken

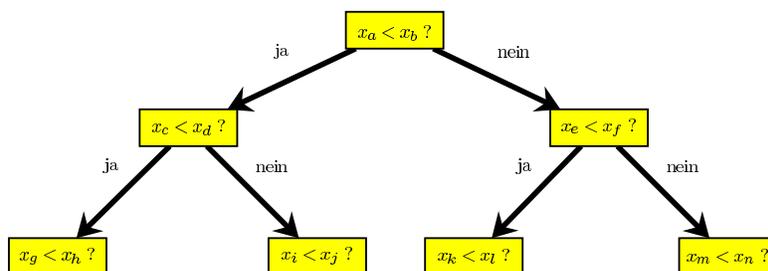
Wenn ein Algorithmus selbst im günstigsten Fall nicht mit einer konstanten Anzahl von Schritten auskommt, muss das noch nicht schlecht sein. Denn beispielsweise lässt sich in einem Array der Länge n , über das keine weiteren Annahmen (wie etwa Sortierung, Größenbeschränkung, etc.) gemacht werden können, das Minimum der Elemente sicher nicht bestimmen, ohne alle Elemente mindestens einmal betrachtet zu haben. Für jeden Minimumsalgorithmus gibt es daher eine Eingabe, für die er eine Laufzeit in $\Omega(n)$ hat.

Wir zeigen hier eine wichtige, weniger offensichtliche untere Schranke.

3.7 Beispiel (Untere Schranke für vergleichsbasiertes Sortieren)

Wenn keine Einschränkungen der zu sortierenden Elemente vorliegen, muss ein Sortieralgorithmus Paare von Elementen vergleichen, um ihre Reihenfolge zu bestimmen (andere Beispiele sind bucket-sort bzw. radix-sort). Wieviele Vergleiche muss der beste Sortieralgorithmus (im ungünstigsten Fall) mindestens machen?

Abhängig vom Ergebnis des ersten Vergleichs wird der Algorithmus irgendwelche weiteren Schritte ausführen, insbesondere weitere Vergleiche. Wir können den Ablauf des Algorithmus daher mit einem Abstieg im Entscheidungsbaum gleich setzen: An der Wurzel steht der erste Vergleich, an den beiden Kindern stehen die Vergleiche, die im Ja- bzw. Nein-Fall als nächste ausgeführt werden, usw.



Bei n verschiedenen zu sortierenden Elementen (wir schätzen den ungünstigsten Fall ab!) hat der Entscheidungsbaum $n!$ Blätter, denn es gibt $n!$ mögliche Eingabereihenfolgen, und wenn zwei verschiedene Eingaben denselben Ablauf (insbesondere die gleichen Umsortierungen) zur Folge haben, wird eine von beiden nicht richtig sortiert. Die Anzahl der Vergleiche entspricht aber gerade der Höhe des Entscheidungsbaumes. In einem Binärbaum haben $n!$ Blätter mindestens $\frac{n!}{2}$ Vorgänger, die wiederum mindestens $\frac{n!}{2^2}$ Vorgänger haben, usw. Der längste Weg zur Wurzel hat damit mindestens

$$\log n! = \log[n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1] \geq \log \left[\left(\frac{n}{2} \right)^{\frac{n}{2}} \right] = \frac{n}{2} \cdot \log \frac{n}{2} \in \Omega(n \log n)$$

Knoten. Es kann daher keinen vergleichsbasierten Sortieralgorithmus geben, der bei jeder Eingabe eine Laufzeit in $o(n \log n)$ hat.

3.2 Rekursionen

In Beispiel 3.5 haben wir die Laufzeit der rekursiven Berechnung der Binomialkoeffizienten nur deshalb leicht abschätzen können, weil die Laufzeit sich wie die Binomialkoeffizienten selbst verhalten hat. Wir behandeln daher einige wichtige Klassen von Rekursionen etwas allgemeiner.

3.8 Definition (Lineare Rekursionen)

Eine Folge $(x_n)_{n \in \mathbb{N}_0}$ reeller Zahlen heißt lineare Rekursion k -ter Ordnung, falls

$$x_n = \begin{cases} b_n & \text{für } n = 0, \dots, k-1 \\ a_1 \cdot x_{n-1} + \dots + a_k \cdot x_{n-k} + b_k & \text{für } n \geq k \end{cases}$$

mit Konstanten $a_1, \dots, a_k, b_0, \dots, b_k \in \mathbb{R}$ und $a_k \neq 0$. Eine Rekursion heißt homogen, falls $b_k = 0$, und inhomogen sonst. Die b_0, \dots, b_{k-1} heißen Anfangswerte oder Randbedingungen.

Um das Wachstum besser überschauen zu können, möchten wir Rekursionen in *geschlossener Form* ausdrücken, d.h. auf der rechten Seite sollen weder Folgenglieder noch indizierte Summen oder Produkte vorkommen.

3.9 Satz (Auflösung linearer Rekursionen 1. Ordnung)

Ist $(x_n)_{n \in \mathbb{N}_0}$ eine lineare Rekursion 1. Ordnung, dann gilt

$$x_n = \begin{cases} b_1 \cdot n + b_0 & \text{falls } a_1 = 1 \\ b_0 \cdot a_1^n + b_1 \cdot \frac{a_1^n - 1}{a_1 - 1} & \text{sonst} \end{cases} \quad \text{für alle } n \in \mathbb{N}_0.$$

■ **Beweis:** Vollständige Induktion über $n \in \mathbb{N}_0$. Offensichtlich gilt die Aussage für $n = 0$. Sei also $n > 0$, dann ist für $a_1 = 1$

$$x_n = x_{n-1} + b_1 = (b_1 \cdot (n-1) + b_0) + b_1 = b_1 \cdot n + b_0$$

und für $a_1 \neq 1$

$$\begin{aligned} x_n &= a_1 \cdot x_{n-1} + b_1 = a_1 \cdot \left(b_0 \cdot a_1^{n-1} + b_1 \cdot \frac{a_1^{n-1} - 1}{a_1 - 1} \right) + b_1 \\ &= b_0 \cdot a_1^n + b_1 \cdot \left(a_1 \cdot \frac{a_1^{n-1} - 1}{a_1 - 1} + 1 \right) = b_0 \cdot a_1^n + b_1 \cdot \frac{a_1^n - 1}{a_1 - 1} \end{aligned}$$

wie behauptet. □

3.10 Folgerung

Im homogenen Fall (d.h. $b_1 = 0$) gilt $x_n = b_0 \cdot a_1^n$.

3.11 Beispiel (Ketten-EMails)

Eine Ketten-EMail fordert dazu auf, sie am Tag nach Erhalt an zehn Bekannte weiterzuleiten. Wie viele Kopien dieser Mail sind nach einem Monat im Umlauf, wenn

- der Initiator sie täglich an zehn Personen schickt,
- sich jeweils nur 15% der Empfänger an die Aufforderung zur Weiterleitung halten und
- niemand sie ein zweites Mal bekommt?

Nennen wir die Anzahl der weitergeleiteten Kopien am n -ten Tag nach der ersten Verschickung durch den Initiator x_n . Dann gibt es zunächst nur die $x_0 = 10$ Kopien des Initiators, aber an jedem weiteren Tag bewirken die x_{n-1} Kopien des Vortages $10 \cdot \frac{15}{100} \cdot x_{n-1}$ Weiterleitungen. Ausserdem kommen noch weitere 10 des Initiators hinzu, sodass

$$x_n = \frac{3}{2} \cdot x_{n-1} + 10 .$$

Es handelt sich also um eine lineare Rekursion 1. Ordnung mit $b_0 = 10 = b_1$ und $a_1 = \frac{3}{2}$. Aus Satz 3.9 erhalten wir

$$x_{30} = 10 \cdot \left(\frac{3}{2}\right)^{30} + 10 \cdot \frac{\left(\frac{3}{2}\right)^{30} - 1}{\frac{3}{2} - 1} \sim 5\,752\,512 .$$

Ohne die fortwährende Verschickung durch den Initiator handelte es sich um eine homogene Rekursion und wir hätten trotzdem noch $x_{30} = 10 \cdot \frac{3^{30}}{2^{30}} \sim 1\,917\,511$ Weiterleitungen am 30. Tag.

— Do., 12.6. (V2) —

3.12 Satz (Auflösung homogener linearer Rekursionen 2. Ordnung)

Sind $(x_n)_{n \in \mathbb{N}_0}$ eine homogene lineare Rekursion 2. Ordnung, $\alpha, \beta \in \mathbb{R}$ Lösungen der Gleichung $t^2 - a_1 \cdot t - a_2 = 0$ und

$$A := \begin{cases} \frac{b_1 - b_0 \cdot \beta}{\alpha - \beta} & \text{falls } \alpha \neq \beta \\ \frac{b_1 - b_0 \cdot \alpha}{\alpha} & \text{falls } \alpha = \beta \end{cases} \quad \text{und} \quad B := \begin{cases} \frac{b_1 - b_0 \cdot \alpha}{\alpha - \beta} & \text{falls } \alpha \neq \beta \\ b_0 & \text{falls } \alpha = \beta , \end{cases}$$

dann gilt

$$x_n = \begin{cases} A \cdot \alpha^n - B \cdot \beta^n & \text{falls } \alpha \neq \beta \\ (A \cdot n + B) \cdot \alpha^n & \text{falls } \alpha = \beta \end{cases} \quad \text{für alle } n \in \mathbb{N}_0 .$$

