VO Diskrete Mathematik

(Modul: “Diskrete Mathematik” (DMA))

Markus Fulmek & Christian Krattenthaler

Sommersemester 2017

Dieses Skriptum basiert großteils auf Vorlesungsskripten von Christian Krattenthaler und Markus Fulmek sowie auf den Büchern von Martin Aigner [**1**] und Peter Cameron [**4**]. Wir versuchen hier, eine (letztlich willkürliche) Auswahl aus grundlegenden Fragestellungen der abzählenden Kombinatorik und der Graphentheorie zu bringen. Für diesen Stoff benötigt man wenig Voraussetzungen — eigentlich genügen Schulwissen, Mengenlehre und eine Vertrautheit mit der mathematischen Ausdrucksweise —, aber Vorkenntnisse im Umfang der Vorlesungen Analysis I+II und Lineare Algebra I sind für das Verständnis sicher hilfreich.
Die Übungsaufgaben sind mit Sternchen versehen, die wie folgt zu interpretieren sind:

- $\star$: Eine sehr einfache Aufgabe, die eine Definition oder Methode illustrieren soll,
- $\star\star$: Eine nicht zu schwere Aufgabe, meist durch direkte analoge Anwendung einer Idee aus der Vorlesung zu lösen,
- $\star\star\star$ Schwierigere Aufgabe (meist mit Anleitung), die ein gewisses Maß an Kreativität (und manchmal Zähigkeit) erfordert.

Was die Notation angeht, so haben wir uns bemüht, den "Standard" (soweit sich ein solcher etabliert hat) zu verwenden. Sicherheitshalber sind alle Notationen auch in einem Glossar (Seite 130) zusammengefaßt (z.B.: ":=" ist zu lesen als "ist definiert als").
Für alle Hinweise auf Fehler und Ungereimtheiten sind wir dankbar. (Einige Fehler wurden durch Hinweise von Prof. Darij Grinberg bereits ausgemerzt.)

Markus Fulmek und Christian Krattenthaler, 27. Mai 2017.

Inhaltsverzeichnis

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1. Was ist das "Diskrete" an der Diskreten Mathematik?

Die *Diskrete Mathematik* ist ein Teilgebiet der Mathematik, das sich (überwiegend) mit mathematischen Strukturen befaßt, die endlich oder abzählbar sind. Das Gegenstück zu diskreter Mathematik ist also keineswegs "indiskrete Mathematik", sondern "kontinuierliche Mathematik": Während in der "kontinuierlichen Mathematik" die reellen Zahlen $\mathbb{R}$ (oder die komplexen Zahlen $\mathbb{C}$) und Eigenschaften wie Stetigkeit oder Differenzierbarkeit die Grundlage bilden, geht es in der Diskreten Mathematik (in der Regel) um die natürlichen Zahlen $\mathbb{N} = \{1, 2, \dots\}$ (oder die ganzen Zahlen $\mathbb{Z} = \{\dots, -1, -2, 0, 1, 2, \dots\}$, oder die rationalen Zahlen $\mathbb{Q}$)[1]. In diesem Sinne wäre also auch die Zahlentheorie zur Diskreten Mathematik zu zählen; für die Zwecke dieses Skriptums werden wir aber unter Diskreter Mathematik im wesentlichen Kombinatorik und Graphentheorie (und deren Anwendungen) verstehen.

Diskrete Mathematik ≠ Mathematik minus (Indiskrete Mathematik)

Damit ist freilich nicht erklärt, was Diskrete Mathematik nun genau ist: Eine exakte "Definition" dafür anzugeben wäre kaum möglich, den Begriff erfaßt man aber sehr gut durch typische Beispiele von Problemstellungen, die der Diskreten Mathematik zuzurechnen sind. Dies wollen wir im folgenden versuchen (und damit zugleich direkt ins Thema einsteigen).

1.2. Abzählung endlicher Mengen.

Das deutsche Wort "Abzählen" klingt vielleicht nicht nach höherer Mathematik (das englische Wort "Enumeration" erscheint da viel vornehmer), aber es sind hier natürlich nicht Fragestellungen gemeint, die man durch "Abzählen an einer Hand" beantworten kann. Wir wollen die typische Fragestellung an zwei sehr einfachen Beispielen illustrieren.

Enumeration von finiten Strukturen?

Beispiel 1.2.1. *In Österreich gibt es ein staatliches Glückspiel, das sogenannte* Lotto 6 aus 45*: Die Mitspieler versuchen jene 6 verschiedenen Zahlen zu erraten, die bei den wöchentlichen Ziehungen zufällig aus den Zahlen* $\{1, 2, \dots, 45\}$ *ermittelt werden. Wer einen sogenannten* Sechser *erzielt (d.h., alle 6 Zahlen richtig errät), gewinnt eine hübsche Summe (die ausbezahlten Gewinne werden durch die Wetteinsätze finanziert), und die naheliegende Frage ist nun, wie* wahrscheinlich *es ist, einen Sechser zu erzielen. Anders ausgedrückt: Wenn ein Mitspieler auf die Zahlen* $\{i_1, i_2, \dots, i_6\}$ *gesetzt hat, wie groß ist die Wahrscheinlichkeit*

$$\mathbf{P}\left(\{i_1, i_2, \dots, i_6\}\right),$$

[1] Manchmal betrachtet man auch nur die *nichtnegativen* ganzen, rationalen oder reellen Zahlen: Wir verwenden für die entsprechenden Zahlmengen die Notationen $\mathbb{Z}^+ := \{0, 1, 2, \dots\}$, $\mathbb{Q}^+$ bzw. $\mathbb{R}^+$.

daß genau diese Kombination tatsächlich gezogen wird?
Unter der (üblichen) Annahme, daß alle möglichen Ziehungen gleich wahrscheinlich *sind, d.h.*

$$\forall\, \{i_1, i_2, \ldots, i_6\} \subset [45] :\ \mathbf{P}\left(\{i_1, i_2, \ldots, i_6\}\right) = \mathbf{P}\left(\{1, 2, \ldots, 6\}\right),$$

ist diese Wahrscheinlichkeit also

$$\frac{1}{\left|\textit{Menge aller möglichen 6–er–Tipps aus } [45]\right|}.$$

Hier haben wir die abkürzenden Notationen

$$[n] := \{1, 2, \ldots, n\}$$

(mit dem "Grenzfall" $[0] := \emptyset$*) und*

$$|X| := \textit{Anzahl (Kardinalität, Mächtigkeit) von } X$$

eingeführt.
Die Fragestellung läuft also darauf hinaus, die Anzahl aller möglichen 6*–elementigen Teilmengen der Menge* $[45]$ *zu bestimmen; bezeichnen wir diese Anzahl mit* $\binom{45}{6}$.
Der wahrscheinlich nächstliegende Zugang dazu wäre wohl: Es gibt 45 Möglichkeiten, das erste Element der Teilmenge zu wählen, dann bleiben 44 Möglichkeiten für das zweite, 43 für das dritte, 42 für das vierte, 41 für das fünfte und 40 für das sechste Element; insgesamt also

$$45 \cdot 44 \cdot 43 \cdot 42 \cdot 41 \cdot 40 = 5864443200$$

Möglichkeiten. Das ist aber noch nicht die richtige Antwort auf unsere Frage, denn damit haben wir die Anzahl der geordneten 6–Tupel *aus* $[45]$ *bestimmt; bei Teilmengen kommt es aber nicht auf die Ordnung an. Z.B. haben wir ja* $(1, 2, 3, 4, 5, 6)$ *und* $(6, 5, 4, 3, 2, 1)$ *als zwei verschiedene geordnete* 6*-Tupel gezählt, obwohl sie dieselbe Teilmenge bestimmen. Genauer besehen, haben wir* jede *Teilmenge genau so oft gezählt, wie sie als geordnetes* 6*–Tupel geschrieben werden kann. Die Anzahl aller solchen Anordnungen einer* 6*–elementigen Menge ist aber mit demselben einfachen Zugang zu ermitteln — es gibt 6 Möglichkeiten, die erste Stelle eines* 6*–Tupels zu besetzen, dann bleiben 5 Möglichkeiten für die zweite Stelle, 4 für die dritte, 3 für die vierte, 2 für die fünfte und nur mehr eine für die sechste Stelle, insgesamt also*

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$$

Möglichkeiten. Zusammenfassend erhalten wir:

$$\binom{45}{6} = \frac{5864443200}{720} = 8145060, \tag{1.1}$$

und die gesuchte Wahrscheinlichkeit ist der Kehrwert dieser Anzahl, also etwa gleich 0.000000122774.

Aufgabe 1 ($\star$)**:** *Berechne die Wahrscheinlichkeit, mit einem Tip beim Lotto "6 aus 45"*

a: *einen Fünfer zu tippen,*
b: *einen Vierer zu tippen.*

Aufgabe 2 ($\star\,\star$)**:** *Im Parlament eines Landes gibt es 151 Sitze und drei Parteien. Wieviele Möglichkeiten der Sitzverteilung gibt es, sodaß keine Partei eine absolute Mehrheit (d.h., mehr als 75 Sitze) hat?*

Um auf den Bruch (1.1) zu kommen, haben wir ein simples Argument verwendet, dessen "abstrakten Kern" wir nun herausschälen wollen: Sei S die Familie der 6–elementigen Teilmengen von $[45]$, und sei T die Familie der geordneten 6–Tupel von $[45]$. Wir betrachten die *Relation*

> "$\sim$": $s \sim t$, wenn s und t dieselben Zahlen (abgesehen von der Ordnung) enthalten; für $s \in S$ und $t \in T$.

Eine Relation ist (sehr abstrakt) eine Teilmenge des cartesischen Produkts, in unserem Fall also eine Teilmenge R von $S \times T$. Diese Teilmenge R können wir uns so vorstellen: Wir betrachten eine $|S| \times |T|$–Matrix M, deren Zeilen mit den Elementen von S "numeriert" sind, und deren Spalten mit den Elementen von T "numeriert" sind. Der Eintrag in Position (s, t) in dieser Matrix sei 1, wenn $s \sim t$, und 0 sonst:

$$M_{s,t} := \begin{cases} 1 & \text{falls } s \sim t, \\ 0 & \text{sonst.} \end{cases}$$

Es ist klar: Die Kardinalität $|R|$ ist gleich der Anzahl der Einser in der Matrix M, und die wiederum können wir auf zwei verschiedene Arten abzählen, nämlich indem wir entweder "über die Zeilen" oder "über die Spalten" von M summieren.

$$|R| = \sum_{s \in S} \text{Anzahl Einser in Zeile } s = \sum_{t \in T} \text{Anzahl Einser in Spalte } t.$$

Allgemein können wir das so formulieren:

GRUNDREGEL 1.2.2. **(Regel von der doppelten Abzählung)**

Seien zwei endliche Mengen S, T gegeben, und sei $\sim$ eine Relation zwischen S und T. Für jedes $s \in S$ bezeichne $r(s)$ die Anzahl der Elemente $t \in T$, für die $s \sim t$ gilt; und ebenso bezeichne $\bar{r}(t)$ für jedes $t \in T$ die Anzahl der Elemente $s \in S$, für die $s \sim t$ gilt. Dann gilt (natürlich):

$$\sum_{s \in S} r(s) = \sum_{t \in T} \bar{r}(t).$$

In Beispiel 1.2.1 ist die Situation besonders einfach: Es gilt nämlich $r(s) \equiv 720$ für alle Teilmengen $s \in S$ ("zu jeder 6–elementigen Teilmenge gibt es 720 Arten, sie zu einem geordneten 6–Tupel zu machen") und $r(t) \equiv 1$ für alle 6–Tupel $t \in T$ ("jedes 6–Tupel bestimmt — durch "Vergessen der Ordnung" — eine eindeutige 6–elementige Teilmenge"), daher haben wir hier

$$|S| \cdot 720 = |T| \cdot 1 = 5864443200.$$

Für die folgende Aufgabe benötigen wir noch eine Definition:

DEFINITION 1.2.3. *Die rationale Zahl*

$$H_n := \sum_{i=1}^{n} \frac{1}{i}$$

heißt harmonische Zahl. *Aus der Analysis ist bekannt, daß H_n ungefähr gleich* $\log(n)$ *ist:*

$$H_n \sim \log(n) + \gamma + \frac{1}{2n},$$

d.h.: $\lim_{n\to\infty}(H_n - \log(n)) = \gamma$ *($\gamma \cong 0.5772156649\ldots$ ist die* Euler–Mascheroni–Konstante*).*

Weiters führen wir die Notation $\lfloor x \rfloor$ bzw. $\lceil x \rceil$ für die nächstkleinere bzw. nächstgrößere ganze Zahl an die reelle Zahl x ein:

$$\lfloor x \rfloor := \max\{z \in \mathbb{Z} : z \leq x\},$$
$$\lceil x \rceil := \min\{z \in \mathbb{Z} : z \geq x\}.$$

Aufgabe 3 ($\star\,\star$)**:** *Die rationale Zahl*

$$H_n := \sum_{i=1}^{n} \frac{1}{i}$$

heißt harmonische Zahl*. Aus der Analysis ist bekannt, daß H_n ungefähr gleich* $\log(n)$ *ist:* $H_n \sim \log(n)$*.*

Sei $j \in \mathbb{N}$ und bezeichne $t(j)$ die Anzahl der positiven Teiler von j. Bezeichne weiters $\bar{t}(n)$ die durchschnittliche *Anzahl der positiven Teiler der Zahlen von 1 bis n, also*

$$\bar{t}(n) := \frac{1}{n}\sum_{i=1}^{n} t(i).$$

Zeige:

$$\bar{t}(n) = \frac{1}{n}\sum_{i=1}^{n} \left\lfloor \frac{n}{i} \right\rfloor.$$

(Hinweis: Dies ist eine Anwendung der Regel von der doppelten Abzählung!)

Schätze die Differenz $\left(H_n - \bar{t}(n)\right)$ (ganz grob) ab und folgere:

$$H_n - 1 \leq \bar{t}(n) \leq H_n.$$

In Beispiel 1.2.1 haben wir *adhoc* eine Frage beantwortet — es liegt aber auf der Hand, daß man die Problemstellung verallgemeinern kann. Insbesondere werden wir die adhoc eingeführte Notation verallgemeinern: $\binom{n}{k}$ bezeichne die Anzahl aller k–elementigen Teilmengen einer n–elementigen Menge.

Beispiel 1.2.4. *Betrachten wir allgemein die Menge $[n]$ der natürlichen Zahlen von* 1 *bis n. Wir interessieren uns für die* Potenzmenge *von $[n]$, das ist die Familie aller Teilmengen von $[n]$. Dafür führen wir die Notation $2^{[n]}$ ein.*

Nun führen wir eine Gewichtsfunktion *ω auf $2^{[n]}$ ein: Jeder Teilmenge $A \in 2^{[n]}$ ordnen wir das Gewicht $\omega(A) := x^{|A|}$ zu (d.h., eine k–elementige Teilmenge erhält das Gewicht x^k). Weiters betrachten wir die sogenannte* erzeugende Funktion *(englisch:* generating function*) $\mathcal{GF}$ von $2^{[n]}$ (in bezug auf das Gewicht ω):*

$$\mathcal{GF}\left(2^{[n]}\right) := \sum_{A \in 2^{[n]}} \omega(A).$$

Es ist klar, daß $\mathcal{GF}\left(2^{[n]}\right)$ *ein Polynom in* x *vom Grad* n *ist. Für den Koeffizienten von* x^k *in* $\mathcal{GF}\left(2^{[n]}\right)$ *führen wir die Bezeichnung* $c_{n,k}$ *ein, sodaß wir also (definitionsgemäß) schreiben können:*

$$\mathcal{GF}\left(2^{[n]}\right) = \sum_{k=0}^{n} c_{n,k} x^k.$$

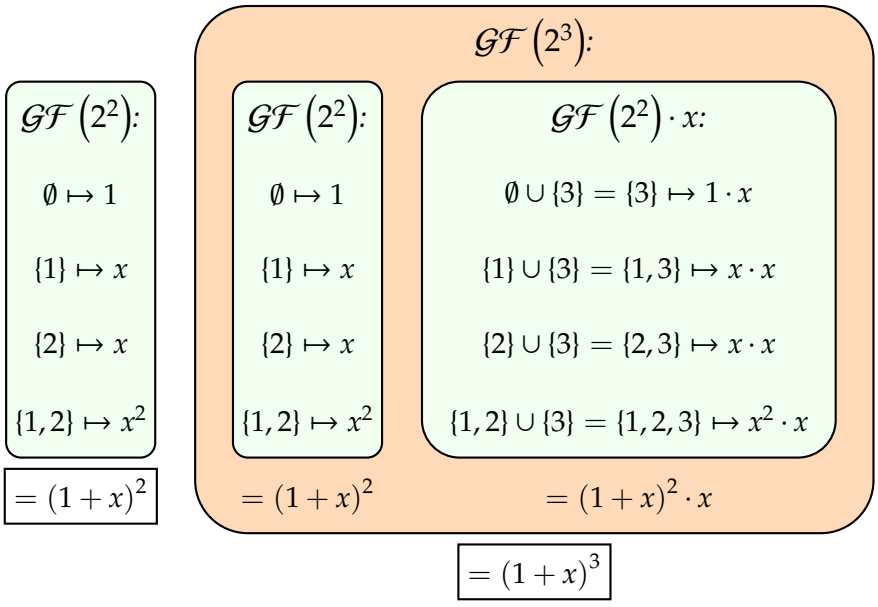
Wir machen dazu eine einfache kombinatorische Überlegung*: Jede Teilmenge von* $[n]$

- *enthält* entweder *das Element* n nicht — *dann kann man sie als Teilmenge* $A \in 2^{[n-1]}$ *auffassen,*
- oder *sie enthält das Element* n *— dann kann man sie auffassen als Vereinigung einer Teilmenge* $B \in 2^{[n-1]}$ *mit dem* Singleton *(einelementige Teilmenge)* $\{n\}$.

Natürlich gilt im letzteren Fall $\omega(B \cup \{n\}) = x \cdot \omega(B)$*, sodaß wir also folgende* Rekursion *für die erzeugenden Funktionen erhalten:*

$$\mathcal{GF}\left(2^{[n]}\right) = \mathcal{GF}\left(2^{[n-1]}\right) + x \cdot \mathcal{GF}\left(2^{[n-1]}\right) = (1+x)\,\mathcal{GF}\left(2^{[n-1]}\right).$$

Die folgende Graphik illustriert diese Rekursion für $n = 3$*:*



Zusammen mit der offensichtlichen Anfangsbedingung $\mathcal{GF}\left(2^{[0]}\right) = 1$ *(die Potenzmenge der leeren Menge* $\emptyset$ *hat als einziges Element die leere Menge* $\emptyset$ *selbst, und* $\omega(\emptyset) = x^{|\emptyset|} = x^0 = 1$*) erhalten wir also:*

$$\mathcal{GF}\left(2^{[n]}\right) = (1+x)^n. \tag{1.2}$$

Die Koeffizienten eines Polynoms $p(x) = \sum_{k=0}^{n} c_k x^k$ *kann man bekanntlich durch Differenzieren und Auswerten bei* 0 *ermitteln, genauer gesagt:*

Taylorscher Lehrsatz: Für Polynome "trivial".

$$c_k = \frac{1}{k!} \frac{\mathbf{d}^k}{\mathbf{d}x^k} p(x)\bigg|_{x=0},$$

wobei $k!$ *(gesprochen:* k Faktorielle *oder* k Fakultät*) gleich dem Produkt* $1 \cdot 2 \cdots k$ *ist. Angewandt auf die Polynome* $\mathcal{GF}\left(2^{[n]}\right)$ *bedeutet dies gemäß* (1.2)*:*

Eine Anwendung von Potenzregel und Kettenregel.

$$c_{n,k} = \frac{n\cdot(n-1)\cdots(n-k+1)}{k!}\underbrace{(1+x)^{n-k}\Big|_{x=0}}_{\equiv 1} = \frac{n^{\underline{k}}}{1\cdot 2\cdots k}.$$

Hier haben wir wieder stillschweigend eine neue Notation eingeführt: Die sogenannten fallenden Faktoriellen *sind definiert als das Produkt*

$$n^{\underline{k}} := n\cdot(n-1)\cdots(n-k+1)\,.$$

Natürlich erkennen wir die direkte Verallgemeinerung der Aufgabenstellung aus Beispiel 1.2.1: Die Koeffizienten $c_{n,k}$ sind nichts anderes als die Anzahlen der k–elementigen Teilmengen einer n–elementigen Menge, für die wir die Bezeichnung $\binom{n}{k}$ eingeführt haben. Da ersichtlich

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

gilt, erhalten wir also die (wohlbekannte) Formel für die sogenannten Binomialkoeffizienten*:*

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

bzw. die wohlbekannte Entwicklung

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k. \tag{1.3}$$

Aufgabe 4 ($\star\,\star$)**:** *Zeige, daß für die Binomialkoeffizienten $\binom{n}{k}$ gilt:*

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2\rfloor} = \binom{n}{\lceil n/2\rceil} > \cdots > \binom{n}{n}.$$

(Diese Eigenschaft heißt Unimodalität *der Binomialkoeffizienten.)*

Bemerkung 1.2.5. *Wir können nun das "Wesen" des typischen Abzählungsproblems beschreiben: Seien Mengen $S(n_1, n_2, \dots)$ definiert, die von ganzzahligen Parametern $n_1, n_2, \dots$ abhängen (in Beispiel 1.2.4 sind das die Mengen der k–elementigen Teilmengen einer n–elementigen Menge, also $n_1 = n$, $n_2 = k$). "Abzählung" bedeutet, für $\big|S(n_1, n_2, \dots)\big|$ eine "möglichst einfache" Formel zu finden.*

Die kombinatorische Überlegung, die wir in Beispiel 1.2.4 für die erzeugende Funktion verwendet haben, führt auch direkt auf die wohlbekannte Rekursion für die Binomialkoeffizienten:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \tag{1.4}$$

mit den Anfangsbedingungen $\binom{n}{0} = \binom{n}{n} = 1$. Diese Aussage über Zahlen (die Mengen abzählen) haben wir aus einer geschickten "Zerlegung" der abzuzählenden Mengen gewonnen — wieder können wir einen "abstrakten Kern" herausschälen:

DEFINITION 1.2.6. *Sei S eine Menge. Unter einer* Partition π *von S in m* Blöcke S_i *verstehen wir eine Familie $\pi = \{S_1, \ldots, S_m\}$ von Teilmengen von S mit den Eigenschaften*

$$S_i \neq \emptyset \quad \forall i,$$
$$S_i \cap S_j = \emptyset \quad \forall i \neq j,$$
$$\bigcup_{i=1}^{m} S_i = S.$$

Für die disjunkte Vereinigung *von Mengen führen wir die Notation $\dot\cup$ ein: $A \dot\cup B$ meint "$A \cup B$, wobei $A \cap B = \emptyset$". Die letzten zwei der obigen Eigenschaften können wir damit auch so schreiben: $S = \dot\bigcup_{i\in[m]} S_i$.*

BEISPIEL 1.2.7. *Sei $S = [8]$. Eine Partition von S in 4 Blöcke ist beispielsweise*

$$\pi = \{\{1,4,5\},\{6\},\{2,8\},\{3,7\}\}.$$

GRUNDREGEL 1.2.8. **(Summenregel)**

Sei S eine Menge, und $S_1, \ldots, S_m$ eine Partition *von S in m Blöcke. Dann gilt (natürlich):*

$$|S| = \sum_{i=1}^{m} |S_i|.$$

Aufgabe 5 ($\star\,\star$)**:** *Man gebe kombinatorische Beweise für die folgenden Binomialidentitäten:*

(a) $n\binom{n-1}{k-1} = k\binom{n}{k}$. *(Anleitung: Wieviele Möglichkeiten gibt es, aus einer n-elementigen Menge eine k-elementige Teilmenge auszuwählen, und in dieser ein Element rot zu färben?)*

(b) $\displaystyle\sum_{i=0}^{n} i\binom{n}{i} = n \cdot 2^{n-1}$.

Aufgabe 6 ($\star\,\star$)**:** *Man gebe kombinatorische Beweise für die folgenden Binomialidentitäten:*

(a) $\displaystyle\binom{n+1}{k+1} = \sum_{m=k}^{n} \binom{m}{k}$.

(b) $\displaystyle\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$.

BEMERKUNG 1.2.9. *Die Rekursion* (1.4) *begründet das sogenannte* Pascalsche Dreieck *der Binomialkoeffizienten:*

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
\cdots & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots
\end{array}$$

Jede Zahl darin ergibt sich als Summe der beiden unmittelbar darüber liegenden Zahlen.

Die Bezeichnung "Binomialkoeffizient" wird verständlich, wenn wir uns vor Augen halten, daß diese Koeffizienten beim Ausmultiplizieren des Binoms $(x+y)^n$ auftreten; eine Tatsache, die unter dem Namen *Binomischer Lehrsatz* wohlbekannt ist.

DEFINITION 1.2.10. *Sei S eine endliche Menge und $T \subseteq S$ eine Teilmenge von S.*

Die charakteristische Funktion $\chi_T : S \to \{0,1\}$ *der Teilmenge T ist dann wie folgt definiert:*

$$\chi_T(i) = \begin{cases} 1 & \text{falls } i \in T, \\ 0 & \text{falls } i \notin T. \end{cases}$$

SATZ 1.2.11 (Binomischer Lehrsatz). *Es gilt:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{1.5}$$

BEWEIS. Wir könnten diese scheinbare Verallgemeinerung von (1.3) ganz leicht aus (1.3) herleiten; stattdessen geben wir einen neuen "direkten" Beweis (und illustrieren so eine weitere typische Idee).

Wenn wir das Produkt

$$(x+y)^n = \underbrace{(x+y)\cdot(x+y)\cdots(x+y)}_{n \text{ Faktoren } (x+y)}$$

formal ausmultiplizieren wollten, dann müßten wir aus jedem der n Faktoren immer entweder x oder y auswählen. Jede solche Auswahl "codieren" wir wie folgt durch eine Binärzahl mit n Bits (also durch ein n–Tupel aus Nullen und Einsern): Wenn wir aus dem j–ten Faktor x auswählen, setzen wir das j–te Bit auf 1; wenn wir aus dem j–ten Faktor y auswählen, setzen wir das j–te Bit auf 0. Es ist klar, daß diese "Codierung" eindeutig ist: Zwischen den Binärzahlen mit n Bits und den beim Ausmultiplizieren auftretenden Monomen gibt es eine *Bijektion*.

Der Koeffizient von $x^k y^{n-k}$ (es ist klar, daß beim Ausmultiplizieren keine anderen Monome auftreten können) ist also gleich der Anzahl der n–stelligen Binärzahlen, die genau k Einser enthalten.

Zwischen der Menge aller n–stelligen Binärzahlen, die genau k Einser enthalten, und der Familie der k–elementigen Teilmengen von $[n]$ gibt es aber auch eine offensichtliche Bijektion: Wir deuten die n–stellige Binärzahl als *charakteristische Funktion* $\chi_A : [n] \to \{0,1\}$ einer gewissen Teilmenge $A \subseteq [n]$.

Die Anzahl der Monome der Gestalt $x^k y^{n-k}$ ist daher gleich groß wie die Anzahl der k–elementigen Teilmengen von $[n]$: $\binom{n}{k}$. □

Im Beweis von Satz 1.2.11 haben wir implizit folgende Selbstverständlichkeit benutzt, die wir wieder allgemein–abstrakt formulieren:

GRUNDREGEL 1.2.12. **(Bijektionsregel)**

Wenn es zwischen zwei Mengen S und T eine Bijektion gibt, dann gilt (natürlich)

$$|S| = |T|\,.$$

Aufgabe 7 ($\star\star$)**:** *Zeige durch eine* Bijektion*: Für $n \geq 1$ ist die Anzahl der Teilmengen von $[n]$ mit* gerader *Mächtigkeit genauso groß wie die Anzahl der Teilmengen von $[n]$ mit* ungerader *Mächtigkeit*

Aufgabe 8 ($\star\star$)**:** *Wieviele Lottotips gibt es bei "6 aus 45", in denen keine zwei* aufeinanderfolgenden *Zahlen vorkommen?*

(Hinweis: Finde eine Bijektion der gesuchten Objekte auf die 6–elementigen Teilmengen aus $[40]$.)

