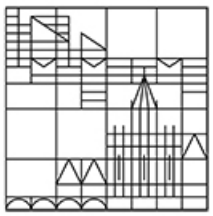
Fachbereich Informatik und
Informationswissenschaft

Universität
Konstanz



Skriptum

zur Vorlesung

Mathematik: Diskrete Strukturen

gehalten im Sommersemester 2015

von

Sven Kosub

13. Mai 2015

Version v4.6

Inhaltsverzeichnis

Kombinatorik 1

Der Schwerpunkt in diesem einführenden Kapitel über Kombinatorik liegt auf dem Abzählen endlicher Mengen.

1.1 Grundregeln des Abzählens

Lemma 1.1 *Es seien A und B endliche Mengen. Es gibt genau dann eine Bijektion $f : A \to B$, wenn $\|A\| = \|B\|$ gilt.*

Beweis: Siehe Satz 3.19 (aus dem Kapitel über Funktionen und Abbildungen im Skriptum *Mathematische Grundlagen der Informatik*). ■

Lemma 1.2 (Summenregel) *Es seien $A_1, \ldots, A_n$ endliche, paarweise disjunkte Mengen. Dann gilt:*

$$\|A_1 \cup \cdots \cup A_n\| = \sum_{j=1}^{n} \|A_j\|$$

Beweis: Wegen der paarweisen Disjunktheit der Mengen kommt jedes Element aus $A_1 \cup \cdots \cup A_n$ in genau einer Menge A_j vor. ■

Lemma 1.3 (Produktregel) *Es seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt:*

$$\|A_1 \times \cdots \times A_n\| = \prod_{j=1}^{n} \|A_j\|$$

Beweis: Wir beweisen die Aussage mittels Induktion über die Anzahl n der Mengen.

- *Induktionsanfang:* Für $n = 1$ ist die Aussage offensichtlich.
- *Induktionsschritt:* Es sei $n > 1$. Weiterhin seien $A_1, \ldots, A_n$ endliche Mengen. Wir setzen

$$\begin{aligned} A^* &=_{\text{def}} A_1 \times \cdots \times A_{n-1} \\ B_y &=_{\text{def}} \{\ (x_1, \ldots, x_{n-1}, y) \mid (x_1, \ldots, x_{n-1}) \in A^*\ \} \qquad \text{für } y \in A_n \end{aligned}$$

Für die so definierten Mengen gelten folgende Eigenschaften:

(i) Die Mengenfamilie $\{ B_y \mid y \in A_n \}$ ist eine Partition von $A_1 \times \cdots \times A_n$.

(ii) Für jedes $y \in A_n$ ist die Funktion

$$f_y : B_y \to A^* : (x_1, \ldots, x_{n-1}, y) \mapsto (x_1, \ldots, x_{n-1})$$

eine Bijektion, d.h. $\|B_y\| = \|A^*\|$ für alle $y \in A_n$ (nach Lemma 1.1).

Damit erhalten wir:

$$\begin{aligned}
\|A_1 \times \cdots \times A_n\| &= \left\| \bigcup_{y \in A_n} B_y \right\| && \text{(nach Eigenschaft (i))} \\
&= \sum_{y \in A_n} \|B_y\| && \text{(nach Lemma 1.2 und Eigenschaft (i))} \\
&= \sum_{y \in A_n} \|A^*\| && \text{(nach Lemma 1.1 und Eigenschaft (ii))} \\
&= \|A^*\| \cdot \|A_n\| \\
&= \left(\prod_{j=1}^{n-1} \|A_j\| \right) \cdot \|A_n\| && \text{(nach Induktionsvoraussetzung)} \\
&= \prod_{j=1}^{n} \|A_j\|
\end{aligned}$$

Damit ist das Lemma bewiesen. ■

Lemma 1.4 (Potenzregel) *Es seien A und B endliche Mengen mit $\|A\| = m$ und $\|B\| = n$. Dann existieren genau n^m Funktionen $f : A \to B$.*

Beweis: Nach Lemma 1.1 dürfen wir $A = \{1, \ldots, m\}$ ohne Beeinträchtigung der Allgemeinheit annehmen. Jeder Funktion $f : A \to B$ kann nun eineindeutig (injektiv) ein Tupel $(f(1), \ldots, f(m)) \in B^m$ zugeordnet werden. Außerdem entspricht jedes Tupel (die Wertetabelle) $(y_1, \ldots, y_m) \in B^m$ einer Funktion $f : A \to B : j \mapsto y_j$. Damit ist die Zuordnung sowohl injektiv als auch surjektiv, also eine Bijektion. Aus Lemma 1.1 und Produktregel (Lemma 1.3) folgt somit

$$\|\{ f \mid f : A \to B \}\| = \|B^m\| = \|B\|^m = n^m.$$

Damit ist das Lemma bewiesen. ■

Beispiel: Wie viele boolesche Funktionen mit n Variablen gibt es? Die Antwort lautet $\|\{ f \mid f : \{0,1\}^n \to \{0,1\} \}\| = 2^{2^n}$.

Korollar 1.5 *Für endliche Mengen A mit $\|A\| = n$ gilt $\|\mathcal{P}(A)\| = 2^n$.*

Beweis: Wir konstruieren eine Bijektion zwischen $\mathcal{P}(A)$ und der Menge der Funktionen $f : A \to \{0,1\}$. Dazu definieren wir für eine Menge $B \in \mathcal{P}(A)$ die Funktion:

$$c_B : A \to \{0,1\} : x \mapsto \begin{cases} 1 & \text{falls } x \in B \\ 0 & \text{falls } x \notin B \end{cases}$$

Diese Zuordnung ist offensichtlich eine Bijektion zwischen $\mathcal{P}(A)$ und der Menge der Funktionen $f : A \to \{0,1\}$. Nach der Potenzregel (Lemma 1.4) und Lemma 1.1 gilt folglich

$$\|\mathcal{P}(A)\| = \|\{\ f \mid f : A \to \{0,1\}\ \}\| = 2^n.$$

Damit ist das Korollar bewiesen. ■

Die im Beweis von Korollar 1.5 angegebenen Funktionen haben einen Namen: Für eine Menge $B \subseteq A$ heißt c_B die *charakteristische Funktion* von B.

1.2 Einfache Urnenmodelle

Urnenmodelle stellen ein typisches Szenario für kombinatorische Problemstellungen dar. Die einfachste Situation ist die folgende: In einer Urne liegen n unterscheidbare Kugeln, von den k Kugel gezogen werden dürfen. Die zu beantwortende Frage ist dann: Wie viele Möglichkeiten gibt es diese k Kugeln zu ziehen? Zur Präzisierung des Szenarios werden Unterschiede danach gemacht, ob

- die Reihenfolge, in der die Kugeln gezogen werden, eine Rolle spielt,
- gezogene Kugeln wieder zurückgelegt werden oder nicht.

Damit ergeben sich vier verschiedene Szenarios.

Theorem 1.6 *Die Anzahl der Möglichkeiten, aus einer Urne mit n Kugeln k Kugeln auszuwählen, ist durch folgende Tabelle gegeben:*

	mit Zurücklegen	*ohne Zurücklegen*
mit Reihenfolge	n^k	$n^{\underline{k}} =_{\text{def}} \dfrac{n!}{(n-k)!}$
ohne Reihenfolge	$\binom{n+k-1}{k}$	$\binom{n}{k} =_{\text{def}} \dfrac{n!}{k!(n-k)!}$

Die im Theorem mitdefinierten Größen $n^{\underline{k}}$ und $\binom{n}{k}$ heißen *fallende Faktorielle von n der Länge k* sowie *Binomialkoeffizient* („n über k“).

Beispiel: Wir geben für jedes der vier Szenarien Beispiele an:

	mit Zurücklegen	ohne Zurücklegen
mit Reihenfolge (geordnet)	PIN-Codes: • $n = 10$ Ziffern • $k = 4$ Stellen • 10.000 Codes	Wettkämpfe: • $n = 10$ Starter • $k = 3$ Medaillen • 720 Siegerehrungen
ohne Reihenfolge (ungeordnet)	Wahlen: • $n = 3$ Kandidaten • $k = 100$ Wähler • 5.151 Wahlausgänge	Lotto: • $n = 49$ Kugeln • $k = 6$ Kugeln • 13.983.816 Ziehungen

Beweis: Wir beweisen alle Fälle einzeln, aber aufeinander aufbauend:

- *Ziehen mit Zurücklegen, mit Reihenfolge:* Jede Auswahlmöglichkeit entspricht einer Funktion $f : \{1, \dots, k\} \to \{1, \dots, n\}$, wobei $f(i)$ genau der Kugel entspricht, die als i-te Kugel gezogen wurde. Nach der Potenzregel (Lemma 1.4) gibt es somit n^k Möglichkeiten.