■ **Beweis:** Wir beweisen die Aussage für den Fall $\alpha \neq \beta$ durch vollständige Induktion (der Fall $\alpha = \beta$ kann ähnlich gezeigt werden). Zunächst gilt

$$\begin{aligned} \frac{b_1 - b_0 \beta}{\alpha - \beta} \cdot \alpha^0 - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \cdot \beta^0 &= \frac{b_1 - b_0 \beta - b_1 + b_0 \alpha}{\alpha - \beta} = b_0 = x_0 , \\ \frac{b_1 - b_0 \beta}{\alpha - \beta} \cdot \alpha^1 - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \cdot \beta^1 &= \frac{b_1 \alpha - b_0 \beta \alpha - b_1 \beta + b_0 \alpha \beta}{\alpha - \beta} = b_1 = x_1 . \end{aligned}$$

Für $n > 1$ erhalten wir unter Verwendung von $t^2 = a_1 t + a_2$ für $t = \alpha, \beta$

$$\begin{aligned}
 x_n &= a_1 \cdot x_{n-1} + a_2 \cdot x_{n-2} + b_2 \\
 &= a_1 \cdot \left(\frac{b_1 - b_0 \beta}{\alpha - \beta} \alpha^{n-1} - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \beta^{n-1} \right) \\
 &\quad + a_2 \cdot \left(\frac{b_1 - b_0 \beta}{\alpha - \beta} \alpha^{n-2} - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \beta^{n-2} \right) + b_2 \\
 &= \frac{b_1 - b_0 \beta}{\alpha - \beta} \cdot (a_1 \alpha^{n-1} + a_2 \alpha^{n-2}) - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \cdot (a_1 \beta^{n-1} + a_2 \beta^{n-2}) + b_2 \\
 &= \frac{b_1 - b_0 \beta}{\alpha - \beta} \cdot \alpha^{n-2} \cdot \underbrace{(a_1 \alpha + a_2)}_{=\alpha^2} - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \cdot \beta^{n-2} \cdot \underbrace{(a_1 \beta + a_2)}_{=\beta^2} + b_2 \\
 &= \frac{b_1 - b_0 \beta}{\alpha - \beta} \cdot \alpha^n - \frac{b_1 - b_0 \alpha}{\alpha - \beta} \cdot \beta^n + b_2 .
 \end{aligned}$$

□

3.13 Beispiel (Fibonacci-Zahlen)

Die Folge $(f_n)_{n \in \mathbb{N}_0}$ der Fibonacci-Zahlen ist gegeben durch die Rekursion

$$\begin{aligned}
 f_0 &= 0, & f_1 &= 1 \\
 f_n &= f_{n-1} + f_{n-2} & & \text{für alle } n > 1.
 \end{aligned}$$

Es handelt sich also um eine lineare Rekursion 2. Ordnung mit $a_1 = a_2 = b_1 = 1$ und $b_0 = b_2 = 0$. Die Lösungen von $t^2 - a_1 \cdot t - a_2 = t^2 - t - 1 = 0$ sind

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad \text{und} \quad \beta = \frac{1 - \sqrt{5}}{2} .$$

Wegen $A, B = \frac{1}{\alpha - \beta} = \frac{1}{\sqrt{5}}$ liefert Satz 3.12 unmittelbar die bekannte Auflösung

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1 - \sqrt{5}}{2} \right)^n .$$

In Teile-und-Herrsche Verfahren werden Instanzen in der Regel in mehrere kleinere ähnlicher Größe aufgeteilt, in der binären Suche z.B. in zwei gleich große Teile von knapp der halben Größe. Die Laufzeit ist daher nicht durch eine lineare Rekursion gegeben. Doch auch für Aufteilungsrekursionen gibt es Auflösungsätze.

3.14 Satz

Gibt es zu einer Folge $T : \mathbb{N}_0 \rightarrow \mathbb{R}$ Konstanten $\alpha \geq 1$, $\beta > 1$ so, dass

$$\begin{aligned} T(0) &= T(1) = 0 \\ T(n) &= \alpha \cdot T\left(\frac{n}{\beta}\right) + n \quad \text{für alle } n > 1 \end{aligned}$$

(wobei $\frac{n}{\beta}$ wahlweise durch $\lfloor \frac{n}{\beta} \rfloor$ oder $\lceil \frac{n}{\beta} \rceil$ zu ersetzen ist), dann gilt

$$T(n) \in \begin{cases} \Theta\left(\frac{\beta}{\beta-\alpha} \cdot n\right) & \text{falls } \alpha < \beta \\ \Theta(n \log_{\beta} n) & \text{falls } \alpha = \beta \\ \Theta\left(\frac{\alpha}{\alpha-\beta} \cdot \left(\frac{\beta}{\alpha}\right)^{\lceil \log_{\beta} n \rceil} \cdot n^{\log_{\beta} \alpha}\right) & \text{falls } \alpha > \beta, \end{cases}$$

wobei $\lceil \log_{\beta} n \rceil$ den nicht-ganzzahligen Anteil von $\log_{\beta} n$ bezeichne.

■ **Beweis:** Die Rekursion kann bis zum Erreichen der Anfangsbedingung abgerollt werden, sodass wir für $t = \lfloor \log_{\beta} n \rfloor$ erhalten

$$\begin{aligned} T(n) &= n + \alpha \cdot T\left(\frac{n}{\beta}\right) \\ &= n + \alpha \cdot \frac{n}{\beta} + \alpha^2 \cdot T\left(\frac{n}{\beta^2}\right) \\ &\quad \vdots \\ &= n + \alpha \cdot \frac{n}{\beta} + \alpha^2 \cdot \frac{n}{\beta^2} + \dots + \alpha^t \cdot \frac{n}{\beta^t} + \underbrace{\alpha^{t+1} \cdot T\left(\frac{n}{\beta^{t+1}}\right)}_{=0} \\ &= n \cdot \left(1 + \frac{\alpha}{\beta} + \dots + \frac{\alpha^t}{\beta^t}\right). \end{aligned}$$

Für $\alpha = \beta$ sind alle Summanden in der Klammer gleich 1, sodass

$$T(n) = n \cdot (\lfloor \log_{\beta} n \rfloor + 1) \in \Theta(n \log_{\beta} n).$$

Ist dagegen $\alpha < \beta$, so ist die Summe in der Klammer für $t \rightarrow \infty$ konvergent. Da mit $n \rightarrow \infty$ auch $t = \lfloor \log_{\beta} n \rfloor \rightarrow \infty$ folgt

$$T(n) \xrightarrow{n \rightarrow \infty} n \sum_{t=0}^{\infty} \left(\frac{\alpha}{\beta}\right)^t = \frac{\beta}{\beta - \alpha} \cdot n, \quad \text{also } T(n) \in \Theta\left(\frac{\beta}{\beta - \alpha} \cdot n\right).$$

Ist andererseits $\alpha > \beta$, so folgt zunächst ganz ähnlich

$$T(n) = n \cdot \left(\frac{\alpha}{\beta}\right)^t \cdot \left(1 + \frac{\beta}{\alpha} + \dots + \frac{\beta^t}{\alpha^t}\right) \xrightarrow{n \rightarrow \infty} n \cdot \frac{\alpha}{\alpha - \beta} \cdot \left(\frac{\alpha}{\beta}\right)^t.$$

Durch Einsetzen von $t = \lfloor \log_\beta n \rfloor = \log_\beta n - \lceil \log_\beta n \rceil$ erhalten wir

$$\begin{aligned} T(n) &\xrightarrow{n \rightarrow \infty} \frac{\alpha}{\alpha - \beta} \cdot n \cdot \left(\frac{\alpha}{\beta}\right)^{\log_\beta n - \lceil \log_\beta n \rceil} = \frac{\alpha}{\alpha - \beta} \cdot \left(\frac{\beta}{\alpha}\right)^{\lceil \log_\beta n \rceil} \cdot n \cdot \frac{\alpha^{\log_\beta n}}{\beta^{\log_\beta n}} \\ &= \frac{\alpha}{\alpha - \beta} \cdot \left(\frac{\beta}{\alpha}\right)^{\lceil \log_\beta n \rceil} \cdot \underbrace{\alpha^{\log_\beta n}}_{=\beta^{(\log_\beta n) \cdot (\log_\beta \alpha)}} = \frac{\alpha}{\alpha - \beta} \cdot \left(\frac{\beta}{\alpha}\right)^{\lceil \log_\beta n \rceil} \cdot n^{\log_\beta \alpha}. \end{aligned}$$

□

3.15 Beispiel (Laufzeit von Quicksort)

Wir analysieren die folgende Version von Quicksort, die ein Array $M[1, \dots, n]$

Algorithmus 3: Quicksort

Eingabe : Array $M[1, \dots, n]$

Ausgabe : nicht-absteigende

```

quicksort( $M, l, r$ ) begin
    if  $l < r$  then
         $p \leftarrow \text{partition}(M, l, r)$ ;
        quicksort( $M, l, p - 1$ );
        quicksort( $M, p + 1, r$ );
    end
partition( $M, l, r$ ) begin
     $x \leftarrow M[r]$ ;  $i \leftarrow l - 1$ ;
    for  $j = l, \dots, r - 1$  do
        if  $M[j] \leq x$  then
             $i \leftarrow i + 1$ ;
            vertausche  $M[i] \leftrightarrow M[j]$ ;
        end if
    end for
    vertausche  $M[i + 1] \leftrightarrow M[r]$ ;
    return  $i + 1$ ;
end
    
```

nicht-absteigend sortiert und mit $\text{quicksort}(M, 1, n)$ aufgerufen wird:

Die Laufzeit bei Eingabe eines Arrays der Länge n ist im wesentlichen

$$T(n) = n + T(p - 1) + T(n - p)$$

also abhängig davon, wieviele Elemente kleiner/größer als das Pivot-Element $M[n]$ sind (denn daraus ergibt sich dessen Position p).