KOROLLAR 1.2.13. *Sei X eine endliche Menge mit $|X| = n$ für ein $n \in \mathbb{N}$. Dann gilt für die Mächtigkeit der Potenzmenge 2^X*

$$\left|2^X\right| = 2^n.$$

(Dies motiviert nachträglich die Notation $2^X :=$ Potenzmenge von X.)

BEWEIS. Wir sind nun so gut vorbereitet, daß wir dieses Korollar auf mehrere Arten beweisen könnten. Um die letzte "Grundregel fürs Abzählen" zu illustrieren, beschreiben wir jede Teilmenge von n durch ihre charakteristische Funktion, interpretieren diese als n–stellige Binärzahl, also als n–Tupel, bei der jede Eintragung aus der Menge $\{0,1\}$ stammt. Insgesamt haben wir damit eine Bijektion der Familie aller Teilmengen von $[n]$ auf das cartesische Produkt $\{0,1\}^n$ beschrieben. □

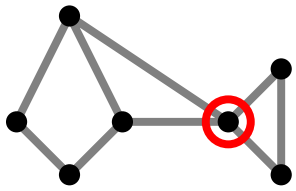
GRUNDREGEL 1.2.14. **(Produktregel)**

Für das cartesische Produkt der Mengen $S_1, \ldots, S_m$ gilt (natürlich)

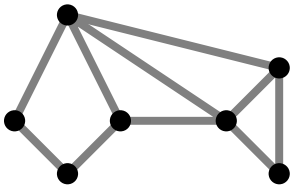
$$|S_1 \times S_2 \times \cdots \times S_m| = \prod_{i=1}^{m} |S_i|\,.$$

1.3. Strukturen und ihre Eigenschaften.

Betrachten wir ein sehr einfaches Computernetzwerk: Zur Visualisierung zeichnen wir für jeden Rechner einen Punkt; und für jedes Kabel, das zwei Rechner verbindet, zeichnen wir eine Linie, die die zugehörigen Punkte verbindet.



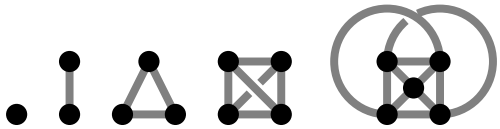
Es ist augenfällig, daß der Rechner, der in der Skizze markiert wurde, eine Sonderrolle einnimmt: Wenn er ausfällt, zerfällt das kleine Netzwerk in 2 Teile, zwischen denen keine Verbindung mehr besteht. Vom Standpunkt der Betriebssicherheit ist es sicher wünschenswert, diese "Schwachstelle" zu beheben; im vorliegenden Fall kann das durch ein einziges neues Kabel bewerkstelligt werden:



Eine Figur wie in der obigen Skizze (Punkte und verbindende Linien) nennt man *Graph*; die Punkte nennt man in diesem Zusammenhang *Knoten* (englisch: *Vertices*; im Deutschen sagt man manchmal auch *Ecken* statt Knoten) und die Linien *Kanten* (englisch: *Edges*). Graphen spielen für viele praktische Anwendungen (insbesondere in der Computerwissenschaft) eine große Rolle, sodaß sich die *Graphentheorie* als eigenständige mathematische Teildisziplin etabliert hat.

BEMERKUNG 1.3.1. *Wir werden hier nur Graphen mit* endlichen *Knoten– und Kantenmengen behandeln, ohne dies immer ausdrücklich zu betonen.*
Viele graphentheoretische Konzepte machen aber auch für unendliche Knotenmengen Sinn und führen auf interessante Fragestellungen.

DEFINITION 1.3.2. *Ein Graph* $\mathbf{G}$ *besteht aus einer (endlichen) Menge* V *von Knoten (Vertices) und einer Teilmenge* $E \subseteq \binom{V}{2}$ *von Kanten (Edges).*
(Hier haben wir die abkürzende Notation $\binom{X}{k} := \{A \subseteq X : \ |A| = k\}$ *für die Familie der* k*–elementigen Teilmengen von* X *eingeführt*[2]*.)*
Manchmal schreibt man auch $\mathbf{G}(V, E)$ *statt* $\mathbf{G}$*, um die Knoten– und Kantenmengen deutlich zu betonen, umgekehrt schreibt man auch* $V(\mathbf{G})$ *und* $E(\mathbf{G})$ *statt* V *und* E*, um den zugehörigen Graphen deutlich zu betonen.*
Der vollständige Graph $\mathbf{K}_n$ *auf* n *Knoten ist dadurch definiert, daß er alle Kanten besitzt, die möglich sind; es gilt also* $E(\mathbf{K}_n) = \binom{V(\mathbf{K}_n)}{2}$.



Eine Wanderung *der* Länge n *in* $\mathbf{G}$*, die von einem Knoten* $p \in V(\mathbf{G})$ *zu einem Knoten* $q \in V(\mathbf{G})$ *führt, ist eine Folge von Knoten*

$$(p = v_0, v_1, \ldots, v_n = q),$$

sodaß $\{v_i, v_{i+1}\} \in E(\mathbf{G})$ *für* $i = 0, 1, \ldots, n-1$*. Wir sagen: Die Wanderung enthält die Kanten* $\{v_i, v_{i+1}\}$*. (Beachte: Die Kanten können sich wiederholen, eine Kante kann also* mehrfach *in einer Wanderung enthalten sein). Im Spezialfall* $p = q$ *sprechen wir von einer* geschlossenen Wanderung*; ein besonders einfacher Fall ist die geschlossene*

[2] "By abuse of notation", denn dieselbe Notation verwenden wir auch für den Binomialkoeffizienten: Die Bedeutung sollte aber aus dem Zusammenhang immer klar sein.

Wanderung der Länge $n = 0$, also die Folge $(p = q = v_0 = v_n)$, die nur aus einem einzigen Knoten besteht.
Wir schreiben abkürzend $p \rightsquigarrow q$, wenn eine Wanderung von p nach q führt. Klarerweise definiert "$\rightsquigarrow$" eine Relation *auf $V(\mathbf{G})$; es ist leicht zu sehen, daß es sich um eine* Äquivalenzrelation *handelt.*

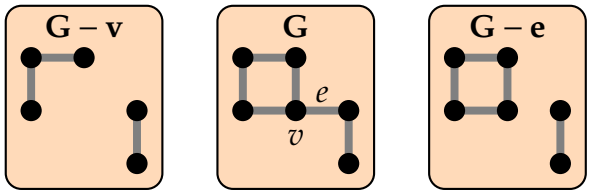
Aufgabe 9 ($\star$)**:** *Veranschauliche die Begriffe Graph und Wanderung durch eine Skizze. Zeige, daß die Relation*

$$p \rightsquigarrow q := \text{"Es gibt eine Wanderung, die von } p \text{ nach } q \text{ führt"}$$

auf der Knotenmenge $V(\mathbf{G})$ eines Graphen $\mathbf{G}$ eine Äquivalenzrelation *ist.*

Definition 1.3.3. *Sei $\mathbf{G}(V, E)$ ein Graph. Eine Teilmenge $V_H \subseteq V$ zusammen mit einer Teilmenge $E_H \subseteq E$ definiert einen* Teilgraphen $\mathbf{H} = \mathbf{H}(V_H, E_H)$*, wenn alle Knoten, die zu Kanten aus E_H gehören, in V_H enthalten sind; also wenn $\left(\bigcup_{e \in E_H} e\right) \subseteq V_H$.*
Sei $e \in E(\mathbf{G})$: Den Teilgraph $\mathbf{H}(V_H, E_H)$ mit $V_H = V(\mathbf{G})$ und $E_H = E(\mathbf{G}) \setminus \{e\}$ ($\mathbf{H}$ entsteht also aus $\mathbf{G}$ "durch Entfernen der Kante e") bezeichnen wir mit $\mathbf{G} - \mathbf{e}$.
Wenn überdies alle *Kanten in $E(\mathbf{G})$, die* beide *Knoten in V_H haben, auch zu E_H gehören (also $\forall e \in E(\mathbf{G}) : \quad e \subseteq V_H \implies e \in E_H$; V_H determiniert dann E_H eindeutig), dann nennt man $\mathbf{H}$ einen (durch V_H)* induzierten Teilgraphen.
Sei $v \in V(\mathbf{G})$: Den induzierten *Teilgraph $\mathbf{H}(V_H, E_H)$ mit $V_H = V(\mathbf{G}) \setminus \{v\}$ ($\mathbf{H}$ entsteht also aus $\mathbf{G}$ "durch Entfernen des Knotens v") bezeichnen wir mit $\mathbf{G} - \mathbf{v}$.*

Beispiel 1.3.4. *Die folgende Graphik illustriert die Begriffe Teilgraph und induzierter Teilgraph:*

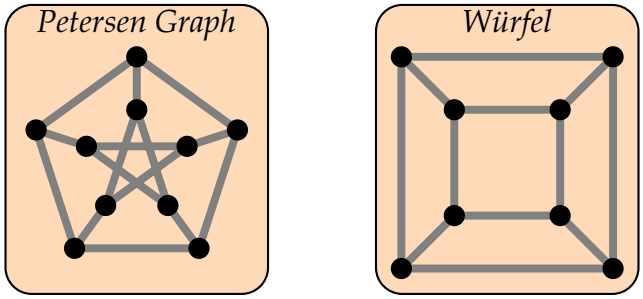


Definition 1.3.5. *Ein Graph $\mathbf{G}$ heißt* zusammenhängend*, wenn je zwei Knoten von $\mathbf{G}$ durch eine Wanderung verbunden sind.*
Die von den Äquivalenzklassen *der Relation "$\rightsquigarrow$" induzierten Teilgraphen von $\mathbf{G}$ heißen die* Zusammenhangskomponenten *von $\mathbf{G}$.*
Eine Zusammenhangskomponente, die nur aus einem einzigen Knoten besteht, heißt isolierter Knoten.
Ein Graph $\mathbf{G}$ heißt d–fach zusammenhängend (für $d \in \mathbb{N}$), wenn

- $\left|V(\mathbf{G})\right| > d$
- *und für* jede *Teilmenge $T \subseteq V(\mathbf{G})$ mit $|T| < d$ der durch $V(\mathbf{G}) \setminus T$ induzierte Teilgraph zusammenhängend ist.*

*Wenn $\mathbf{G}$ zusammenhängend ist, dann heißt die größte ganze Zahl k, für die $\mathbf{G}$ k–*fach zusammenhängend *ist, der* Zusammenhangsgrad *von $\mathbf{G}$ (wenn $\mathbf{G}$ unzusammenhängend ist, ist der Zusammenhangsgrad von $\mathbf{G}$ als 0 definiert).*

Beispiel 1.3.6. *Die folgende Graphik zeigt zwei dreifach zusammenhängende Graphen:*



Aufgabe 10 (⋆)**:** *Zeige, daß alle vollständigen Graphen* $\mathbf{K}_n$ *(für* $n > 0$*) stets zusammenhängend sind.*

Zeige, daß die Graphen

Zusammenhangsgrad 1 bzw. 2 haben.

Zeige, daß ein Graph genau dann Zusammenhangsgrad 0 *hat, wenn er entweder unzusammenhängend ist oder gleich dem vollständigen Graphen* $\mathbf{K}_1$ *ist.*

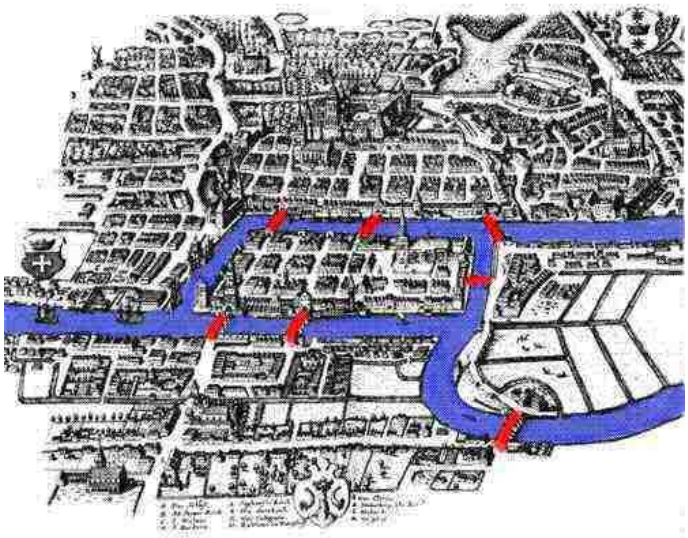
Zeige, daß der Zusammenhangsgrad des vollständigen Graphen $\mathbf{K}_n$ *gleich* $n-1$ *ist.*

Zeige, daß jeder induzierte *Teilgraph eines vollständigen Graphen wieder ein vollständiger Graph ist.*

Zeige, daß ein Graph $\mathbf{G}\,(V, E)$ *mit* $\left|V\,(\mathbf{G})\right| \geq 3$ *zweifach zusammenhängend ist, wenn es für je zwei Knoten* v *und* w *aus* V *einen* Kreis *(das ist eine geschlossene Wanderung* $v_0, \ldots, v_n$ *in* $\mathbf{G}$*, wobei* $v_i \neq v_j$ *für alle* $i \neq j$ *mit der einzigen Ausnahme* $v_0 = v_n$*) gibt, der* v *und* w *enthält.*

1.4. Existenz/Nichtexistenz: Konstruktion von Lösungen.

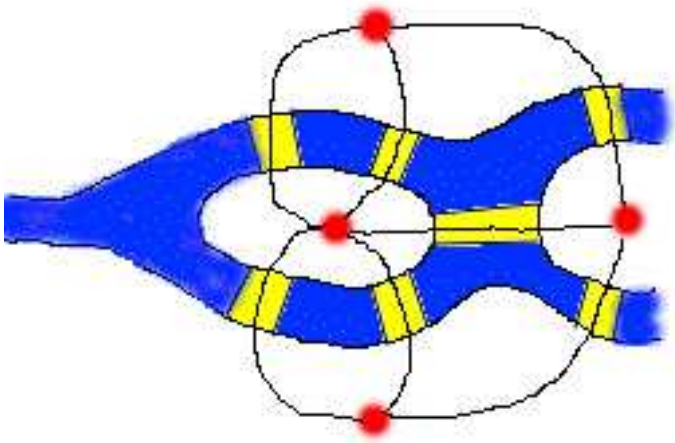
Ein altes unterhaltungsmathematisches Problem ist das *Königsberger Brückenproblem*. Zu Lebzeiten von Leonhard Euler sah der Verlauf des Flusses Pregel durch Königsberg so aus:



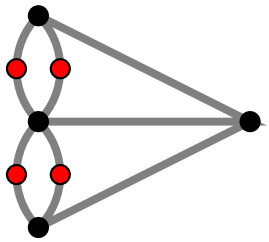
In der Darstellung sind (leider nicht sehr gut) die 7 Brücken erkennbar. Die Frage lautet nun:

> Ist es möglich, einen Rundgang zu machen, bei dem jede Brücke *genau einmal* überquert wird?

Es ist dies ganz offensichtlich eine graphentheoretische Fragestellung — wenn man geeignet abstrahiert . . .



. . . erhält man folgenden Graphen (um mehrfache Kanten[3] zu vermeiden, haben wir vier zusätzliche Knoten eingeführt):



Die Frage ist nun, ob es in diesem Graphen eine geschlossene Wanderung gibt, in der jede der 11 Kanten genau einmal benutzt wird. Die Antwort ist nein, denn für eine solche Wanderung $v_0, v_1, \ldots, v_{11} = v_0$ der Länge 11, die jede der 11 Kanten *genau einmal* enthält, müßte für *jeden* Knoten v die Anzahl der Kanten, die v enthalten, immer *gerade* sein. (Denn für jede Kante $\{u, v\}$, über die wir den Knoten v im Zuge der Wanderung "betreten", muß es eine eindeutig bestimmte weitere Kante $\{v, w\}$ geben, über die wir den Knoten anschließend wieder "verlassen": $u = v_{i-1}, v = v_i, w = v_{i+1}$, wobei der Index i modulo 11 gerechnet wird).

Definition 1.4.1. *Sei* $\mathbf{G}$ *ein Graph. Man sagt, ein Knoten* $v \in V(\mathbf{G})$ *ist mit einer Kante* $e \in E(\mathbf{G})$ *(bzw. die Kante* e *mit dem Knoten* v*)* inzident *(oder* v *inzidiert mit* e*, bzw.* e *inzidiert mit* v*), wenn* $v \in e$ *ist (also: Der Knoten gehört zur Kante; in der graphischen Darstellung verbindet die Kante den Knoten mit einem andren Knoten). Für jeden Knoten* v *ist der* Grad $\deg(v)$ *definiert als die Anzahl der Kanten, mit denen* v *inzidiert.*

[3] Mehrfache Kanten behandeln wir in Kapitel 3.

PROPOSITION 1.4.2. *Sei* $\mathbf{G}(V,E)$ *ein Graph. Dann gilt:*

$$\sum_{v\in V(\mathbf{G})} \deg(v) = 2\cdot|E|. \tag{1.6}$$

Insbesondere gilt: Die Anzahl der Knoten von $\mathbf{G}$*, die* ungeraden *Grad haben, ist* gerade.

Aufgabe 11 ($\star\star$)**:** *Beweise die Aussage: Sei* $\mathbf{G}(V,E)$ *ein Graph. Dann gilt:*

$$\sum_{v\in V(\mathbf{G})} \deg(v) = 2\cdot|E|.$$

(Hinweis: Das ergibt sich durch die Regel von der doppelten Abzählung!)

DEFINITION 1.4.3. *Ein Graph, in dem jeder Knoten geraden Grad hat, heißt ein* Eulerscher Graph.
Eine geschlossene Wanderung in einem Graphen $\mathbf{G}$*, die jede Kante aus* $E(\mathbf{G})$ *genau einmal enthält, heißt* Eulersche Wanderung.

SATZ 1.4.4 (Satz von Euler). *In einem zusammenhängenden Graphen* $\mathbf{G}$ *gibt es genau dann eine Eulersche Wanderung, wenn* $\mathbf{G}$ *ein Eulerscher Graph ist.*

BEWEIS. Daß ein Graph, in dem es eine Eulerschen Wanderung gibt, notwendigerweise ein Eulerscher Graph sein muß, ist nach der obigen Überlegung zum Königsberger Brückenproblem bereits klar.
Umgekehrt konstruieren wir nun "algorithmisch" für jeden zusammenhängenden Eulerschen Graphen $\mathbf{G}$ eine Eulersche Wanderung w.

D.h., wir skizzieren ein "Computerprogramm".

`/* Initialisierung: */`
$k \leftarrow 0$ und $\mathbf{H} \leftarrow \mathbf{G}$, wähle v_0 beliebig aus $V(\mathbf{H})$ und beginne mit der Wanderung $w = (v_0)$ der Länge $k = 0$.
`/* Schleife: Wird wiederholt, solange die Bedingung erfüllt ist. */`
while (Bedingung: Der Graph $\mathbf{H}$ enthält eine mit v_k inzidente Kante.) **do**
  Wähle von den mit v_k inzidenten Kanten eine aus (bezeichne sie mit $e = \{v_k, v_{k+1}\}$), sodaß der Teilgraph $\mathbf{T} = \mathbf{H} - \mathbf{e} := \mathbf{T}(V(\mathbf{H}), E(\mathbf{H}) \setminus \{e\})$ von $\mathbf{H}$
  - entweder wieder zusammenhängend ist — setze in diesem Fall $\mathbf{H} = \mathbf{T}$,
  - oder in genau zwei Zusammenhangskomponenten zerfällt, von denen eine das Singleton $\{v_k\}$ ist — setze in diesem Fall $\mathbf{H}$ gleich der andren Zusammenhangskomponente (diese enthält dann v_{k+1}).

  Verlängere die Wanderung w mit dem Knoten v_{k+1}
  $k \leftarrow k+1$
end while

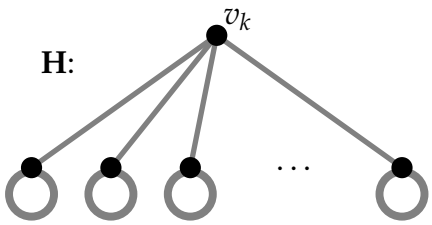
Wir müssen noch nachweisen, daß die Kante e im "Wiederholungsschritt" tatsächlich immer so gewählt werden kann, daß die "Zusammenhangsbedingungen" erfüllt sind — wenn wir dies aber für den Moment voraussetzen, dann gilt in jedem Schritt des Algorithmus:

- $\mathbf{H}$ ist ein zusammenhängender Graph, der jene Kanten von $\mathbf{G}$ enthält, die *nicht* in der Wanderung w vorkommen,

- w ist eine Wanderung, in der jede Kante aus $E(\mathbf{G})$ höchstens einmal vorkommt,
- der Anfangspunkt v_0 und der aktuelle Endpunkt der Wanderung w, v_k, sind Knoten in $\mathbf{H}$; der Grad dieser beiden Knoten in $\mathbf{H}$ ist immer *ungerade*, außer wenn $v_k = v_0$, insbesondere also zu Beginn (im Initialisierungsschritt) und am Ende (wenn der Algorithmus stoppt).

Der Algorithmus stoppt erst dann, wenn wir mit der Wanderung w wieder den Ausgangspunkt v_0 erreicht und alle Kanten in $\mathbf{G}$ "verbraucht" haben, er liefert also die gesuchte Eulersche Wanderung.

Es bleibt noch zu zeigen, daß immer eine geeignete Kante e für den "Wiederholungsschritt" existiert. Angenommen, dies wäre nicht der Fall, dann würde also die Entfernung *jeder Kante*, die mit v_k inzident ist, zu zwei Zusammenhangskomponenten führen, sodaß aber v_k kein isolierter Knoten ist. Der Graph $\mathbf{H}$ sieht dann also schematisch so aus:



Die Kreise symbolisieren hier zusammenhängende Teilgraphen von $\mathbf{H}$, nach Annahme gibt es davon mindestens zwei. Einer dieser Teilgraphen enthält daher v_0 *nicht*: Sei W seine Knotenmenge; wir betrachten nun den von $W \cup \{v_k\}$ induzierten Teilgraphen $\mathbf{K}$ von $\mathbf{H}$. Nach Konstruktion hätten alle Knoten von $\mathbf{K}$ geraden Grad, nur der einzige Knoten v_k hat ungeraden Grad (nämlich 1). Die Summe der Grade der Knoten von $\mathbf{K}$ wäre also ungerade, ein Widerspruch zu Proposition 1.4.2. □

Gegeben seien 10 Säcke (numeriert von 1 bis 10), jeder Sack enthält genau 63 äußerlich ununterscheidbare Goldmünzen. Wir wissen, daß 1 Sack lauter gefälschte Münzen enthält, alle anderen Münzen sind echt. Weiters wissen wir, daß jede echte Münze 10 Dekagramm wiegt und jede falsche 9 Dekagramm. Diesmal haben wir eine elektronische Küchenwaage gegeben (also keine Balkenwaage!), die das Gewicht aufs Gramm genau anzeigt.

Was ist hier die geringste Anzahl von Wägungen, mit der wir *in jedem Fall* die falschen Münzen identifizieren können?

1.5. Optimierung: Konstruktion von bestmöglichen Lösungen.

Für viele praktische Anwendung genügt es nicht, die *Existenz* einer Lösung nachzuweisen — entscheidend ist die konkrete Konstruktion eines Lösungsweges, der zudem möglichst *effizient* sein soll. Das folgende unterhaltungsmathematische Problem illustriert diesen Sachverhalt (daß eine Lösung dafür *existiert*, ist trivial).

Beispiel 1.5.1. *Gegeben seien 12 äußerlich völlig gleiche Münzen, wovon genau eine falsch ist. Wir wissen zwar, daß die falsche Münze ein anderes Gewicht hat als die richtige, wir wissen aber* nicht, *ob sie schwerer oder leichter ist: Die echten Münzen wiegen alle 100 Gramm, die falsche wiegt entweder 95 Gramm oder 105 Gramm. Das einzige Instrument, mit dem wir die falsche Münze identifizieren können, ist eine gewöhnliche (aber aufs Gramm genaue) Balkenwaage. Die Aufgabe besteht darin, die falsche Münze mit möglichst wenigen Wägungen zu identifizieren* und *festzustellen, ob sie schwerer oder leichter ist.*

Wenn wir die Münzen mit $1, 2, \ldots, 9, a, b, c$ *bezeichnen und den Sachverhalt "Münze x ist leichter bzw. schwerer als die anderen Münzen" mit* $\underline{x}$ *bzw.* $\overline{x}$ *notieren, dann umfaßt der "Suchraum" (also die Menge der möglichen Sachverhalte) zu Beginn 24 Elemente*

$$\underline{1}, \overline{1}, \underline{2}, \overline{2}, \ldots, \underline{c}, \overline{c}.$$

Bei jeder Wägung werden wir k Münzen in die linke und k Münzen in die reche Waagschale legen (denn andre Wägungen bringen keinerlei Informationsgewinn); die möglichen Ergebnisse der Wägung sind

- *Münzen in linker Waagschale leichter,*
- *Münzen in linker und rechter Waagschale sind gleich schwer,*
- *Münzen in linker Waagschale sind schwerer.*

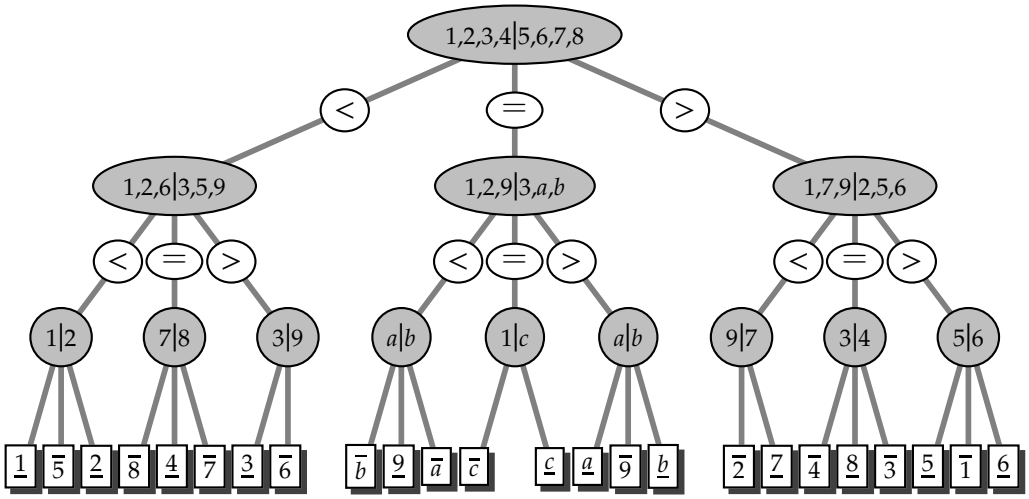
Jedes Ergebnis einer (sinnvollen) Wägung wird den Suchraum verkleinern, und wenn der Suchraum nach etlichen Wägungen nur mehr ein Element umfaßt, sind wir fertig. Wir wollen ein "System von Wägungen" konzipieren, mit dem wir in jedem Fall[4] *nach höchstens m Wägungen fertig sind, wobei m möglichst klein sein soll. Eine gute Strategie wird darin bestehen, die Wägungen so zu konzipieren, daß der jeweils noch in Frage kommende Suchraum in drei möglichst gleichgroße Teile zerfällt.*

Wenn wir z.B. für die erste Wägung die Münzen $1, 2, 3, 4$ *in die linke Waagschale legen und die Münzen* $5, 6, 7, 8$ *in die rechte, dann zerfällt der Suchraum durch die Wägung wie folgt:*

- *links leichter* $\rightarrow \left\{\underline{1}, \underline{2}, \underline{3}, \underline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\right\}$,
- *links* $=$ *rechts* $\rightarrow \left\{\overline{9}, \underline{9}, \overline{a}, \underline{a}, \overline{b}, \underline{b}, \overline{c}, \underline{c}\right\}$
- *links schwerer* $\rightarrow \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}\right\}$,

Ein System von Wägungen, mit dem man in jedem Fall nach 3 Wägungen zum Ziel kommt, ist hier in Form eines Entscheidungsbaumes *dargestellt: Ersichtlich haben wir einen speziellen Graphen vor uns, der sich von oben nach unten baumartig "verzweigt" (und zwar nach links, wenn die Münzen in der linken Waagschale leichter sind, nach rechts, wenn die Münzen in der linken Waagschale schwerer sind, und nach unten, wenn die Münzen in den Waagschalen gleich schwer sind).*

[4] Also unabhängig vom tatsächlichen Sachverhalt.