- *Ziehen ohne Zurücklegen, mit Reihenfolge:* Für die erste gezogene Kugel gibt es n Möglichkeiten, für die zweite gezogene Kugel gibt es $n - 1$ Möglichkeiten. Für die k-te gezogene Kugel ($k \leq n$) gibt es mithin noch $n - k + 1$ Möglichkeiten. Insgesamt gibt es damit
$$n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!} = n^{\underline{k}}$$
Möglichkeiten.

- *Ziehen ohne Zurücklegen, ohne Reihenfolge:* Mit Berücksichtigung der Reihenfolge gibt es $\frac{n!}{(n-k)!}$ Auswahlmöglichkeiten. Wenn die Reihenfolge keine Rolle mehr spielt, zählen alle Auswahlfolgen, bei denen die gleichen k Kugeln gezogen wurden, nur noch als eine Auswahlmöglichkeit. Dies sind gerade $k!$ viele. Damit gibt es insgesamt
$$\frac{n!}{(n-k)!} \cdot \frac{1}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$
Möglichkeiten.

- *Ziehen mit Zurücklegen, ohne Reihenfolge:* Da jede Kugel mehrmals gezogen werden kann, die Reihenfolge jedoch keine Rolle spielt, ist nur wichtig, wie oft eine Kugel gezogen wird. Es sei also $(a_1, \dots, a_n)$ ein Tupel mit den entsprechenden Anzahlen, wobei a_j gerade angibt, wie oft die Kugel j gezogen wird. Für ein Anzahltupel $(a_1, \dots, a_n)$ muss nun gelten:

  (i) $a_j \in \{0, \dots, k\}$ für alle $j \in \{1, \dots, n\}$

(ii) $a_1 + \cdots + a_n = k$

Wir müssen nun zählen, wie viele derartige Tupel es geben kann. Dazu repäsentieren wir die Tupel in einer anderen Weise, die es uns ermöglicht, das Szenario zu wechseln. Wir verwenden k-mal das Symbol $*$ und $(n-1)$-mal das Symbol $|$. Ein Anzahltupel $(a_1, \ldots, a_n)$ wird nun (injektiv) durch die Symbolfolge

$$\underbrace{*\,*\,\ldots\,*}_{a_1}|\underbrace{*\,*\,\ldots\,*}_{a_2}|\ldots|\underbrace{*\,*\,\ldots\,*}_{a_n}$$

repräsentiert. Umgekehrt entspricht auch jede Symbolfolge, die k-mal das Symbol $*$ und $(n-1)$-mal das Symbol $|$ enthält, einem Anzahltupel mit obigen Eigenschaften. Demzufolge ist die Repräsentierung eine Bijektion zwischen der Menge der Anzahltupel und der Menge der Symbolfolgen. Die Anzahl möglicher Symbolfolgen zu bestimmen, entspricht aber gerade dem Ziehen von k Positionen für das Symbol $*$ aus $n+k-1$ möglichen Positionen ohne Zurücklegen und ohne Reihenfolge. Mithin gibt es insgesamt

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

Möglichkeiten.

Damit ist das Theorem bewiesen. ■

1.3 Binomialkoeffizienten

Aus dem letzten Abschnitt (Theorem 1.6) wissen wir, dass die Anzahl der Möglichkeiten aus n Kugeln k Kugeln ungeordnet ohne Zurücklegen zu ziehen gerade dem Binomialkoeffizienten $\binom{n}{k}$ entspricht. Da Binomialkoeffizienten auch über die reine Kombinatorik hinaus wichtig sind, wollen in diesem Abschnitt die wichtigsten Eigenschaften von Binomialkoeffizienten festhalten. Dazu definieren wir den Binomialkoeffzienten noch einmal explizit: Für $n, k \in \mathbb{N}$ definieren wir

$$\binom{n}{k} =_{\text{def}} \frac{n!}{k!(n-k)!}, \qquad \text{mit } \binom{n}{k} = 0 \qquad \text{für } k > n\ .$$

Ein einfache, sofort einsichtige Beobachtung ist:

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

Damit lässt sich der Binomialkoeffizient konsistent auch für negative Werte für k definieren:

$$\binom{n}{k} =_{\text{def}} 0 \qquad \text{für } k \in \mathbb{Z} \setminus \mathbb{N}\ .$$

Theorem 1.7 (PASCALsches Dreieck) *Für $n \in \mathbb{N}_+$ und $k \in \mathbb{N}$ gilt*

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

Wir geben zwei Beweise für das Theorem an.

Beweis: (*rechnerisch*) Wir führen eine Fallunterscheidung bezüglich der Werte von k durch:

- Für $k = 0$ und $n > 1$ gilt $\binom{n}{0} = 1 = \binom{n-1}{-1} + \binom{n-1}{0}$.
- Für $0 < k < n$ rechnen wir aus:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k)!} \cdot \frac{k}{k} + \frac{(n-1)!}{k!(n-1-k)!} \cdot \frac{n-k}{n-k} \\
&= \frac{(n-1)! \cdot k}{k!(n-k)!} + \frac{(n-1)!(n-k)}{k!(n-k)!} \\
&= \frac{(n-1)!(k+n-k)}{k!(n-k)!} \\
&= \frac{(n-1)! \cdot n}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

- Für $k = n$ und $n > 1$ gilt $\binom{n}{n} = 1 = \binom{n-1}{n-1} + \binom{n-1}{n}$.
- Für $k > n > 1$ gilt $\binom{n}{k} = 0 = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Damit ist das Theorem durch Nachrechnen bewiesen. ∎

Beweis: (*kombinatorisch*) Wir interpretieren die Gleichung als Bestimmung der Kardinalität von Mengen auf zwei verschiedene Weisen. Es seien $n \in \mathbb{N}_+$ und $k \in \mathbb{N}$. Wir definieren folgende Mengenfamilien:

$$\begin{aligned}
\mathcal{F} &=_{\text{def}} \{\, \{a_1, \ldots, a_k\} \mid a_i \in \{1, \ldots, n\} \text{ und } a_i \neq a_j \text{ für } i \neq j \,\} \\
\mathcal{F}_+ &=_{\text{def}} \{\, A \mid A \in \mathcal{F} \text{ und } 1 \in A \,\} \\
\mathcal{F}_- &=_{\text{def}} \{\, A \mid A \in \mathcal{F} \text{ und } 1 \notin A \,\}
\end{aligned}$$

Die einzelnen Mengenfamilien stehen für folgende Urnenmodelle:

- $\mathcal{F}$ entspricht dem ungeordneten Ziehen von k Kugeln aus n Kugeln ohne Zurücklegen.
- $\mathcal{F}_+$ entspricht dem ungeordneten Ziehen von k Kugeln aus n Kugeln ohne Zurücklegen, wobei Kugel 1 *immer* gezogen wird.
- $\mathcal{F}_-$ entspricht dem ungeordneten Ziehen von k Kugeln aus n Kugeln ohne Zurücklegen, wobei Kugel 1 *nie* gezogen wird.

Nun gilt offensichtlich $\mathcal{F} = \mathcal{F}_+ \cup \mathcal{F}_-$ sowie $\mathcal{F}_+ \cap \mathcal{F}_- = \emptyset$, also $\|\mathcal{F}\| = \|\mathcal{F}_+\| + \|\mathcal{F}_-\|$ nach der Summenregel (Lemma 1.2). Nach Theorem 1.6 gilt:

$$\|\mathcal{F}\| = \binom{n}{k}, \qquad \|\mathcal{F}_+\| = \binom{n-1}{k-1}, \qquad \|\mathcal{F}_-\| = \binom{n-1}{k}$$

Mithin erhalten wir:

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

Damit ist das Theorem kombinatorisch bewiesen. ■

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 1.7 lässt sich leicht veranschaulichen und ist schon aus der Schule bekannt:

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}
\qquad
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Theorem 1.8 (Binomialtheorem) *Für alle $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$ gilt*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Das Binomialtheorem kann durch vollständige Induktion über n bewiesen werden. Dies ist eine gute Übung zu Anwendung des PASCALschen Dreiecks. Wir geben einen anderen Beweis.