Günstigster Fall: Wegen $T(n) > n$ wird die Laufzeit am kleinsten, wenn die beiden Teilarrays möglichst gleich groß sind, also $p = \lceil \frac{n}{2} \rceil$. Gilt das in jeder Stufe der Rekursion, so können wir Satz 3.14 mit $\alpha = \beta = 2$ anwenden und erhalten $T(n) \in \Theta(n \log n)$.

Ungünstigster Fall: Die unausgewogenste Aufteilung erzeugt für $p = 1$ ein rechtes Teilarray, das gerade nur um 1 kürzer ist als das Ausgangsarray. Passiert dies in jeder Stufe der Rekursion, dann ist jeweils $T(n) = n + 1 + T(n - 1)$ (lineare Rekursion erster Ordnung). Nach Abrollen der Rekursion folgt aus der Gaußschen Summenformel $T(n) \in \Theta(n^2)$.

Mittlerer Fall: Jedes Element von M wird genau einmal zum Pivot-Element. Ist die Eingabereihenfolge in M zufällig, dann auch die Reihenfolge, in der die Elemente zu Pivot-Elementen werden.

Da die Anzahl der Schritte von der Anzahl der Vergleiche in *partition* dominiert wird, bestimmen wir den Erwartungswert der Anzahl von Paaren, die im Verlauf des Algorithmus verglichen werden. Die Elemente von M seien entsprechend ihrer korrekten Sortierung mit $x_1 < \dots < x_n$ bezeichnet. Werden Elemente $x_i, x_j, i < j$, verglichen, dann ist eines von beiden zu diesem Zeitpunkt Pivot-Element, und keins der Elemente $x_{i+1} < \dots < x_{j-1}$ war bis dahin Pivot (sonst wären x_i und x_j in verschiedenen Teilarrays). Wegen der zufälligen Reihenfolge der Pivot-Wahlen ist die Wahrscheinlichkeit, dass von den Elementen $x_i < \dots < x_j$ gerade x_i oder x_j zuerst gewählt werden, gerade $\frac{1}{j-i+1} + \frac{1}{j-i+1}$. Dies gilt für jedes Paar, sodass sich als erwartete Anzahl von Vergleichen und damit mittlere Laufzeit ergibt

$$\sum_{i=1}^{n-1} \sum_{j=i+1}^n \frac{2}{j-i+1} = \sum_{i=1}^{n-1} \sum_{k=2}^{n-i+1} \frac{2}{k} \leq 2 \sum_{i=1}^n \sum_{k=1}^n \frac{1}{k} = 2n \cdot H_n \stackrel{\text{Satz 3.4}}{\in} \Theta(n \log n) .$$

Im allgemeinen ist die Laufzeit also irgendwo in $\Omega(n \log n) \cap \mathcal{O}(n^2)$, meistens jedoch nahe der unteren Schranke.

3.16 Bemerkung

Die average-case Analyse zeigt, dass eine randomisierte Variante von Quicksort, in der das Pivot-Element zufällig (statt immer von der letzten Position) gewählt wird, im Mittel auch auf Eingaben schnell ist, die lange vorsortierte Teilfolgen enthalten.

Zum Abschluss geben wir noch eine allgemeinere Fassung von Satz 3.14 an; deren Beweis wäre allerdings zu aufwändig.

3.17 Satz (Master-Theorem)

Gibt es zu einer Folge $T : \mathbb{N} \rightarrow \mathbb{R}$ Konstanten $\alpha \geq 1$, $\beta > 1$ und $C \geq 0$ sowie Folgen $c_i : \mathbb{N} \rightarrow [-C, C]$, $i = 1, \dots, \lfloor \alpha \rfloor$, und $b : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$ so, dass

$$\begin{aligned} T(1) &= 0 \\ T(n) &= T\left(\frac{n}{\beta} + c_1(n)\right) + \dots + T\left(\frac{n}{\beta} + c_{\lfloor \alpha \rfloor}(n)\right) + b(n) \quad \text{für } n > 1 \end{aligned}$$

(wobei $\frac{n}{\beta} + c_i(n)$ wieder durch $\lfloor \frac{n}{\beta} + c_i(n) \rfloor$ oder $\lceil \frac{n}{\beta} + c_i(n) \rceil$ zu ersetzen ist), dann gilt

$$T(n) \in \begin{cases} \Theta(n^{\log_\beta \alpha}) & \text{falls } b(n) \in \mathcal{O}(n^{\log_\beta \alpha - \varepsilon}) \text{ für ein } \varepsilon > 0 \\ \Theta(b(n) \cdot \log n) & \text{falls } b(n) \in \Theta(n^{\log_\beta \alpha} \cdot (\log n)^\delta) \text{ für ein } \delta \geq 0 \\ \Theta(b(n)) & \text{falls } b(n) \in \Omega(n^{\log_\beta \alpha + \varepsilon}) \text{ für ein } \varepsilon > 0. \end{cases}$$

3.18 Beispiel (Multiplikation großer Zahlen)

Wegen der festen Größe numerischer Standarddatentypen müssen die Grundrechenarten für sehr große Zahlen eigens implementiert werden. Ist w die Speicherwortlänge, dann können wir große Zahlen zur Basis $\beta = 2^w$ darstellen. Die Multiplikation von n -stelligen Zahlen mit der Schulmethode („schriftliches Multiplizieren“) braucht dann $\Theta(n^2)$ Zeit. Aus der Aufteilung der Zahlen in zwei gleich große Teile leiten wir eine schnellere, rekursive Methode her.

Seien a, b zwei n -stellige Zahlen, wobei wir der Einfachheit halber $n = 2^k$, $k \in \mathbb{N}$, annehmen. Dann haben sie Darstellungen

$$a = A_1 \cdot \beta^{\frac{n}{2}} + A_0 \quad \text{und} \quad b = B_1 \cdot \beta^{\frac{n}{2}} + B_0$$

und es gilt

$$a \cdot b = (A_1 \cdot \beta^{\frac{n}{2}} + A_0) \cdot (B_1 \cdot \beta^{\frac{n}{2}} + B_0) = A_1 B_1 \beta^n + (A_1 B_0 + A_0 B_1) \beta^{\frac{n}{2}} + A_0 B_0$$

Da A_1, A_0, B_1 und B_0 jeweils $\frac{n}{2}$ -stellig sind, ist die Laufzeit eines rekursiven Multiplikationsalgorithmus

$$T(n) = 4 \cdot T\left(\frac{n}{2}\right) + \Theta(n),$$

da nach den vier kleineren Multiplikationen nur noch addiert werden muss. Mit dem Master-Theorem 3.17 folgt $T(n) \in \Theta(n^{\log_2 4}) = \Theta(n^2)$, also keine Verbesserung. Die Kosten entstehen durch den vierfachen Aufruf der Rekursion, sodass weniger Multiplikationen wünschenswert sind. Die Darstellung

$$a \cdot b = A_1 B_1 (\beta^n + \beta^{\frac{n}{2}}) + (A_1 - A_0) \cdot (B_0 - B_1) \beta^{\frac{n}{2}} + A_0 B_0 (\beta^{\frac{n}{2}} + 1)$$

führt auf einen rekursiven Algorithmus mit Laufzeit

$$T'(n) = 3 \cdot T' \left(\frac{n}{2} \right) + \Theta(n) ,$$

für den das Master-Theorem $T'(n) \in \Theta(n^{\log_2 3})$ liefert. Wegen $\log_2 3 \sim 1.59$ ist das (zumindest asymptotisch) eine deutliche Verbesserung.

Kapitel 4

Graphentheorie

— Di., 17.6. (V1) —

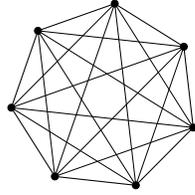
Beziehungen zwischen Objekten werden sehr oft durch binäre Relationen modelliert. Wir beschäftigen uns in diesem Kapitel mit speziellen binären Relationen, die nicht nur besonders anschaulich sind, sondern auch in zahllosen Anwendungen auftreten.

Eine symmetrische und irreflexive binäre Relation $E \subseteq V \times V$ kann auch als Menge von zweielementigen Teilmengen $\{u, v\} \subseteq V$ aufgefasst werden, da $(u, v) \in E \iff (v, u) \in E$ (Symmetrie) und $E \cap \{(v, v) : v \in V\} = \emptyset$ (Irreflexivität).

4.1 Definition (Graph)

Ein Paar $G = (V, E)$ aus Mengen V und $E \subseteq \binom{V}{2}$ heißt (endlicher, ungerichteter) Graph. Die Elemente von V heißen Knoten, die von E Kanten. Wenn keine Missverständnisse zu befürchten sind, schreiben wir kurz $n = n(G) = |V|$ und $m = m(G) = |E|$ für deren Anzahl.