Aufgabe 12 (⋆)**:** *Gegeben seien 3 äußerlich völlig gleiche Münzen, wovon genau eine falsch ist. Wir wissen zwar, daß die falsche Münze ein anderes Gewicht hat als die richtige, wir wissen aber* nicht, *ob sie schwerer oder leichter ist. Das einzige Instrument, mit dem wir die falsche Münze identifizieren können, ist eine gewöhnliche Balkenwaage. Die Aufgabe besteht darin, die falsche Münze mit möglichst wenigen Wägungen zu identifizieren* und *festzustellen, ob sie schwerer oder leichter ist.*
Was ist hier die geringste Anzahl von Wägungen, mit der wir in jedem Fall *die falsche Münze identifizieren und feststellen können, ob sie leichter ist oder schwerer?*

Bemerkung 1.5.2. *Man kann den optimalen Algorithmus für das "allgemeine Münzwägeproblem" (für $n \geq 3$) explizit angeben: Der Beweis ist "elementar, aber kompliziert"; siehe Satz A.1.1 im Appendix.*

KAPITEL 2

Abzählende Kombinatorik

2.1. Elementares Abzählen

In diesem Kapitel behandeln wir einige grundlegende kombinatorische Objekte (Mengen, Teilmengen, geordnete n–Tupel, etc.) und ihre Abzählung.

2.1.1. Funktionen zwischen endlichen Mengen. Wir betrachten in der Folge Funktionen $f : [k] \to [n]$ und formulieren damit einfache Abzählungsfragen.

Wieviele Funktionen $f : [k] \to [n]$ gibt es?

Wir bezeichnen die Menge solcher Funktionen mit $\mathrm{abb}(k, n)$ (allgemeiner für Funktionen $f : X \to Y$, für beliebige Mengen X und Y: $\mathrm{abb}(X, Y)$).
Jede solche Funktion f kann eindeutig als (geordnetes) *k–Tupel*

$$(f(1), f(2), \ldots, f(k))$$

"codiert" werden, wobei jede Eintragung beliebige Werte aus $[n]$ annehmen kann. Die Menge aller solchen Funktionen steht also in Bijektion mit dem k–fachen cartesischen Produkt $[n]^k$, ihre Kardinalität ist also (gemäß Bijektionsregel 1.2.12 und Produktregel 1.2.14):

$$\left|\mathrm{abb}(k, n)\right| = n^k. \tag{2.1}$$

Aufgabe 13 ($\star\star$)**:** *Sei S eine Menge mit $|S| = n$. Wieviele k–Tupel*

$$(T_1, T_2, \ldots, T_k)$$

von Teilmengen von S gibt es, sodaß

$$T_1 \subseteq T_2 \subseteq \cdots \subseteq T_k \ ?$$

Wieviele injektive Funktionen $f : [k] \to [n]$ gibt es?

Wir bezeichnen die Menge solcher Funktionen mit $\mathrm{inj}(k, n)$ (allgemeiner für injektive Funktionen $f : X \to Y$, für beliebige Mengen X und Y: $\mathrm{inj}(X, Y)$).
Dazu verallgemeinern wir die Überlegung, die wir bereits in Beispiel 1.2.1 angestellt hatten: Für $f(1)$ haben wir n Möglichkeiten, für $f(2)$ bleiben dann nur mehr $n-1$ Moglichkeiten, und so fort — für $f(k)$ haben wir noch $n-k+1$ Möglichkeiten zur Auswahl. Insgesamt entspricht die gesuchte Anzahl also den *fallenden Faktoriellen*

$$\left|\mathrm{inj}(k, n)\right| = n^{\underline{k}} = n \cdot (n-1) \cdots (n-k+1) = \prod_{i=1}^{k} (n-i+1). \tag{2.2}$$

Aufgabe 14 (⋆)**:** *Wieviele Möglichkeiten gibt es, k einander nicht schlagende Türme auf einem $n \times n$ Schachbrett zu placieren?*

Der Spezialfall $k = n$ dieser Formel beantwortet die Frage:

Wieviele bijektive Funktionen $f : [n] \to [n]$ gibt es?

Solche Funktionen heißen auch *Permutationen* (von n Elementen), ihre Anzahl ist also

$$n^{\underline{n}} = n \cdot (n-1) \cdots 2 \cdot 1 = n!.$$

Aufgabe 15 (⋆ ⋆)**:** *Wieviele verschiedene Möglichkeiten gibt es, n Personen um einen runden Tisch zu setzen? (Zwei Anordnungen π und τ betrachten wir in diesem Zusammenhang als "gleich", wenn alle Personen in π denselben linken und denselben rechten Nachbarn haben wie in τ.)*

Aufgabe 16 (⋆ ⋆)**:** *Auf wieviele verschiedene Arten kann man $2n$ Personen zu n (ungeordneten) Paaren zusammenfassen? Gib alle Möglichkeiten für $n = 1, 2, 3$ explizit an.*

Aufgabe 17 (⋆ ⋆)**:** *An einem Bridgeturnier nehmen $4n$ Spieler teil, und das Turnier findet an n Tischen statt. Jeder Spieler benötigt einen anderen Spieler als Partner, und jedes Paar von Partnern benötigt ein anderes Paar als Gegner. Auf wieviele Arten kann die Wahl von Partner und Gegner erfolgen?*

Aufgabe 18 (⋆ ⋆)**:** *Auf wieviele Arten können wir die Zahlen $1, 2, \ldots, n$ anordnen, sodaß — abgesehen vom ersten Element — die Zahl k nur dann placiert werden kann, falls $k-1$ oder $k+1$ bereits placiert wurden (also links von k stehen)? (Zum Beispiel für $n = 6$: 3 2 4 5 1 6 oder 4 3 5 2 1 6.)*

Man beachte, daß Formel (2.2) auch den richtigen Wert (nämlich 0) liefert für den Fall, daß $k > n$ ist — denn dann gibt es natürlich keine injektiven Funktionen, eine Tatsache, die unter der Bezeichnung *Schubfachprinzip* bekannt ist:

GRUNDREGEL 2.1.1. **(Schubfachprinzip)**

Wenn man k Elemente auf n Fächer verteilt, wobei $k > n$, dann gibt es mindestens ein Fach, das zwei *Elemente enthält.*

Aufgabe 19 (⋆)**:** *Zeige folgende Verschärfung des Schubfachprinzips:*

Sei $f : [k] \to [n]$ mit $k > n$, dann gibt es ein Element $m \in [n]$, für das gilt:

$$\left|f^{-1}(m)\right| \geq \left\lfloor \frac{k-1}{n} \right\rfloor + 1.$$

2.1.1.1. *Die Stirling–Zahlen der zweiten Art.* Die nächste naheliegende Frage erfordert ein bißchen Vorarbeit:

DEFINITION 2.1.2. *Die Anzahl aller Partitionen von $[n]$ mit k Blöcken heißt* Stirling–Zahl der zweiten Art, *wir bezeichnen sie mit $S_{n,k}$.*

Zum Beispiel ist:

$$\begin{aligned} S_{n,k} &= 0 \quad \text{für } k > n, \\ S_{n,0} &= [n = 0], \\ S_{n,1} &= 1, \\ S_{n,2} &= 2^{n-1} - 1, \\ S_{n,n} &= 1, \\ S_{n,n-1} &= \binom{n}{2}. \end{aligned}$$

Hier haben wir *Iversons Notation* eingeführt:

$$[\text{eine Aussage } A] := \begin{cases} 1 & \text{wenn Aussage } A \text{ wahr ist,} \\ 0 & \text{wenn Aussage } A \text{ falsch ist.} \end{cases}$$

(Das ist eine Verallgemeinerung des bekannten *Kronecker–Delta*: $\delta_{x,y} := [x = y]$.)
Wir verschieben eine genauere Betrachtung der Stirling–Zahlen zweiter Art zunächst und wenden uns der Frage zu:

Wieviele surjektive Funktionen $f : [k] \to [n]$ gibt es?

Wir bezeichnen die Menge solcher Funktionen mit $\operatorname{surj}(k, n)$ (allgemeiner für surjektive Funktionen $f : X \to Y$, für beliebige Mengen X und Y: $\operatorname{surj}(X, Y)$).

Eine Funktion f ist surjektiv, wenn alle Urbilder $f^{-1}(1), \ldots, f^{-1}(n)$ nicht–leer sind: Sie bilden also eine *Partition* von $[k]$ mit n Blöcken. Umgekehrt liefert *jede* Partition von k mit n Blöcken genau $n!$ verschiedene surjektive Funktionen; wir erhalten also (wenn man will: nach der Regel von der doppelten Abzählung 1.2.2):

$$\left|\operatorname{surj}(k, n)\right| = n! \cdot S_{k,n}. \tag{2.3}$$

Jede Funktion $f \in \operatorname{abb}(k, n)$ hat ein eindeutiges *Bild* $Y = f([k]) \subseteq [n]$ und ist "surjektiv aufs Bild Y" (d.h., wenn man f als Funktion $[k] \to Y$ auffaßt, dann ist diese Funktion natürlich surjektiv). Wenn wir die Menge $\operatorname{abb}(k, n)$ *aller* Funktionen nach den jeweiligen Bildern Y partitionieren, dann liefert eine direkte Anwendung der Summenregel folgenden interessanten Zusammenhang:

$$\begin{aligned} n^k = \left|\operatorname{abb}(k, n)\right| &= \sum_{Y \subseteq [n]} \left|\operatorname{surj}([k], Y)\right| \\ &= \sum_{i=0}^{n} \sum_{|Y|=i} \left|\operatorname{surj}([k], Y)\right| \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot i! \cdot S_{k,i} \\ &= \sum_{i=0}^{k} S_{k,i} \cdot n^{\underline{i}}. \end{aligned}$$

In der letzen Zeile haben wir den oberen Summationsindex n durch k ersetzt wegen $S_{k,i} = 0$ für $i > k$: Denn natürlich ist $\left|\text{surj}\,(k,i)\right| = 0$ für $i > k$.

Für beliebiges, aber *festes* k sind sowohl x^k also auch $x^{\underline{k}} = \prod_{i=0}^{k-1}(x-i)$ *Polynome* in x. Die Rechnung, die wir soeben durchgeführt haben, besagt also:

$$x^k = \sum_{i=0}^{k} S_{k,i} \cdot x^{\underline{i}} \tag{2.4}$$

ist richtig für alle $n \in \mathbb{N}$. Ein bekannter Satz aus der Algebra besagt:

GRUNDREGEL 2.1.3. **(Polynomargument)**

Wenn zwei Polynome p und q über $\mathbb{C}$ vom Grad $\leq k$ an mehr als k verschiedenen Stellen übereinstimmen, dann sind sie überhaupt identisch; insbesondere also

$$\forall n \in \mathbb{N} : p(n) = q(n) \implies p \equiv q.$$

Gleichung (2.4) ist also eine *Polynomidentität*! Wir können sie mit den Begriffen der Linearen Algebra wie folgt deuten: Bekanntlich bilden die Polynome mit komplexen Koeffizienten einen (unendlichdimensionalen) Vektorraum über dem Körper $\mathbb{C}$. In diesem Vektorraum bilden sowohl die Polynome $(x^n)_{n=0}^{\infty}$ als auch die Polynome $(x^{\underline{n}})_{n=0}^{\infty}$ eine Basis. Gleichung (2.4) besagt, daß die entsprechende Basistransformation durch die Stirling–Zahlen der zweiten Art beschrieben wird.

2.1.2. Teilmengen und Multimengen; Kompositionen. Die folgende Frage wiederholen wir der Vollständigkeit halber — wir haben sie bereits in der Einleitung behandelt:

Wieviele k–elementige Teilmengen von $[n]$ gibt es?

Die Antwort lautet bekanntlich $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{(n-k)!k!}$. Wir bemerken, daß wir den Binomialkoeffizienten für jedes feste k auch als Polynom auffassen können: $\binom{x}{k} = \frac{x^{\underline{k}}}{k!}$. Eine weitere Anwendung des Polynomarguments 2.1.3 liefert die folgende wichtige Identität:

SATZ 2.1.4 (Chu–Vandermonde Identität).

$$\binom{x+y}{k} = \sum_{l=0}^{k} \binom{x}{l}\binom{y}{k-l}. \tag{2.5}$$

BEWEIS. Wir zeigen "nur", daß dies immer richtig ist, wenn man für die Variablen x und y natürliche Zahlen m und n einsetzt: Auf der linken Seite steht die Anzahl aller k-elementigen Teilmengen von $[m+n]$. Die Familie dieser Teilmengen partitionieren wir danach, wieviele ihrer k Elemente in $[m]$ (sei l diese Anzahl) und wieviele im Rest $[m+n] \setminus [m]$ enthalten sind (das müssen dann

$k-l$ sein): Der entsprechende Block der Partition enthält $\binom{m}{l} \cdot \binom{n}{k-l}$ Teilmengen, und aus der Summenregel 1.2.8 folgt die Behauptung.

Daß es sich tatsächlich um eine Polynomidentität handelt, folgt aus dem Polynomargument[1]. □

Bemerkung 2.1.5. *Da zwei Polynome genau dann gleich sind, wenn alle ihre Koeffizienten identisch sind, können wir die Identität* (2.5) *für* $x, y \in \mathbb{N}$ *auch durch* Koeffizientenvergleich *aus der simplen Polynomidentität*

$$(1+z)^{x+y} = (1+z)^x (1+z)^y$$

ableiten.

Definition 2.1.6. *Sei X eine Menge. Eine* Multimenge[2] *von X ist, salopp gesprochen, eine Ansammlung von Elementen aus X, wobei aber Elemente* mehrfach *vorkommen können. Mathematisch exakt kann man das definieren, indem man den Begriff der* charakteristischen Funktion χ *erweitert: Eine Multimenge M von X wird beschrieben durch ihre charakteristische Funktion* $\chi_M : X \to \mathbb{Z}^+$ *($\mathbb{Z}^+$ bezeichnet die Menge der nichtnegativen ganzen Zahlen),*

$$\chi_M(i) := \textit{ Anzahl der Vorkommnisse von Element i in M.}$$

$\chi_M(i)$ *nennt man auch die* Vielfachheit *von i in M.*

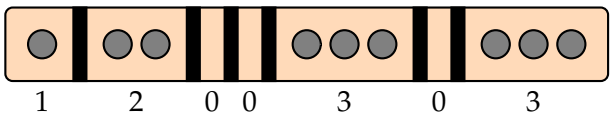
Beispiel 2.1.7. *Wenn wir z.B. die Menge* $[7]$ *betrachten, dann wäre*

$$M = \{1,2,2,5,5,5,7,7,7\}$$

eine 9–elementige Multimenge von $[7]$*. Die charakteristische Funktion (dargestellt als 7–Tupel) von M ist dann* $(1,2,0,0,3,0,3)$*.*

Wieviele k–elementige Multimengen von $[n]$ gibt es?

Betrachten wir nochmals Beispiel 2.1.7. Die charakteristische Funktion $\chi_M = (1,2,0,0,3,0,3)$ von $M = \{1,2,2,5,5,5,7,7,7\}$ könnten wir auch so "kodieren":



Wir sehen: Die charakteristische Funktion *jeder* 9–elementigen Multimenge von $[7]$ kann *bijektiv* interpretiert werden als "Konfiguration" von 9 "Kugerln" und $7-1=6$ "Trennstrichen". Jede solche "Konfiguration" denken wir uns wiederum so: Von $9+7-1=15$ "Positionen" wählen wir 9 aus, die wir mit "Kugerln" besetzen, die restlichen besetzen wir mit "Trennstrichen". Wenn wir diese Beobachtung verallgemeinern, erhalten wir also mit der Bijektionsregel: Die Anzahl

[1] Ganz genau betrachtet, müssen wir das Polynomargument hier zweimal anwenden, für die zwei Variablen x und y.

[2] Eigentlich müßte man "Multi–Teilmenge" sagen, aber das ist ein unhandliches Wortungetüm.

der k–elementigen Multimengen einer n–elementigen Menge ist gleich der Anzahl der k–elementigen Teilmengen einer $k+(n-1)$–elementigen Menge von Objekten; die gesuchte Anzahl ist also

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

Wenn wir den Binomialkoeffizienten als Polynom $\frac{x^{\underline{k}}}{k!}$ auffassen, können wir für x insbesondere auch negative Zahlen einsetzen und das Ergebnis so schreiben:

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

DEFINITION 2.1.8. *Eine Komposition von n ist eine Darstellung von n als Summe natürlicher Zahlen*

$$n=a_1+a_2+\cdots+a_k,$$

wobei es auf die Reihenfolge *der Summanden ankommt (es sind also z.B. $10=3+2+5$ und $10=5+2+3$ zwei* verschiedene *Kompositionen von 10).*

BEISPIEL 2.1.9. *Es gibt insgesamt 8 Kompositionen von $n=4$:*

$$4,\ 3+1,\ 1+3,\ 2+1+1,\ 1+2+1,\ 1+1+2,\ 2+2,\ 1+1+1+1.$$

BEMERKUNG 2.1.10. *Kompositionen von n, "bei denen es* nicht *auf die Reihenfolge der Summanden ankommt", nennt man (Zahl–)Partitionen von n . Daher nennt man Kompositionen manchmal auch* geordnete (Zahl–)Partitionen.

Wieviele Kompositionen von n mit genau k Summanden gibt es?

"Umkehrabbildung" von "Partialsummen bilden" ist "Differenzen bilden"!

Wir lösen diese Abzählungsfrage bijektiv: Jeder Komposition $n=a_1+a_2+\cdots+a_k$ von n mit k Summanden ordnen wir die Menge ihrer ersten $k-1$ Partialsummen zu, also

$$a_1+a_2+\cdots+a_k\mapsto\{a_1,a_1+a_2,\ldots,a_1+a_2+\cdots+a_{k-1}\}.$$

Diese Menge ist eine $(k-1)$–elementige Teilmenge von $[n-1]$, denn $a_1+a_2+\cdots+a_{k-1}=n-a_k<n$. Die Bijektionsregel liefert also die Antwort auf unsere Abzählungsfrage für $(n\geq k>0)$:

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

(Für $n=k=0$ gibt es "definitionsgemäß" genau eine Komposition.)

Die Antwort auf die folgende Frage gelingt nun ganz leicht (entweder bijektiv oder unter Verwendung der Summenregel):

Wieviele Kompositionen von n gibt es insgesamt?

$$\begin{cases}1 & \text{für } n=0,\\ 2^{n-1} & \text{für } n>0\end{cases}.$$

Aufgabe 20 (⋆ ⋆)**:** *Sei* $1 \leq k < n$*. Zeige, daß unter allen* 2^{n-1} *Kompositionen von* n *der Teil* k *genau* $(n-k+3)2^{n-k-2}$ *mal auftritt. Nimmt man zum Beispiel* $n = 4$ *und* $k = 2$*, dann tritt 2 in* $2+1+1, 1+2+1, 1+1+2$ *je einmal, in* $2+2$ *zweimal auf, also insgesamt* 5*–mal.*

2.1.3. Permutationen.

Definition 2.1.11. *Sei* X *eine endliche Menge: Eine* Permutation *von* X *ist eine beliebige* Anordnung *der Elemente dieser Menge. Dies ist sichtlich äquivalent zu unserer früheren Definition (in Abschnitt 2.1.1): Eine Permutation ist eine* Bijektion $X \to X$*.*

Wir werden in der Regel Permutationen von $[n]$ betrachten und diese meist in einzeiliger Notation

$$a_1\, a_2 \ldots a_n$$

anschreiben. Wenn wir den Aspekt der *Bijektion* $[n] \to [n]$ hervorheben wollen, dann verwenden wir die zweizeilige Notation

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

Beispiel 2.1.12. *Für* $n = 5$ *ist z.B.* 2 1 4 5 3 *eine Permutation, die in zweizeiliger Notation so aussieht:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

Alle *Permutationen von* $[3]$ *sind (in* lexikographischer Ordnung[3]*):*

$$1\,2\,3,\quad 1\,3\,2,\quad 2\,1\,3,\quad 2\,3\,1,\quad 3\,1\,2,\quad 3\,2\,1.$$

Definition 2.1.13. *Wenn wir die Permutationen als Bijektionen von* $[n]$ *sehen, dann ist eine natürliche Verknüpfung durch Hintereinanderausführung von zwei Permutationen* π_1, π_2 *definiert:*

$$(\pi_1 \circ \pi_2)\,(i) := \pi_1\,(\pi_2\,(i))\,.$$

(Aus Bequemlichkeit werden wir das Verknüpfungssymbol "$\circ$*" in der Folge oft weglassen und einfach* $\pi_1\pi_2$ *schreiben.)*

Also NICHT die umgedrehte Notation $(\pi_1\pi_2)\,(i) = \pi_2\,(\pi_1\,(i))$!!

Es ist wohlbekannt (und leicht nachzuprüfen), daß die Permutationen von $[n]$ *bezüglich dieser Verknüpfung eine (nichtkommutative) Gruppe bilden, die sogenannten* symmetrische Gruppe*; wir bezeichnen sie mit* $\mathfrak{S}_n$*. Ihr Einheitselement ist die* identische Permutation ϵ*, die alle Elemente* i *auf sich selbst abbildet:* $\epsilon\,(i) = i$ *für* $i = 1, \ldots, n$ *(*$\epsilon \in \mathfrak{S}_n$ *hat also* n *Fixpunkte.)*

Aus Abschnitt 2.1.1 wissen wir bereits:

$$|\mathfrak{S}_n| = n!.$$

Aufgabe 21 (⋆ ⋆)**:** *Finde eine möglichst einfache Methode, um die* k*–te Permutation der* $\mathfrak{S}_n$ in lexikographischer Ordnung *zu finden. (Die "triviale Methode" — erzeuge alle* $n!$ *Permutationen der* $\mathfrak{S}_n$*, ordne sie lexikographisch und wähle das* k*–te Element — gilt hier natürlich* nicht *als "einfach".)*

[3] Das ist die übliche "alphabetische" Ordnung in einem Lexikon (oder Telephonbuch) — nur besteht unser Alphabet hier aus Zahlen.

Aufgabe 22 (⋆ ⋆)**:** *Zeige: Jede natürliche Zahl n besitzt eine (bis auf führende Nullen) eindeutig bestimmte Darstellung der Form*

$$n = a_1 \cdot 1! + a_2 \cdot 2! + \cdots + a_k \cdot k!, \quad \text{mit } 0 \leq a_i \leq i.$$

Ist k die größte Zahl mit $a_k \neq 0$, so schreibt man $n = (a_1, a_2, \ldots, a_k)$.
Finde eine möglichst einfache Methode zur Berechnung der Ziffern a_i und berechne die Darstellung von 1,000.000. Wie erkennt man an den Ziffern, daß $(a_1, \ldots, a_k) < (b_1, \ldots, b_l)$ gilt?

Aufgabe 23 (⋆)**:** *Die größte Zahl, die sich in der Darstellung aus Aufgabe 22 mit n Ziffern schreiben läßt, ist einerseits $(1, 2, 3, \ldots, n)$ und andererseits $(n+1)! - 1$. Daher gilt*

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1.$$

Finde einen einfacheren Beweis für diese Formel!

2.1.3.1. *Disjunkte Zyklenzerlegung von Permutationen.* Eine andere Art, Permutationen zu notieren, ist die *disjunkte Zyklenzerlegung*.

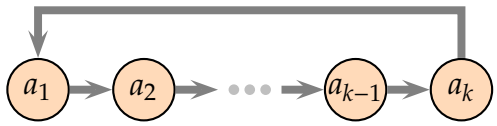
Definition 2.1.14. *Eine* zyklische Permutation *(kurz: ein* Zyklus*) der Länge k ist eine Permutation der Gestalt*

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ a_2 & a_3 & \ldots & a_k & a_1 \end{pmatrix}.$$

Wir werden dafür in der Folge die kürzere Notation $(a_1\ a_2\ \ldots\ a_k)$ benutzen.
Ein Zyklus der Länge 1 heißt ein Fixpunkt.

Zyklus: Kreis.

Die Bezeichnung "Zyklus" wird klar, wenn man sich die zyklische Permutation π als Bijektion vorstellt — in der folgenden Graphik wird die Abbildung π durch kleine Pfeile symbolisiert:



Für *jede* Permutation $\pi \in \mathfrak{S}_n$ gehört *jedes* $i \in [n]$ zu einem *eindeutig bestimmten* Zyklus. Denn die Folge

$$i, \pi(i), \pi^2(i) := \pi(\pi(i)), \pi^3(i), \ldots$$

muß sich einmal wiederholen — es gibt also ein minimales k mit $\pi^k(i) = i$. Wenn wir π auf die Menge

$$S := \left\{ i, \pi(i), \pi^2(i), \ldots, \pi^{k-1}(i) \right\}$$

einschränken, so haben wir sichtlich eine zyklische Permutation von S vor uns. Aus dieser "Konstruktion" der Zyklen kann niemals ein Zyklus der Länge 0 entstehen (außer evtl. im wenig interessanten Fall $\mathfrak{S}_0$; der Gruppe der Bijektionen der leeren Menge). Zwei *verschiedene* Zyklen π_i und π_j können wir als Permutationen von *disjunkten* Teilmengen X_1 und X_2 von $[n]$ auffassen. *Daher* kommutieren π_1 und π_2, wenn wir sie als Permutationen in $\mathfrak{S}_n$ auffassen, die alle Elemente in $[n] \setminus X_1$ bzw. in $[n] \setminus X_2$ *fixieren* (d.h., $\pi_1(x) = x$ für alle $x \notin X_1$ bzw. $\pi_2(x) = x$ für alle $x \notin X_2$):

$$\pi_1 \circ \pi_2 = \pi_2 \circ \pi_1.$$

Zusammenfassend:

KOROLLAR 2.1.15. *Sei $n \in \mathbb{N}$. Jede Permutation $\pi \in \mathfrak{S}_n$ läßt sich* eindeutig *(bis auf die Reihenfolge) in* paarweise disjunkte *(und daher* paarweise kommutierende*) Zyklen $\pi_1, \pi_2, \dots \pi_k$ zerlegen, d.h.:*

- *Jede Zahl $i \in [n]$ gehört genau einem Zyklus an,*
- *Jeder Zyklus π_i hat Länge ≥ 1,*
- *Zwei verschiedene Zyklen π_i, π_j haben kein Element gemeinsam,*
- $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_k$.

DEFINITION 2.1.16. *Die Zerlegung einer Permutation π in ihre Zyklen entsprechend Korollar 2.1.15 nennen wir die* Zyklenzerlegung *von π.*

BEISPIEL 2.1.17. *Die folgende Permutation "zerfällt" in die Zyklen:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 1 & 6 & 5 & 4 & 2 & 9 & 8 \end{pmatrix} = (1\,7\,2\,3)\,(4\,6)\,(5)\,(8\,9).$$

Die Permutation hat einen Fixpunkt, nämlich (5).

2.1.3.2. *Stirling–Zahlen der ersten Art.* Die Eigenschaften einer Zyklenzerlegung haben eine starke formale Ähnlichkeit mit den Eigenschaften einer Partition. Wir stellen eine ähnliche Frage wie bei den Partitionen:

Wieviele Permutationen in $\mathfrak{S}_n$ mit k Zyklen gibt es?