Beweis: (*kombinatorisch*) Es seien $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$ beliebig. Durch Ausmultiplizieren von $(x+y)^n$ erhalten wir:

$$\begin{aligned}(x+y)^n \quad = \quad & \overbrace{x \cdot \ \cdots \ \cdot x \cdot x}^{n \text{ Faktoren}} + \\ & + x \cdot \ \cdots \ \cdot x \cdot y + \\ & + x \cdot \ \cdots \ \cdot y \cdot x + \\ & + x \cdot \ \cdots \ \cdot y \cdot y + \\ & \vdots \\ & + \underbrace{y \cdot \ \cdots \ \cdot y \cdot y}_{n \text{ Faktoren}}\end{aligned}$$

Die Summanden können zusammengefasst werden zu Produkten von jeweils n Faktoren, von denen k Faktoren gerade y und $n-k$ Faktoren gerade x sind. Die Summanden sind also von der Form $x^{n-k}y^k$, da die Reihenfolge bei der Multiplikation keine Rolle spielt. Die Anzahl der Produkte $x^{n-k}y^k$ entspricht somit gerade dem Ziehen von k Kugeln (die Positionen für y im Produkt) aus n Kugeln (die Gesamtheit aller Positionen für Faktoren), d.h. $\binom{n}{k}$. Folglich gilt insgesamt:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Damit ist das Theorem bewiesen. ∎

Korollar 1.9 *Für alle $n \in \mathbb{N}_+$ gilt*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Beweis: Nach dem Binomialtheorem gilt

$$0 = (1-1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

Damit ist das Korollar bewiesen. ∎

Korollar 1.10 *Für alle $n \in \mathbb{N}$ gilt*

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

Beweis: Nach dem Binomialtheorem gilt

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

Damit ist das Korollar bewiesen. ■

Theorem 1.11 (VANDERMONDEsche Identität) *Für $k, m, n \in \mathbb{N}$ gilt*

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

Beweis: (*kombinatorisch*) Es seien A und B disjunkte Mengen mit $\|A\| = n$ und $\|B\| = m$. Für jedes $j \in \{0, \ldots, k\}$ definieren wir die Mengenfamilie

$$\mathcal{X}_j =_{\text{def}} \{\ X \mid X \subseteq A \cup B, \|X \cap A\| = j \text{ und } \|X \cap B\| = k - j\ \}$$

Es gibt $\binom{n}{j}$ viele j-elementige Teilmengen von A und $\binom{m}{k-j}$ viele $(k-j)$-elementige Teilmengen von B. Damit gilt

$$\|\mathcal{X}_j\| = \binom{n}{j} \binom{m}{k-j}.$$

Wegen $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ für $i \neq j$ folgt nun

$$\binom{n+m}{k} = \sum_{j=0}^{k} \|\mathcal{X}_j\| = \sum_{j=0}^{k} \binom{n}{j} \binom{m}{k-j}.$$

Damit ist das Theorem bewiesen. ■

Beispiel: Die Beweistechnik für Theorem 1.11 heißt *Doppeltes Abzählen*. Wenn zum Beispiel in einer Vorlesung $n + m$ Studenten sitzen, n weibliche und m männliche, wie viele verschiedene Gruppen mit genau k Studenten gibt es dann? Dies lässt sich auf zwei Arten bestimmen:

- Ohne Berücksichtigung des Geschlechts erhalten wir $\binom{n+m}{k}$ Gruppen.
- Mit Berücksichtigung des Geschlechts zählen wir für jedes $j \in \{0, 1, \ldots, k\}$ alle Gruppen mit jeweils genau j weiblichen und genau $k - j$ männlichen Studenten, damit also insgesamt $\sum_{j=0}^{k} \binom{n}{j}\binom{m}{k-j}$ Gruppen.

Da wir über dieselbe Menge von Studenten argumentieren, sind beide Anzahlen gleich.

1.4 Permutationen

Es sei A eine endliche Menge mit $\|A\| = n$. Eine *Permutation* von A ist eine bijektive Funktion $\pi : A \to A$. Ohne Beeinträchtigung der Allgemeinheit setzen wir stets $A = \{1, \ldots, n\}$ voraus. Die Menge $\{1, \ldots, n\}$ notieren wir auch als $[n]$. Weiterhin definieren wir die Menge

$$\mathcal{S}_n =_{\text{def}} \{\ \pi \mid \pi : [n] \to [n] \text{ ist eine Permutation }\},$$

die sogenannte *symmetrische Gruppe* von n Elementen.

Theorem 1.12 *Für alle $n \in \mathbb{N}_+$ gilt $\|\mathcal{S}_n\| = n!$.*

Beweis: $\|\mathcal{S}_n\|$ entspricht dem Ziehen von n Kugeln aus einer Urne mit n Kugeln ohne Zurücklegen mit Berücksichtigung der Reihenfolge. Nach Theorem 1.6 gilt

$$\|\mathcal{S}_n\| = \frac{n!}{(n-n)!} = n!.$$

Damit ist das Theorem bewiesen. ■

Ohne Beweis geben wir folgendes Resultat über das Verhalten der Fakultätsfunktion an:

Theorem 1.13 (STIRLING**sche Formel)** *Für alle $n \in \mathbb{N}_+$ gilt*

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}},$$

wobei $e = e^1 = 2,718281828459\ldots$ die EULERsche Konstante *ist.*

Permutationen können auf verschiedene Arten geschrieben werden. Im Folgenden behandeln wir drei Schreibweisen:

Matrixschreibweise: Dazu schreiben wir die Permutation $\pi : [n] \to [n]$ als $2 \times n$-Matrix der Form

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

Da π bijektiv ist, kommen alle Werte $1, \ldots, n$ in der zweiten Zeile vor.

Beispiel: Folgende Permutation ist in Matrixschreibweise gegeben:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$$

Tupelschreibweise: Im Prinzip genügt es, von der Matrixschreibweise lediglich die zweite Zeile zu übernehmen, d.h. Permutationen können angegeben werden in der Form

$$\pi = (\pi(1), \pi(2), \pi(3), \ldots, \pi(n)).$$

Beispiel: $\pi = (4, 1, 6, 2, 5, 3)$ ist obige Permutation in Tupelschreibweise.

Zyklenschreibweise: Die Zyklenschreibweise entsteht, wenn wir für $x \in [n]$ die iterierte Hintereinanderausführung von π auf x betrachten. Dadurch entsteht eine Folge:

$$\begin{aligned}
\pi^0(x) &=_{\text{def}} x,\\
\pi^1(x) &=_{\text{def}} \pi(x),\\
\pi^2(x) &=_{\text{def}} \pi(\pi(x)),\\
&\vdots\\
\pi^k(x) &=_{\text{def}} \pi(\pi^{k-1}(x)),\\
&\vdots
\end{aligned}$$

Für jedes $x \in [n]$ gibt es dann ein minimales $0 < k < n$ mit $\pi^k(x) = x$.

Beispiel: Für die Permutation $\pi = (4, 1, 6, 2, 5, 3)$ gilt

$$\begin{array}{llll}
\pi^0(1) = 1, & \pi^1(1) = 4, & \pi^2(1) = 2, & \pi^3(1) = 1;\\
\pi^0(2) = 2, & \pi^1(2) = 1, & \pi^2(2) = 4, & \pi^3(2) = 2;\\
\pi^0(3) = 3, & \pi^1(3) = 6, & \pi^2(3) = 3; & \\
\pi^0(4) = 4, & \pi^1(4) = 2, & \pi^2(4) = 1, & \pi^3(4) = 4;\\
\pi^0(5) = 5, & \pi^1(5) = 5; & & \\
\pi^0(6) = 6, & \pi^1(6) = 3, & \pi^2(6) = 6. &
\end{array}$$

Eine Folge $x, \pi(x), \pi^2(x), \ldots, \pi^{k-1}(x)$ mit minimalem $k > 0$, so dass $\pi^k(x) = x$, heißt *Zyklus* der Länge k und wird als $(x\ \pi(x)\ \pi^2(x)\ \ldots\ \pi^{k-1}(x))$ geschrieben.