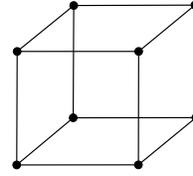
Graphen können sehr anschaulich dargestellt werden, indem man die Knoten durch Punkte und die Kanten durch Kurven, welche die Punkte ihrer beiden Knoten verbinden, repräsentiert. Die folgenden Beispiele sind Darstellungen einiger wichtiger Familien von Graphen.



vollständige Graphen K_n

$$V = \{1, \dots, n\}$$

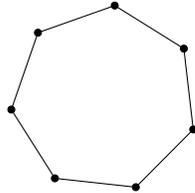
$$E = \binom{\{1, \dots, n\}}{2}$$



Hyperwürfel Q_d

$$V = \{0, 1\}^d$$

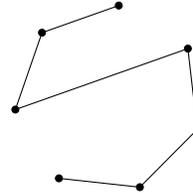
$$E = \{(a_1, \dots, a_d), (b_1, \dots, b_d) : \sum_{i=1}^d |a_i - b_i| = 1\}$$



Zykel oder Kreise C_n

$$V = \{0, \dots, n-1\}$$

$$E = \{\{i, i+1 \pmod n\} : i = 0, \dots, n-1\}$$



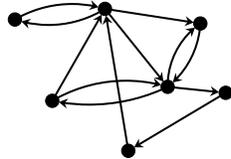
Wege P_n

$$V = \{0, \dots, n\}$$

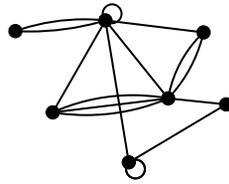
$$E = \{\{i, i+1\} : i = 0, \dots, n-1\}$$

4.2 Bemerkung

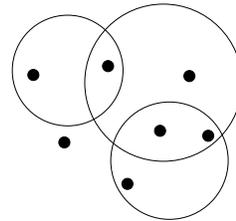
In der Graphentheorie werden auch allgemeinere binäre Relationen behandelt, in denen man auf Symmetrie (\rightarrow gerichtete Graphen), Irreflexivität (\rightarrow Graphen mit Schleifen) oder beides verzichtet. Gelegentlich werden auch Multiteilmengen (so genannte Mehrfachkanten) von $V \times V$ (\rightarrow Multigraphen) oder Kanten mit beliebiger Knotenzahl (\rightarrow Hypergraphen) betrachtet.



gerichteter Graph



Multigraph
(mit Schleifen
und Mehrfachkanten)



Hypergraph
(mit drei Hyperkanten)

Wir beschränken uns jedoch auf den Fall ungerichteter Graphen ohne Schleifen oder Mehrfachkanten; diese werden zur besseren Unterscheidung oft als

schlichte Graphen bezeichnet.

4.3 Definition (Adjazenz, Inzidenz, Grad)

Ist $G = (V, E)$ ein Graph, dann heißen zwei Knoten $u, v \in V$ adjazent (auch: benachbart), falls es eine Kante $\{u, v\} \in E$ gibt, und die Matrix $A(G) = (a_{v,w})_{v,w \in V}$ mit

$$a_{v,w} = \begin{cases} 1 & \text{falls } \{v, w\} \in E \\ 0 & \text{sonst} \end{cases}$$

Adjazenzmatrix des Graphen. Ein Knoten $v \in V$ und eine Kante $e \in E$ heißen inzident, falls $v \in e$, und die Matrix $I(G) = (i_{v,e})_{\substack{v \in V \\ e \in E}}$ mit

$$i_{v,e} = \begin{cases} 1 & \text{falls } v \in e \\ 0 & \text{sonst} \end{cases}$$

Inzidenzmatrix des Graphen. Die Menge $N_G(v) = \{w \in V : \{v, w\} \in E\}$ der zu $v \in V$ adjazenten Knoten heißt Nachbarschaft von v und wir nennen deren Kardinalität

$$d_G(v) = |N_G(v)| = \sum_{w \in V} a_{v,w} = \sum_{e \in E} i_{v,e} ,$$

d.h. die Zeilensumme von v in $A(G)$ oder $I(G)$, den Grad von v . Der minimale und maximale Grad werden mit $\delta(G) = \min_{v \in V} d_G(v)$ bzw. $\Delta(G) = \max_{v \in V} d_G(v)$ bezeichnet.

— Di., 24.6. (V1) —

4.4 Lemma (Handschlaglemma)

Für alle Graphen $G = (V, E)$ gilt

$$\sum_{v \in V} d_G(v) = 2m .$$

■ **Beweis:** Prinzip des doppelten Abzählens: auf der linken Seite der Gleichung wird über alle Zeilen der Inzidenzmatrix summiert. Da jede Spalte einer Kante entspricht und jede Kante genau zwei verschiedene Knoten enthält, ergibt die Summe über alle Spalten gerade zweimal die Anzahl der Kanten. □

4.5 Folgerung

Die Anzahl der Knoten ungeraden Grades ist gerade.

■ **Beweis:** Sei $V_i = \{v \in V : d_G(v) \equiv i \pmod{2}\}$, $i = 0, 1$, die Menge der Knoten mit geradem bzw. ungeradem Grad. Mit dem Handschlaglemma 4.4 gilt

$$2m = \sum_{v \in V} d_G(v) = \underbrace{\sum_{v \in V_0} d_G(v)}_{\text{gerade}} + \sum_{v \in V_1} d_G(v),$$

also ist auch die hinterste Summe gerade, sodass, weil jeder ihrer Summanden ungerade ist, deren Anzahl gerade sein muss. \square

4.6 Satz

Es gibt immer zwei Knoten mit gleichem Grad.

■ **Beweis:** Für alle $v \in V$ gilt $0 \leq d_G(v) \leq n-1$. Gibt es einen Knoten mit Grad 0, dann gibt es keinen mit Grad $n-1$, und umgekehrt (ein Knoten vom Grad 0 ist mit keinem anderen benachbart, einer vom Grad $n-1$ mit allen anderen Knoten; beides zusammen geht nicht). Also gilt in einem Graphen sogar $0 \leq d_G(v) \leq n-2$ oder $1 \leq d_G(v) \leq n-1$ für alle $v \in V$. Mit dem Tauberschlagprinzip folgt, dass von den n Knoten mindestens zwei den gleichen der $n-1$ möglichen Grade haben. \square

4.7 Definition (Teilgraphen)

Sind $G = (V, E)$ ein Graph sowie $V' \subseteq V$ und $E' \subseteq E$ Teilmengen seiner Knoten und Kanten, dann ist $G' = (V', E')$ ein Teilgraph von G , falls $E' \subseteq \binom{V'}{2}$. Wir sagen dann G enthält G' und schreiben $G' \subseteq G$. Die Teilgraphen

$$G[V'] = (V', E \cap \binom{V'}{2}) \quad \text{und} \quad G[E'] = (\bigcup_{e \in E'} e, E')$$

heißen der von V' knoten- bzw. von E' kanteninduzierte Teilgraph. Ein Teilgraph heißt aufspannend, falls er alle Knoten enthält.

Wir werden außerdem Schreibweisen wie z.B. $G - v$ für $G[V \setminus \{v\}]$ oder $G + e$ für den Graphen $G' = (V, E \cup e)$ verwenden. Um die Knoten- und Kantenmenge eines Graphen G von anderen zu unterscheiden, schreiben wir auch $V(G)$ und $E(G)$.

4.8 Definition (Graphenisomorphismus)

Gibt es zu zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ eine bijektive Abbildung $\alpha : V_1 \rightarrow V_2$ mit

$$\{u, v\} \in E_1 \iff \{\alpha(u), \alpha(v)\} \in E_2 ,$$

dann heißen die Graphen G_1 und G_2 isomorph, $G_1 \cong G_2$, und α Graphenisomorphismus.

Wir interessieren uns vor allem für strukturelle Eigenschaften und werden isomorphe Graphen daher nicht unterscheiden. Dadurch können wir z.B. von *dem* vollständigen Graphen mit 7 Knoten sprechen, auch wenn seine Knotenmenge nicht $\{1, \dots, 7\}$ ist.

4.9 Definition (Wege und Kreise in einem Graphen)

Ein Graph $G = (V, E)$ mit $s, t \in V$ enthält einen (s, t) -Weg der Länge k , falls er einen zu P_k isomorphen Teilgraphen mit Endknoten s und t enthält, d.h. es gibt einen Teilgraphen $P = (V(P), E(P)) \subseteq G$ mit $s, t \in V(P)$ und einen Isomorphismus $\alpha : \{0, \dots, k\} \rightarrow V(P)$ von P_k so, dass $\alpha(0) = s$ und $\alpha(k) = t$.

Die Länge eines kürzesten (s, t) -Weges heißt Abstand (auch: Distanz) von s und t und wird mit $d_G(s, t)$ bezeichnet.

Der Graph enthält einen Kreis der Länge k , falls er einen zu C_k isomorphen Teilgraphen enthält.

4.10 Definition (Zusammenhang)

Ein Graph $G = (V, E)$ heißt zusammenhängend, wenn er zu je zwei Knoten $s, t \in V$ einen (s, t) -Weg enthält. Die inklusionsmaximalen Teilgraphen eines Graphen sind seine (Zusammenhangs)komponenten und ihre Anzahl wird mit $\kappa(G)$ bezeichnet.

4.1 Bäume und Wälder

— Do., 26.6. (V2) —

Die folgende spezielle Klasse von Graphen ist uns schon begegnet und eine zentrale Struktur der Informatik.

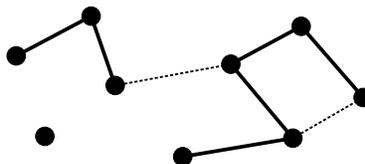
4.11 Definition (Baum)

Ein zusammenhängender Graph ohne Kreise heißt Baum. Ein Graph, dessen sämtliche Zusammenhangskomponenten Bäume sind, heißt Wald.

4.12 Satz

Für jeden Graphen $G = (V, E)$ gilt $m \geq n - \kappa(G)$. Gleichheit gilt genau dann, wenn G ein Wald ist.

■ **Beweis:** Induktion über die Anzahl m der Kanten bei fester Anzahl n von Knoten. Enthält ein Graph keine Kante, sind keine zwei Knoten durch einen Weg verbunden, jeder bildet also seine eigene Komponente (und damit einen trivialen Baum) und es gilt $m = 0 = n - \kappa(G)$. Fügt man zu einem Graphen eine Kante zwischen bestehenden Knoten hinzu, verbindet sie zwei Knoten, die entweder in derselben oder in zwei verschiedenen Komponenten (die dann vereinigt werden) liegen.