Wir bezeichnen diese Anzahl mit $c(n,k)$. Einige spezielle Werte können wir sofort angeben:

$$\begin{aligned} c(n,k) &= 0 \quad \text{für } k > n, \\ c(n,0) &= [n=0], \\ c(n,n) &= 1, \\ c(n,1) &= (n-1)!. \end{aligned}$$

Um das Abzählproblem zu lösen, leiten wir zunächst einmal eine *Rekursion* her:

$$c(n,k) = c(n-1,k-1) + (n-1)c(n-1,k). \tag{2.6}$$

Dies ergibt sich aus der Summenregel, denn die Menge *aller* Zyklenzerlegungen von $[n]$ mit k Zyklen zerfällt in zwei disjunkte Teilmengen, nämlich

- Jene Zyklenzerlegungen, bei denen (n) einen eigenen Zyklus bildet (also einen Fixpunkt darstellt),
- und jene Zyklenzerlegungen, bei denen (n) keinen eigenen Zyklus bildet.

Im ersten Fall können wir den Zyklus (n) weglassen und erhalten eine Zyklenzerlegung von $[n-1]$ in $(k-1)$ Zyklen — die Anzahl dieser Zerlegungen ist $c\,(n-1,k-1)$.
Im zweiten Fall können wir das Element n aus seinem Zyklus entfernen: Übrig bleibt eine Zerlegung von $[n-1]$ in k Zyklen — die Anzahl dieser Zyklenzerlegungen ist $c\,(n-1,k)$; und aus *jeder* solchen Zyklenzerlegung können wir $(n-1)$ verschiedene Zyklenzerlegungen von $[n]$ machen, indem wir das Element n hinter eines der vorhandenen $(n-1)$ Elemente "dazustecken". Insgesamt sehen wir: Die Anzahl der Permutationen im zweiten Fall ist $(n-1)\cdot c\,(n-1,k)$.

Im nächsten Schritt gewinnen wir aus der Rekursion (2.6) eine Gleichung für erzeugende Funktionen. Dazu führen wir für eine Permutation $\pi \in \mathfrak{S}_n$ das Gewicht $\omega(\pi) := x^{\text{Anzahl der Zyklen von } \pi}$ ein und betrachten:

$$\mathcal{GF}(\mathfrak{S}_n) := \sum_{\pi \in \mathfrak{S}_n} \omega(\pi) = \sum_{k=0}^{n} c(n,k)\, x^k. \tag{2.7}$$

Wenn wir beide Seiten der Rekursion (2.6) mit x^k multiplizieren und über alle k von 0 bis n summieren, erhalten wir die Gleichung

$$\mathcal{GF}(\mathfrak{S}_n) = (x+n-1)\,\mathcal{GF}(\mathfrak{S}_{n-1}).$$

Diese einfache Rekursion ist durch *Iteration* ganz leicht zu lösen: Mit der offensichtlichen Anfangsbedingung $\mathcal{GF}(\mathfrak{S}_1) = x$ (oder $\mathcal{GF}(\mathfrak{S}_0) = 1$) erhalten wir

$$\mathcal{GF}(\mathfrak{S}_n) = (x+n-1)(x+n-2)\cdots x. \tag{2.8}$$

Das Produkt auf der rechten Seite nennt man *steigende Faktorielle*; wir verwenden hier die Notation

$$x^{\overline{k}} := x(x+1)\cdots(x+k-1) = \prod_{i=1}^{k}(x+i-1).$$

Für die steigenden Faktoriellen wird sehr häufig die Notation $(x)_k$ verwendet, das sogenannte *Pochhammer–Symbol*. Setzt man in (2.8) $x = 1$, dann kommt (natürlich) gerade $k!$ heraus.

Wir sehen also: Die gesuchten Zahlen treten als Koeffizienten auf, wenn wir das Polynom $x(x+1)\cdots(x+n-1)$ ausmultiplizieren, oder vornehmer ausgedrückt: In der Basis $(x^n)_{n=0}^{\infty}$ entwickeln.

$$x(x+1)\cdots(x+n-1) = \sum_{k=0}^{n} c(n,k)\, x^k.$$

Wenn wir hier x durch $-x$ ersetzen und beide Seiten mit $(-1)^n$ multiplizieren, erhalten wir

$$\sum_{k=0}^{n}(-1)^{n-k}c(n,k)x^k = x(x-1)\cdots(x-n+1) = x^{\underline{n}}. \tag{2.9}$$

(Denn es gilt ganz allgemein $x^{\overline{k}} = (-1)^k(-x)^{\underline{k}}$.)

Definition 2.1.18. *Die in* (2.9) *auftretenden Koeffizienten* $(-1)^{n-k}c(n,k)$ *werden* Stirling–Zahlen der ersten Art *genannt und meist mit* $s_{n,k}$ *bezeichnet*[4].

[4] Die Koeffizienten $c(n,k)$ werden manchmal die vorzeichenlosen Stirling–Zahlen der ersten Art genannt.

Betrachten wir nun diese Gleichung (mit der neuen Notation) zusammen mit der Gleichung (2.4) für die Stirling–Zahlen der zweiten Art:

$$x^{\underline{n}} = \sum_{k=0}^{n} s_{n,k} x^k, \tag{2.10}$$

$$x^n = \sum_{k=0}^{n} S_{n,k}\, x^{\underline{k}}. \tag{2.11}$$

Wir erkennen die enge Beziehung der Stirling–Zahlen erster und zweiter Art: Die Stirling–Zahlen *zweiter Art* treten auf, wenn wir die Basis $(x^n)_{n=0}^{\infty}$ des Vektorraums aller Polynome in der Basis $(x^{\underline{n}})_{n=0}^{\infty}$ entwickeln, und die Stirling–Zahlen *erster Art* treten auf, wenn wir das Umgekehrte tun! In den Begriffen der Linearen Algebra haben wir es mit einer Basistransformation und ihrer Inversen zu tun, konkret bedeutet dies, daß die entsprechenden Koeffizientenmatrizen $\left(S_{n,k}\right)_{n,k\geq 0}$ und $\left(s_{k,l}\right)_{k,l\geq 0}$ invers sind.
Diese Tatsache sehen wir auch rechnerisch, wenn wir die Formel (2.10) für die fallenden Faktoriellen in der Formel (2.11) einsetzen

$$x^n = \sum_{k=0}^{n} S_{n,k} \sum_{l=0}^{k} s_{k,l} x^l$$

und den Koeffizienten von x^l vergleichen:

$$\sum_{k=0}^{n} S_{n,k} s_{k,l} = [n = l]\,.$$

2.1.3.3. *Inversionen und Signum von Permutationen.*

Definition 2.1.19. *Eine* Inversion einer Permutation $\pi \in \mathfrak{S}_n$ *ist ein Paar* (i, j) *mit* $i < j$ *und* $\pi(i) > \pi(j)$.
Die Anzahl aller Inversionen von π *wird mit* $\operatorname{inv}\pi$ *bezeichnet.*

Beispiel 2.1.20. *Wir betrachten die Permutation*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 1 & 5 & 2 & 4 & 6 & 7 \end{pmatrix} \begin{matrix} \text{“Positionen” } i \\ \text{“Zahlen” } \pi(i) \end{matrix}$$

der $\mathfrak{S}_8$. *Die Inversionen von* π *sind die “Paare von Positionen, wo Zahlen in der falschen Reihenfolge erscheinen”, also*

$$(1,3),\ (1,5),\ (2,3),\ (2,4),\ (2,5), (2,6),\ (2,7),\ (2,8),\ (4,5),\ (4,6).$$

Aufgabe 24 ($\star\star$)**:** *Zeige: Für alle* $n \in \mathbb{N}$ *und jede Permutation* $\pi \in \mathfrak{S}_n$ *gilt stets:*

$$\operatorname{inv}\pi = \operatorname{inv}\pi^{-1}.$$

Wir wollen nun die erzeugende Funktionen der $\mathfrak{S}_n$ in bezug auf die Gewichtsfunktion $\omega(\pi) := q^{\operatorname{inv}\pi}$ bestimmen. “By abuse of notation” verwenden wir dieselbe Notation wie in (2.7) und schreiben also

$$\mathcal{GF}(\mathfrak{S}_n) = \sum_{\pi\in S_n} q^{\operatorname{inv}\pi}.$$

Es ist leicht zu sehen, daß diese erzeugende Funktion ein Polynom in q vom Grad $\binom{n}{2}$ ist, denn $\max_{\pi\in\mathfrak{S}_n}(\operatorname{inv}\pi) = 1+2+\cdots+(n-1) = \binom{n}{2}$.

BEISPIEL 2.1.21. *Betrachten wir den Fall $n = 2$:*

$$\sum_{\pi\in S_2} q^{\operatorname{inv}\pi} = q^{\operatorname{inv}(12)} + q^{\operatorname{inv}(21)} = q^0 + q^1 = 1+q.$$

Im Fall $n = 3$ ergibt sich aus der Tabelle

π	$\operatorname{inv}\pi$	π	$\operatorname{inv}\pi$
123	0	231	2
132	1	312	2
213	1	321	3

die erzeugende Funktion

$$\sum_{\pi\in S_3} q^{\operatorname{inv}\pi} = 1+2q+2q^2+q^3 = (1+q)(1+q+q^2).$$

Wir erraten daraus die allgemeine Formel

$$\mathcal{GF}(\mathfrak{S}_n) = \sum_{\pi\in\mathfrak{S}_n} q^{\operatorname{inv}\pi} = (1+q)(1+q+q^2)\cdots(1+q+\cdots+q^{n-1}), \qquad (2.12)$$

die wir mit Induktion nach n nachweisen. Für den Induktionsschritt genügt es, die folgende Rekursion zu zeigen:

$$\mathcal{GF}(\mathfrak{S}_n) = (q^{n-1}+q^{n-2}+\cdots+q+1)\cdot\mathcal{GF}(\mathfrak{S}_{n-1}).$$

Dazu überlegen wir, daß das Element n in einer Permutation π genau dann $n-i$ zur Anzahl der Inversionen beiträgt, wenn es in π an Position i steht. Umgekehrt: Wenn wir in eine Permutation $\tau\in\mathfrak{S}_{n-1}$ das Element n an Stelle i ($i = 1,\ldots,n$) einfügen, dann erhalten wir eine Permutation in $\mathfrak{S}_n$ mit $\operatorname{inv}\tau + n - i$ Inversionen, also mit dem Gewicht $q^{\operatorname{inv}\tau}q^{n-i}$. Damit ist die Behauptung gezeigt. (2.12) reduziert sich für $q = 1$ (natürlich) auf die Aussage, daß es $n!$ Permutationen in $\mathfrak{S}_n$ gibt.

Aufgabe 25 ($\star\star$)**:** *Für verschiedene Zwecke benötigt man eine Durchnumerierung aller Permutationen von $[n]$, sodaß man π_k sofort angeben kann, ohne vorher die anderen Permutationen zu konstruieren.*

In Aufgabe 21 war die Durchnumerierung der Permutationen durch die lexikographische Ordnung gegeben; eine weitere Möglichkeit besteht im Abzählen der Inversionen: Sei π eine Permutation von $[n]$. Sei a_i die Anzahl der Inversionen (k,l) mit $\pi(l) = n-i$ für $i = 1,2,\ldots,n-1$. Zum Beispiel ist für $n = 7$, $\pi = 5\ 3\ 7\ 2\ 1\ 6\ 4$ die entsprechende Folge durch $(a_1,a_2,\ldots,a_6) = (1,0,3,1,3,4)$ gegeben.

Zeige: Es gilt $0 \le a_i \le i$, $i = 1,2,\ldots,n-1$.

Jede solche Folge, kurz Inversionsfolge genannt, definiert eine eindeutig bestimmte Permutation π. Man kann also jeder Zahl k mit $0 \le k \le n!-1$ eine eindeutig bestimmte Permutation π zuordnen: Schreibe einfach k in der Gestalt

$$k = a_1\cdot 1! + a_2\cdot 2! + \cdots + a_{n-1}\cdot(n-1)!$$

(siehe Aufgabe 22) und interpretiere $(a_1,a_2,\ldots,a_{n-1})$ als Inversionsfolge.

Finde eine möglichst einfache Methode, um aus der Inversionsfolge die Permutation π zu konstruieren.

Bemerkung 2.1.22 (Delta–Operator). *Aus der Linearen Algebra wissen wir, daß die Menge aller Polynome mit reellen (oder komplexen oder rationalen) Koeffizienten ein Vektorraum über* $\mathbb{R}$ *(oder über* $\mathbb{C}$ *oder über* $\mathbb{Q}$*) ist (mit den "normalen" Operationen Addition und Skalarmultiplikation).*
Auf diesem Vektorraum ist (natürlich) die Identität $\mathbf{I}$

$$(\mathbf{I}(p))(x) := p(x)$$

ein (invertierbarer) linearer Operator, ebenso auch der Verschiebungsoperator $\mathbf{E}$

$$(\mathbf{E}(p))(x) := p(x+1),$$

dessen inverser Operator (natürlich) durch

$$\left(\mathbf{E}^{-1}(p)\right)(x) := p(x-1)$$

gegeben ist.
Die Differenz dieser Operatoren

$$\mathbf{\Delta} = \mathbf{E} - \mathbf{I}$$

hat eine nützliche Eigenschaft: Die fallenden Faktoriellen $x^{\underline{k}}$ *bilden eine Basis für den Vektorraum aller Polynome, und die Wirkung von* $\mathbf{\Delta}$ *auf diese Basis sieht der Wirkung des* Differentialoperators *auf die Standardbasis* x^n *zum Verwechseln ähnlich. Eine einfache Rechnung zeigt nämlich, daß*

$$\mathbf{\Delta} x^{\underline{n}} = n \cdot x^{\underline{n-1}}.$$

Aufgabe 26 (⋆ ⋆ ⋆)**:** *Sei* $I(n,k)$ *die Anzahl der Permutationen* $\pi \in \mathfrak{S}_n$ *mit* k *Inversionen (*$I(n,k) = 0$ *für* $k < 0$*).*

(1) *Zeige, daß*

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

gilt.

(2) *Folgere mittels der obigen Rekursion, daß die Zahl* $I(n,k)$ *ein Polynom in* n *vom Grad* k *und führendem Koeffizienten* $1/k!$ *ist. Für* $n \geq 2$ *gilt beispielsweise* $I(n,2) = \frac{1}{2}(n+1)(n-2)$*. Berechne das Polynom für* $I(n,3)$*. (Hinweis: Induktion nach* k *unter Verwendung von Bemerkung 2.1.22!)*

Definition 2.1.23. *Ein Zyklus einer Permutation* $\pi \in \mathfrak{S}_n$ *der Länge* 2 *heißt* Transposition*: Eine Transposition* vertauscht *also genau zwei Elemente.*
Einen beliebigen Zyklus $(i_1, \ldots, i_k)$ *einer Permutation* $\pi \in \mathfrak{S}_n$ *können wir, wie gesagt, selbst als Permutation* σ *in* $\mathfrak{S}_n$ *auffassen, wenn wir uns denken, daß* σ *alle anderen Elemente (außer* $i_1, \ldots, i_k$*) fixiert. So gesehen ist also jede Transposition* $\tau = (i,j) \in \mathfrak{S}_n$ *eine* Involution *(also eine selbstinverse Permutation) in* $\mathfrak{S}_n$*, d.h.,* $\tau^{-1} = \tau$*.*
Eine Transposition heißt kanonisch*, wenn es eine Transposition der Form* $(i, i+1)$ *ist,* $i = 1, \ldots, n-1$*, also wenn zwei* aufeinanderfolgende *Elemente vertauscht werden.*

Bemerkung 2.1.24. *Sei* $\pi = (\pi_1, \ldots, \pi_n) \in \mathfrak{S}_n$*. Dann sieht man sofort*

$$\pi \circ (i, i+1) = (\pi_i, \pi_{i+1}) \circ \pi,$$

d.h., die "Rechtsmultiplikation" mit der kanonischen Permutation $(i, i+1)$ *bewirkt eine Vertauschung der* nebeneinander stehenden *Elemente* (π_i, π_{i+1}) *in der Permutation* π*. Daraus erkennt man sofort*

$$\operatorname{inv}(\pi \circ (i, i+1)) = \operatorname{inv}(\pi) \pm 1. \tag{2.13}$$

PROPOSITION 2.1.25. *Jede Permutation $\pi \in \mathfrak{S}_n$ kann als Produkt von* $\operatorname{inv}\pi$ kanonischen *Transpositionen geschrieben werden.*
$\operatorname{inv}\pi$ *ist dabei die* minimale *Anzahl an kanonischen Transpositionen in einer solchen Produktdarstellung.*

BEWEIS. Die Beweisidee ist die: Wir überlegen uns (anhand eines Beispiels), daß man jede Permutation π durch kanonische Transpositionen in die Identität "umformen" kann, genauer gesagt:

$$\epsilon = \pi \circ (i_1, i_1+1) \circ (i_2, i_2+1) \circ \cdots \circ (i_k, i_k+1)\,.$$

Dann folgt "rein algebraisch" (denn Transpositionen sind Involutionen):

$$\pi = (i_k, i_k+1) \circ \cdots \circ (i_2, i_2+1) \circ (i_1, i_1+1)\,.$$

$\operatorname{inv}\pi + \sum_{i=1}^{k} \pm 1 = 0 \implies k \geq \operatorname{inv}\pi.$

Gemäß (2.13) verändert *jede* solche Operation die Anzahl der Inversionen um ± 1: Um auf $\operatorname{inv}\epsilon = 0$ zu kommen, braucht man also *zumindest* $\operatorname{inv}\pi$ Operationen.
— Nun also das illustrierende Beispiel: Betrachten wir die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Produkt von 2 Permutationen in "dreizeiliger Notation".

Wir bringen zunächst den Einser (in der unteren Zeile) "sukzessive nach vorne"; dazu sollten wir ihn zuerst mit dem Dreier vertauschen. Das kann durch Aufmultiplizieren mit einer geeigneten kanonischen Transposition von rechts erreicht werden:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \circ (2,3).$$

Dann sollten wir ihn mit dem Vierer vertauschen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ (1,2).$$

Jetzt steht der Einser an der "richtigen" Stelle; wir machen mit dem Zweier weiter:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \circ (3,4),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \circ (2,3).$$

Zum Schluß kommt noch der Dreier nach vorne:

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \circ (3,4).$$

"Rein algebraisch" erhalten wir also:

$$(3,4) \circ (2,3) \circ (3,4) \circ (1,2) \circ (2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Es ist klar, daß der hier skizzierte "Algorithmus" auch im allgemeinen funktioniert: Man bewegt der Reihe nach $1, 2, \ldots n-1$ in die richtige Position. Offensichtlich senkt jeder dieser Schritte die Anzahl der Inversionen um 1, sodaß insgesamt genau $\operatorname{inv}\pi$ Schritte benötigt werden. □

Eine Darstellung als Produkt von kanonischen Transpositionen ist keineswegs eindeutig. Es gilt beispielsweise:

$$(1,3) = (2,3)\,(1,2)\,(2,3) = (1,2)\,(2,3)\,(1,2).$$

Es gilt aber immerhin:

Korollar 2.1.26. *Sei $\pi \in \mathfrak{S}_n$. Die Anzahl der Faktoren in einer (beliebigen) Produktdarstellung von π durch kanonische Transpositionen ist* modulo *2 eindeutig (d.h., sie ist immer entweder gerade oder ungerade).*

Beweis. Betrachten wir zwei beliebige Darstellungen von $\pi \in \mathfrak{S}_n$ als Produkt von kanonischen Transpositionen

$$\pi = \tau_1\tau_2\cdots\tau_k = \sigma_1\sigma_2\cdots\sigma_l.$$

Dann folgt

$$\tau_1\tau_2\cdots\tau_k\sigma_l\sigma_{l-1}\cdots\sigma_1 = \epsilon.$$

Gemäß (2.13) ist die Anzahl der Inversionen auf der linken Seite *modulo* 2 gleich $k+l$, auf der rechten Seite aber einfach 0 (denn ϵ hat keine Inversionen). Somit erhalten wir $k + l \equiv 0 \mod 2 \iff k \equiv l \mod 2$, wie behauptet. □

Definition 2.1.27. *Das* Vorzeichen *oder* Signum *einer Permutation $\pi \in \mathfrak{S}_n$ ist durch $(-1)^{\operatorname{inv}\pi}$ definiert und wird mit $\operatorname{sgn}\pi$ bezeichnet.*

Eine Permutation π mit $\operatorname{sgn}\pi = +1$ wird gerade Permutation *genannt, eine Permutation π mit $\operatorname{sgn}\pi = -1$ wird* ungerade Permutation *genannt.*

Bemerkung 2.1.28. *Es ist leicht zu sehen: Der Zyklus*

$$(a_1, a_2, \ldots, a_{k-2}, a_{k-1}, a_k)\,,$$

ist darstellbar durch das Produkt der $k-1$ Transpositionen

$$(a_1, a_2)\cdot(a_2, a_3)\cdots(a_{k-2}, a_{k-1})\cdot(a_{k-1}, a_k)\,.$$

Proposition 2.1.29. *Seien $\pi, \rho \in \mathfrak{S}_n$. Für das Signum gelten die folgenden Tatsachen:*

(1) $\operatorname{sgn}(\pi\circ\rho) = \operatorname{sgn}(\pi)\cdot\operatorname{sgn}(\rho)$.
(2) *Sei $\tau = (i, j)$ $(i \neq j)$ eine* beliebige *Transposition. Dann gilt $\operatorname{sgn}\tau = -1$.*
(3) *Wenn $\pi = \tau_1\tau_2\cdots\tau_m$ eine Darstellung von π durch* beliebige *Transpositionen τ_i ist, dann gilt $\operatorname{sgn}\pi = (-1)^m$.*
(4) *Für einen Zyklus $(a_1, a_2, \ldots, a_m)$ der Länge m gilt*

$$\operatorname{sgn}(a_1, a_2, \ldots, a_m) = (-1)^{m-1}.$$

(5) *Sei $z(\pi)$ die Anzahl der Zyklen in der disjunkten Zyklenzerlegung von π. Dann gilt $\operatorname{sgn}\pi = (-1)^{n-z(\pi)}$.*

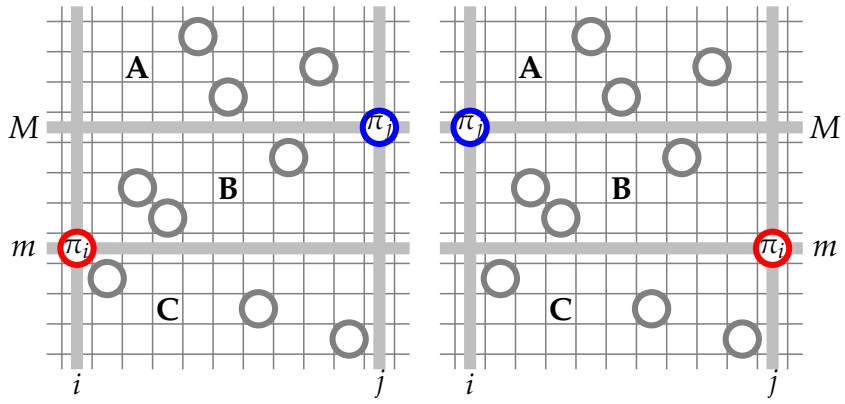
BEWEIS. Für (1) schreiben wir π und ρ als Produkte von *kanonischen* Transpositionen gemäß Proposition 2.1.25:

$$\pi = \sigma_1\sigma_2\cdots\sigma_k,\ \rho = \tau_1\tau_2\cdots\tau_l.$$

Aus Korollar 2.1.26 erhalten wir sofort daß $\operatorname{sgn}\pi = (-1)^k$, $\operatorname{sgn}\rho = (-1)^l$ und $\operatorname{sgn}(\pi\circ\rho) = (-1)^{k+l} = (\operatorname{sgn}\pi)\cdot(\operatorname{sgn}\rho)$.
(2) Sei $\pi \in \mathfrak{S}_n$ beliebig: Wenn wir

$$(-1)^{\operatorname{inv}(\pi\circ(i,j))} = -(-1)^{\operatorname{inv}\pi}$$

zeigen können, dann folgt die Behauptung aus (1). Betrachten wir dazu den "Graphen" der Permutation π (also $\{(1,\pi_1),\ldots,(n,\pi_n)\} \subset \mathbb{N}^2$) und überlegen, welchen Effekt die Vertauschung der Elemente an den Positionen i und j auf die Anzahl der Inversionen hat. Sei o.B.d.A. $i < j$. Setze $S := \left\{\pi_{i+1},\ldots,\pi_{j-1}\right\}$, $m := \min\left(\pi_i,\pi_j\right)$, $M := \max\left(\pi_i,\pi_j\right)$. Sei $A := |\{x \in S : x > M\}|$, $C := |\{x \in S : x < m\}|$ und $B := |S| - A - C$. Die folgende Graphik ...



... führt uns klar vor Augen:

- Für $\pi_i < \pi_j$ ist $\operatorname{inv}(\pi\circ(i,j)) = \operatorname{inv}(\pi) + 1 + 2B$,
- Für $\pi_i > \pi_j$ ist $\operatorname{inv}(\pi\circ(i,j)) = \operatorname{inv}(\pi) - 1 - 2B$.

(3) folgt sofort aus (1) und (2).
Für (4) schreiben wir den Zyklus gemäß Bemerkung 2.1.28 als Produkt von $m-1$ Transpositionen:

$$(a_1,a_2,\ldots,a_m) = (a_1,a_2)\,(a_2,a_3)\cdots(a_{m-1},a_m).$$

Aus (3) folgt nun $\operatorname{sgn}(a_1,a_2,\ldots,a_m) = (-1)^{m-1}$.
Für (5) betrachten wir die eindeutige Zerlegung von π in $k = z(\pi)$ disjunkte Zyklen z_i der Länge $\ell(z_i)$:

$$\pi = z_1 z_2 \cdots z_k.$$

Aus (1) und (4) zusammen mit $\sum_{i=1}^{k}\ell(z_i) = n$ folgt die Behauptung:

$$\operatorname{sgn}\pi = (-1)^{\ell(z_1)-1}(-1)^{\ell(z_2)-1}\cdots(-1)^{\ell(z_k)-1} = (-1)^{n-z(\pi)}.$$

□

2.1.3.4. *Eine spielerische Anwendung*. Ein Spiel aus dem vorigen Jahrhundert besteht aus einem quadratischen Rahmen mit 15 beweglichen quadratischen Plättchen, die mit den Zahlen von 1 bis 15 bedruckt sind. Die Plättchen lassen sich nach rechts/links/oben/unten verschieben (sofern die entsprechende Position frei ist), und die Aufgabe besteht darin, die Plättchen in die "Grundstellung"

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

zu bringen.
Es ist leicht zu sehen, daß die folgende Konstellation *nicht* (jedenfalls nicht durch zulässige Spielzüge) in obige Grundstellung gebracht werden kann:

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

Denn wenn wir das leere Feld mit 16 bezeichnen, dann können wir eine beliebige Konstellation der Plättchen als Permutation von $1, 2, \ldots, 16$ auffassen; und die "zulässigen Spielzüge" sind sämtlich *Transpositionen* — *stets* mit dem Element 16, das bei jedem Zug "bewegt" wird. Wenn wir mit der obigen Konstellation starten, ist 16 in Position rechts unten; ebenso wie in der "Grundstellung" — d.h., wir müssen eine *gerade* Anzahl von "zulässigen Zügen" machen. Dies bedeutet aber, daß die obige Konstellation einer geraden Permutation entsprechen müßte — dies ist aber *nicht* der Fall, denn die entsprechende Permutation kann als Produkt von 7 Transpositionen

Denn für jede Bewegung nach links oder nach oben müssen wir eine Bewegung nach rechts oder nach unten machen ...

$$(1, 15)\,(2, 14)\,(3, 13)\,(4, 12)\,(5, 11)\,(6, 10)\,(7, 9)$$

geschrieben werden, ist also *ungerade*.

2.1.4. Inklusion–Exklusion. Wir haben die Frage nach der Anzahl der surjektive Funktionen von $[k]$ nach $[n]$ zunächst "ausweichend" beantwortet (durch adhoc–Einführung der Stirling–Zahlen der zweiten Art). Nun wollen wir die Sache mit einer einfachen Idee erneut angreifen, die wir zuerst anhand eines einfachen Beispiels aus der Zahlentheorie illustrieren.