Beispiel: $\pi = (4, 1, 6, 2, 5, 3)$ enthält die Zyklen (1 4 2), (3 6) und (5).

Jede Permutation kann als *Produkt von Zyklen* geschrieben werden, indem die Zyklen einfach hintereinander gesetzt werden. Die Schreibweise ist jedoch nicht eindeutig. Insbesondere kann jeder Zyklus der Länge k auf genau k Arten geschrieben werden.

Beispiel: Die Permutation $\pi = (4, 1, 6, 2, 5, 3)$ können wir als Produkt von Zyklen wie folgt schreiben:

$$(4, 1, 6, 2, 5, 3) \quad = \quad (1\ 4\ 2)(3\ 6)(5)$$

$$\begin{aligned} &= (4\ 2\ 1)(6\ 3)(5) \\ &= (5)(2\ 1\ 4)(6\ 3) \end{aligned}$$

Insbesondere gilt $(1\ 4\ 2) = (4\ 2\ 1) = (2\ 1\ 4)$.

Die Anzahl der Zyklen, aus der eine Permutation bestehen kann, liegt zwischen 1, wie in $(1\ 2\ 3\ \ldots\ n)$, und n, wie in $(1)(2)(3)\ldots(n)$. Im Folgende wollen wir die Anzahl der Permutationen mit genau k Zyklen genauer bestimmen.

Für $n, k \in \mathbb{N}$ sei $s_{n,k}$ (manchmal auch $\left[{n \atop k}\right]$ geschrieben) die Anzahl der Permutationen von n Elementen mit genau k Zyklen. Dann gilt also

$$\sum_{k=1}^{n} s_{n,k} = n!.$$

Die Zahlen $s_{n,k}$ heißen STIRLING-*Zahlen erster Art.* Folgende Sonderfälle sind zu beachten:

- Für $k > n$ gilt $s_{n,k} = 0$, da eine Permutation von n Elementen höchstens n Zyklen enthalten kann.
- Für $n > 0$ gilt $s_{n,0} = 0$, da jede Permutation mindestens einen Zyklus enthält.
- Wir definieren $s_{0,0} =_{\text{def}} 1$.

Mit diesen Sonderfällen können wir wiederum eine Rekursionsvorschrift für die Berechnung der STIRLING-Zahlen erster Art angeben.

Theorem 1.14 (STIRLING-Dreieck erster Art) *Für alle $k, n \in \mathbb{N}$ mit $n \geq k$ gilt*

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

Beweis: (*kombinatorisch*) Es sei $\pi \in \mathcal{S}_n$ eine Permutation mit k Zyklen. Dann kann π auf zwei Arten aus einer Permutation aus $\mathcal{S}_{n-1}$ entstanden sein:

(i) Einfügen eines Zyklus (n) in Permutationen aus $\mathcal{S}_{n-1}$ mit $k-1$ Zyklen

(ii) Einfügen des Elementes n in einen der Zyklen einer Permutation aus $\mathcal{S}_{n-1}$ mit k Zyklen

Beide Fälle sind disjunkt. Für die Anzahl der Möglichkeiten, Permutationen mit k Zyklen auf diese zwei Arten zu erzeugen, ergibt sich jeweils:

(i) $s_{n-1,k-1}$

(ii) $(n-1) \cdot s_{n-1,k}$ (denn für das Einfügen eines Elementes in einen Zyklus der Länge t gibt es t Möglichkeiten–Einfügen als erstes und Einfügen als letztes Element erzeugen den gleichen Zyklus)

Insgesamt gilt also $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$. Damit ist das Theorem bewiesen. ■

Beispiel: Um die Konstruktion aus dem Beweis von Theorem 1.14 zu verdeutlichen, betrachten wir die 6 Permutationen von 4 Elementen mit 3 Zyklen:

(1)(2 3)(**4**)	(1 **4**)(2)(3)
(1 2)(3)(**4**)	(1)(2 **4**)(3)
(1 3)(2)(**4**)	(1)(2)(3 **4**)

Die linken Permutationen entstehen aus den Permutationen (1)(2 3), (1 2)(3) und (1 3)(2) durch Einfügen des Einerzyklus (4). Die rechten Permutationen entstehen aus der Permutation (1)(2)(3) durch Einfügen von 4 in jeden Einerzyklus.

Um einen Eindruck von Wachstum der STIRLING-Zahlen erster Art zu erhalten, können die Werte analog dem PASCALschen Dreieck angeordnet werden.

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 1.14 lässt sich wie folgt veranschaulichen:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 0 & & 1 & & & & \\
 & & & 0 & & 1 & & 1 & & & \\
 & & 0 & & 2 & & 3 & & 1 & & \\
 & 0 & & 6 & & 11 & & 6 & & 1 & \\
0 & & 24 & & 50 & & 35 & & 10 & & 1 \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

Mit Permutationen, insbesondere mit der symmetrischen Gruppe, werden wir uns im Kapitel über algebraische Strukturen noch einmal ausführlich beschäftigen.

1.5 Mengenpartitionen

In diesem Abschnitt wollen wir bestimmen, wie viele Möglichkeiten es gibt n-elementige Grundmengen in k nichtleere, disjunkte Komponenten zu zerlegen.

Es sei A eine endliche Menge mit $\|A\| = n$. Eine *k-Partition* $\mathcal{F} = \{A_1, A_2, \ldots, A_k\}$ ist eine k-elementige Familie von nichtleeren Teilmengen von A mit $A_1 \cup A_2 \cdots \cup A_k = A$ und $A_i \cap A_j = \emptyset$, falls $i \neq j$.

Es sei $S_{n,k}$ (manchmal auch: $\left\{ {n \atop k} \right\}$) die Anzahl der k-Partitionen einer n-elementigen Grundmenge. Die Zahlen $S_{n,k}$ heißen *Stirling-Zahlen zweiter Art*. Folgende Spezialfälle sind zu beachten:

- Für $k > n$ gilt $S_{n,k} = 0$, da die n Elemente höchstens in n Komponenten liegen können.
- Für $k = 0$ gilt $S_{n,0} = 0$, da die n Elemente in wenigstens einer Komponenten liegen müssen.
- Wir definieren $S_{0,0} =_{\text{def}} 1$.

Wir können nun eine ähnliche rekursive Darstellung wie in Theorem 1.14 für die Stirling-zahlen erster Art auch für die Stirling-Zahlen zweiter Art beweisen.

Theorem 1.15 (Stirling-Dreieck zweiter Art) *Für alle $k, n \in \mathbb{N}$ mit $n \geq k$ gilt*

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

Beweis: (*kombinatorisch*) Es sei $\mathcal{F}$ eine k-Partition einer n-elementigen Menge. Dann kann $\mathcal{F}$ auf zwei Arten aus einer Partition einer $(n-1)$-elementigen Menge entstehen:

(i) Hinzufügen der Menge $\{n\}$ zu einer $(k-1)$-Partition von $n-1$ Elementen

(ii) Einfügen von n in einer der Mengen einer k-Partition von $n-1$ Elementen

Die Anzahl der Möglichkeiten k-Partitionen von n Elementen zu bilden, ist wie folgt:

(i) $S_{n-1,k-1}$

(ii) $k \cdot S_{n-1,k}$

Mithin gilt also $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$. Damit ist das Theorem bewiesen. ■

Wir geben wieder einen Eindruck für das Wachstum der Zahlen $S_{n,k}$ gemäß Theorem 1.15.

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 1.15 lässt sich wie folgt veranschaulichen:

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 0 & & 1 & & & & & \\
 & & & & 0 & & 1 & & 1 & & & & \\
 & & & 0 & & 1 & & 3 & & 1 & & & \\
 & & 0 & & 1 & & 7 & & 6 & & 1 & & \\
 & 0 & & 1 & & 15 & & 25 & & 10 & & 1 & \\
0 & & 1 & & 31 & & 90 & & 65 & & 15 & & 1 \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

Interessieren wir uns nur für die Anzahl aller möglichen Partitionen einer Grundmenge A mit $\|A\| = n$, so kann man die *Bell-Zahlen* bestimmen:

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

Insbesondere gibt B_n also die Anzahl aller Äquivalenzrelationen auf n Elementen an.