Die Zahl der Komponenten verringert sich also um maximal eins, sodass die Ungleichung weiterhin gilt. Wenn durch die neue Kante zwei Komponenten vereinigt werden, entsteht kein neuer Kreis, denn sonst müsste es zwischen den beiden neu verbundenen Knoten vorher schon einen Weg gegeben haben. \square

4.13 Satz

Für einen Graphen $G = (V, E)$ sind folgende Aussagen äquivalent:

- (i) G ist ein Baum.
- (ii) Zwischen je zwei Knoten in G existiert genau ein Weg.

- (iii) G ist zusammenhängend und hat $n - 1$ Kanten.
- (iv) G ist minimal zusammenhängend, d.h. G ist zusammenhängend und für alle $e \in E$ ist $G - e$ unzusammenhängend.
- (v) G ist maximal kreisfrei (azyklisch), d.h. G ist kreisfrei und für alle $e \in \binom{V}{2} \setminus E$ enthält $G + e$ einen Kreis.

■ **Beweis:** (i) \iff (ii): Da Bäume zusammenhängend sind, gibt es zwischen je zwei Knoten mindestens einen Weg. Gäbe es zwei verschiedene, so enthielte deren Vereinigung einen Kreis. Gibt es umgekehrt immer genau einen Weg, dann ist der Graph kreisfrei, weil es andernfalls zwei Wege zwischen je zwei Knoten des Kreises gäbe.

(i) \iff (iii): Folgt unmittelbar aus Satz 4.12.

(iii) \implies (iv): Wegen Satz 4.12 kann ein Graph mit $n - 2$ Kanten nicht zusammenhängend sein.

(iv) \implies (v): Enthielte G einen Kreis, so könnte eine beliebige Kante des Kreises entfernt werden und G wäre immer noch zusammenhängend. Könnte man eine Kante hinzufügen, ohne einen Kreis zu erzeugen, kann es vorher keinen Weg zwischen den beiden Knoten der neuen Kante gegeben haben, der Graph wäre also nicht zusammenhängend gewesen.

(v) \implies (i): Da G kreisfrei ist, müssen wir nur zeigen, dass G auch zusammenhängend ist. Wäre G nicht zusammenhängend, so könnte zwischen zwei Knoten in verschiedenen Komponenten eine Kante eingefügt werden, ohne einen Kreis zu erzeugen. \square

4.14 Folgerung

Jeder zusammenhängende Graph enthält einen aufspannenden Baum.

Die Anzahl

$$\mu(G) = m - n + \kappa(G)$$

der Kanten, die man aus einem Graphen entfernen muss/kann, um einen aufspannenden Wald mit gleicher Anzahl von Komponenten zu erhalten, heißt auch zyklomatische Zahl des Graphen.

4.15 Satz

Zu $n \in \mathbb{N}$ gibt es n^{n-2} verschiedene Bäume mit Knotenmenge $\{1, \dots, n\}$.

■ **Beweis:** Da die Aussage für $n = 1$ offensichtlich stimmt, können wir $n \geq 2$ annehmen. Wir wenden das Identitätsprinzip an, indem wir die Bäume bijektiv auf $\{1, \dots, n\}^{n-2}$ abbilden.

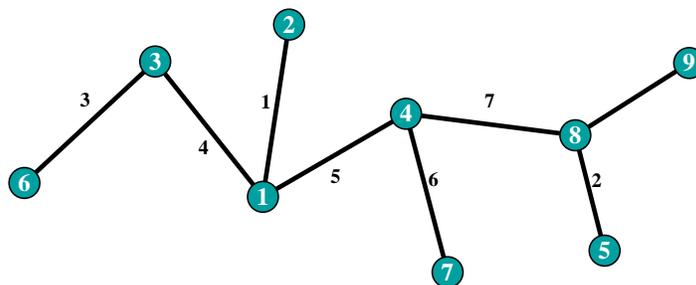
Einem Baum wird ein Tupel (v_1, \dots, v_{n-2}) wie folgt zugewiesen. Ein Baum hat immer einen Knoten vom Grad 1, denn wenn alle Knoten einen größeren Grad hätten, wäre die Summe der Knotengrade größer oder gleich $2n$, sodass aus dem Handschlaglemma 4.4 die Existenz von mindestens $\frac{2n}{2} = n$ Kanten folgte (Widerspruch zu Satz 4.13). Unter den Knoten vom Grad 1 sei v der kleinste. Der eindeutige Nachbar definiert v_1 . Werden danach v und die eine zu v inzidente Kante entfernt, erhalten wir wieder einen Baum und wählen erneut den kleinsten Knoten vom Grad 1. Dessen Nachbar definiert v_2 , usw. Das so konstruierte Tupel (v_1, \dots, v_{n-2}) heißt *Prüfercode* des Baums. Man beachte, dass zum Schluss eine Kante übrig bleibt, da nur $n - 2$ Kanten entfernt werden.

Wir zeigen, dass die dadurch definierte Abbildung injektiv und surjektiv ist, indem wir zeigen, dass zu jedem $(v_1, \dots, v_{n-2}) \in \{1, \dots, n\}^{n-2}$ genau ein Baum mit Prüfercode (v_1, \dots, v_{n-2}) existiert.

Wir stellen zunächst fest, dass ein Knoten, der im Baum den Grad d hat, im Prüfercode genau $d - 1$ mal auftritt (nämlich immer dann, wenn ein Nachbar entfernt wird, der Knoten selbst aber noch einen weiteren Nachbarn im Baum hat). Knoten vom Grad 1 treten im Prüfercode also nicht auf. Der kleinste nicht auftretende Knoten muss derjenige sein, der als erster entfernt wurde, und sein Nachbar war v_1 . Der kleinste von den $n - 1$ anderen Knoten, der nicht in (v_2, \dots, v_{n-2}) auftritt, muss Nachbar von v_2 gewesen sein, usw. Nachdem so $n - 2$ mal ein Knoten bestimmt worden ist, sind nur v_{n-2} und ein weiterer Knoten übrig. Die letzte hinzuzufügende Kante muss dann diese beiden verbinden und der bei der Erzeugung des Prüfercodes übrig gebliebenen entsprechen. \square

4.16 Beispiel

Der Prüfercode des folgenden Baums ist $(1, 8, 3, 1, 4, 4, 8)$ und die Kantenbeschriftungen geben die Reihenfolge an, in der sie entfernt wurden.



Bei der Rekonstruktion werden die Kanten in derselben Reihenfolge eingefügt, die unbeschriftete zuletzt.

4.2 Durchläufe

In diesem Abschnitt werden wir Graphen *durchlaufen*, um Eigenschaften zu testen oder Teilgraphen zu identifizieren. Durchlaufen bedeutet dabei, an einem Knoten zu starten und jeweils von einem bereits besuchten Knoten über eine Kante den benachbarten Knoten aufzusuchen. Dazu werden zunächst die Definitionen von Wegen und Kreisen verallgemeinert.

4.17 Definition (Graphenhomomorphismus)

Gibt es zu zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ eine Abbildung $\alpha : V_1 \rightarrow V_2$ mit

$$\{u, v\} \in E_1 \implies \{\alpha(u), \alpha(v)\} \in E_2 ,$$

dann heißt α (Graphen)homomorphismus und wir nennen den Teilgraphen

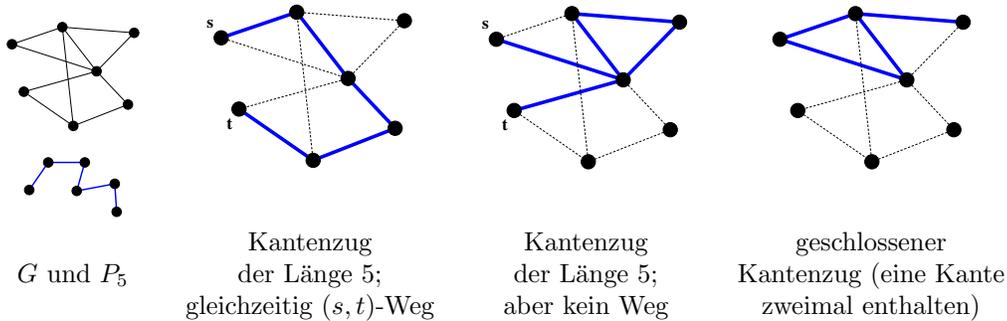
$$\alpha(G_1) = (\alpha(V_1), \{\{\alpha(u), \alpha(v)\} \in E_2 : \{u, v\} \in E_1\}) \subseteq G_2$$

homomorphes Bild von G_1 in G_2 .

4.18 Definition (Kantenzug und Tour)

Ist $G = (V, E)$ ein Graph und $\alpha : V(P_k) \rightarrow V(G)$ ein Homomorphismus, dann heißt $\alpha(P_k) \subseteq G$ Kantenzug der Länge k . Ein Kantenzug heißt geschlossen oder Tour, falls $\alpha(0) = \alpha(k)$ (in diesem Fall ist $\alpha(P_k)$ auch homomorphes Bild des Kreises C_k).

Eine Kante $\{v, w\} \in E$ ist $|\{\{i, i + 1\} \in E(P_k) : \{\alpha(i), \alpha(i + 1)\} = \{v, w\}\}|$ mal im Kantenzug $\alpha(P_k)$ enthalten.



4.2.1 Eulertouren und Hamiltonkreise

Manche Graphenprobleme unterscheiden sich nur geringfügig in der Definition, aber erheblich im Schwierigkeitsgrad. Wir beginnen mit einem „leichten“, dass gleichzeitig das erste in der Graphentheorie betrachtete war.

Euler,
1736

4.19 Definition (Eulertour)

Eine Tour heißt Eulertour, falls sie jede Kante genau einmal enthält.