Beispiel 2.1.30. *Wir wollen in der Menge* $[60] = \{1, 2, \ldots, 59, 60\}$ *jene Zahlen bestimmen, die relativ prim zu* 60 *sind. Dazu betrachten wir die* Primfaktoren *von* 60 *(das sind die Zahlen* 2, 3 *und* 5*) und bilden die Mengen der entsprechenden Vielfachen zwischen* 1 *und* 60*, also*

Vornehmer ausgedrückt: Bestimme die primen Restklassen in $\mathbb{Z}_{60}$.

$$\begin{aligned}
\mathbf{M}_2 &= \{2, 4, 6, \ldots, 58, 60\}, \\
\mathbf{M}_3 &= \{3, 6, 9 \ldots, 57, 60\}, \\
\mathbf{M}_5 &= \{5, 10, 15, \ldots, 55, 60\}.
\end{aligned}$$

Die Menge S der gesuchten Zahlen ergibt sich dann als

$$S = [60] \setminus (\mathbf{M}_2 \cup \mathbf{M}_3 \cup \mathbf{M}_5) = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}.$$

Wenn wir nur an der Kardinalität $|S| = 16$ *von S interessiert sind, könnten wir wie folgt beginnen:*

$$|S| = \left|[60] \setminus (\mathbf{M}_2 \cup \mathbf{M}_3 \cup \mathbf{M}_5)\right| \overset{???}{=} 60 - |\mathbf{M}_2| - |\mathbf{M}_3| - |\mathbf{M}_5|.$$

Das Fragezeichen über dem zweiten Gleichheitszeichen deutet an, daß das so nicht stimmt: Denn für jeden Teiler d von 60 gilt

$$|\mathbf{M}_d| = 60/d,$$

und

$$60 - 60/2 - 60/3 - 60/5 = -2.$$

Der Fehler rührt daher, daß ja z.B. die Zahl 6 in $\mathbf{M}_2$ und $\mathbf{M}_3$ *enthalten ist:* Alle *Zahlen in* $\mathbf{M}_2 \cap \mathbf{M}_3 = \mathbf{M}_6$ *(und ebenso alle Zahlen in* $\mathbf{M}_2 \cap \mathbf{M}_5 = \mathbf{M}_{10}$ *und in* $\mathbf{M}_3 \cap \mathbf{M}_5 = \mathbf{M}_{15}$*) sind also* zweimal *weggezählt worden. Wir müßten obiges daher wie folgt korrigieren:*

$$\begin{aligned} |S| &\overset{???}{=} 60 - |\mathbf{M}_2| - |\mathbf{M}_3| - |\mathbf{M}_5| + |\mathbf{M}_6| + |\mathbf{M}_{10}| + |\mathbf{M}_{15}| \\ &= 60 - 60/2 - 60/3 - 60/5 + 60/6 + 60/10 + 60/15 = 18. \end{aligned}$$

Das ist noch immer falsch: Denn die Zahlen 30 und 60 sind ja ursprünglich dreimal *weggezählt worden, nun aber* dreimal *wieder dazugezählt worden! Richtig lautet die Rechnung also:*

$$\begin{aligned} |S| &= 60 - |\mathbf{M}_2| - |\mathbf{M}_3| - |\mathbf{M}_5| + |\mathbf{M}_6| + |\mathbf{M}_{10}| + |\mathbf{M}_{15}| - |\mathbf{M}_{30}| \\ &= 60 - 60/2 - 60/3 - 60/5 + 60/6 + 60/10 + 60/15 - 60/30 \\ &= 16. \end{aligned}$$

Nun versuchen wir, die Idee aus diesem konkreten Beispiel auf unsere Fragestellung zu übertragen: Natürlich können wir die Anzahl der surjektiven Funktionen $\left|\mathrm{surj}\,(k,n)\right|$ auch dadurch bestimmen, daß wir von der Anzahl *aller* Funktionen $\left|\mathrm{abb}\,(k,n)\right| = n^k$ die Anzahl der "nicht–surjektiven" Funktionen abziehen. Eine "nicht–surjektive" Funktion nimmt (mindestens) ein Element $i \in [n]$ *nicht* als Wert an, und jede solche Funktion können wir als Element in $\mathrm{abb}\,([k], [n] \setminus \{i\})$ deuten. Für die Anzahl solcher Funktionen gilt natürlich (unabhängig von i) $\left|\mathrm{abb}\,([k], [n] \setminus \{i\})\right| = \left|\mathrm{abb}\,(k, n-1)\right| = (n-1)^k$. Als ersten Schritt in diese Richtung erhalten wir also

$$n^k - \sum_{i=1}^{n} \left|\mathrm{abb}\,([k], [n] \setminus \{i\})\right| = n^k - n \cdot (n-1)^k.$$

Genau wie in Beispiel 2.16

Klarerweise ist das nicht die richtige Antwort — der Fehler, den wir gemacht haben, liegt darin, daß wir ja jene Funktionen, die *zwei* verschiedene Elemente

$\{i,j\} \subseteq [n]$ *nicht* als Wert annehmen, *doppelt* weggezählt haben. Wir müßten also im zweiten Schritt

$$\sum_{\{i,j\}\in[n]} \left|\mathrm{abb}\left([k], [n]\setminus\{i,j\}\right)\right| = \binom{n}{2}\cdot(n-2)^k$$

wieder dazuzählen. Das Problem ist nun wiederum, daß wir damit jene Funktionen, die *drei* verschiedene Elemente $\{i,j,l\}$ *nicht* als Wert annehmen, dreimal dazuzählen (nämlich je einmal für $\{i,j\}$, $\{i,l\}$ und $\{j,l\}$) — diese wurden aber schon im ersten Schritt dreimal weggezählt (nämlich je einmal für i, j und l); sie sind also "netto" in

Genau wie in Beispiel 2.16

$$n^k - n\cdot(n-1)^k + \binom{n}{2}\cdot(n-2)^k$$

wieder vorhanden und müßten im dritten Schritt nach derselben Logik neuerlich weggezählt werden:

$$\binom{n}{0}n^k - \binom{n}{1}\cdot(n-1)^k + \binom{n}{2}\cdot(n-2)^k - \binom{n}{3}\cdot(n-3)^k.$$

Die Sache wird also einerseits unübersichtlich; andrerseits legen unsere bisherigen Überlegungen folgende Vermutung nahe: Die Anzahl der surjektiven Funktionen von $[k]$ nach $[n]$ ist für $k \geq n$

Indextransformation $i \mapsto n-i$.

$$\left|\mathrm{surj}\,(k,n)\right| = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^k = \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}i^k. \tag{2.14}$$

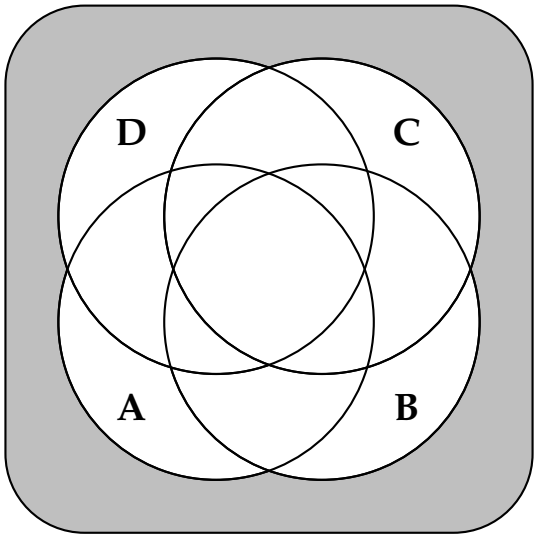
(Für $k < n$ ist die Anzahl natürlich 0.) Wenn wir k und n vertauschen, so folgt daraus gemäß (2.3) eine Formel für die Stirling–Zahlen zweiter Art:

$$S_{n,k} = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n. \tag{2.15}$$

Statt den speziellen Fall (2.14) zu beweisen, schälen wir ein allgemeineres Prinzip heraus: Unsere Idee bestand ja darin, daß wir von der Menge $\mathrm{abb}\,(k,n)$ aller Funktionen von $[k]$ nach $[n]$ die *Vereinigungsmenge* $\bigcup_{i=1}^{n}\mathrm{abb}\left([k], [n]\setminus\{i\}\right)$ aller Funktionen, die ein Element $i \in [n]$ *nicht* als Wert annehmen, abziehen wollen, also die Kardinalität der Menge

$$\mathrm{abb}\,(k,n)\setminus\left(\bigcup_{i=1}^{n}\mathrm{abb}\left([k], [n]\setminus\{i\}\right)\right)$$

bestimmen wollten. Unsere Probleme ergaben sich daraus, daß die Mengen $\mathrm{abb}\left([k], [n]\setminus\{i\}\right)$ nicht *disjunkt* sind (sonst hätten wir gemäß der Summenregel schon im ersten Schritte die richtige Lösung gehabt). Das folgende "Mengendiagramm" illustriert die allgemeine Situation:



SATZ 2.1.31 (Inklusion–Exklusion). *Sei S eine Menge, sei $T_1, \ldots, T_m$ eine Familie von Teilmengen (nicht notwendig disjunkt!) von S. Dann gilt:*

$$\left| S \setminus \left(\bigcup_{i=1}^{m} T_i \right) \right| = |S| + \sum_{k=1}^{m} (-1)^k \sum_{\substack{A \subseteq [m] \\ |A|=k}} \left| \bigcap_{i \in A} T_i \right|. \tag{2.16}$$

Diese Aussage wird das *Prinzip der Inklusion–Exklusion* genannt.

BEMERKUNG 2.1.32. *Die Gleichung* (2.16) *ist sehr "kompakt" hingeschrieben. Zur besseren Verständlichkeit halten wir fest, daß auf der* linken *Seite von* (2.16) *die Anzahl aller Elemente von S steht, die* in keiner einzigen *Menge T_i enthalten sind; die* rechte *Seite von* (2.16) *können wir "ausführlicher" so schreiben:*

$$\begin{aligned}
&|S| \\
&- |T_1| - |T_2| - \cdots - |T_m| \quad \leftarrow k{=}1 \\
&+ |T_1 \cap T_2| + |T_1 \cap T_3| + \cdots + |T_1 \cap T_m| + |T_2 \cap T_3| + \cdots \quad \leftarrow k{=}2 \\
&- |T_1 \cap T_2 \cap T_3| - |T_1 \cap T_2 \cap T_4| - \cdots \quad \leftarrow k{=}3 \\
&+ |T_1 \cap T_2 \cap T_3 \cap T_4| + |T_1 \cap T_2 \cap T_3 \cap T_5| + \cdots \quad \leftarrow k{=}4 \\
&\vdots
\end{aligned}$$

Oder unter Verwendung der Summennotation:

$$|S| - \underbrace{\sum_{1 \le i_1 \le m} \left| T_{i_1} \right|}_{k=1} + \underbrace{\sum_{1 \le i_1 < i_2 \le m} \left| T_{i_1} \cap T_{i_2} \right|}_{k=2} - \underbrace{\sum_{1 \le i_1 < i_2 < i_3 \le m} \left| T_{i_1} \cap T_{i_2} \cap T_{i_3} \right|}_{k=3} + - \cdots$$

Oder in Worten: Von der Kardinalität von S werden die Kardinalitäten der k–fachen Durchschnitte der Mengen T_i alternierend subtrahiert/addiert.

BEWEIS. Überlegen wir uns, wie oft ein Element $x \in S$ in der rechten Seite von (2.16) gezählt wird.

Es ist klar, daß jedes Element im Komplement $S \setminus \left(\bigcup_{i=1}^{m} T_i\right)$ genau *einmal* (nämlich durch den ersten Summanden $|S|$) gezählt wird.

Sei nun ein x *genau* in den $k \geq 1$ Teilmengen $T_{i_1}, T_{i_2}, \ldots, T_{i_k}$ enthalten (also in *keinem anderen* T_j). Dann wird x durch den ersten Term (S) einmal dazugezählt, dann k–mal abgezogen (je einmal für $T_{i_1}, T_{i_2}, \ldots, T_{i_k}$), dann $\binom{k}{2}$–mal dazugezählt (je einmal für $T_{i_1} \cap T_{i_2}$, $T_{i_1} \cap T_{i_3}$, $\ldots$, $T_{i_{m-1}} \cap T_{i_m}$), und so weiter. Insgesamt wird x also genau

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + - \cdots + (-1)^k \binom{k}{k} = 0$$

mal gezählt. □

Die Richtigkeit von (2.14) ergibt sich also aus dem Prinzip der Inklusion–Exklusion und der Beobachtung, daß die Durchschnitte von l verschiedenen Mengen $T_{i_j} = \operatorname{abb}\left([k], [n] \setminus \left\{i_j\right\}\right)$ *immer* Kardinalität $(n-l)^k$ haben; *unabhängig* von den konkreten Indizes $i_1, \ldots, i_l$.

DEFINITION 2.1.33. *Ein* Fixpunkt *einer Permutation π ist ein Element $x \in X$ mit $\pi(x) = x$. Eine Permutation, die keine Fixpunkte enthält, heißt* fixpunktfreie Permutation.

Aufgabe 27 ($\star\star$)**:** *Zeige: Die Anzahl aller fixpunktfreien Permutationen von $[n]$ ist gleich*

$$n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - + \cdots + (-1)^n \frac{1}{n!}\right).$$

Aufgabe 28 ($\star\star$)**:** *Sei n eine natürliche Zahl. Die* Eulersche ϕ–Funktion *von n ist die Anzahl der zu n relativ primen Zahlen k, $1 \leq k \leq n$. Verwende das Prinzip der Inklusion–Exklusion, um die aus der Zahlentheorie bekannte Formel*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right)$$

zu beweisen (wobei $p_1, \ldots, p_t$ die Primteiler *von n sind).*

2.1.5. Rekursionen. Unter einer rekursiven Definition einer Zahlenfolge c_n versteht man allgemein, daß die Folgenglieder jeweils durch eine Formel gegeben sind, in der die vorangegangenen Folgenglieder vorkommen, also etwas der Art

$$c_n = \text{“Formel”}\,(c_1, c_2, \ldots, c_{n-1})$$

(z.B.: $c_n = \sum_{i=1}^{n-1} c_i$), zusammen mit Anfangsbedingungen, also etwas der Art

$$c_1 = a, c_2 = b, \ldots, c_m = m$$

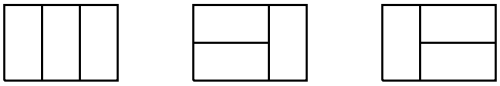
(z.B.: $c_1 = 1$).

Viele Abzählungsfragen führen auf Rekursionen, wir betrachten hier zwei typische Beispiele.

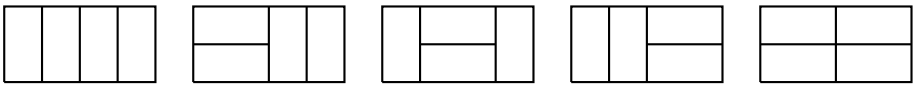
2.1.5.1. *Fibonacci–Zahlen.* Die folgende Fragestellung führt auf die berühmten *Fibonacci–Zahlen*.

Gegeben sei ein $2 \times n$ Rechteck. Wieviele verschiedene Zerlegungen dieses Rechtecks gibt es in 2×1 Dominos?

Betrachten wir etwa $n = 3$. Da gibt es die folgenden drei Möglichkeiten:



Für $n = 4$ gibt es die fünf Möglichkeiten:



Bezeichne $f(n)$ die gesuchte Anzahl. Die Menge aller Zerlegungen des Rechtecks zerfällt in 2 disjunkte Teilmengen:

- Am rechten Ende finden wir entweder ein vertikales Domino,
- oder zwei übereinander liegende horizontale Dominos.

Entfernt man diese Dominos, dann bleibt im ersten Fall eine Zerlegung des $2 \times (n-1)$ Rechtecks in Dominos übrig, wofür es $f(n-1)$ Möglichkeiten gibt, und im zweiten Fall eine Zerlegung des $2 \times (n-2)$ Rechtecks in Dominos, wofür es $f(n-2)$ Möglichkeiten gibt. Insgesamt erhalten wir also die Rekursion

$$f(n) = f(n-1) + f(n-2) \tag{2.17}$$

mit der Anfangsbedingung $f(0) = f(1) = 1$.
Die Zahlen $f(n)$ heißen *Fibonacci–Zahlen* und werden meistens mit F_n bezeichnet.

Aufgabe 29 ($\star\star$)**:** *Zeige, daß für die Fibonacci–Zahlen F_n für $n \geq 2$ die Matrixidentität*

$$\begin{pmatrix} F_{n-2} & F_{n-1} \\ F_{n-1} & F_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n$$

gilt, und folgere daraus

$$F_n F_{n-2} - F_{n-1}^2 = (-1)^n.$$

Aufgabe 30 ($\star\star$)**:** *Drücke die folgenden Zahlen durch Fibonaccizahlen aus:*

(a) *Anzahl aller Kompositionen von n, deren Teile entweder gleich 1 oder 2 sind,*
(b) *Anzahl aller Kompositionen von n, deren Teile alle größer oder gleich 2 sind,*
(c) *Anzahl aller Kompositionen von n in ungerade Teile.*

Wir können durch einen adhoc gewählten *Ansatz* eine einfache Formel für die Fibonacci–Zahlen finden: Wenn wir einmal auf die Anfangsbedingungen vergessen und annehmen, daß die Lösung der Rekursion die Gestalt z^n hat, dann führt (2.17) auf die Gleichung

$$z^2 = z + 1$$

mit den beiden Lösungen $z_0 = \frac{1-\sqrt{5}}{2}$ und $z_1 = \frac{1+\sqrt{5}}{2}$. Es ist leicht zu sehen, daß *jede* Linearkombination $g(n) := \alpha \cdot z_0^n + \beta \cdot z_1^n$ (α und β seien beliebige, aber feste komplexe Zahlen) *dieselbe* Rekursionsgleichung (2.17) erfüllt wie die Fibonacci–Zahlen, also $g(n) = g(n-1) + g(n-2)$.

Damit die Anfangsbedingungen für die Fibonacci–Zahlen erfüllt werden, müssen wir also das Gleichungssystem

$$g(0) = \alpha + \beta = f(0) = 1$$
$$g(1) = \alpha\frac{1-\sqrt{5}}{2} + \beta\frac{1+\sqrt{5}}{2} = f(1) = 1$$

lösen. Daraus ergibt sich $\alpha = -\frac{1-\sqrt{5}}{2\sqrt{5}}$ und $\beta = \frac{1+\sqrt{5}}{2\sqrt{5}}$. Die n–te Fibonacci–Zahl ist also gleich

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right). \tag{2.18}$$

Die Folge der Fibonacci–Zahlen $(F_n)_{n\geq 0}$ beginnt so:

$$(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots)$$

Aus unserer Formel (2.18) erkennt man, daß sich die Fibonaccizahlen *asymptotisch* wie

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

verhalten, denn $\frac{1-\sqrt{5}}{2} \simeq -0.618034$ ist dem Betrag nach kleiner als 1.

2.1.5.2. *Die Catalan–Zahlen.*

Definition 2.1.34. *Für $n \geq 0$ definieren wir*

$$C_n := \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}. \tag{2.19}$$

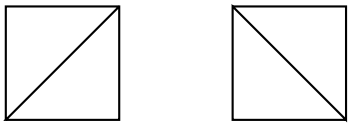
Die Zahlen C_n heißen die Catalan–Zahlen*; die Folge $(C_n)_{n\geq 0}$ beginnt so:*

$$(1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, \dots)$$

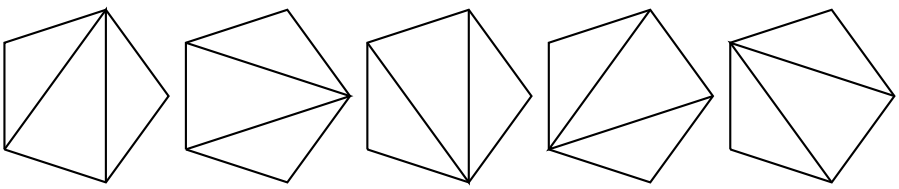
Definition 2.1.35. *Unter einer* Triangulierung eines n-Ecks *verstehen wir eine vollständige Zerlegung des n-Ecks in Dreiecke durch Diagonalen, die Ecken verbinden.*

Wieviele verschiedene Triangulierungen des n-Ecks gibt es?

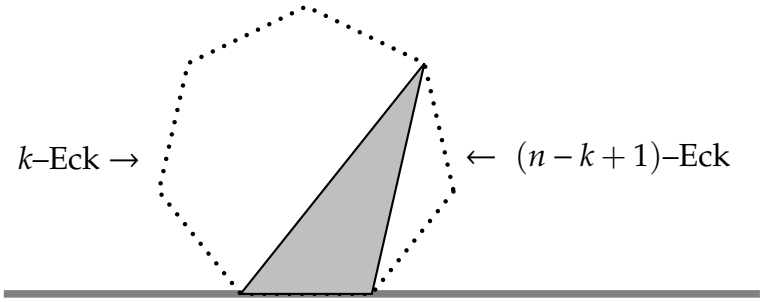
Betrachten wir etwa $n = 4$. Dann gibt es die folgenden zwei Möglichkeiten:



Für $n = 5$ gibt es schon fünf Möglichkeiten:



Sei die gesuchte Anzahl $f(n)$. Wieder wollen wir eine Rekursion für die Folge $f(n)$ herleiten. Wir stellen uns dazu das n-Eck auf einer fixierten Seite ruhend vor. In einer vorgegebenen Triangulierung gehört diese fixierte Seite zu einem eindeutig bestimmten Dreieck. Dieses zerteilt das n-Eck in einen Teil "links davon" und einen Teil "rechts davon".



Beide Teile sind ebenfalls Triangulierungen, und zwar eines k-Ecks und eines $(n-k+1)$-Ecks. Dies ergibt die Rekursion

$$f(n) = \sum_{k=2}^{n-1} f(k)\, f(n-k+1) \text{ für } n \geq 3 \tag{2.20}$$

mit der Anfangsbedingung $f(2) = 1$.
Die Folge der Zahlen $(f(n+2))_{n\geq 0}$ beginnt so:

$$(1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, \dots)$$

Diese Glieder stimmen augenscheinlich genau mit den *Catalan–Zahlen* überein.

2.2. Erzeugende Funktionen und Formale Potenzreihen

Ein sehr mächtiges Hilfsmittel bei Abzählproblemen, aber auch allgemeineren Situationen (z.B. bei Rekursionen), sind *erzeugende Funktionen*. Einen kleinen Vorgeschmack haben wir ja schon in Beispiel 1.2.4 im einleitenden Kapitel erhalten (dort hatten wir die erzeugende Funktion aller Teilmengen der Menge $[n]$ betrachtet, ein Polynom vom Grad n), nun wollen wir dieses Konzept wesentlich erweitern.

DEFINITION 2.2.1. *Das "typische Abzählproblem", mit dem wir es bisher zu tun hatten, sah so aus: Gegeben sei eine Familie von "kombinatorischen Objekten"* $\mathcal{O}$ *(z.B. Kompositionen von n, Anzahl der Zerlegungen eines* $2 \times n$*–Rechtecks in Dominos, etc.) wobei jedes einzelne Objekt eine offensichtliche (ganze, in unseren bisherigen Beispielen stets nicht–negative) "Kennzahl" (in den meisten obigen Beispielen: n; manchmal k) besitzt. Wir fragten immer nach der Anzahl aller derartigen Objekte mit fester "Kennzahl".*
Wie in Beispiel 1.2.4 betrachten wir eine Gewichtsfunktion ω*, die jedem Objekt* $o \in \mathcal{O}$ *das Gewicht*

$$\omega(o) := z^{\text{"Kennzahl" von } o}$$

zuordnet, und definieren die erzeugende Funktion *von* $\mathcal{O}$ *als die (formale) Summe*

$$\mathcal{GF}(\mathcal{O}) := \sum_{o\in\mathcal{O}} \omega(o)\,.$$

Wie gesagt, sind wir in der Regel "nur" an den Anzahlen *aller Objekte mit "Kennzahl" n interessiert. Wenn wir für diese Anzahlen die Notation c_n wählen, können wir die erzeugende Funktion auch in Form einer* Potenzreihe[5] *schreiben:*

$$\mathcal{GF}(O) := \sum_{n=0}^{\infty} c_n z^n.$$

Wenn wir uns "nur" mit der Folge $(c_n)_{n=0}^{\infty}$ konfrontiert sehen, verwenden wir für dieselbe Potenzreihe ebenfalls die Bezeichnung erzeugende Funktion *von $(c_n)_{n=0}^{\infty}$, schreiben dann aber meist einfacher*

$$c(z) := \sum_{n=0}^{\infty} c_n z^n.$$

Die Zahlen c_n erscheinen als die *Koeffizienten* von z^n in $\mathcal{GF}(O)$. Allgemein führen wir für den Koeffizienten von z^n in einer Potenzreihe $f(z)$ die Notation $[\![z^n]\!]\ f(z)$ ein. Im folgenden werden wir auch oft davon ausgehen, daß "die Potenzreihe genauso bezeichnet ist wie ihre Koeffizienten", d.h., wenn wir eine Potenzreihe g betrachten (und sonst nichts dazusagen), dann bezeichnen wir oft "stillschweigend" den Koeffizenten $[\![z^n]\!]\ g$ mit g_n, sehen die Potenzreihe also gegeben als $g(z) = \sum_{n=0}^{\infty} g_n z^n$.

2.2.1. Nochmals die Fibonacci–Zahlen. Als motivierendes Beispiel betrachten wir noch einmal die Rekursion (2.17) für die Fibonaccizahlen F_n: Ganz naiv und formal (d.h., ohne Fragen wie Konvergenz etc. zu betrachten) multiplizieren wir beide Seiten in (2.17) mit z^n und summieren (formal[6]) über alle $n \geq 2$. Das ergibt

$$\sum_{n=2}^{\infty} F_n z^n = \sum_{n=2}^{\infty} F_{n-1} z^n + \sum_{n=2}^{\infty} F_{n-2} z^n.$$

Mit der erzeugenden Funktion $F(z) = \sum_{n=0}^{\infty} F_n z^n$ der Fibonacci–Zahlen können wir das nun so schreiben:

$$F(z) - F_1 z - F_0 = z\left(F(z) - F_0\right) + z^2 F(z).$$

Da $F_0 = F_1 = 1$, können wir die erzeugende Funktion $F(z)$ "ausrechnen":

$$F(z) = \frac{1}{1 - z - z^2}.$$

Um aus dieser Darstellung eine Formel für die Koeffizienten F_n zu extrahieren, bestimmen wir die sogenannte *Partialbruchzerlegung*

$$F(z) = \frac{1}{z_1 - z_0}\left(\frac{z_1}{1 - z_1 z} - \frac{z_0}{1 - z_0 z}\right),$$

[5] Für unsere "formalen" Zwecke können wir eine Potenzreihe einfach als "Polynom von unendlichem Grad" ansehen.

[6] D.h.: Die unendliche Summe ist zunächst nur eine *Schreibweise* für die Gleichungen (2.17)! Die Gleichung für die Reihen besagt einfach, daß die Koeffizienten von z^n der linken und der rechten Seite für alle $n \geq 2$ gleich sind.

wobei $z_0 = \frac{1-\sqrt{5}}{2}$ und $z_1 = \frac{1+\sqrt{5}}{2}$ (wie zuvor) die Lösungen der Gleichung $x^2 - x - 1 = 0$ sind.[7] Auf der rechten Seite stehen geometrische Reihen[8], die man entwickelt:

$$\begin{aligned} F(z) &= \frac{1}{z_1 - z_0}\left(\sum_{n\geq 0} z_1^{n+1} z^n - \sum_{n\geq 0} z_0^{n+1} z^n\right) \\ &= \frac{1}{\sqrt{5}} \sum_{n\geq 0} z^n \left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right). \end{aligned}$$

Durch *Koeffizientenvergleich* (d.h.: Gleichsetzen der Koeffizienten von z^n auf beiden Seiten der Gleichung) erhält man wieder unser früheres Ergebnis (2.18).