1.6 Zahlpartitionen

In diesem Abschnitt gehen wir der Frage nach, wie viele Möglichkeiten es gibt, einen Zahl als Summe anderer Zahlen darzustellen.

Eine *Zahlpartition* von $n \in \mathbb{N}$ mit k Summanden besteht aus ganzen Zahlen $n_1, \ldots, n_k > 0$ mit $n = n_1 + \cdots + n_k$. Spielt die Reihenfolge der Summanden keine Rolle, dann heißt die Zahlpartition *ungeordnet*, sonst *geordnet*.

Beispiel: $7 = 1 + 1 + 2 + 3$ ergibt eine Zahlpartition von 7 mit 4 Summanden. Ungeordnet repräsentieren $1, 1, 2, 3$ und $3, 2, 1, 1$ die gleiche, georndet unterschiedliche Zahlpartitionen.

Die Frage ist also: Wie viele Zahlpartitionen von n mit k Summanden gibt es?

Ungeordnete Zahlpartitionen: Es sei $P_{n,k}$ die Anzahl der Möglichkeiten die Zahl n ungeordnet in k Summanden zu zerlegen. Klarerweise gilt $P_{n,n} = 1$ sowie $P_{n,1} = 1$ für $n \geq 1$. Außerdem sind folgende Spezialfälle zu beachten:

- Für $k > n$ gilt $P_{n,k} = 0$.
- Für $n \geq 1$ gilt $P_{n,0} = 0$.
- Wir definieren $P_{0,0} =_{\text{def}} 1$.

Folgendes Theorem gibt eine rekursive Vorschrift zur Berechnung von $P_{n,k}$ an.

Theorem 1.16 *Für $n, k \in \mathbb{N}_+$ mit $n \geq k$ gilt*

$$P_{n+k,k} = \sum_{j=1}^{k} P_{n,j}.$$

Beweis: (*kombinatorisch*) Wir unterscheiden die Summanden bei der Zerlegung von $n+k$ in k Summanden nach Einsen und größeren Summanden. Für eine Partition mit genau i Einsen gilt

$$n + k = \underbrace{1 + 1 + \cdots + 1}_{i} + \underbrace{n_{i+1} + n_{i+2} + \cdots + n_k}_{k-i}$$

mit $n_{i+1}, \ldots, n_k \geq 2$. Wir definieren $n'_j =_{\text{def}} n_j - 1$ für $j \in \{1, \ldots, k\}$. Dann gilt

$$\begin{aligned} n'_{i+1} + n'_{i+2} + \cdots + n'_k &= n_{i+1} + n_{i+2} + \cdots + n_k - (k - i) \\ &= n + (k - i) - (k - i) \\ &= n \end{aligned}$$

Mithin ist $n'_{i+1}, \ldots, n'_k$ eine Zahlpartition von n mit $k - i$ Summanden. Umgekehrt kann jede Zahlpartition von n mit $k - i$ Summanden in eine Zahlpartition von $n + k$ mit k Summanden, von denen genau i den Wert 1 haben, umgewandelt werden. Insgesamt gilt also

$$P_{n+k,k} = \sum_{i=0}^{k-1} P_{n,k-i} = \sum_{j=1}^{k} P_{n,j}.$$

Damit ist das Theorem bewiesen. ∎

Beispiel: Es gilt $P_{5,3} = 2$. Einserseits sind die Zahlpartitionen $1 + 1 + 3 = 5$ sowie $1+2+2 = 5$. Andererseits ergibt sich mit der Formel aus obigem Theorem

$$P_{5,3} = \sum_{j=1}^{3} P_{2,j} = P_{2,1} + P_{2,2} + P_{2,3} = 1 + 1 + 0 = 2.$$

Geordnete Zahlpartitionen: Die Anzahl der Möglichkeiten, die Zahl n geordnet in k Summanden zu verteilen, kann auf bereits bekannte Größen zurückgeführt werden.

Theorem 1.17 *Für alle $n, k \in \mathbb{N}_+$ mit $n \geq k$ gibt es*

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

geordnete Zahlpartitionen von n mit k Summanden.

Beweis: Jede Zahl $n \geq 2$ kann mit n Einsen dargestellt werden:

$$n = \overbrace{\underbrace{1+\cdots+1}_{x_1}+\underbrace{1+\cdots+1}_{x_2}+\cdots+\underbrace{1+\ldots+1}_{x_k}}^{n}$$

Somit kann jede geordnete Zahlpartition von n mit k Summanden umkehrbar eindeutig durch die Positionen der Pluszeichen zwischen Einserblöcken repräsentiert werden. Folglich werden aus $n-1$ möglichen Positionen genau $k-1$ ausgewählt. Insgesamt ergeben sich

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

Möglichkeiten. Damit ist das Theorem bewiesen. ■

Beispiel: Wie viele Lösungen besitzt die lineare Gleichung

$$x_1 + x_2 + \cdots + x_k = n$$

in den natürlichen Zahlen? Die Null ist hier also als Summand zugelassen. Wegen

$$x_1 + x_2 + \cdots + x_k = n \iff (x_1+1) + (x_2+1) + \cdots + (x_k+1) = n + k$$

gibt es genau $\binom{n+k-1}{k-1}$ Lösungen.

1.7 Mehrfache Urnenmodelle

Im Folgenden betrachten wir ein verallgemeinertes kombinatorisches Szenario, in dem viele der bisher angestellten Überlegungen zur Anwendung kommen: Wie viele Möglichkeiten gibt es, n Bälle auf m Urnen zu verteilen?

Hierbei sind wieder verschiedene Szenarien möglich, je nachdem

- ob die Bälle unterscheidbar oder nicht unterscheidbar sind,

- ob die Urnen unterscheidbar oder nicht unterscheidbar sind und
- ob die Urnen jeweils mindestens, genau oder höchstens einen Ball enthalten müssen.

Theorem 1.18 fasst für alle möglichen Szenarien die Anzahlen zusammen.

Theorem 1.18 *Die Anzahl der Möglichkeiten, n Bälle auf m Urnen zu verteilen, ist durch folgende Tabelle angegeben:*

$\|B\| = n$, $\|U\| = m$	*Zuordnung beliebig*	*Zuordnung injektiv*	*Zuordnung surjektiv*	*Zuordnung bijektiv*
B untersch., U untersch.	m^n	$\begin{cases} m^{\underline{n}} & m \geq n \\ 0 & m < n \end{cases}$	$m! \cdot S_{n,m}$	$\begin{cases} n! & m = n \\ 0 & m \neq n \end{cases}$
B nicht untersch., U untersch.	$\binom{m+n-1}{n}$	$\binom{m}{n}$	$\binom{n-1}{m-1}$	$\begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$
B untersch., U nicht untersch.	$\sum_{k=1}^{m} S_{n,k}$	$\begin{cases} 1 & m \geq n \\ 0 & m < n \end{cases}$	$S_{n,m}$	$\begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$
B nicht untersch., U nicht untersch.	$\sum_{k=1}^{m} P_{n,k}$	$\begin{cases} 1 & m \geq n \\ 0 & m < n \end{cases}$	$P_{n,m}$	$\begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$

Beweis: Der Beweis des Theorems bleibt als Übungsaufgabe überlassen. ■

1.8 Weitere Abzählprinzipien

Im letzten Abschnitt diese Kapitels über Kombinatorik diskutieren wir noch zwei weitere Abzählprinzipien.

Inklusion-Exklusion. Zunächst wollen wir eine Verallgemeinerung der Summenregel (siehe Lemma 1.2) auf beliebige, nicht notwendig paarweise disjunkte Mengen angeben.

Theorem 1.19 (Inklusions-Exkusions-Prinzip) *Es seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt:*

$$\left\| \bigcup_{j=1}^{n} A_j \right\| = \sum_{\emptyset \neq K \subseteq \{1,\ldots,n\}} (-1)^{1+\|K\|} \left\| \bigcap_{k \in K} A_k \right\|$$

Beispiel:

- Für $n = 2$ reduzieren sich die Ausdrücke in Theorem 1.19 zu folgender Identität:

$$\|A_1 \cup A_2\| \;=\; \|A_1\| + \|A_2\| - \|A_1 \cap A_2\|$$

- Für $n = 3$ reduzieren sich die Ausdrücke in Theorem 1.19 zu folgender Identität:

$$\begin{aligned}\|A_1 \cup A_2 \cup A_3\| &= \|A_1\| + \|A_2\| + \|A_3\| \\ &\quad - \|A_1 \cap A_2\| - \|A_1 \cap A_3\| - \|A_2 \cap A_3\| \\ &\quad + \|A_1 \cap A_2 \cap A_3\|\end{aligned}$$

Beweis: Wir bestimmen, wie oft jedes Element auf beiden Seiten der Gleichung gezählt wird. Es sei $x \in \bigcup_{j=1}^{n} A_j$.