4.20 Satz

Ein zusammenhängender Graph enthält genau dann eine Eulertour, wenn alle Knoten geraden Grad haben.

■ **Beweis:** Der Graph $G = (V, E)$ enthalte eine Eulertour, d.h. es gebe eine homomorphe Abbildung von C_m , dem Kreis mit m Kanten, auf G . Da jede Kante nur einmal in der Tour vorkommt, sorgt jeder Knoten des Kreises dafür, dass zwei zum selben Knoten von G inzidente Kanten in der Tour enthalten sind. Da aber alle Kanten in der Tour vorkommen, muss die Anzahl der zu einem Knoten von G inzidente Kanten gerade sein.

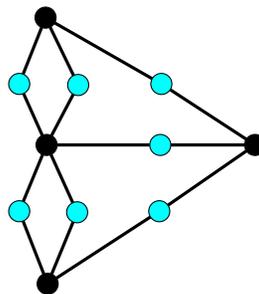
Betrachte nun umgekehrt einen zusammenhängenden Graphen, in dem jeder Knoten geraden Grad hat. Beginne bei irgendeinem Knoten und wähle eine Kante. Am benachbarten Knoten wähle eine noch nicht gewählte Kante und fahre so fort. Dies geht solange, bis man wieder den ersten Knoten erreicht, denn an jedem anderen gibt es wegen des geraden Grades immer eine noch nicht gewählte Kante. Die gewählten Kanten sind homomorphes Bild eines Kreises und an jedem Knoten ist die Anzahl der gewählten und ungewählten Kanten gerade. Falls es noch einen Knoten mit ungewählten Kanten gibt, dann wegen des Zusammenhangs auch einen, der zu schon gewählten Kanten inzident ist. Wiederhole die Konstruktion von diesem Knoten aus und füge die beiden homomorphen Bilder von Kreisen zu einem zusammen (Anfangsstück des ersten bis zum gemeinsamen Knoten, dann der zweite Kantenzug und schließlich das Endstück des ersten), bis alle Kanten einmal gewählt wurden.

Algorithmus
von Hier-
holzer

□

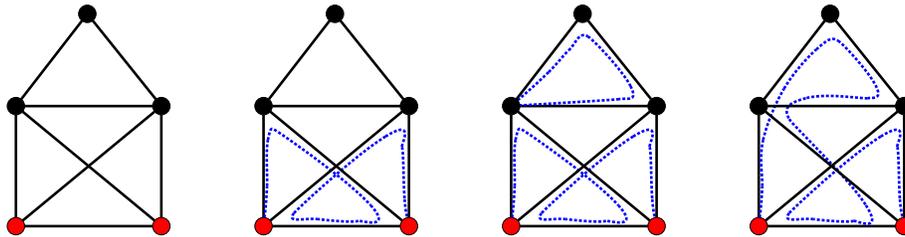
4.21 Beispiel (Königsberger Brückenproblem)

Der unten stehende Graph stellt sieben Brücken (helle Knoten) über den durch Königsberg fließenden Fluss Pregel dar. Da nicht alle Knoten geraden Grad haben, gibt es keine Eulertour (und damit keinen Rundgang, der jede der Brücken genau einmal überquert).



4.22 Beispiel (Haus vom Nikolaus)

Wenn man sich mit einem (nicht notwendig geschlossenen) Kantenzug, der alle Kanten genau einmal enthält, begnügt, dann funktioniert die Konstruktion aus dem Beweis von Satz 4.20 auch dann noch, wenn es zwei Knoten ungeraden Grades gibt. Man muss dann allerdings bei einem davon anfangen und wird beim anderen aufhören.



Eine leichte Modifikation der Fragestellung führt auf ein wesentlich schwierigeres Problem.

4.23 Definition (Hamiltonkreis)

Ein Kreis heißt Hamiltonkreis, falls er jeden Knoten genau einmal enthält.

4.24 Satz

Das Entscheidungsproblem, ob eine Graph einen Hamiltonkreis enthält, ist \mathcal{NP} -vollständig.

Reduktion von
VERTEX COVER

4.2.2 Tiefensuche

Der Algorithmus zur Konstruktion einer Eulertour durchläuft solange Kanten vom jeweils zuletzt besuchten Knoten, bis dieser nicht mehr zu unbesuchten Kanten inzident ist. In diesem Fall wird an irgendeinem zu unbesuchten Kanten inzidenten Knoten weitergemacht.

In der Variante in Algorithmus 4 wird immer vom zuletzt *gefundenen* (statt besuchten) Knoten aus weitergesucht. Auf diese Weise können z.B. ein aufspannender Baum, ein Kreis oder ein Weg zwischen zwei Knoten konstruiert werden.

Algorithmus 4: Tiefensuche (*depth-first search, DFS*)

Eingabe: Graph $G = (V, E)$, Wurzel $s \in V$

Daten: Knotenstack S , Zähler d

Ausgabe: Tiefensuchnummern DFS (initialisiert mit ∞)
Vorgänger $pred$ (initialisiert mit nil)

$DFS[s] \leftarrow 1; \quad d \leftarrow 2;$

markiere s ; $push\ S \leftarrow s$;

while S nicht leer **do**

$v \leftarrow top(S)$;

if es ex. unmarkierte Kante $\{v, w\} \in E$ **then**

 markiere $\{v, w\}$;

if w nicht markiert **then**

$DFS[w] \leftarrow d; \quad d \leftarrow d + 1;$

 markiere w ; $push\ S \leftarrow w$;

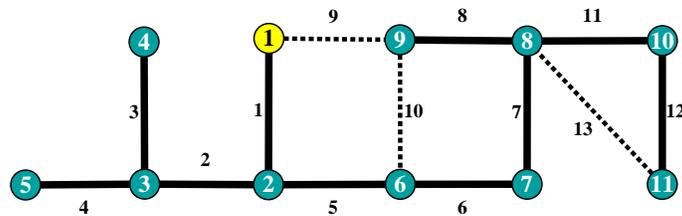
$pred[w] \leftarrow v$;

else $pop\ v \leftarrow S$;

Offensichtlich erhalten alle Knoten eines Graphen, die im Verlauf des Algorithmus' markiert werden, eine endliche Tiefensuchnummer $DFS[v]$. Falls nach Ablauf des Algorithmus' $pred[w] = v$ gilt, heißt die Kante $\{v, w\}$ Baumkante, alle anderen markierten Kanten heißen Nichtbaumkanten (auch: Rückwärtskanten).

4.25 Beispiel

Tiefensuche vom hellen Knoten aus: die Knoten sind mit ihren Tiefensuchnummern und die Kanten in Reihenfolge ihres Durchlaufs beschriftet.



Beobachtung: Die Tiefensuche liefert einen aufspannenden Baum (Baumkanten durchgezogen). Die Knoten einer Nichtbaumkante (gestrichelt) sind durch einen monoton nummerierten Weg im Baum verbunden.

4.26 Lemma

Wenn $v \in V$ auf S abgelegt wird, sei $M \subseteq (V \setminus \{v\})$ die Menge aller anderen bereits markierten Knoten. Der Knoten v wird erst von S entfernt, nachdem alle Knoten $t \in V \setminus M$, für die es einen (v, t) -Weg in $G[V \setminus M]$ gibt, ebenfalls markiert wurden.

■ **Beweis:** Angenommen, es gibt einen Knoten, für den die Aussage falsch ist. Wähle unter allen diesen dasjenige $v \in V$ mit maximaler $\text{DFS}[v]$ und einen Knoten $t \in V$, der bei Entfernen von v aus S noch nicht markiert ist.

Gibt es einen (v, t) -Weg über unmarkierte Knoten, dann beginnt er mit einem unmarkierten Nachbarn von v . In der **while**-Schleife werden alle Nachbarn von v markiert, bevor v aus S entfernt wird, und wegen der Maximalität von $\text{DFS}[v]$ wird t markiert, bevor dieser Nachbar aus S entfernt wird. Das ist ein Widerspruch. \square

4.27 Satz

Ist $B \subseteq E$ die Menge der Baumkanten nach einer Tiefensuche auf $G = (V, E)$ mit Wurzel $s \in V$, dann ist $(G[B] + s) \subseteq G$ ein aufspannender Baum der Zusammenhangskomponente, die s enthält.

■ **Beweis:** Wir stellen zunächst fest, dass alle zu Baumkanten inzidenten Knoten markiert werden. Der von den Baumkanten induzierte Graph ist

zusammenhängend, da jede neue Baumkante immer inzident zu einem bereits markierten Knoten ist. Er ist außerdem kreisfrei, denn jede neue Baumkante enthält genau einen Knoten, der zuvor nicht markiert war (ein Kreis kann also niemals geschlossen werden).

Weil Lemma 4.26 insbesondere für die Wurzel selbst gilt, werden alle Knoten der Zusammenhangskomponente von s markiert. \square

Durch mehrfache Tiefensuche können daher alle Zusammenhangskomponenten bestimmt werden.

Der folgende Satz besagt, dass Nichtbaumkanten immer nur zwischen Knoten verlaufen, die mit der Wurzel auf einem gemeinsamen Weg liegen. Daher kann man die Tiefensuche z.B. auch benutzen, um in Komponenten, die keine Bäume sind, als *Zertifikat* einen Kreis zu konstruieren.

4.28 Satz

Ist $B \subseteq E$ die Menge der Baumkanten nach einer Tiefensuche auf $G = (V, E)$, $\{v, w\} \in E$ eine Nichtbaumkante mit $\text{DFS}[w] < \text{DFS}[v]$ und $v = v_1, v_2, \dots, v_k = w$ der eindeutige (v, w) -Weg in $G[B]$, dann gilt $\text{pred}[v_i] = v_{i+1}$ für alle $i = 1, \dots, k - 1$.