2.2.2. Formale Potenzreihen. Es ist nun an der Zeit, den *Kalkül der formalen Potenzreihen* einzuführen und zu begründen, warum er (nicht nur in unserem motivierenden Beispiel mit den Fibonacci–Zahlen) "funktioniert".

Definition 2.2.2. *Eine* formale Potenzreihe *über dem Körper der komplexen Zahlen*[9] $\mathbb{C}$ *ist eine Folge* $(a_0, a_1, a_2, \dots)$ *mit* $a_i \in \mathbb{C}$ *für alle* i*. Wir bezeichnen die Menge aller solchen formalen Potenzreihen mit* $\mathbb{C}[[z]]$*.*

Auf $\mathbb{C}[[z]]$ *definieren wir eine* komponentenweise *Addition "+" durch*

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots).$$

Für ein $\lambda \in \mathbb{C}$ *definieren wir eine* komponentenweise *Skalarmultiplikation "$\cdot$" durch*

$$\lambda \cdot (a_0, a_1, a_2, \dots) := (\lambda a_0, \lambda a_1, \lambda a_2, \dots).$$

Weiters definieren wir eine Multiplikation (die wir ebenfalls mit $\cdot$ notieren[10]*) zweier formalen Potenzreihen durch*

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) := (c_0, c_1, c_2, \dots),$$

wobei

$$c_n := \sum_{k=0}^{n} a_k b_{n-k}$$

ist. (Dieses Produkt heißt auch Konvolutionsprodukt*.)*

[7] Auch wenn man nicht — aus der Analysis — weiß, wie diese Partialbruchzerlegung zustandegekommen ist, kann man ihre Richtigkeit leicht durch direkte Rechnung — auf gleichen Nenner bringen und vereinfachen — nachprüfen.

[8] Wieder etwas, das man aus der Analysis mitbringt: $\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$, gültig für z vom Betrag kleiner 1.

[9] Man könnte $\mathbb{C}$ auch durch einen beliebigen anderen Körper ersetzen. Für manche Eigenschaften genügt es, nur einen Ring (z.B. einen Polynomring) vorzugeben.

[10] "By abuse of notation" — aus dem Kontext wird aber immer klar sein, welche der beiden Multiplikationen gemeint sind

Die folgenden speziellen Potenzreihen werden sehr oft vorkommen und erhalten deshalb abkürzende Symbole:

$$\begin{aligned} 0 &:= (0,0,0,\dots), \\ 1 &:= (1,0,0,\dots), \\ -a &:= (-1)\cdot a. \end{aligned}$$

Diese Definition ist so formal, daß zunächst vielleicht nicht klar ist, warum wir hier von *Potenzreihen* sprechen: Aus der Analysis ist aber bekannt[11], daß diese formalen Operationen genau der Addition und Multiplikation von Potenzreihen entsprechen; daher schreibt man formale Potenzreihen $(a_0, a_1, \dots)$ praktisch immer in der Form

$$a_0 + a_1 z + a_2 z^2 + \cdots = \sum_{n\geq 0} a_n z^n.$$

Wir gehen die Sache hier deshalb so formalistisch an, um klar herauszuarbeiten, daß für unsere Zwecke Potenzreihen keine *analytischen Funktionen* sind, sondern "nur" zweckmäßig–intuitive "Schreibweisen" für die Folgen der Koeffizienten $(a_0, a_1, \dots)$.

2.2.2.1. *Algebraische Struktur der formalen Potenzreihen.* Es ist leicht nachzurechnen, daß für (formale) Potenzreihen $a = (a_0, a_1, \dots)$, $b = (b_0, b_1, \dots)$, $c = (c_0, c_1, \dots)$ und $\lambda, \mu \in \mathbb{C}$ die folgenden Gesetze erfüllt sind:

$$a + (b + c) = (a + b) + c \quad (\textit{Assoziativität der Addition}) \tag{2.21}$$
$$a + 0 = 0 + a = a \quad (\textit{neutrales Element der Addition}) \tag{2.22}$$
$$a + (-a) = 0 \quad (\textit{inverses Element der Addition}) \tag{2.23}$$
$$a + b = b + a \quad (\textit{Kommutativität der Addition}) \tag{2.24}$$
$$1 \cdot a = a \tag{2.25}$$
$$\lambda(\mu a) = (\lambda\mu) \cdot a \tag{2.26}$$
$$\lambda(a + b) = \lambda a + \lambda b \tag{2.27}$$
$$(\lambda + \mu)a = \lambda a + \mu a \tag{2.28}$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad (\textit{Assoziativität der Multiplikation}) \tag{2.29}$$
$$a \cdot 1 = 1 \cdot a \quad (\textit{neutrales Element der Multiplikation}) \tag{2.30}$$
$$a \cdot b = b \cdot a \quad (\textit{Kommutativität der Multiplikation}) \tag{2.31}$$
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (\textit{Distributivität}) \tag{2.32}$$

In der Sprache der Algebra besagen die Gesetze (2.21)–(2.28), daß $\mathbb{C}[[z]]$ mit Addition und Skalarmultiplikation ein *Vektorraum* über $\mathbb{C}$ ist. Alle Gesetze (2.21)–(2.32) zusammen besagen, daß $\mathbb{C}[[z]]$ mit der Addition, Multiplikation und Skalarmultiplikation eine *kommutative Algebra mit Einselement* über $\mathbb{C}$ ist.

Ein multiplikatives Inverses existiert hingegen nicht in allen Fällen:

[11] Man kann die Sache auch so sehen: Addition und Multiplikation "funktionieren" genau wie bei Polynomen — nur daß wir hier "Polynome von unendlichem Grad" betrachten.

SATZ 2.2.3. *Die Potenzreihe $a(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ besitzt genau dann eine bezüglich der Multiplikation inverse Potenzreihe, wenn $a_0 \neq 0$. Die inverse Reihe ist in diesem Fall eindeutig bestimmt.*

BEWEIS. "⇒"Angenommen $a(z)$ besitzt eine inverse Reihe $b(z) = b_0 + b_1 z + b_2 z^2 + \cdots$. Per Definition gilt dann $a(z)\,b(z) = 1$. Insbesondere gilt $a_0 b_0 = 1$: Das ist nur möglich, wenn $a_0 \neq 0$.
"⇐"Sei $a_0 \neq 0$. Wir geben die Koeffizienten einer inversen Reihe $b(z) = b_0 + b_1 z + b_2 z^2 + \cdots$ durch direkte Rechnung an. Es gilt ja

$$a_0 b_0 = 1$$

und für $n \geq 1$

$$\sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k} = 0.$$

Daraus lassen sich die Koeffizienten b_n *in eindeutiger Weise* rekursiv berechnen, denn aus der ersten Gleichung erhalten wir $b_0 = \frac{1}{a_0}$, und aus der zweiten Gleichung erhalten wir rekursiv $b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}$. □

BEISPIEL 2.2.4. *(1) Sei $a(z) = 1 - z = 1 - z + 0 \cdot z^2 + 0 \cdot z^3 + \cdots$. Der konstante Koeffizient von $a(z)$ ist $1 \neq 0$, daher existiert die inverse Reihe $(1-z)^{-1}$. Wie leicht nachzurechnen ist, ist dies die* geometrische Reihe $1 + z + z^2 + \cdots = \sum_{n \geq 0} z^n$.
(2) Allgemeiner, sei $a(z) = 1 - \alpha z$ für ein $\alpha \in \mathbb{C}$. Dann gilt

$$(1 - \alpha z)^{-1} = 1 + \alpha z + \alpha^2 z^2 + \cdots = \sum_{n \geq 0} \alpha^n z^n.$$

(3) Die erzeugende Funktion der Fibonaccizahlen erfüllte die Gleichung $F(z)\,(1 - z - z^2) = 1$. Sie ist daher die multiplikativ inverse Reihe zu $(1 - z - z^2)$, und diese ist wohl definiert, da $1 \neq 0$.

BEMERKUNG 2.2.5. *Wir werden in der Folge oft statt $(1-z)^{-1}$ die Schreibweise $\frac{1}{1-z}$ verwenden.*

Eine weitere wichtige Reihe ist die *Exponentialreihe*

$$\exp(\alpha z) := \sum_{n \geq 0} \frac{\alpha^n}{n!} z^n$$

für ein $\alpha \in \mathbb{C}$. $\exp(\alpha z)$ ist für uns nur eine Schreibweise für die formale Potenzreihe; natürlich erwarten wir aber, daß wesentliche Eigenschaften der Exponentialfunktion der Analysis auch "formal" gelten. Zum Beispiel haben wir

$$\exp(\alpha z) \exp(\beta z) = \exp((\alpha + \beta) z).$$

Denn zwei (formale) Potenzreihen sind genau dann gleich, wenn ihre Koeffizienten übereinstimmen. Wenn wir also die Koeffizienten von z^n auf beiden Seiten vergleichen, erhalten wir:

$$\sum_{k=0}^{n} \frac{\alpha^k}{k!} \frac{\beta^{n-k}}{(n-k)!} = \frac{(\alpha + \beta)^n}{n!},$$

oder äquivalent

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

Das ist aber genau der Binomische Lehrsatz 1.2.11!

Insbesondere gilt:

$$(\exp(\alpha z))^{-1} = \exp(-\alpha z).$$

BEMERKUNG 2.2.6. *Wir werden in der Folge oft statt* $\exp(\alpha z)$ *die Schreibweise* $\mathrm{e}^{\alpha z}$ *verwenden*[12].

2.2.2.2. *Zusammensetzung von Potenzreihen.* Wir führen für Potenzreihen noch eine weitere Verknüpfung ein, die *Zusammensetzung* oder *Komposition* von Potenzreihen:

DEFINITION 2.2.7. *Gegeben seien zwei Potenzreihen* $a(z)$ *und* $b(z)$*, wobei* $b(z)$ *verschwindenden konstanten Koeffizienten hat (also* $b_0 = 0$*:* $b(z) = b_1 z + b_2 z^2 + \dots$*). Die Zusammensetzung* $(a \circ b)(z)$ *von a und b ist definiert durch*

$$(a \circ b)(z) := \sum_{i \geq 0} a_i \left(b(z)\right)^i.$$

Diese Definition erscheint zunächst problematisch: Zwar können wir alle Produkte $(b(z))^i$ (im Prinzip ...) ausrechnen, aber beim Zusammenzählen dieser unendlich vielen Produkte könnten *unendliche Summen komplexer Zahlen* für die Koeffizienten von z^n auftreten, mit denen wir in der Diskreten Mathematik "nichts anfangen können". Wegen der Bedingung $b_0 = 0$ "fängt aber die Potenzreihe $(b(z))^i$ frühestens mit z^i an" (d.h., alle Koeffizienten von z^k mit $k < i$ sind 0). Daher benötigen wir für den Koeffizienten von z^n in $(a \circ b)(z)$ nur die *endlich vielen* Potenzen $(b(z))^i$, $i = 0, \dots, n$. Ganz konkret können wir die Koeffizienten der Zusammensetzung

$$(a \circ b)(z) = \sum_{n \geq 0} c_n z^n$$

wie folgt anschreiben:

$$c_0 = a_0, \text{ und für } n \geq 1 : c_n = \sum_{i=0}^{n} a_i \sum_{\nu_1 + \nu_2 + \dots + \nu_i = n} b_{\nu_1} b_{\nu_2} \cdots b_{\nu_i}, \tag{2.33}$$

die c_n sind also sichtlich durch *endliche Summen* gegeben. Für die Summationsindices ν_i können wir $\nu_i \geq 1$ annehmen, da ja $b_0 = 0$ ist: Der Summationsbereich der inneren Summe entspricht dann der Menge aller Kompositionen von n mit i Teilen.

[12] e steht hier für die *Eulersche Zahl* — aber diese "analytische Bedeutung" ist für uns irrelevant.

BEISPIEL 2.2.8. *Die erzeugende Funktion der Fibonaccizahlen,*

$$F(z) = \left(1 - z - z^2\right)^{-1}$$

kann auch als Zusammensetzung

$$F(z) = \left((1-z)^{-1}\right) \circ \left(z + z^2\right)$$

geschrieben werden. Daher können wir wie folgt rechnen:

$$\begin{aligned} F(z) &= \sum_{i\geq 0} (z+z^2)^i = \sum_{i\geq 0} z^i (1+z)^i \\ &= \sum_{i\geq 0} z^i \sum_{k=0}^{i} \binom{i}{k} z^k = \sum_{0\leq k\leq i} \binom{i}{k} z^{i+k} \\ &= \sum_{n\geq 0} z^n \sum_{k\geq 0} \binom{n-k}{k}. \end{aligned}$$

Koeffizientenvergleich liefert somit folgende Darstellung der Fibonaccizahlen als Summe:

$$F_n = \sum_{k\geq 0} \binom{n-k}{k}.$$

SATZ 2.2.9. *Die Zusammensetzung ist assoziativ. Das heißt, für Potenzreihen $a(z)$, $b(z)$ und $c(z)$, wobei $b(z)$ und $c(z)$ verschwindenden konstanten Term haben, gilt*

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

BEWEIS. Wir müssen zeigen, daß die Koeffizienten von z^n auf beiden Seiten gleich sind: Die einzige Schwierigkeit liegt hier in der umständlichen Notation. Gemäß (2.33) ist der konstante Term (also der Koeffizient von z^0) auf beiden Seiten a_0.
Nun vergleichen wir die Koeffizienten von z^n, $n \geq 1$; wieder gemäß (2.33).
Für die linke Seite berechnen wir $[\![z^n]\!]\ (a \circ (b \circ c))$ (beachte, daß der Koeffizient $(b \circ c)_0 := [\![z^0]\!]\ (b \circ c) = b_0 = 0$ ist):

$$\begin{aligned} &\sum_{i=0}^{n} a_i \sum_{\nu_1+\nu_2+\cdots+\nu_i=n} (b\circ c)_{\nu_1}(b\circ c)_{\nu_2}\cdots(b\circ c)_{\nu_i} \text{ (gemäß (2.33))} \\ &\quad = \sum_{i=0}^{n} a_i \sum_{\nu_1+\cdots+\nu_i=n} \prod_{k=1}^{i} \left(\sum_{j_k=1}^{\nu_k} b_{j_k} \sum_{\mu_1+\cdots+\mu_{j_k}=\nu_k} c_{\mu_1}\cdots c_{\mu_{j_k}} \right) \text{ (gemäß (2.33))} \\ &\quad = \sum_{i=0}^{n} a_i \sum_{j_1+\cdots+j_i\leq n} b_{j_1}\cdots b_{j_i} \sum_{\substack{\nu_1+\nu_2+\cdots+\nu_i=n \\ \nu_1\geq j_1,\ldots,\nu_i\geq j_i}} \prod_{k=1}^{i} \left(\sum_{\mu_1+\cdots+\mu_{j_k}=\nu_k} c_{\mu_1}\cdots c_{\mu_{j_k}} \right) \\ &\quad = \sum_{i=0}^{n} a_i \sum_{j_1+\cdots+j_i\leq n} b_{j_1}\cdots b_{j_i} \sum_{\substack{\mu_1+\cdots+\mu_s=n \\ s=j_1+\cdots+j_i}} c_{\mu_1}\cdots c_{\mu_s}. \end{aligned}$$

Von der zweiten auf die dritte Zeile haben wir einfach ausmultipliziert und die Summation vertauscht. Von der dritten auf die vierte Zeile haben wir benutzt, daß wegen $\mu_1 + \cdots + \mu_{j_k} = \nu_k$ (und $\mu_\ell \geq 1$ für alle ℓ) die Bedingung $\nu_k \geq j_k$ *automatisch* gilt und somit weggelassen werden kann.
Für die rechte Seite berechnen wir $[\![z^n]\!]\ ((a \circ b) \circ c)$:

$$\begin{aligned}
&\sum_{i=0}^{n} (a \circ b)_i \sum_{\nu_1+\nu_2+\cdots+\nu_i=n} c_{\nu_1} c_{\nu_2} \cdots c_{\nu_i} \text{ (gemäß (2.33))} \\
&\quad = \sum_{i=0}^{n} \sum_{j=0}^{i} a_j \sum_{\mu_1+\mu_2+\cdots+\mu_j=i} b_{\mu_1} \cdots b_{\mu_j} \sum_{\nu_1+\cdots+\nu_i=n} c_{\nu_1} \cdots c_{\nu_i} \text{ (gemäß (2.33))} \\
&\quad = \sum_{j=0}^{n} a_j \sum_{i=j}^{n} \sum_{\mu_1+\mu_2+\cdots+\mu_j=i} b_{\mu_1} \cdots b_{\mu_j} \sum_{\nu_1+\cdots+\nu_i=n} c_{\nu_1} \cdots c_{\nu_i} \\
&\quad = \sum_{j=0}^{n} a_j \sum_{\mu_1+\cdots+\mu_j \leq n} b_{\mu_1} \cdots b_{\mu_j} \sum_{\substack{\nu_1+\cdots+\nu_i=n \\ i=\mu_1+\cdots+\mu_j}} c_{\nu_1} \cdots c_{\nu_i},
\end{aligned}$$

was (abgesehen von Umbenennungen) genau dasselbe ist. □

Die nächste Frage ist die nach einem Inversen.

Satz 2.2.10. *Sei $a(z) = a_1 z + a_2 z^2 + \cdots$ eine Potenzreihe mit verschwindendem konstanten Term. Dann gibt es genau dann eine zusammensetzungsinverse Potenzreihe $b(z) = b_1 z + b_2 z^2 + \cdots$, das heißt eine Reihe mit*

$$(a \circ b)(z) = (b \circ a)(z) = z,$$

wenn $a_1 \neq 0$.

Beweis. Es ist klar, daß $a_1 \neq 0$ sein muß, wenn eine zusammensetzungsinverse Potenzreihe zu $a(z)$ existiert, denn sonst wäre $[\![z]\!]\ (a \circ b) = 0 \neq 1$ für jede Potenzreihe b mit $b_0 = 0$.
Wenn aber $a_1 \neq 0$ gilt, dann kann man aus der Gleichung

$$(b \circ a)(z) = z$$

die b_n durch Koeffizientenvergleich gemäß (2.33) rekursiv berechnen.
Denn zunächst erhält man $b_1 a_1 = 1$, also $b_1 = 1/a_1$.
Für $n > 1$ gilt

$$[\![z^n]\!]\ (b \circ a) = \sum_{i=1}^{n} b_i \sum_{\nu_1+\nu_2+\cdots+\nu_i=n} a_{\nu_1} a_{\nu_2} \cdots a_{\nu_i} = 0,$$

also lautet die Rekursion für b_n:

$$b_n = -\frac{1}{a_1^n} \sum_{i=1}^{n-1} b_i \sum_{\nu_1+\nu_2+\cdots+\nu_i=n} a_{\nu_1} a_{\nu_2} \cdots a_{\nu_i}.$$

Somit ist gezeigt, daß es eine eindeutig bestimmte Reihe $b(z)$ mit $(b \circ a)(z)$ gibt.

Es ist nun eine einfache algebraische Tatsache, daß daraus auch umgekehrt $(a \circ b)(z) = z$ folgt. Denn für $b(z)$ gibt es ja dann *ebenfalls* eine eindeutig bestimmte Reihe $c(z)$, sodaß $(c \circ b)(z) = z$ ist. Dann folgt:

$$c(z) = (c \circ (b \circ a))(z) = ((c \circ b) \circ a)(z) = a(z).$$

□

BEMERKUNG 2.2.11. *Zum praktischen Berechnen der zusammensetzungsinversen Reihe gibt es die sogenannte* Lagrangesche Inversionsformel*, die in vielen Fällen schnell zum Ziel führt; siehe Korollar A.3.5 im Appendix.*

BEISPIEL 2.2.12. *Betrachten wir die Reihe* $e^z - 1 = z + \frac{z^2}{2!} + \cdots$*. Gemäß Satz 2.2.10 müsste eine zusammensetzungsinverse Reihe existieren. Wenn wir die Koeffizienten dieser Inversen der Reihe nach ausrechnen, erhalten wir*

$$z - \frac{z^2}{2} + \frac{z^3}{3} - \frac{z^4}{4} + - \cdots$$

Vom Standpunkt der Analysis ist das wenig überraschend, da die inverse Funktion *von* $e^z - 1$ *eben* $\log(1+z)$ *ist — und die hat genau die obige Potenzreihenentwicklung.*
Wir führen also die Schreibweise *ein:*

$$\log(1+z) := \sum_{n \geq 1} (-1)^{n-1} \frac{z^n}{n}.$$

Noch ist aber eigentlich nicht klar, ob diese formale Potenzreihe tatsächlich zusammensetzungsinvers zu $e^z - 1$ *ist, also ob*

$$e^{\log(1+z)} - 1 = \log(1 + (e^z - 1)) = z$$

eine Identität für formale Potenzreihen ist. Es wäre ziemlich umständlich, dies direkt *durch Koeffizientenvergleich zu beweisen.*
Für einen einfachen Beweis haben wir zwei Möglichkeiten:

(1) *Wir können nachweisen, daß Identitäten aus der Analysis, sofern sie auch für formale Potenzreihen* sinnvoll *sind (also z.B. keine unendlichen Summen für Koeffizienten implizieren), auch automatisch Identitäten für die entsprechenden formalen Potenzreihen sind. (Diesen Gedanken werden wir in Abschnitt 2.2.2.4 ausführen.)*
(2) *Wir können mit dem* Differentiationsoperator *rechnen.*

2.2.2.3. *Der Differentiationsoperator für formale Potenzreihen.* Als letzte Definition im Zusammenhang mit formalen Potenzreihen führen wir den *Differentiationsoperator* **D** ein, wiederum in Analogie zur Analysis.

DEFINITION 2.2.13. *Sei* $a(z) = a_0 + a_1 z + a_2 z^2 + \cdots = \sum_{n \geq 0} a_n z^n$ *eine formale Potenzreihe. Der Differentiationsoperator* **D** *ist durch*

$$\mathbf{D}\, a := a_1 + 2a_2 z + 3a_3 z^2 + \cdots = \sum_{n \geq 1} n\, a_n z^{n-1}$$

definiert.

Wie in der Analysis üblich werden wir oft a' statt $\mathbf{D}a$ schreiben.

Die folgenden Rechenregeln für den Differentationsoperator sind leicht nachzurechnen.

SATZ 2.2.14. *Für Potenzreihen $a = a(z)$, $b = b(z)$, $n \in \mathbb{Z}$ und $\lambda \in \mathbb{C}$ gilt:*

$$\begin{aligned}
\mathbf{D}(a+b) &= \mathbf{D}a + \mathbf{D}b \\
\mathbf{D}(\lambda a) &= \lambda\, \mathbf{D}a \\
\mathbf{D}(ab) &= (\mathbf{D}a)b + a(\mathbf{D}b) \\
\mathbf{D}(a^n) &= na^{n-1}(\mathbf{D}a) \qquad \textit{(wir setzen } a_0 \neq 0 \textit{ voraus, falls } n < 0\textit{)} \\
\mathbf{D}\left(\frac{a}{b}\right) &= \frac{(\mathbf{D}a)b - a(\mathbf{D}b)}{b^2} \quad \textit{für } b_0 \neq 0 \\
\mathbf{D}(a \circ b) &= ((\mathbf{D}a) \circ b) \cdot (\mathbf{D}b)
\end{aligned}$$

Aufgabe 31 ($\star\star$)**:** *Man zeige für die Fibonaccizahlen F_n die Identität*

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

DEFINITION 2.2.15. *Die* Binomialreihe *ist für eine beliebige komplexe Zahl α definiert als*

$$\sum_{n \geq 0} \binom{\alpha}{n} z^n.$$

(Hier betrachten wir den Binomialkoeffizienten $\binom{x}{k}$ als Polynom in x; für x können wir also beliebige Zahlen einsetzen.)

Analog zur Analysis bezeichnen wir diese Potenzreihe mit $(1+z)^\alpha$.

BEISPIEL 2.2.16. *(1) Es gilt $\mathbf{D}\, \mathrm{e}^z = \mathrm{e}^z$.*

(2) Es gilt $\mathbf{D}\,(1+z)^\alpha = \alpha(1+z)^{\alpha-1}$ (denn $n \cdot \binom{\alpha}{n} = \alpha \cdot \binom{\alpha-1}{n-1}$).

(3) Es gilt $\mathbf{D} \log(1+z) = \frac{1}{1+z}$.

(4) Es gilt $\mathbf{D}\left(\mathrm{e}^{\alpha \log(1+z)}\right) = \mathrm{e}^{\alpha \log(1+z)} \frac{\alpha}{1+z}$.

Es ist leicht zu sehen, daß die Differentialgleichung

$$\mathbf{D}\, f(z) = \frac{\alpha}{1+z} f(z)$$

für formale Potenzreihen nur *eine* Lösung (abgesehen von konstanten Vielfachen) haben kann. Die beiden Lösungen, die wir eben in Beispiel 2.2.16(2) bzw. (4) gesehen haben, müssen also übereinstimmen:

$$\mathrm{e}^{\alpha \log(1+z)} = (1+z)^\alpha.$$

Wenn wir $\alpha = 1$ setzen, dann folgt insbesondere

$$\mathrm{e}^{\log(1+z)} - 1 = z,$$

d.h., $\log(1+z)$ ist tatsächlich die zusammensetzungsinverse Reihe zu $\mathrm{e}^z - 1$.

Aufgabe 32 (⋆ ⋆)**:** *Mit Hilfe des Differenzenoperators* Δ*, definiert durch*

$$\Delta p(x) := p(x+1) - p(x),$$

kann man die Koeffizienten in Reihenentwicklungen der Gestalt

$$q(x) = \sum_k c_k x^{\underline{k}}$$

berechnen ($x^{\underline{k}} = x(x-1)\cdots(x-k+1)$*): Es gilt nämlich*

$$c_k = \frac{1}{k!}\Delta^k q(x)|_{x=0}.$$

(Siehe auch Bemerkung 2.1.22.) Benutze dies, um für $n > 0$ *die Formel*

$$x^{\overline{n}} = x(x+1)\cdots(x+n-1) = \sum_{k=0}^{n} \frac{n!}{k!}\binom{n-1}{k-1} x^{\underline{k}}$$

zu beweisen.

2.2.2.4. *Potenzreihen in der Analysis/in der Diskreten Mathematik.* Es ist tatsächlich so, daß wegen der *Eindeutigkeit der Reihenentwicklung* (die in der Analysis bewiesen wird) eine analytische Identität für Potenzreihen "automatisch" eine Identität für formale Potenzreihen ist und umgekehrt — *sofern* die Identität *sowohl* als analytische Identität *als auch* als formale Identität sinnvoll ist.
Die Einschränkung ist hier nicht leer: Zum Beispiel gilt als *analytische Identität*

$$\mathrm{e}^{\log(2+z)} = 2 + z$$

für alle z vom Betrag kleiner 2; für formale Potenzreihen ist die Zusammensetzung $\exp(\log(2+z))$ aber einfach nicht definiert. Umgekehrt ist

$$\mathbf{D}\left(\sum_{n\geq 1}(n-1)!\, z^n\right) = \sum_{n\geq 1} n!\, z^{n-1}$$

natürlich eine Identität für *formale Potenzreihen*; in der Analysis ist das aber sinnlos, da die Reihen nur für $z = 0$ konvergieren.
Wir halten also fest:

GRUNDREGEL 2.2.17. **Übertragungsprinzip**

Wenn eine Identität für analytische Funktionen auch für die entsprechenden formalen Potenzreihen sinnvoll ist, dann ist sie automatisch auch eine Identität für formale Potenzreihen.
Umgekehrt: Wenn eine Identität für formale Potenzreihen auch für die entsprechenden analytischen Funktionen sinnvoll ist (das heißt, daß es einen nichttrivialen gemeinsamen Konvergenzradius für alle involvierten Reihen gibt), dann ist sie automatisch auch eine Identität für analytische Funktionen.