- *Linke Seite:* Das Element x wird genau einmal gezählt.
- *Rechte Seite:* Wir müssen zeigen, dass x auch hier genau einmal gezählt wird. Dazu sei $\ell =_{\text{def}} \|\{\, j \mid x \in A_j \,\}\|$. Ohne Beeinträchtigung der Allgemeinheit komme x genau in den Mengen $A_1, \ldots, A_\ell$ vor. Dann gilt:
  - Für $\emptyset \neq K \subseteq \{1, \ldots, \ell\}$ wird x genau $(-1)^{1+\|K\|}$-mal gezählt.
  - Für alle anderen Menge K wird x gar nicht gezählt.

  Somit folgt für den Beitrag von x zur rechten Seite der Gleichung insgesamt:

$$\begin{aligned}\sum_{\emptyset \neq K \subseteq \{1,\ldots,\ell\}} (-1)^{1+\|K\|} &= \sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^{1+k} = -\sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^k \\ &= 1 - \sum_{k=0}^{\ell} \binom{\ell}{k} (-1)^k \\ &= 1 \qquad \text{(nach Korollar 1.10)}\end{aligned}$$

Damit ist das Theorem bewiesen. ∎

Wir wollen an einem Beispiel verdeutlichen, wie der doch recht kompliziert wirkende Ausdruck auf der rechten Seite gewinnbringend angewendet werden kann.

Beispiel: Wie viele Primzahlen gibt es zwischen 2 und 100? Um diese Frage zu beantworten, bestimmen wir die zusammengesetzten Zahlen zwischen 2 und 100 mit Hilfe des Inklusions-Exklusions-Prinzip. Es sei $A =_{\text{def}} \{2, \ldots, 100\}$. Eine Zahl $x \in A$ ist zusammengesetzt, falls $x = p \cdot n$ für geeignete Zahlen $p, n \in A$ gilt, wobei p eine Primzahl mit $p \leq \sqrt{100} = 10$ ist. Damit kommen als Primzahlen nur $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ und $p_4 = 7$ in Frage. Für $i \in \{1, 2, 3, 4\}$ betrachten wir die Menge der Vielfachen von p_i, d.h. die Menge

$$A_i =_{\text{def}} \{\, x \in A \mid (\exists n \in A)[x = p_i \cdot n] \,\}.$$

Damit gilt:

- $A_1 \cup A_2 \cup A_3 \cup A_4$ ist die Menge der zusammengesetzten Zahlen aus A

- Die Kardinalitäten der möglichen Schnittmengen sind

$$\begin{aligned} \|A_i\| &= \left\lfloor \frac{100}{p_i} \right\rfloor - 1 \quad (\text{da } p_i \notin A_i) \\ \left\| \bigcap_{j=1}^{k} A_{i_j} \right\| &= \left\lfloor \frac{100}{\prod_{j=1}^{k} p_{i_j}} \right\rfloor \quad \text{für } k \in \{2,3,4\} \text{ und } 1 \leq i_1 < \ldots < i_k \leq 4 \end{aligned}$$

Nach Theorem 1.19 erhalten wir:

$$\begin{aligned} &\|A_1 \cup A_2 \cup A_3 \cup A_4\| \\ &= \left(\left\lfloor \frac{100}{2} \right\rfloor - 1 + \left\lfloor \frac{100}{3} \right\rfloor - 1 + \left\lfloor \frac{100}{5} \right\rfloor - 1 + \left\lfloor \frac{100}{7} \right\rfloor - 1 \right) \\ &\quad - \left(\left\lfloor \frac{100}{6} \right\rfloor + \left\lfloor \frac{100}{10} \right\rfloor + \left\lfloor \frac{100}{14} \right\rfloor + \left\lfloor \frac{100}{15} \right\rfloor + \left\lfloor \frac{100}{21} \right\rfloor + \left\lfloor \frac{100}{35} \right\rfloor \right) \\ &\quad + \left(\left\lfloor \frac{100}{30} \right\rfloor + \left\lfloor \frac{100}{42} \right\rfloor + \left\lfloor \frac{100}{70} \right\rfloor + \left\lfloor \frac{100}{105} \right\rfloor \right) \\ &\quad - \left\lfloor \frac{100}{210} \right\rfloor \\ &= 49 + 32 + 19 + 13 - 16 - 10 - 7 - 6 - 4 - 2 + 3 + 2 + 1 + 0 - 0 \\ &= 74 \end{aligned}$$

Damit gibt es $99 - 74 = 25$ Primzahlen zwischen 2 und 100.

Schubfachschluss. Ein weiteres wichtiges Abzählprinzip, um die Existenz von Objekten zu beweisen, ist der Schubfachschluss (engl. *pigeonhole principle*).

Theorem 1.20 (Schubfachschluss) *Es seien A und B endliche Mengen mit $\|A\| > \|B\| > 0$ und $f : A \to B$ eine Funktion. Dann gibt es ein $y \in B$ mit $\|f^{-1}(y)\| > 1$.*

Beweis: (*Widerspruch*) Angenommen es gilt $\|f^{-1}(y)\| \leq 1$ für alle $y \in B$. Dann wissen wir aus dem letzten Semester, dass f eine injektive Funktion ist. Daraus folgt $\|A\| \leq \|B\|$. Dies ist ein Widerspruch zu $\|A\| > \|B\|$. Mithin war die Annahme falsch, und das Theorem ist beweisen. ■

Mit anderen Worten: Um $\|A\|$ Objekte in $\|B\|$ Schubfächer zu stecken, müssen sich in mindestens einem Schubfach 2 Objekte befinden (falls $\|A\| > \|B\|$ ist).

Beispiele: An folgenden Fällen wollen wir die Anwendung des Schubfachschlusses demonstrieren:

- Von 13 Personen feiern mindestens zwei Personen im gleichen Monat ihren Geburtstag.
- In jeder Menge P von mindestens zwei Personen gibt es immer mindestens zwei Personen, die die gleiche Anzahl von Personen in P kennen. (Hierbei sei angenommen, dass „kennen“ eine symmetrische Relation ist.)

  Zur Begründung: Es seien $P = \{p_1, \ldots, p_n\}$ die Personenmenge mit $n \geq 2$ Personen sowie $f : P \to \{0, \ldots, n-1\}$ eine Funktion, die der Person p_i die Anzahl ihrer Bekannten in P zuordnet. Wegen $\|P\| = \|\{0, \ldots, n-1\}\| = n$ kann Theorem 1.20 nicht direkt angewendet werden. Eine genauere Analyse ermöglicht jedoch die folgende Fallunterscheidung:

  – Es gibt ein $p \in P$ mit $f(p) = 0$. Wegen der Symmetrie der Bekanntschaftsrelation gibt es auch keine Person, die alle Personen in P kennt. Also gilt $f(q) \neq n-1$ für alle $q \in P$ und folglich $f(P) \subseteq \{0, \ldots, n-2\}$.
  – Für alle $p \in P$ gilt $f(p) \neq 0$. Damit gilt $f(P) \subseteq \{1, \ldots, n-1\}$.

  In beiden Fällen gilt also $\|f(P)\| < \|P\|$. Nach Theorem 1.20 folgt die Aussage.