■ **Beweis:** Die Existenz der Nichtbaumkante zeigt, dass v und w in der selben Zusammenhangskomponente liegen, und $\text{DFS}[w] < \text{DFS}[v]$ bedeutet, dass v später als w gefunden wird. Die Nichtbaumkante wird daher markiert während v (und nicht w) oben auf dem Stack liegt (andernfalls wäre sie eine Baumkante). Das bedeutet aber, dass w zu diesem Zeitpunkt noch in S ist, weil ein Knoten erst entfernt wird, nachdem alle inzidenten Kanten markiert wurden. Die Behauptung folgt damit aus der Beobachtung, dass für einen Knoten u , der auf dem Stack unmittelbar auf einen Knoten u' gelegt wird, $\text{pred}[u] = u'$ gilt. \square

4.2.3 Breitensuche

Wir ändern die Durchlaufreihenfolge nun so, dass immer vom *zuerst* gefundenen Knoten aus weitergesucht wird. Dadurch kann nicht nur wieder ein aufspannender Wald konstruiert werden, sondern auch kürzeste Wege von einem Anfangsknoten zu allen anderen in seiner Komponente.

Algorithmus 5: Breitensuche (*breadth-first search, BFS*)

Eingabe: Graph $G = (V, E)$, Wurzel $s \in V$

Daten: Knotenwarteschlange Q

Ausgabe: Breitensuchnummern BFS (initialisiert mit ∞)
Vorgänger pred (initialisiert mit nil)

```

BFS[s] ← 0;
markiere s; enqueue Q ← s;
while Q nicht leer do
    dequeue v ← Q;
    for unmarkierte Kanten {v, w} ∈ E do
        markiere {v, w};
        if w nicht markiert then
            BFS[w] ← BFS[v] + 1;
            markiere w; enqueue Q ← w;
            pred[w] ← v;

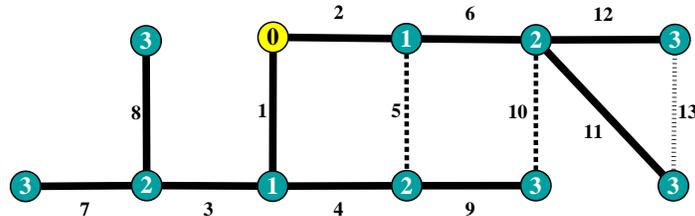
```

Offensichtlich erhalten alle Knoten eines Graphen, die im Verlauf des Algorithmus' markiert werden, eine endliche Breitensuchnummer $\text{BFS}[v]$. Falls nach Ablauf des Algorithmus' $\text{pred}[w] = v$ gilt, heißt die Kante $\{v, w\}$ Baumkante, alle anderen markierten Kanten heißen Nichtbaumkanten.

Man beachte, dass für Baumkanten $\text{BFS}[w] = \text{BFS}[v] + 1$ gilt. Gilt dies für eine Nichtbaumkante, nennen wir sie auch Vorwärtskante, andernfalls Querkante.

4.29 Beispiel

Breitensuche vom hellen Knoten aus: die Knoten sind mit ihren Breitensuchnummern und die Kanten in Reihenfolge ihres Durchlaufs beschriftet.



Beobachtung: Die Breitensuche liefert einen aufspannenden Baum (Baumkanten sind durchgezogen, Vorwärtskanten gestrichelt, Querkanten gepunktet). Die Breitensuchnummern sind gerade die Längen kürzester Wege von der Wurzel aus.

4.30 Lemma

Alle Knoten und Kanten der Zusammenhangskomponente der Wurzel werden markiert. Für jede markierte Kante $\{v, w\}$ gilt $|BFS[v] - BFS[w]| \leq 1$.

■ **Beweis:** Wird ein Knoten markiert, dann auch alle seine inzidenten Kanten und alle seine Nachbarn. Eine nicht markierte Kante kann also nicht zu einem markierten Knoten inzident sein.

Angenommen, es gibt einen nicht markierten Knoten v in der Zusammenhangskomponente der Wurzel s . Nach Definition des Zusammenhangs gibt es einen (v, s) -Weg. Da s markiert wird, muss es auf diesem Weg zwei adjazente Knoten geben, von denen genau einer markiert ist. Das ist ein Widerspruch.

Die Breitensuchnummern der Knoten in der Warteschlange unterscheiden sich um höchstens 1 und die Knoten mit kleinerer Nummer werden zuerst entnommen, denn wenn ein Knoten w markiert und eingefügt wird, wurde zuvor ein Knoten v mit um 1 kleinerer Nummer entnommen. Wird eine weitere zu w inzidente Kante von einem Knoten v' aus markiert, dann ist w selbst noch in der Warteschlange (sonst wären alle inzidenten Kanten bereits markiert), sodass der Nachbar v' nach v und vor w eingefügt wurde und seine Breitensuchnummer zwischen denen von v und w liegt. \square

4.31 Satz

Ist $B \subseteq E$ die Menge der Baumkanten nach einer Breitensuche auf $G = (V, E)$ mit Wurzel $s \in V$, dann ist $(G[B] + s) \subseteq G$ ein aufspannender Baum der Zusammenhangskomponente, die s enthält.

■ **Beweis:** Ist n_s die Anzahl der Knoten in der Zusammenhangskomponente von s , dann ist $|B| = n_s - 1$, denn nach Lemma 4.30 werden alle n_s Knoten markiert, und eine Baumkante kommt genau dann hinzu, wenn ein anderer Knoten als s markiert wird.

Wegen Satz 4.13 brauchen wir also nur noch zu zeigen, dass $G[B]$ für $B \neq \emptyset$ zusammenhängend ist. Ein anderer Knoten als s wird aber nur dann markiert, wenn er einen bereits markierten Nachbarn hat. \square

4.32 Satz

Der eindeutige Weg von der Wurzel s zu einem Knoten $v \in V$ in $G[B] + s$ ist ein kürzester (s, v) -Weg in G und $\text{BFS}[v] = d_G(s, v)$.

■ **Beweis:** Wenn in der Breitensuche eine Baumkante $\{\text{pred}[w], w\}$ durchlaufen wird, erhält w die Breitensuchnummer $\text{BFS}[\text{pred}[w]] + 1$. Der eindeutige (s, v) -Weg im Baum hat daher die Länge $\text{BFS}[v]$.

Sind $s = v_0, v_1, \dots, v_k = v$ die Knoten auf einem (s, v) -Weg in G , dann gilt $|\text{BFS}[v_i] - \text{BFS}[v_{i-1}]| \leq 1$ für alle $i = 1, \dots, k$ wegen Lemma 4.30. Weil $\text{BFS}[s] = 0$ hat jeder solche Weg mindestens $\text{BFS}[v]$ Kanten. \square

4.3 Matchings und Färbungen

— Bonusabschnitt —

In diesem Abschnitt betrachten wir zunächst binäre Relationen, die zwar symmetrisch und irreflexiv sind, aber Teilmengen des kartesischen Produkts zweier verschiedener Mengen (d.h. $E \subseteq U \times W$).

4.33 Definition (bipartiter Graph)

Ein Graph $G = (V, E)$ mit $V = U \uplus W$ heißt bipartit, falls $\binom{U}{2} \cap E = \emptyset = \binom{W}{2} \cap E$.

Die Existenz einer Bipartition kann strukturell charakterisiert werden.

4.34 Satz

Ein Graph ist genau dann bipartit, wenn er keine Kreise ungerader Länge enthält.

■ **Beweis:** Der Graph sei bipartit mit Bipartition seiner Knotenmenge in Mengen V_0 und V_1 . Angenommen, er enthalte einen Kreis ungerader Länge aus Knoten v_1, \dots, v_{2k+1} . Wir können ferner annehmen, dass $v_1 \in V_1$ (sonst umbenennen). Dann muss aber $v_2 \in V_0$ gelten und weiter $v_i \in V_{(i \bmod 2)}$ für alle $i = 1, \dots, 2k + 1$, insbesondere gilt für die beiden adjazenten Knoten $v_1, v_{2k+1} \in V_1$. Das ist ein Widerspruch zur Bipartitheit.

Umgekehrt enthalte der Graph keine Kreise ungerader Länge. Man erhält dann eine Bipartition $V = U \uplus W$ der Knotenmenge, indem in jeder Komponente ein Knoten ausgewählt und zu U hinzugefügt wird. Alle Nachbarn von Knoten aus U werden zu W hinzugefügt, dann alle Nachbarn von Knoten in W zu U , usw. Die Menge, zu der ein Knoten hinzugefügt wird, kann nur dann von mehr als einem Nachbarn bestimmt werden, wenn ein Kreis aus bereits klassifizierten Knoten geschlossen wird. Da alle Kreise gerade Länge haben, ist das aber kein Problem. \square

Der zweite Teil des Beweises legt die folgende Modifikation der Breitensuche nahe, um einen beliebigen Graphen auf Bipartitheit zu testen.

Algorithmus 6: Test auf Bipartitheit (Modifikation von Algorithmus 5)

...

```

if  $w$  nicht markiert then
    | ...
else
    | if  $BFS[v] = BFS[w]$  then
    | |   output „nicht bipartit“;
    | |   halt;
output „bipartit“;

```

4.35 Satz

Algorithmus 6 testet in $\mathcal{O}(n + m)$ Zeit, ob die Zusammenhangskomponente der Wurzel bipartit ist.

■ **Beweis:** Wir nehmen an, der Graph sei zusammenhängend (ansonsten sind alle Argumente auf die Zusammenhangskomponente der Wurzel einzuschränken).

Gegenüber der Breitensuche ist der zusätzliche Aufwand linear in der Anzahl der Kanten, sodass die Gesamtzeit linear in der Größe des Graphen bleibt.