BEISPIEL 2.2.18. *In der Analysis gilt*

$$\mathrm{e}^{\alpha z}\mathrm{e}^{\beta z} = \mathrm{e}^{(\alpha+\beta)z}.$$

Die Identität ist sinnvoll *für formale Potenzreihen, daher* gilt *sie automatisch auch für formale Potenzreihen.*

Umgekehrt haben wir für formale Potenzreihen die Identität $(1-z)^{-1} = 1 + z + z^2 + \cdots$ *bewiesen. Diese Identität ist für* z *vom Betrag kleiner* 1 (1 *ist der Konvergenzradius der rechten Seite) auch für analytische Funktionen sinnvoll, daher* gilt *sie automatisch auch im Sinn der Analysis.*

Aufgabe 33 ($\star\star$)**:** *Sei* $F(z) = \sum_{n=0}^{\infty} n!\, z^n$.

(1) *Eine Permutation* $a_1 a_2 \dots a_n$ *von* $[n]$ *heißt unzerlegbar, falls* n *die kleinste natürliche Zahl* j *ist, für die* $\{a_1, a_2, \dots, a_j\} = \{1, 2, \dots, j\}$ *gilt. Sei* $f(n)$ *die Anzahl aller unzerlegbaren Permutationen von* $[n]$. *Zeige:*

$$\sum_{n=1}^{\infty} f(n) z^n = 1 - F(z)^{-1}\,.$$

(2) *In einer Permutation* $a_1 a_2 \dots a_n$ *von* $[n]$ *heißt* a_i *ein starker Fixpunkt, falls (1)* $j < i \Rightarrow a_j < a_i$, *und (2)* $j > i \Rightarrow a_j > a_i$. *Sei* $g(n)$ *die Anzahl aller Permutationen von* $[n]$, *die keinen starken Fixpunkt besitzen. Zeige:*

$$\sum_{n=0}^{\infty} g(n) z^n = F(z)(1 + zF(z))^{-1}\,.$$

2.2.3. Lineare Rekursionen mit konstanten Koeffizienten.

Definition 2.2.19. *Eine Folge* $(a_n)_{n=0}^{\infty}$ *komplexer Zahlen wird durch eine* lineare Rekursion mit konstanten Koeffizienten *beschrieben, wenn für ein festes* $k \in \mathbb{N}$ *und feste komplexe Zahlen* $c_1, \dots c_k$ *gilt:*

$$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k} \text{ für } n \geq k.$$

Der Parameter k heißt in diesem Zusammenhang die Ordnung *der Rekursion.*
$(a_n)_{n=0}^{\infty}$ *ist aber nicht die einzige Lösung dieser* Rekursionsgleichung*: Die "allgemeine Lösung"* $(d_n)_{n=0}^{\infty}$ *hängt von k frei wählbaren Parametern ab und wird erst eindeutig durch die Vorgabe der* Anfangsbedingungen

$$d_0 = a_0,\ d_1 = a_1, \dots, d_{k-1} = a_{k-1}.$$

Anhand der Fibonacci–Rekursion hatten wir gesehen, wie erzeugende Funktionen zu einer expliziten Formel für die Fibonacci–Zahlen geführt haben. Daß dieses Verfahren für lineare Rekursionen "immer funktioniert", wollen wir nun anhand eines weiteren Beispiels demonstrieren.

Beispiel 2.2.20. *Betrachten wir die Rekursionsgleichung*

$$a_n = 5a_{n-1} - 8a_{n-2} + 4a_{n-3}, \quad n \geq 3,$$

mit den Anfangsbedingungen

$$a_0 = -1, a_1 = 1, a_2 = 7.$$

Wir multiplizieren beide Seiten der Rekursion mit z^n *und summieren über alle* $n \geq 3$ *(im allgemeinen Fall summiert man über* $n \geq k$, *wenn k die Ordnung der Rekursion ist).*
Wenn man die erzeugende Funktion der Folge $(a_n)_{n=0}^{\infty}$ *mit* $a(z)$ *bezeichnet, also*

$$a(z) = \sum_{n \geq 0} a_n z^n,$$

dann kann man das so schreiben:

$$a(z) - 7z^2 - z + 1 = 5z(a(z) - z + 1) - 8z^2(a(z) + 1) + 4z^3 a(z).$$

Daraus rechnet man $a(z)$ *aus:*

$$a(z) = \frac{-6z^2 + 6z - 1}{1 - 5z + 8z^2 - 4z^3}.$$

Es ist klar, daß das auch im allgemeinen funktioniert — als Ergebnis wird man die erzeugende Funktion immer als rationale Funktion *erhalten, also als Quotienten von Polynomen:* $f(z) = \frac{p(z)}{q(z)}$.

Mit dem *Taylorschen Lehrsatz* der Analysis könnten wir nun direkt die Reihenentwicklung bestimmen; wir können aber zweckmäßiger wie folgt vorgehen. Bekanntlich besagt der *Fundamentalsatz der Algebra*, daß man ein Polynom mit komplexen Koeffizienten immer in Linearfaktoren zerlegen kann. Aus der Analysis kennen wir die Partialbruchzerlegung, die für die Integration rationaler Funktionen gebraucht wird.

Satz 2.2.21 (Partialbruchzerlegung). *Sei* $f(z) = \frac{p(z)}{q(z)}$ *eine rationale Funktion, sei* d_p *der Grad von* p *und* d_q *der Grad von* q*, und sei die Zerlegung in Linearfaktoren für* q *bekannt:*

$$q(z) = (1 - \alpha_1 z)^{e_1}(1 - \alpha_2 z)^{e_2} \cdots (1 - \alpha_\ell z)^{e_\ell}.$$

Dann kann man f *in der Form*

$$f(z) = R(z) + \frac{C_{1,1}}{(1-\alpha_1 z)} + \frac{C_{1,2}}{(1-\alpha_1 z)^2} + \cdots + \frac{C_{1,e_1}}{(1-\alpha_1 z)^{e_1}} + \cdots + \frac{C_{\ell,1}}{(1-\alpha_\ell z)} + \frac{C_{\ell,2}}{(1-\alpha_\ell z)^2} + \cdots + \frac{C_{\ell,e_\ell}}{(1-\alpha_\ell z)^{e_\ell}} \quad (2.34)$$

schreiben, mit gewissen eindeutig bestimmten Koeffizienten $C_{i,j} \in \mathbb{C}$ *und einem eindeutig bestimmten Polynom* R *vom Grad* $d_p - d_q$*; falls* $d_q > d_p$*, ist* $R \equiv 0$*.*

In jedem konkreten Fall ist die Partialbruchzerlegung immer "leicht" durchzuführen (wenn man einmal das Nennerpolynom faktorisiert hat): Zunächst bestimmen wir (falls notwendig, d.h., falls $d_p \geq d_q$) das Polynom R durch Division mit Rest, und lesen dann (2.34) als "*unbestimmten Ansatz*" für die gesuchten Koeffizienten $C_{i,j}$. Wenn wir dann die rechte Seite von (2.34) auf gleichen Nenner bringen, erhalten wir durch *Koeffizientenvergleich* ein lineares Gleichungssystem, das wir mit den bekannten Methoden der Linearen Algebra lösen können.

Beispiel 2.2.22. *Wir führen unser obiges Beispiel fort und bestimmen zunächst die Faktorisierung für das Nennerpolynom:*

$$a(z) = \frac{-6z^2 + 6z - 1}{(1-2z)^2(1-z)}.$$

Das Polynom R *ist hier* 0*, da der Grad des Zählerpolynoms (*2*) kleiner ist als der Grad des Nennerpolynoms (*3*).*

Als nächstes bestimmen wir die Partialbruchzerlegung *mit dem unbestimmten Ansatz:*

$$\frac{-6z^2+6z-1}{(1-2z)^2(1-z)} = \frac{A}{1-2z} + \frac{B}{(1-2z)^2} + \frac{C}{1-z}.$$

Wir bringen die rechte Seite auf gleichen Nenner und kürzen:

$$-6z^2+6z-1 = A(1-2z)(1-z) + B(1-z) + C(1-2z)^2.$$

Wir multiplizieren die rechte Seite aus und erhalten

$$-6z^2+6z-1 = (2A+4C)\,z^2 - (3A+B+4C)\,z + (A+B+C)\,.$$

Koeffizientenvergleich für z^0, z^1 und z^2 liefert drei Gleichungen in den drei Unbekannten A, B, C:

$$\begin{aligned} -6 &= 2A+4C \\ 6 &= -3A-B-4C \\ -1 &= A+B+C \end{aligned}$$

Als Lösung erhalten wir $A = -1$, $B = 1$ und $C = -1$. Somit lässt sich unsere erzeugende Funktion als

$$a(z) = -\frac{1}{1-2z} + \frac{1}{(1-2z)^2} - \frac{1}{1-z}$$

schreiben.
Alle Brüche auf der rechten Seite haben die Gestalt $\frac{\beta}{(1+\alpha\cdot z)^m}$ (es ist klar, daß das auch auch im allgemeinen gilt!) und sind somit Binomialreihen, die wir explizit hinschreiben können:

$$a(z) = -\sum_{n\geq 0} 2^n z^n + \sum_{n\geq 0}(n+1)2^n z^n - \sum_{n\geq 0} z^n.$$

Durch Koeffizientenvergleich erhalten wir die Formel

$$a_n = n2^n - 1.$$

Wir können diese Methode zur Lösung linearer Rekursionen wie folgt zusammenfassen:

(1) *Gewinne aus der Rekursion eine Gleichung für die erzeugende Funktion*: Multipliziere beide Seiten mit z^n, summiere über alle n.
(2) *Löse die Gleichung für die erzeugende Funktion*: Man erhält in jedem Fall eine rationale Funktion.
(3) *Führe die Partialbruchzerlegung durch.*
(4) *Entwickle die entstandenen Brüche in Binomialreihen.*
(5) *Lies die Koeffizienten ab.*

Aus unseren Überlegungen können wir das folgende Korollar ableiten:

KOROLLAR 2.2.23. *Gegeben sei die Rekursion*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \quad n \geq k.$$

Wir nehmen weiters an, daß das zugehörige charakteristische Polynom *die Faktorisierung*

$$1 - c_1 x - c_2 x^2 - \cdots - c_k x^k = (1-\alpha_1 x)^{e_1}(1-\alpha_2 x)^{e_2}\cdots(1-\alpha_\ell x)^{e_\ell}$$

besitzt.
Dann hat jede Lösung der Rekursion die Gestalt

$$a_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_\ell(n)\alpha_\ell^n,$$

wo $P_i(n)$ ein Polynom in n vom Grad $e_i - 1$[13] *ist. Umgekehrt ist* jede *derart gegebene Folge (a_n) eine Lösung der Rekursion.*

Aufgabe 34 ($\star\,\star$)**:** *Finde einen geschlossenen Ausdruck für die Glieder der Folge $(a_n)_{n\in\mathbb{N}_0}$, die der Rekursion $a_n = a_{n-1} + 2a_{n-2} + (-1)^n$ mit den Anfangsbedingungen $a_0 = a_1 = 1$ genügt.*

Aufgabe 35 ($\star\,\star$)**:** *Finde einen geschlossenen Ausdruck für die Glieder der Folge $(a_n)_{n\in\mathbb{N}_0}$, die der Rekursion $a_n = -a_{n-1} + 5a_{n-2} - 3a_{n-3}$ mit den Anfangsbedingungen $a_0 = 7$, $a_1 = -12$, $a_2 = 49$ genügt.*

Aufgabe 36 ($\star\,\star$)**:** *Finde einen geschlossenen Ausdruck für die Glieder der Folge $(a_n)_{n\in\mathbb{N}_0}$, die der Rekursion $a_n = 6a_{n-1} - 4a_{n-2}$ mit den Anfangsbedingungen $a_0 = 1$, $a_1 = 3$ genügt. Zeige, daß $a_n = \lceil \frac{(3+\sqrt{5})^n}{2} \rceil$.*

Aufgabe 37 ($\star\,\star$)**:** *Löse die Rekursion $a_n = 3a_{n-1} - a_{n-2}$ mit den Anfangsbedingungen $a_0 = 1$, $a_1 = 2$. Hat das etwas mit Fibonaccizahlen zu tun?*

Aufgabe 38 ($\star\,\star\,\star$)**:** *Auf wieviele Arten kann ein Pfeiler, der die Form eines $2\times 2\times n$-Quaders besitzt, aus $2\times 1\times 1$-Ziegeln aufgebaut werden?*
Anleitung: Sei a_n die gesuchte Zahl und b_n die entsprechende Anzahl, einen $2\times 2\times n$-Pfeiler, dem in der obersten Ebene ein Ziegel fehlt, aus solchen Ziegeln zusammenzusetzen. Zeige zunächst die Rekurrenzen

$$\begin{aligned} a_n &= 2a_{n-1} + 4b_{n-1} + a_{n-2} + [n=0]\,, \\ b_n &= a_{n-1} + b_{n-1}\,. \end{aligned}$$

Leite daraus 2 Gleichungen für die entsprechenden erzeugenden Funktionen her und gewinne daraus die gesuchte erzeugende Funktion.

2.2.4. Nochmals die Catalan–Zahlen. Wir betrachten noch einmal die Rekursion (2.20) für die Triangulierungen des $(n+2)$–Ecks. Wieder multiplizieren wir beide Seiten mit z^n in (2.20) und summieren über alle $n \geq 3$ auf. Diesmal definieren wir (aus rein "technischen Gründen") die erzeugende Funktion "etwas verschoben":

$$F(z) = \sum_{n\geq 0} f(n+2)\, z^n.$$

Wir erhalten die Funktionalgleichung

$$z^2 F(z) - z^2 = z^3 F(z)^2\,,$$

oder äquivalent

$$zF(z)^2 - F(z) + 1 = 0.$$

Das ist eine quadratische Gleichung in F, die wir lösen können:

$$F(z) = \frac{1 \pm \sqrt{1-4z}}{2z}.$$

[13] Denn $\binom{-e}{n}$ ist ein Polynom in n vom Grad $e-1$.

Nur eine dieser Lösungen ist eine Potenzreihenlösung (nämlich die mit dem Minuszeichen[14]):

$$F(z) = \frac{1 - \sqrt{1-4z}}{2z}.$$

Benutzt man wieder die Binomialreihenentwicklung, dann erhält man:

$$\begin{aligned}
F(z) &= \frac{1-(1-4z)^{1/2}}{2z} \\
&= \frac{1}{2z}\left(1 - \sum_{n\geq 0}\binom{1/2}{n}(-4)^n z^n\right) \\
&= -\sum_{n\geq 0}\binom{1/2}{n+1}\frac{(-4)^{n+1}}{2}z^n \\
&= -\sum_{n\geq 0}\frac{(\frac{1}{2})(-\frac{1}{2})\cdots(\frac{1}{2}-n)}{(n+1)!}\cdot\frac{(-4)^{n+1}}{2}z^n \\
&= \sum_{n\geq 0}\frac{1\cdot 1\cdot 3\cdots(2n-1)}{(n+1)!}2^n z^n \\
&= \sum_{n\geq 0}\frac{(2n)!}{(n+1)!\,n!}z^n.
\end{aligned}$$

Durch Koeffizientenvergleich erhalten wir also wieder die Catalan–Zahlen aus (2.19) als Koeffizienten; es gilt also $f(n+2) = C_n$.

Aufgabe 39 ($\star\star$)**:** *Bestimme jene eindeutig bestimmte Folge $(a_n)_{n\in\mathbb{N}_0}$, für die $a_0 = 1$ und*

$$\sum_{k=0}^{n} a_k a_{n-k} = 1$$

für alle $n \in \mathbb{N}$ gilt.

2.2.5. Nochmals die Stirling–Zahlen der zweiten Art. Wir wollen nun erzeugende Funktionen für die Stirling–Zahlen zweiter Art finden. Ganz analog zu den bisherigen Beispielen beginnen wir mit einer Rekursion:

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

Dies ergibt sich im wesentlichen aus der Summenregel, denn die Menge *aller* Partitionen von $[n]$ zerfällt in zwei disjunkte Teilmengen, nämlich

- Jene Partitionen, bei denen n einen eigenen Block bildet,
- und jene Partitionen, bei denen n keinen eigenen Block bildet.

Im ersten Fall können wir den Singleton–Block $\{n\}$ weglassen und erhalten eine Partition von von $[n-1]$ in $(k-1)$ Blöcke — die Anzahl dieser Partitionen ist $S_{n-1,k-1}$.

Im zweiten Fall können wir das Element n aus seinem Block entfernen: Übrig bleibt eine Partition von $[n-1]$ in k Blöcke — die Anzahl dieser Partitionen ist $S_{n-1,k}$; und aus *jeder* solchen Partition können wir k verschiedene Partitionen

[14] Für Analytiker: Die andere Lösung hat einen Pol bei 0.

von $[n]$ machen, indem wir das Element n in einen der k Blöcke "dazustecken". Insgesamt sehen wir: Die Anzahl der Partitionen im zweiten Fall ist $k \cdot S_{n-1,k}$.

Nun multiplizieren wir beide Seiten der Rekursion mit $\frac{z^{n-1}}{(n-1)!}$ (diese Modifikation stellt sich als bequem heraus) und summieren über alle $n \geq 1$. Betrachten wir die "modifizierte erzeugende Funktion"

$$S_k(z) := \sum_{n \geq 0} S_{n,k} \frac{z^n}{n!}$$

(man nennt diese Form auch die *exponentiell erzeugende Funktion*). Dann erhalten wir für alle k

$$\mathbf{D}\, S_k(z) = S_{k-1}(z) + k \cdot S_k(z),$$

also ein unendliches System von Differentialgleichungen.

Als Anfangsbedingung haben wir $S_0(z) = 1$, also haben wir für $k = 1$ die Differentialgleichung:

$$\mathbf{D}\, S_1(z) = S_0(z) + S_1(z) = 1 + S_1(z).$$

Diese *lineare Differentialgleichung mit konstanten Koeffizienten* läßt sich (mit Methoden aus der Vorlesung "Differentialgleichungen"...) leicht lösen; wir geben hier die Lösung einfach an (daß sie richtig ist, ist sehr leicht zu sehen):

$$S_1(z) = \mathrm{e}^z - 1.$$

Für $k = 2$ haben wir dann die Differentialgleichung:

$$\mathbf{D}\, S_2(z) = S_1(z) + 2S_2(z) = \mathrm{e}^z - 1 + 2S_2(z).$$

Wieder borgen wir uns die Lösung von der Theorie der Differentialgleichungen (die Richtigkeit ist sofort leicht nachprüfbar):

$$S_2(z) = \frac{(\mathrm{e}^z - 1)^2}{2}.$$

Etwas kühn vermuten wir schon an dieser Stelle die allgemeine Lösung

$$S_k(z) = \frac{(\mathrm{e}^z - 1)^k}{k!}, \tag{2.35}$$

deren Richtigkeit wir ohne Schwierigkeiten durch Induktion nach k nachrechnen können.

Aus dem Binomischen Lehrsatz folgt nun

$$S_k(z) = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} \mathrm{e}^{iz},$$

und durch Koeffizientenvergleich erhalten wir

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} i^n; \tag{2.36}$$

dasselbe Ergebnis wie in (2.15).

2.2.6. Nochmals die Stirling–Zahlen der ersten Art. Nun wollen wir auch noch die exponentiell erzeugende Funktionen

$$s_k(z) := \sum_{n\geq 0} s_{n,k}\frac{z^n}{n!}$$

für die Stirling–Zahlen der ersten Art ausrechnen; analog zu (2.35).

Wir ersetzen zuerst in der Rekursion (2.6) $c(n,k)$ durch $(-1)^{n-k}s_{n,k}$:

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

Dann multiplizieren wir wieder beide Seiten mit $\frac{z^{n-1}}{(n-1)!}$ und summieren über alle n. Dadurch erhalten wir für alle k die Differentialgleichung

$$\mathbf{D}s_k(z) = s_{k-1}(z) - z\cdot\mathbf{D}s_k(z),$$

oder äquivalent

$$(1+z)\,\mathbf{D}s_k(z) = s_{k-1}(z).$$

Die Anfangsbedingung lautet $s_0(z) = 1$. Es ist wieder nicht schwer[15], die allgemeine Lösung zu erraten:

$$s_k(z) = \frac{(\log(1+z))^k}{k!}. \tag{2.37}$$

Die Richtigkeit dieser Lösung ist leicht (durch Induktion nach k) nachprüfbar.

Bemerkung 2.2.24. *Wenn man die Gestalt der erzeugenden Funktionen für die Stirling–Zahlen erster und zweiter Art (also Gleichungen* (2.37) *und* (2.35)*) vergleicht, dann sieht man, daß erstere durch* $\log(1+z)$ *"erzeugt" werden, während letztere durch* $e^z - 1$ *"erzeugt" werden. Diese beiden Reihen sind zueinander (bezüglich der Zusammensetzung) invers. Es ist kein Zufall, daß auch die Matrizen der Stirling–Zahlen der ersten und zweiten Art zueinander invers sind (wie wir zuvor gesehen haben): Es gibt eine ganze Theorie, die sich um diesen Sachverhalt (und andere) rankt, den sogenannten* Umbralen Kalkül, *siehe dazu* **[6]**.

2.2.7. (Zahl–)Partitionen. Eine (Zahl–)Partition einer natürlichen Zahl n ist "eine Komposition von n, bei der es auf die Reihenfolge nicht ankommt":

Definition 2.2.25. *Eine* (Zahl–)Partition *von* $n \in \mathbb{Z}^+$ *(mit k Teilen) ist eine Darstellung von n als Summe natürlicher Zahlen*

$$n = a_1 + a_2 + \cdots + a_k,$$

wobei es auf die Reihenfolge *der Summanden* nicht *ankommt — daher können wir annehmen, daß die* Teile *(also die Summanden) in absteigender Größe numeriert sind, also* $a_1 \geq a_2 \geq \cdots \geq a_k$.

Die Anzahl aller *(Zahl–)Partitionen von n bezeichnen wir mit* $\mathbf{p}(n)$.

Speziell setzen wir $\mathbf{p}(0) = 1$ *— wenn man will, kann man das so sehen, daß die einzige Partition von* 0 *die leere Summe* $\sum_{i=1}^{0} a_i$ *ist.*

[15] . . . wenn man Kenntnisse aus Differentialgleichungen hat . . .

BEMERKUNG 2.2.26. *In der Regel nennt man diese Objekte einfach Partitionen; wir verwenden hier die Bezeichnung (Zahl–)Partitionen, um eine Verwechslung mit den* Mengen–Partitionen *zu vermeiden.*

BEISPIEL 2.2.27. *Die ersten 5 Werte von* $\mathbf{p}(n)$ *lauten:*

$$\begin{aligned}
&\mathbf{p}(0) = 1 : 0 = \sum_{i=1}^{0} a_i, \\
&\mathbf{p}(1) = 1 : 1 = (1), \\
&\mathbf{p}(2) = 2 : 2 = (2) = (1+1), \\
&\mathbf{p}(3) = 3 : 3 = (3) = (2+1) = (1+1+1), \\
&\mathbf{p}(4) = 5 : 4 = (4) = (3+1) = (2+2) = (2+1+1) = (1+1+1+1).
\end{aligned}$$

Die nächsten Werte lauten $\mathbf{p}(5) = 7$ *und* $\mathbf{p}(6) = 11$. *Die Folge wächst sehr schnell, z.B. ist* $\mathbf{p}(100) = 190569292$.

Für die Zahlenfolge $(\mathbf{p}(n))_{n=0}^{\infty}$ gibt es keine so einfache Formel wie für die Folge der Kompositionen; aber die erzeugende Funktion dieser Folge können wir sehr kompakt als unendliches Produkt[16] schreiben.

SATZ 2.2.28. *Sei* $H \subseteq \mathbb{N}$, *und sei* $\mathbf{p}(H,n)$ *die Anzahl aller (Zahl–)Partitionen von* n, *deren Teile sämtlich Elemente aus* H *sind. (Die "normale Funktion"* $\mathbf{p}(n)$ *ist also gleich* $\mathbf{p}(\mathbb{N},n)$.*) Dann gilt für die erzeugende Funktion*

$$F_H(z) := \sum_{n\geq 0} \mathbf{p}(H,n)\, z^n = \prod_{n\in H} \frac{1}{1-z^n}.$$

BEWEIS. Der ganze Beweis besteht lediglich in simplem Ausmultiplizieren!

$$\begin{aligned}
\prod_{n\in H} \frac{1}{1-z^n} &= \prod_{n\in H} \left(1 + z^n + z^{2n} + z^{3n} + \cdots\right) \\
&= \left(1 + z^{h_1} + z^{2h_1} + z^{3h_1} + \cdots\right) \\
&\times \left(1 + z^{h_2} + z^{2h_2} + z^{3h_2} + \cdots\right) \\
&\times \left(1 + z^{h_3} + z^{2h_3} + z^{3h_3} + \cdots\right) \\
&\times \cdots \\
&= \sum_{i_1\geq 0} \sum_{i_2\geq 0} \sum_{i_3\geq 0} \cdots z^{i_1 h_1 + i_2 h_2 + i_3 h_3 + \cdots},
\end{aligned}$$

und den Exponenten von z deuten wir als die Partition

$$\left(\underbrace{h_1 + \cdots + h_1}_{i_1\text{–mal}} + \underbrace{h_2 + \cdots + h_2}_{i_2\text{–mal}} + \underbrace{h_3 + \cdots + h_3}_{i_3\text{–mal}} + \cdots \right),$$

[16] Eigentlich haben wir unendliche Produkte noch nicht "formal eingeführt", aber nach unseren guten Erfahrungen mit formalen Potenzreihen sind wir wohl gut vorbereitet.

die natürlich nur Teile $h_i \in H$ enthält. Die Potenz z^n kommt also in der Entwicklung so oft vor, wie es Partitionen von n mit Teilen aus H gibt. □

Aufgabe 40 ($\star\star$)**:** *Sei $\mathbf{p}^*(n)$ die Anzahl aller Partitionen von n, bei denen*

- *der Teil 1 beliebig oft vorkommen kann,*
- *der Teil 3 höchstens 4–mal vorkommen darf,*
- *der Teil 7 entweder gar nicht oder genau 2–mal vorkommen darf,*
- *und sonst keine andren Teile vorkommen dürfen.*

Wie sieht die erzeugende Funktion der Folge $(\mathbf{p}^*(n))_{n=0}^{\infty}$ aus?

Aufgabe 41 ($\star\star$)**:** *Beweise, daß die Anzahl der (Zahl–)Partitionen von n, deren Summanden alle nicht durch 3 teilbar sind, gleich ist der Anzahl der Partitionen, in denen kein Summand mehr als zweimal erscheint.*
Beispiel: $4=4,\ 2+2,\ 2+1+1,\ 1+1+1+1$ *beziehungsweise* $4=4,\ 3+1,\ 2+2,\ 2+1+1$.
(Anleitung: Drücke beide Anzahlen unter Verwendung des Prinzipes der Inklusion–Exklusion durch die Partitionsfunktion $p(.)$ aus, wobei $p(n)$ $alle$ Partitionen von n bezeichnet.)

Wir können hier nicht weiter auf (Zahl–)Partitionen eingehen: Eine Fülle an Material zu diesem Thema findet man in [**2**].

KAPITEL 3

Graphen und Netzwerke

3.1. Graphen und Digraphen

Den Begriff *Graph* haben wir bereits im einleitenden Kapitel kennengelernt. Für manche Zwecke ist es aber notwendig, die Definition 1.3.2, die wir dort gegeben haben, zu erweitern. (Wir betrachten hier *nur endliche* Graphen.)

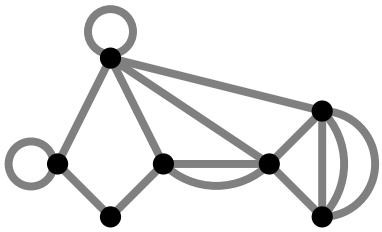
DEFINITION 3.1.1. *Ein* Graph **G** *ist gegeben durch eine (endliche) Menge V von Knoten und eine (endliche)* Multimenge *E von Kanten. In Erweiterung von Definition 1.3.2 lassen wir als Kanten nun auch zu:*

- *Schlingen: Unter einer* Schlinge *verstehen wir eine Kante, die einen Knoten v mit sich selbst verbindet; eine Schlinge entspricht also der* Multimenge $\{v, v\}$.