Theorem 1.21 (Verallgemeinerter Schubfachschluss) *Es seien A und B endliche, nichtleere Mengen und $f : A \to B$ eine Funktion. Dann existiert ein $y \in B$ mit $\|f^{-1}(y)\| \geq \left\lceil \frac{\|A\|}{\|B\|} \right\rceil$.*

Beweis: (*Widerspruch*) Wir nehmen wiederum an, dass $\|f^{-1}(y)\| \leq \left\lceil \frac{\|A\|}{\|B\|} \right\rceil - 1$ für alle $y \in B$ gilt. Dann folgt:

$$\begin{aligned}
\|A\| &= \sum_{y \in B} \|f^{-1}(y)\| \\
&\leq \|B\| \cdot \left(\left\lceil \frac{\|A\|}{\|B\|} \right\rceil - 1 \right) \\
&\leq \|B\| \cdot \left(\frac{\|A\| + \|B\| - 1}{\|B\|} - 1 \right) \\
&= \|B\| \cdot \frac{\|A\| - 1}{\|B\|} \\
&= \|A\| - 1
\end{aligned}$$

Dies ist jedoch ein Widerspruch. Mithin war die Annahme falsch, und das Theorem ist bewiesen. ■

Beispiel: Wir wollen wieder anzwei Beispielen den verallgemeinerten Schubfachschluss verdeutlichen.

- Von 100 Personen feiern mindestens 9 Personen im gleichen Monat ihren Geburtstag.
- In jeder Menge von 6 Personen gibt es 3 Personen, die sich alle untereinander kennen, oder 3, die sich alle nicht kennen. (Hierbei nehmen wir wiederum an, dass „kennen“ eine symmetrische Relation ist.)

  Zur Begründung: Es sei $P = \{p_1, \ldots, p_6\}$ eine beliebige Personenmenge. Wir betrachten für die Person p_1 die Funktion

  $$f : \{p_2, \ldots, p_5\} \to \{\text{„bekannt“}, \text{„nicht bekannt“}\},$$

  die jeder Person $p_2, \ldots, p_5$ zuordnet, ob p_1 diese Person kennt. Nach Theorem 1.21 sind $\lceil \frac{5}{2} \rceil = 3$ Personen mit p_1 „bekannt“ oder 3 Personen mit p_1 „nicht bekannt“. Ohne Beeinträchtigung der Allgemeinheit seien 3 Personen mit p_1 bekannt (sonst vertauschen wir in nachfolgender Argumentation einfach „kennen“ und „nicht kennen“) und zwar p_2, p_3 und p_4. Nun gibt es zwei Möglichkeiten für die Personen p_2, p_3 und p_4:
  - Es gibt zwei Personen in $\{p_2, p_3, p_4\}$, die sich kennen. Diese beiden Personen kennen aber auch p_1. Somit gibt es also 3 Personen, die sich alle untereinander kennen.
  - Die Personen p_2, p_3 und p_4 kennen sich nicht. Also gibt es 3 Personen, die sich untereinander nicht kennen.

Rekursionen 2

2.1 Analyse von Algorithmen

Rekursionsgleichungen treten häufig bei Laufzeitanalysen von Algorithmen auf. Exemplarisch werden wir dies am wohlbekannten euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen diskutieren. Zur Erinnerung geben wir den Algorithmus noch einmal an (für Korrektheit und Herleitung siehe Skriptum „Brückenkurs Mathematik“):

Algorithmus:	EUKLID
Eingabe:	positive natürliche Zahlen n, m mit $m \leq n$
Ausgabe:	$\mathrm{ggT}(m, n)$

1. IF m teilt n
2. RETURN m
3. ELSE
4. RETURN EUKLID$(\mathrm{mod}(n, m), m)$

Die Laufzeit des Algorithmus wird sicher maßgeblich von der Anzahl der rekursiven Aufrufe bestimmt. Es ist also die Frage zu beantworten, wie viele rekursive Aufrufe von EUKLID(m,n) benötigt werden. Wir nehmen im Folgenden stets an, dass $m \leq n$ gilt.

Beispiel: Eine triviale obere Schranke für die Anzahl der Aufrufe ist sicher n. Dabei sind wir aber viel zu pessimistisch. Beispielsweise gilt

$$\text{EUKLID}(36, 120) = \text{EUKLID}(12, 36) = 12,$$

womit also nur eine rekursiver Aufrufe erfolgt. Für EUKLID$(89, 144)$ werden genau 9 rekursive Aufrufe benötigt. Und dies ist die maximale Anzahl rekursive Aufrufe von EUKLID$(m, 144)$ für alle $1 \leq m \leq 144$.

Die maximale Anzahl der rekursiven Aufrufe ist eng mit den FIBONACCI-Zahlen verbunden. Die n-te FIBONACCI-Zahl F_n ist wiederum rekursiv wie folgt definiert:

$$\begin{aligned} F_n &=_{\text{def}} F_{n-1} + F_{n-2} && \text{für } n \geq 2 \\ F_1 &=_{\text{def}} 1 \\ F_0 &=_{\text{def}} 0 \end{aligned}$$

Die Folge der FIBONACCI-Zahlen beginnt mit $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$. Die in obigem Beispiel verwendeten Zahlen 89 und 144 sind also gerade F_{11} und F_{12}. Benachbarte FIBONACCI-Zahlen sind nun gerade schlechteste Eingaben für den euklidischen Algorithmus.

Lemma 2.1 *Es seien $k, m, n \in \mathbb{N}_+$ beliebige natürliche Zahlen. Dann gilt:*

1. $\textsc{Euklid}(F_{k+2}, F_{k+3})$ *benötigt genau k rekursive Aufrufe.*
2. *Wenn* $\textsc{Euklid}(m, n)$ *mindestens k rekursive Aufrufe benötigt, dann gilt $n \geq F_{k+3}$ und $m \geq F_{k+2}$*

Beweis: (*Induktion*) Wir zeigen beide Aussagen im Block mittels vollständiger Induktion über k.

- *Induktionsanfang*: Es sei $k = 1$. Es gilt $F_3 = 2$ und $F_4 = 3$.
  1. Wegen $\textsc{Euklid}(2, 3) = \textsc{Euklid}(1, 2) = 1$ erfolgt genau ein rekursiver Aufruf.
  2. Wir betrachten alle Fälle mit $n < 3$ oder $m < 2$. Wegen $\textsc{Euklid}(2, 2) = 2$ und $\textsc{Euklid}(1, n) = 1$ erfolgt in allen diesen Fällen kein rekursiver Aufruf. Damit ist die Kontraposition der Aussage für $k = 1$ gezeigt und die Aussage ist wahr.
- *Induktionsschritt*: Es sei $k > 1$. Damit gilt

$$1 \leq F_{k+1} < F_{k+2} < F_{k+3} = F_{k+2} + F_{k+1} < 2 \cdot F_{k+2}$$

  und folglich $F_{k+2} \nmid F_{k+3}$ mit $\mathrm{mod}(F_{k+3}, F_{k+2}) = F_{k+1}$.
  1. Es gilt $\textsc{Euklid}(F_{k+2}, F_{k+3}) = \textsc{Euklid}(F_{k+1}, F_{k+2})$. Nach Induktionsvoraussetzung benötigt $\textsc{Euklid}(F_{(k-1)+2}, F_{(k-1)+3})$ genau $k-1$ rekursive Aufrufe. Mithin benötigt $\textsc{Euklid}(F_{k+2}, F_{k+3})$ genau k rekursive Aufrufe.
  2. Für m und n benötige $\textsc{Euklid}(m, n)$ mindestens $k \geq 2$ rekursive Aufrufe. Dann gilt $\textsc{Euklid}(m, n) = \textsc{Euklid}(\mathrm{mod}(n, m), m)$ und $\textsc{Euklid}(\mathrm{mod}(n, m), m)$ benötigt mindestens $k-1 \geq 1$ rekursive Aufrufe. Nach Induktionsvoraussetzung gilt $m \geq F_{(k-1)+3}$ sowie $\mathrm{mod}(n, m) \geq F_{(k-1)+2}$. Mithin gilt:

$$n \geq m + \mathrm{mod}(n, m) \geq F_{k+2} + F_{k+1} = F_{k+3}$$

Damit ist das Lemma bewiesen. ∎

Korollar 2.2 *Es seien $m, n \in \mathbb{N}_+$ beliebige natürliche Zahlen mit $m \leq n$. Dann ist die Anzahl der rekursiven Aufrufe von* $\textsc{Euklid}(m, n)$ *nach oben beschränkt (mit Gleichheit) durch*

$$k^* =_{\mathrm{def}} \max \{\ k \mid F_{k+3} \leq n\ \}.$$

Mit dem Wissen um die Formel

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \tag{2.1}$$

folgt $k^* = O(\log n)$ und damit eine asymptotisch präzise Aussage über das Laufzeitverhalten von Euklid. Der Algorithmus terminiert also für alle Eingaben mit höchstens logarithmisch vielen rekursiven Aufrufen im Wert der größeren Zahl und ist damit schnell.