Tritt der zum Abbruch führende Fall $\text{BFS}[v] = \text{BFS}[w]$ niemals ein, so unterscheiden sich die Breitensuchnummern von je zwei adjazenten Knoten genau um 1. Jede Kante hat also einen Knoten mit gerader und einen mit ungerader Breitensuchnummer. Partitioniert man die Knotenmenge in $V = U \uplus W$ mit $U = \{u \in V : \text{BFS}[u] \text{ ungerade}\}$ und $W = \{w \in V : \text{BFS}[w] \text{ gerade}\}$, dann gilt $U \cap e \neq \emptyset \neq e \cap W$ für alle $e \in E$, die Breitensuchnummern liefern also einen Beweis für die Bipartitheit.

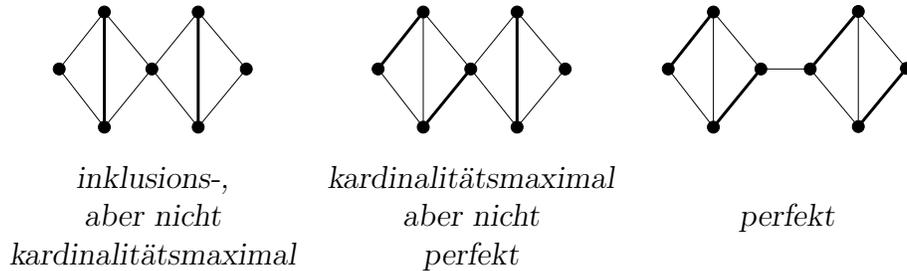
Aus der Bedingung für den vorzeitigen Abbruch folgt mit Lemma 4.30, dass die Knoten v und w den gleichen Abstand von der Wurzel haben. Wähle zwei kürzeste Wege von v und w zur Wurzel, die nur aus bereits markierten Kanten bestehen und betrachte den ersten gemeinsamen Knoten u (spätestens die Wurzel selbst). Da schon bei der ersten Querkante abgebrochen wird, sind bis dahin nur Baum- und Vorwärtskanten aufgetreten, die Breitensuchnummer der beiden inzidente Knoten unterscheiden sich also jeweils um genau 1. Folglich sind der (v, u) - und der (w, u) -Weg gleich lang, sodass sie zusammen mit der Querkante einen Kreis ungerader Länge bilden. Wegen Satz 4.34 ist dieser Kreis ein Beweis für die Nicht-Bipartitheit des Graphen. \square

4.36 Definition (Matching)

Ist $G = (V, E)$ ein Graph, dann heißt eine Kantenteilmenge $M \subseteq E$ Matching, falls $e \cap e' = \emptyset$ für alle $e \neq e' \in M$. Ein Matching M heißt inklusionsmaximal, wenn es kein Matching M' mit $M \subset M'$ gibt, kardinalitätsmaximal, wenn es kein Matching M' mit $|M| < |M'|$ gibt, und perfekt, wenn $|M| = \lfloor \frac{n}{2} \rfloor$.

4.37 Bemerkung

Ein kardinalitätsmaximales Matching ist auch inklusionsmaximal, aber ein inklusionsmaximales Matching ist nicht notwendig kardinalitätsmaximal. Ein perfektes Matching ist inklusions- und kardinalitätsmaximal, aber ein kardinalitätsmaximales Matching ist nicht notwendig perfekt.



In bipartiten Graphen $G = (U \uplus W, E)$ ordnet ein Matching jedem Knoten von U höchstens einen Knoten von W zu und umgekehrt.

4.38 Beispiel (Arbeitsvermittlung)

Einer Menge U von Jobsuchenden steht eine Menge W von Jobs gegenüber. Wir definieren einen bipartiten Graphen $G = (U \uplus W, E)$, dessen Kanten $\{u, w\}$ ausdrücken, dass u für w geeignet ist.

Da jede/r nur einen Job erhalten soll und jeder Job nur einmal vergeben werden kann, entspricht eine Vermittlung einem Matching. Natürlich ist man an einem Matching größtmöglicher Kardinalität interessiert.

4.39 Satz (Heiratssatz)

In einem bipartiten Graphen $G = (U \uplus W, E)$ existiert ein Matching der Kardinalität $|U|$ genau dann, wenn für jede Teilmenge $X \subseteq U$ gilt

$$|X| \leq |N_G(X)| ,$$

wobei $N_G(X) = \bigcup_{u \in X} N_G(u)$ die vereinigten Nachbarschaften sind.

■ **Beweis:** Es gebe ein Matching M mit $|M| = |U|$. Wir betrachten eine beliebige Teilmenge $X \subseteq U$. Da keine zwei Kanten eines Matchings zu einem gemeinsamen Knoten inzident sind, müssen in $G[M]$ die Nachbarn der Knoten in X alle verschieden sein. Daraus folgt, dass die Nachbarschaft von X in G mindestens $|X|$ Knoten enthält.

Umgekehrt gelte die Ungleichung für alle $X \subseteq U$. Angenommen, für ein kardinalitätsmaximales Matching M wäre $|M| < |U|$. Dann gibt es ein $u_0 \in U$, dass zu keiner Kante in M inzident ist. Da $|N_G(\{u_0\})| \geq |\{u_0\}|$ nach Voraussetzung, hat u_0 mindestens einen Nachbarn $w_0 \in W$. Gibt es zu diesem eine Kante $\{w_0, u_1\} \in M$, dann finden wir wegen $|N_G(\{u_0, u_1\})| \geq |\{u_0, u_1\}|$ einen weiteren Knoten $w_1 \neq w_0$, der über eine Kante in $E \setminus M$ mit $\{u_0, u_1\}$

verbunden ist. Gibt es auch zu w_1 eine inzidente Matchingkante $\{u_2, w_1\}$, dann ist $u_2 \notin \{u_0, u_1\}$ und wir können wegen der Ungleichungsbedingung das Verfahren fortsetzen, bis wir ein w_k finden, das zu keiner Matchingkante inzident ist.

Da wir in jedem Schritt eine zu genau einem neuen Knoten inzidente Kante gewählt haben, ist der von diesen Kanten induzierte Teilgraph ein Baum. Der eindeutige Weg von u_0 nach w_k beginnt und endet mit einer Kante aus $E \setminus M$, und hat dazwischen abwechselnd Kanten aus M und $E \setminus M$. Da weder u_0 noch w_k zu einer Matchingkante inzident sind, können wir die Zugehörigkeit der Kanten des (u_0, w_k) -Weges zu M und $E \setminus M$ vertauschen und erhalten ein Matching M' mit einer Kante mehr als M . Das ist ein Widerspruch zur Kardinalitätsmaximalität von M . \square

4.40 Bemerkung

Inklusionsmaximale Matchings können auch in bipartiten Graphen, welche die Bedingungen in Satz 4.39 nicht erfüllen, und sogar in Graphen, die nicht einmal bipartit sind, effizient bestimmt werden.

Die Einteilung der Knoten eines bipartiten Graphen in zwei Klassen kann wie folgt verallgemeinert werden.

4.41 Definition (Färbung)

Eine Abbildung $c : V \rightarrow C$ heißt (Knoten)färbung eines Graphen $G = (V, E)$, wenn für alle Kanten $\{v, w\} \in E$ gilt $c(v) \neq c(w)$. Eine Färbung heißt minimal, wenn $|C|$ minimal unter allen Färbungen von G ist. Für eine minimale Färbung f heißt $\chi(G) = |C|$ auch die chromatische Zahl des Graphen.

Offensichtlich ist $\chi(G) \leq 2$ für alle bipartiten Graphen G und $\chi(G) \leq 1$ nur für Graphen ohne Kanten. Doch schon die Klasse der Graphen, die mit 3 Farben gefärbt werden können, ist nicht leicht zu bestimmen.

4.42 Satz

Für Graphen G ist das Entscheidungsproblem $\chi(G) \leq 3$ \mathcal{NP} -vollständig.

Reduktion
von 3-SAT

Immerhin kann man leicht eine obere Schranke für die benötigte Anzahl von Farben angeben.

4.43 Satz

Zu einem Graphen $G = (V, E)$ existiert immer eine Färbung $c : V \rightarrow C$ mit $\chi(G) \leq |C| \leq \max_{v \in V} d_G(v) + 1$.

■ **Beweis:** Für $C = \{0, \dots, \max_{v \in V} d_G(v)\}$ geben wir eine Färbung $c : V \rightarrow C$ von G an. Dazu werden die Knoten zunächst in eine beliebige Reihenfolge v_1, \dots, v_n gebracht. Der erste Knoten wird mit $c(v_1) = 0$ gefärbt. Die anderen Knoten werden der Reihe nach mit jeweils der kleinsten erlaubten Farbe gefärbt, d.h. wir setzen

$$c(v_i) = \min (C \setminus (N_G(v_i) \cap \{v_1, \dots, v_{i-1}\})) .$$

Da kein Knoten mehr als $\max_{v \in V} d_G(v)$ Nachbarn hat, ist immer eine Farbe frei, und kein Knoten erhält eine schon an einen Nachbarn vergebene Farbe.

□

Literaturverzeichnis

- [1] Martin Aigner, *Diskrete Mathematik*. Vieweg, 1993.
- [2] Reinhard Diestel, *Graphentheorie*. Springer, 2000.
- [3] Rudolf Mathar und Dietmar Pfeifer, *Stochastik für Informatiker*. Teubner, 1990.
- [4] Angelika Steger, *Diskrete Strukturen I: Kombinatorik – Graphentheorie – Algebra*. Springer, 2001.
- [5] Thomas Schickinger und Angelika Steger: *Diskrete Strukturen II: Wahrscheinlichkeitstheorie und Statistik*. Springer, 2001.