Im Folgenden wollen Gleichheiten wie die Formel (2.1) beweisen und auch herleiten.

2.2 Lineare Rekursionsgleichungen

Definition 2.3 *Eine* Rekursionsgleichung *der Form*

$$x_n = a_1 x_{n-1} + \cdots + a_k x_{n-k} + b_k \qquad \textit{für alle } n \geq k$$

mit den Anfangsbedingungen

$$x_i = b_i \qquad \textit{für alle } i \in \{0, \ldots, k-1\}$$

heißt lineare Rekursionsgleichung k-ter Ordnung. *Für $b_k = 0$ heißt die Rekursionsgleichung* homogen *sonst* inhomogen.

Beispiel: Die einfachsten, nicht trivialen Rekursionsgleichungen sind homogene, lineare Rekursionsgleichungen erster Ordnung:

$$\begin{aligned} x_n &= a \cdot x_{n-1} && \text{für } n \geq 1 \\ x_0 &= b_0 \end{aligned}$$

Die Lösung der Gleichung ist sofort einzusehen: $x_n = b_0 \cdot a^n$.

Theorem 2.4 *Es sei eine inhomogene, lineare Rekursionsgleichung erster Ordnung*

$$\begin{aligned} x_n &= a \cdot x_{n-1} + b_1 && \textit{für } n \geq 1 \\ x_0 &= b_0 \end{aligned}$$

mit beliebigen Konstanten a, b_0, b_1 gegeben. Dann hat die Lösung der Gleichung die Form:

$$x_n = \begin{cases} b_0 \cdot a^n + b_1 \cdot \dfrac{a^n - 1}{a - 1}, & \textit{falls } a \neq 1 \\ b_0 + n \cdot b_1 & \textit{falls } a = 1 \end{cases}$$

Beweis: (*Induktion*) Wir zeigen das Theorem mittels vollständiger Induktion über n.

- *Induktionsanfang*: Es sei $n = 0$. Dann gilt für $a \neq 1$

$$x_0 = b_0 \cdot a^0 + b_1 \cdot \frac{a^0 - 1}{a - 1} = b_0$$

und für $a = 1$

$$x_0 = b_0 + 0 \cdot b_1 = b_0.$$

- *Induktionsschritt*: Es sei $n > 1$. Für $a \neq 1$ gilt

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

Für $a = 1$ ergibt sich aus der rekursiven Definition und der Induktionsvoraussetzung

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

Damit ist das Theorem bewiesen. ■

Theorem 2.5 *Es sei eine homogene, lineare Rekursionsgleichung zweiter Ordnung*

$$\begin{aligned} x_n &= a_1 \cdot x_{n-1} + a_2 \cdot x_{n-2} && \text{für } n \geq 2 \\ x_1 &= b_1 \\ x_0 &= b_0 \end{aligned}$$

mit $a_1 \neq 0$ oder $a_2 \neq 0$ gegeben. Es seien $\alpha, \beta \in \mathbb{R}$ Lösungen von $t^2 - a_1 t - a_2 = 0$ und $A, B \in \mathbb{R}$ wie folgt definiert:

$$A =_{\text{def}} \begin{cases} \dfrac{b_1 - b_0\beta}{\alpha - \beta}, & \text{falls } \alpha \neq \beta \\ \dfrac{b_1 - b_0\alpha}{\alpha}, & \text{falls } \alpha = \beta \end{cases}$$

$$B =_{\text{def}} \begin{cases} \dfrac{b_1 - b_0\alpha}{\alpha - \beta}, & \text{falls } \alpha \neq \beta \\ b_0, & \text{falls } \alpha = \beta \end{cases}$$

Dann hat die Lösung der Gleichung die Form:

$$x_n = \begin{cases} A\alpha^n - B\beta^n, & \text{falls } \alpha \neq \beta \\ (An + B)\alpha^n, & \text{falls } \alpha = \beta \end{cases}$$

Beweis: (*Induktion*) Wir zeigen das Theorem nur für den Fall $\alpha \neq \beta$ und verwenden dazu wiederum vollständige Induktion über n.

- *Induktionsanfang*: Es sei $n \in \{0, 1\}$. Für $n = 0$ gilt

$$x_0 = A\alpha^0 - B\beta^0 = A - B = \frac{b_1 - b_0\beta - b_1 + b_0\alpha}{\alpha - \beta} = b_0 \cdot \frac{\alpha - \beta}{\alpha - \beta} = b_0$$

  und für $n = 1$ gilt

$$x_1 = A\alpha^1 - B\beta^1 = A\alpha - B\beta = \frac{b_1\alpha - b_0\alpha\beta - b_1\beta + b_0\alpha\beta}{\alpha - \beta} = b_1 \cdot \frac{\alpha - \beta}{\alpha - \beta} = b_1.$$

- *Induktionsschritt*: Es sei $n > 1$. Dann gilt:

$$\begin{aligned}
x_n &= a_1 \cdot x_{n-1} + a_2 \cdot x_{n-2} && \text{(nach Definition)} \\
&= a_1 \cdot \left(A\alpha^{n-1} - B\beta^{n-1}\right) + a_2 \cdot \left(A\alpha^{n-2} - B\beta^{n-2}\right) \\
& && \text{(nach Induktionsvoraussetzung)} \\
&= a_1 A\alpha^{n-1} + a_2 A\alpha^{n-2} - a_1 B\beta^{n-1} - a_2 B\beta^{n-2} \\
&= A\alpha^{n-2} \cdot (a_1\alpha + a_2) - B\beta^{n-2} \cdot (a_1\beta + a_2) \\
&= A\alpha^{n-2} \cdot \alpha^2 - B\beta^{n-2} \cdot \beta^2 \\
& && \text{(wegen } \alpha^2 - a_1\alpha - a_2 = 0 \text{ und } \beta^2 - a_1\beta - a_2 = 0) \\
&= A\alpha^n - B\beta^n
\end{aligned}$$

Damit ist das Theorem bewiesen. ∎

Die Folge der FIBONACCI-Zahlen ist durch eine homogene, lineare Rekursionsgleichung zweiter Ordnung gegeben. Somit kann das Theorem 2.5 angewendet werden.

Korollar 2.6 *Für alle $n \in \mathbb{N}$ gilt*

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

Beweis: Nach Definition der FIBONACCI-Zahlen ist $a_1 = a_2 = 1$. Die Nullstellen von $t^2 - t - 1$ sind

$$\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}, \qquad \beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}.$$

Für A und B rechnen wir aus:

$$A = \frac{1 - 0 \cdot \beta}{\sqrt{5}} = \frac{1}{\sqrt{5}}, \qquad B = \frac{1 - 0 \cdot \alpha}{\sqrt{5}} = \frac{1}{\sqrt{5}}$$

Aus Theorem 2.5 folgt die Formel und das Korollar ist bewiesen. ∎

Literaturverzeichnis

[GKP94] Ronald L. Graham, Donald E. Knuth und Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. 2. Auflage. Addison-Wesley Longman, Amsterdam, 1994.

[KP09] Bernd Kreußler und Gerhard Pfister. *Mathematik für Informatiker*. Springer-Verlag, Berlin, 2009.

[MM06] Christoph Meinel und Martin Mundhenk. *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung*. 3., überarbeitete und erweiterte Auflage. B. G. Teubner Verlag, Wiesbaden, 2006.

[Ste07] Angelika Steger. *Diskrete Strukturen. Band 1: Kombinatorik-Graphentheorie-Algebra*. 2. Auflage. Springer-Verlag, Berlin, 2007.

[SS02] Thomas Schickinger und Angelika Steger. *Diskrete Strukturen. Band 2: Wahrscheinlichkeitstheorie und Statistik*. Springer-Verlag, Berlin, 2002.

[Wag03] Klaus W. Wagner. *Theoretische Informatik. Eine kompakte Einführung*. 2. überarbeitete Auflage. Springer-Verlag, Berlin, 2003.

[WHK04] Manfred Wolff, Peter Hauck und Wolfgang Küchlin. *Mathematik für Informatik und Bioinformatik*. Springer-Verlag, Berlin, 2004.

[Wil03] Herbert S. Wilf. *generatingfunctionology*. 3. Auflage. CRC Press, Boca Raton, FL, 2005.