  Abstrakt: Für einen Graphen mit Schlingen ist E gegeben durch eine Teilmenge der Familie der 2–elementigen Multimengen von V.
- *mehrfache Kanten: Von einer* mehrfachen Kante *sprechen wir, wenn ein und dasselbe Paar von Knoten durch mehrere Kanten verbunden ist. (Falls ein und derselbe Knoten durch mehrere Schlingen mit sich selbst verbunden ist, sprechen wir von* mehrfachen Schlingen.*)*
  Abstrakt: Für einen Graphen mit mehrfachen Kanten und Schlingen ist E gegeben durch eine Multimenge der Familie der 2–elementigen Multimengen von V.

Einen Graphen ohne Schlingen und ohne mehrfache Kanten bezeichnen wir ab jetzt als einfachen Graphen*.*

Die folgende Graphik illustriert diesen Begriff:



BEMERKUNG 3.1.2. *Eine Schlinge $\{v, v\}$ trägt 2 zum Grad (siehe Definition 1.4.1) von v bei; sie wird als mit v inzidente Kante also "doppelt gezählt".*

Weiters brauchen wir eine Spezialisierung des Begriffs *Wanderung* (siehe Definition 1.3.2).

DEFINITION 3.1.3. *Sei* **G** *ein Graph. Eine Wanderung $v_0, v_1, \ldots, v_n$ in G mit der Eigenschaft, daß*

- *alle Knoten (außer eventuell der erste und der letzte) verschieden sind (d.h.: für* $0 \leq i < j \leq n$, $(i,j) \neq (0,n)$ *gilt* $v_i \neq v_j$*),*
- *und alle Kanten* $\{v_{i-1}, v_i\}$ *verschieden sind*[1]*,*

nennen wir

- *einen* Weg *von* v_0 *nach* v_n*, wenn* $v_0 \neq v_n$*,*
- *einen* Kreis*, wenn* $v_0 = v_n$*.*

Bemerkung 3.1.4. *Eine Schlinge ist ein Spezialfall eines Kreises. Die scheinbar überflüssige Bedingung, daß alle Kanten verschieden sein sollen, spielt nur in einem weiteren Spezialfall eine Rolle:* (v_0, v_1, v_0) *kann ein Kreis sein — aber nur dann, wenn* $\{v_0, v_1\}$ *eine* mehrfache *Kante ist.*

Für Fragen des *Zusammenhangs* (siehe Definition 1.3.5) in Graphen ist es egal, ob wir Wanderungen oder Wege betrachten:

Proposition 3.1.5. *Sei G ein Graph. Zwei Knoten v, u in G sind genau dann durch einen Weg verbunden, wenn sie durch eine Wanderung verbunden sind.*

Beweis. Jeder Weg *ist* eine Wanderung, daher ist die eine Richtung klar.

Umgekehrt überlegen wir, daß jede Wanderung $v = v_0, v_1, \ldots, v_n = u$ zu einem Weg "verkürzt" werden kann: Solange es einen Knoten w in der Wanderung gibt, der mehrfach vorkommt, schneiden wir das Stück zwischen dem ersten und letzten Vorkommnis von w heraus:

$$\left(v_0, \ldots, v_k, \underbrace{w, \ldots, w}_{\text{ausschneiden!}}, v_m, \ldots, v_n \right) \to (v_0, \ldots, v_k, w, v_m, \ldots, v_n)\,.$$

Wenn es keinen solchen Knoten (mehr) gibt, haben wir einen Weg vor uns, der v mit u verbindet. □

Aufgabe 42 (⋆ ⋆)**:** *Sei* **G** *ein einfacher Graph mit* n *Knoten; und sei für je zwei Knoten* v_1, v_2, *die nicht durch eine Kante verbunden sind, die Summe ihrer Grade mindestens* $n-1$*. Zeige:* **G** *ist zusammenhängend.*

Definition 3.1.6. *Sei* $\mathbf{G}$ (V, E) *ein Graph. Die* Adjazenzmatrix *von* $\mathbf{G}$ *ist eine* $|V| \times |V|$ *Matrix* $A(\mathbf{G})$*, deren Zeilen und Spalten wir uns durch die Knoten aus V bezeichnet denken, und deren Eintrag in Zeile* v_i*, Spalte* v_j *gleich der Vielfachheit von* $\{v_i, v_j\}$ *in E ist.*

Aufgabe 43 (⋆ ⋆)**:** *Sei* **G** *ein Graph mit Adjazenzmatrix* $A = A(\mathbf{G})$*. Zeige: Der Eintrag in Zeile* v_i*, Spalte* v_j *in* A^m *ist gleich der Anzahl der Wanderungen der Länge* m *von* v_i *nach* v_j*.*

Bemerkung 3.1.7. *Klarerweise ist* $A(\mathbf{G})$ *eine reelle symmetrische Matrix und daher diagonalisierbar: Die Untersuchung ihrer Eigenwerte kann interessante Aussagen über den zugrundeliegenden Graphen liefern, siehe etwa das Lehrbuch von N. Biggs* **[3]**.

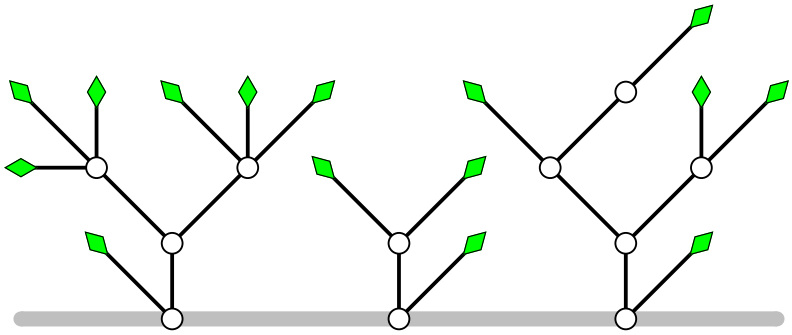
[1] Diese Bedingung wird nur für einen Spezialfall benötigt: (v_0, v_1, v_0) kann nur dann ein Kreis sein, wenn es zwei *verschiedene* Kanten von v_0 nach v_1 gibt!

3.2. Bäume und Wälder

DEFINITION 3.2.1. *Ein* Wald *ist ein Graph, der keinen Kreis enthält.*
Ein Baum *ist ein zusammenhängender Wald.*
Ein Knoten vom Grad 1 *in einem Wald heißt ein* Blatt.

Diese vom botanischen Standpunkt abwegige Definition wird etwas plausibler, wenn man sich vor Augen hält, daß die *Zusammenhangskomponenten* (siehe Definition 1.3.5) eines Waldes Bäume sind. Die folgende Graphik zeigt einen Wald mit drei Bäumen; seine Blätter sind hier als Rhomben gezeichnet:

Ein Wald besteht aus Bäumen!



Bäume haben wir bereits (in Form von *Entscheidungsbäumen*) in Abschnitt 1.5 kennengelernt: Das "Wesen" eines Baumes ist, daß sich seine Äste "immer weiter verzweigen" können, aber niemals "zusammenwachsen" (was einen Kreis ergeben würde).

LEMMA 3.2.2. *Ein Baum* **T** *mit* $n > 1$ *Knoten hat (mindestens) ein Blatt.*

BEWEIS. Angenommen, es gäbe keinen Knoten vom Grad 1. Da ein Baum zusammenhängend ist, gibt es (außer für $n = 1$) keinen *isolierten Knoten* (das ist ein Knoten vom Grad 0, der eine eigene Zusammenhangskomponente darstellt). Daher müßte also jeder Knoten Grad mindestens 2 haben. Dies wiederum würde bedeuten, daß es beliebig lange Wanderungen in **T** gibt, bei denen *niemals* eine Kante zweimal *unmittelbar hintereinander* durchlaufen wird. Es würde also eine solche Wanderung w geben, deren Länge größer ist als n: Darin muß es dann aber notwendigerweise (mindestens) einen Knoten geben, der (mindestens) zweimal vorkommt. Ein *minimaler* Abschnitt in w[2] von einem solchen Knoten v zu dem nächsten Auftreten von v in der Wanderung

$$\Big(\ldots, \underbrace{v, \ldots, v}_{\text{geschlossener Weg} = \text{Kreis!}}, \ldots \Big)$$

würde einen Kreis bilden (denn der Abschnitt kann nicht vom Typ (v, x, v) sein, da niemals eine Kante unmittelbar hintereinander zweimal durchlaufen wird); ein Widerspruch. □

[2]Genauer: Sei $w = (v_1, v_2, \ldots, v_n)$. Ordne die Menge aller Paare (i, j) mit $1 < i < j < n$ und $v_i = v_j$, durch $(i, j) \leq (k, l) :\Leftrightarrow i \geq k$ und $j \leq l$ ("Intervall–Inklusion"): In dieser teilweise geordneten Menge gibt es minimale Elemente.

Ein *zusammenhängender* Graph hat "relativ viele Kanten", ein Graph *ohne Kreise* hat "relativ wenige Kanten": Für einen *Baum* mit n Knoten ist die Anzahl seiner Kanten eindeutig festgelegt, wie das nächste Resultat zeigt.

LEMMA 3.2.3. *Ein Baum* $\mathbf{T}$ *mit genau* n *Knoten hat genau* $n-1$ *Kanten.*

BEWEIS. Wir zeigen die Behauptung mit Induktion. Die Sache ist klar für $n = 1$ (denn die einzigen möglichen Kanten in diesem Fall wären Schlingen, die bilden aber Kreise).
Für den Induktionsschritt von $n-1$ auf n wählen wir ein Blatt, also einen Knoten v vom Grad 1 in $\mathbf{T}$ (den es nach Lemma 3.2.2 geben muß) und betrachten den Graphen $\mathbf{T} - \mathbf{v}$, der aus $\mathbf{T}$ entsteht, wenn wir den Knoten v zusammen mit der (einzigen) inzidenten Kante entfernen. $\mathbf{T} - \mathbf{v}$ hat $n-1$ Knoten, enthält keinen Kreis und ist zusammenhängend (denn kein Weg in $\mathbf{T}$, der zwei Knoten $x, y \neq v$ verbindet, kann den Knoten v enthalten): $\mathbf{T} - \mathbf{v}$ ist also ein Baum und hat nach Induktionsvoraussetzung $n-2$ Kanten, $\mathbf{T}$ hat also $n-1$ Kanten. □

KOROLLAR 3.2.4. *Ein Baum* $\mathbf{T}$ *mit* $n > 1$ *Knoten hat (mindestens) zwei Blätter.*

BEWEIS. Wir erinnern uns an Proposition 1.4.2:

$$\sum_{v \in V(\mathbf{T})} \deg(v) = 2 \cdot \left|E(\mathbf{T})\right| = 2 \cdot (n-1).$$

Angenommen, es gäbe nur *ein* Blatt b, dann wäre

$$\sum_{v \in V(\mathbf{T})} \deg(v) = 1 + \sum_{v \in V(\mathbf{T}) \setminus \{b\}} \underbrace{\deg(v)}_{\geq 2} \geq 1 + 2 \cdot (n-1),$$

ein Widerspruch. □

KOROLLAR 3.2.5. *Ein* Wald *mit* n *Knoten und* m *Zusammenhangskomponenten hat* $n-m$ *Kanten; insbesondere hat er also* höchstens $n-1$ *Kanten (mit Gleichheit dann und nur dann, wenn er ein Baum ist).*

BEWEIS. Für einen Wald $\mathbf{F}$ mit n Knoten und mit m Komponenten $\mathbf{T}_1, \ldots, \mathbf{T}_m$, die jeweils $a_1, \ldots, a_m$ Knoten enthalten, gilt $\sum_{i=1}^{m} a_i = n$. Jede Komponente $\mathbf{T}_i$ ist ein Baum und hat nach Lemma 3.2.3 also $a_i - 1$ Kanten. Also hat $\mathbf{F}$

$$\sum_{i=1}^{m} (a_i - 1) = n - m$$

Kanten. □

KOROLLAR 3.2.6. *Ein* zusammenhängender Graph *mit* n *Knoten hat* mindestens $n-1$ *Kanten; er hat* genau $n-1$ *Kanten dann und nur dann, wenn er ein Baum ist.*

BEWEIS. Wir betrachten einen beliebigen zusammenhängenden Graphen $\mathbf{G}$, der *kein* Baum ist. Dann gibt es also einen Kreis C in $\mathbf{G}$. Sei e eine Kante in C, und sei $\mathbf{G} - \mathbf{e}$ der Graph, der aus $\mathbf{G}$ durch das Entfernen von e entsteht. $\mathbf{G} - \mathbf{e}$ ist noch immer zusammenhängend (denn in jeder Wanderung in $\mathbf{G}$, die die Kante e benutzt, kann e durch den Weg $C - e$ ersetzt werden). Dieses "Zerstören von Kreisen" können wir solange wiederholen, bis ein Baum entstanden ist:

Angenommen, wir brauchen dafür r Schritte, dann enthält der ursprüngliche Graph $\mathbf{G}$ also $n-1+r$ Kanten, $r>0$. □

Definition 3.2.7. *Sei $\mathbf{G}=\mathbf{G}(V,E)$ ein Graph. Ein Teilgraph $\mathbf{H}=\mathbf{H}(V_H,E_H)$ von $\mathbf{G}$ heißt* spannender Teilgraph, *wenn $V_H=V$.*
Ein spannender Teilgraph von $\mathbf{G}$, der ein Wald bzw. ein Baum ist, heißt spannender Wald *bzw.* spannender Baum *von $\mathbf{G}$.*

"Spannend" nicht im Sinne von "aufregend", sondern von "aufspannend".

Korollar 3.2.8. *Jeder zusammenhängende Graph hat einen spannenden Baum.*

Beweis. Das folgt an sich sofort aus dem Beweis für Korollar 3.2.6. Wir geben hier aber einen zweiten "algorithmischen" Beweis.
Sei $\mathbf{G}(V,E)$ ein zusammenhängender Graph.

```
/* Initialisierung: */
```
$S\leftarrow\emptyset$, $\mathbf{T}\leftarrow\mathbf{T}(V,S)$
```
/* Schleife: Wird wiederholt, solange die Bedingung erfüllt ist. */
```
while (Bedingung: Der $\mathbf{T}$ ist nicht zusammenhängend.) **do**
  Wähle eine beliebige Kante $e\in E$, die Knoten in verschiedenen Zusammenhangskomponenten von $\mathbf{T}$ verbindet,
  $S\leftarrow S\cup\{e\}$
  $\mathbf{T}\leftarrow\mathbf{T}(V,S)$
end while

1: Man findet in jedem Schritt eine geeignete Kante e: Denn sei $\mathbf{Z}$ eine Zusammenhangskomponente von $\mathbf{T}$ und $\mathbf{Y}$ der "restliche Graph" (also die übrigen Zusammenhangskomponenten). Seien z bzw. y zwei Knoten aus $\mathbf{Z}$ bzw. $\mathbf{Y}$. In $\mathbf{G}$ gibt es einen Weg, der z mit y verbindet — der muß eine Kante e enthalten, die "$\mathbf{Z}$ mit $\mathbf{Y}$ verbindet" (d.h., einen Knoten aus $\mathbf{Z}$ und einen aus $\mathbf{Y}$ enthält). Diese Kante e ist eine geeignete Wahl im Wiederholungsschritt.
2: Der Graph $\mathbf{T}$ enthält keine Kreise: Denn im Initialisierungsschritt ist das klar. Und durch das Hinzufügen der Kanten e (deren Existenz wir eben gezeigt haben) zu einem Graphen ohne Kreise kann kein Kreis C entstehen, denn dieser müßte die Kante e enthalten — diese verbindet aber nach Konstruktion zwei verschiedene Zusammenhangskomponenten $\mathbf{Z_1}$ und $\mathbf{Z_2}$. (C müßte ja die Kante e "benutzen", um von $\mathbf{Z_1}$ nach $\mathbf{Z_2}$ zu gelangen — aber für die "Rückkehr" von $\mathbf{Z_2}$ nach $\mathbf{Z_1}$ steht ja wieder nur dieselbe Kante e zur Verfügung.) □

3.3. Minimale spannende Bäume

Angenommen, wir müßten n Städte durch Glasfaserkabel verbinden, sodaß ein zusammenhängendes Computernetzwerk entsteht. Die Kosten für die Verlegung eines Verbindungskabels seien für jedes Paar von Städten gegeben. Die Frage ist, wie diese Verkabelung am billigsten geschehen kann. Diese Problemstellung können wir wie folgt formalisieren:

Definition 3.3.1. *Sei $\mathbf{G}$ ein zusammenhängender Graph mit einer* Gewichtsfunktion $\omega: E\to\mathbb{R}^+\setminus\{0\}$ *auf der Menge seiner Kanten. In der Familie aller zusammenhängenden spannenden Teilgraphen von $\mathbf{G}$ betrachten wir jenen, $\mathbf{K}$, für den das Gesamtgewicht der Kanten von $\mathbf{K}$ minimal ist: Dieser Graph ist notwendigerweise ein Baum und wird* minimaler spannender Baum *genannt.*

Einen minimalen spannenden Baum kann man mit einem sehr einfachen Algorithmus finden, der den Algorithmus aus dem Beweis von Korollorar 3.2.8 zur Konstruktion eines (normalen) spannenden Baumes spezialisiert. Das Verfahren wurde zuerst von Kruskal beschrieben und heißt daher *Kruskals Algorithmus*; es ist ein Beispiel für einen *Greedy Algorithm* (also "gierigen Algorithmus"[3]).

PROPOSITION 3.3.2 (Kruskals Greedy Algorithmus). *Sei* $\mathbf{G}\,(V, E)$ *ein zusammenhängender Graph mit einer* Gewichtsfunktion $\omega : E \to \mathbb{R}$ *auf der Menge seiner Kanten. Der folgende "greedy algorithm" liefert einen minimalen spannenden Baum:*

`/* Initialisierung: */`

$S \leftarrow \emptyset$, $\mathbf{T} \leftarrow \mathbf{T}\,(V\,(\mathbf{G})\,, S)$.

`/* Schleife: Wird wiederholt, solange die Bedingung erfüllt ist. */`

while *(Bedingung: Der* $\mathbf{T}$ *ist nicht zusammenhängend.)* ***do***

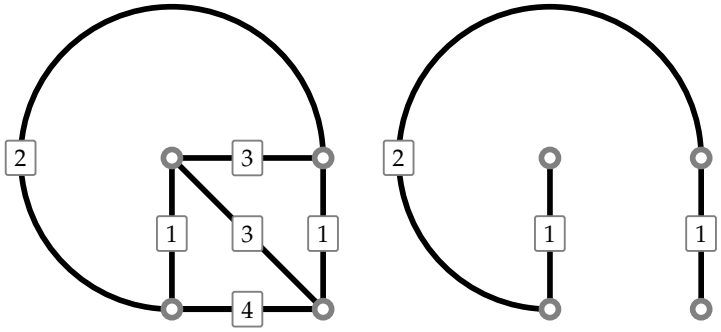
Wähle unter den Kanten in $E\,(\mathbf{G})$*, die Knoten in verschiedenen Zusammenhangskomponenten von* $\mathbf{T}$ *verbinden, eine von* minimalem Gewicht *(deshalb heißt das Verfahren "gieriger" Algorithmus), e,*

$S \leftarrow= S \cup \{e\}$

$\mathbf{T} \leftarrow= \mathbf{T}\,(V\,(\mathbf{G})\,, S)$.

end while

BEISPIEL 3.3.3. *Das linke Bild in der folgenden Graphik zeigt einen zusammenhängenden Graphen mit 4 Knoten; die Gewichte der Kanten sind in kleine Kästchen eingetragen.*



Das rechte Bild zeigt den (in diesem Fall eindeutigen) minimalen spannenden Baum, der aus den drei Kanten mit den kleinsten Gewichten besteht: Es ist offensichtlich, daß der Greedy Algorithm hier das richtige Ergebnis liefert.

BEWEIS. Daß der Algorithmus einen spannenden Baum liefert, wissen wir bereits: Zu zeigen ist also, daß das Resultat ein *minimaler* spannender Baum ist.

Sei n die Anzahl der Knoten von $\mathbf{G}$, und sei $e_1, \ldots, e_{n-1}$ die Folge der Kanten von $\mathbf{T}$ in der Reihenfolge, wie sie vom greedy algorithm gewählt werden. Es gilt:

$$\omega\,(e_1) \leq \cdots \leq \omega\,(e_{n-1})\,.$$

Angenommen, es gäbe einen spannenden Baum mit Kanten $f_1, \ldots, f_{n-1}$, die auch nach dem Gewicht geordnet seien, also

$$\omega\,(f_1) \leq \cdots \leq \omega\,(f_{n-1})\,,$$

[3] Denn in "gierigiger" Weise wird immer die unmittelbar günstigste Kante gewählt; siehe auch `http://en.wikipedia.org/wiki/Greedy_algorithm`.

der ein kleineres Gesamtgewicht der Kanten hat, also

$$\sum_{i=1}^{n-1} \omega(f_i) < \sum_{i=1}^{n-1} \omega(e_i).$$

Nun wähle k minimal, sodaß

$$\sum_{i=1}^{k} \omega(f_i) < \sum_{i=1}^{k} \omega(e_i).$$

Es ist sicher $k > 1$, denn der greedy algorithm wählt im ersten Schritt eine Kante von minimalem Gewicht. Es gilt also nach Wahl von k

$$\sum_{i=1}^{k-1} \omega(f_i) \geq \sum_{i=1}^{k-1} \omega(e_i),$$

daher muß gelten:

$$\omega(f_1) \leq \cdots \leq \omega(f_k) < \omega(e_k).$$

Das wiederum heißt: Der greedy algorithm wählt im k-ten Schritt Kante e_k und *keine* der Kanten $f_1, \ldots, f_k$, die kleineres Gewicht haben.
Also kann keine der Kanten $f_1, \ldots, f_k$ verschiedene Zusammenhangskomponenten im Graphen

$$\mathbf{T}^e = \mathbf{T}(V, \{e_1, \ldots, e_{k-1}\})$$

verbinden.
Das bedeutet aber, daß die Knotenmenge jeder Zusammenhangskomponente von

$$\mathbf{T}^f = \mathbf{T}(V, \{f_1, \ldots, f_k\})$$

in der Knotenmengen einer Zusammenhangskomponente von $\mathbf{T}^e$ *enthalten* ist, insbesondere hat also $\mathbf{T}^f$ mindestens so viele Zusammenhangskomponenten wie $\mathbf{T}^e$.
Kurz nachdenken!
Dies ist aber ein Widerspruch, denn $\mathbf{T}^e$ und $\mathbf{T}^f$ sind Wälder, und die Anzahl ihrer Komponenten ist $n - (k-1) > n - k$. □

3.4. Travelling Salesman Problem

Angenommen, wir müßten eine *Rundreise* durch n Städte planen und dabei jede Stadt genau einmal aufsuchen. Wie im vorigen Abschnitt sind die Kosten für die Reise für jedes Paar von Städten gegeben. Die Frage ist, wie diese Rundreise am billigsten geschehen kann. Diese Problemstellung können wir wie folgt formalisieren:

Definition 3.4.1. *Ein Kreis in einem Graphen* $\mathbf{G}$*, der alle Knoten von* $\mathbf{G}$ *enthält, heißt* Hamiltonscher Kreis.
Sei $\mathbf{K}_n$ *der vollständige Graph mit n Knoten, und sei eine* Gewichtsfunktion $\omega : E \to \mathbb{R}$ *auf der Menge seiner Kanten gegeben. In der Familie aller Hamiltonschen Kreise des* $\mathbf{K}_n$ *betrachten wir jenen, H, für den das Gesamtgewicht seiner Kanten minimal ist: Dieser Kreis ist eine Lösung für das mit* $\mathbf{K}_n$ *und Gewichtsfunktion* ω *verbundene* Travelling Salesman Problem *(die Lösung des Problems ist also ein* minimaler Hamiltonscher Kreis*).*

Das Travelling Salesman Problem ist eine *viel komplexere* Aufgabe als die Konstruktion eines minimalen spannenden Baumes: Es ist bis heute nicht klar, ob die Lösung im allgemeinen "wesentlich effizienter" gefunden werden kann als durch das Durchprobieren aller möglichen zyklischen Permutationen der n Knoten (dieser "triviale Algorithmus" braucht $(n-1)!$ Schritte[4]). Es gibt aber in speziellen Fällen immerhin näherungsweise Resultate.

DEFINITION 3.4.2. *Sei* $\mathbf{K}_n$ *der vollständige Graph mit n Knoten, und sei eine* Gewichtsfunktion $\omega : E \to \mathbb{R}$ *auf der Menge seiner Kanten gegeben. Wir sagen, die Gewichtsfunktion erfüllt die* Dreiecksungleichung, *wenn für je drei paarweise verschiedene Knoten a, b und c gilt:*

$$\omega(\{a,b\}) + \omega(\{b,c\}) \geq \omega(\{a,c\})$$

SATZ 3.4.3. *Sei* $\mathbf{K}_n$ *der vollständige Graph mit n Knoten, und sei eine* Gewichtsfunktion $\omega : E \to \mathbb{R}$ *auf der Menge seiner Kanten gegeben, die die Dreiecksungleichung erfüllt. Sei m bzw. M das Gesamtgewicht der Kanten eines minimalen spannenden Baumes bzw. eines minimalen Hamiltonschen Kreises. Dann gilt:*

$$m \leq M \leq 2m.$$

Kurz nachdenken!

BEWEIS. Daß $m \leq M$ ist, folgt einfach daraus, daß ein Hamiltonscher Kreis natürlich zusammenhängend ist (und ein minimaler spannender Baum ist ein zusammenhängender Graph mit minimalem Gesamtgewicht der Kanten).

Die zweite Ungleichung sieht man wie folgt: Zunächst konstruieren wir einen minimalen spannenden Baum $\mathbf{T}$ in $\mathbf{K}_n$. Diesen Baum machen wir zu einem Eulerschen Graphen (mit mehrfachen Kanten), indem wir alle seine Kanten "verdoppeln". In diesem Eulerschen Graphen konstruieren wir eine Eulersche Wanderung. Um nun einen Hamiltonschen Kreis zu konstruieren, folgen wir dieser Wanderung — aber immer, wenn wir einen Knoten erreichen, den wir schon besucht hatten, setzen wir mit dem *nächsten* Knoten auf der Wanderung fort, der noch *nicht* besucht wurde.

Es ist klar, daß so ein Hamiltonscher Kreis C entsteht — die Frage ist, wie groß das Gewicht der Kanten von C ist. Nach Konstruktion haben wir immer "Abkürzungen gemacht", also Abschnitte $v_i, v_{i+1}, \ldots, v_j$ der Eulerschen Wanderung durch einfache Kanten $\left(v_i, v_j\right)$ ersetzt: Wegen der Dreiecksungleichung[5] ist aber

$$\omega(\{v_i, v_{i+1}\}) + \cdots + \omega\left(\left\{v_{j-1}, v_j\right\}\right) \geq \omega\left(\left\{v_i, v_j\right\}\right),$$

daher ist das Gewicht der Kanten von $C \leq$ dem Gewicht der Kanten der Eulerschen Wanderung, also $\leq 2m$. □

3.5. Digraphen und Netzwerke

Für verschiedene Anwendungen benötigen wir eine weitere Variation des Begriffs Graph:

[4] Für nur 50 Städte bräuchte man ja schon $6.082818640342675 \times 10^{62}$ Schritte — das ist in der Praxis natürlich undurchführbar.

[5] . . . und Induktion.

DEFINITION 3.5.1. *Ein* gerichteter Graph *(englisch:* directed graph*, oder kurz* Digraph*)* $\mathbf{D} = \mathbf{D}(V, E)$ *(mit mehrfachen Kanten) ist gegeben durch eine Menge V von Knoten und eine Multimenge E der Familie der* geordneten Paare *von V.*

Die Kanten eines gerichteten Graphen $\mathbf{D}$ *besitzen also eine* Orientierung*, d.h., eine Kante $e = (v, u)$ verbindet nicht einfach Knoten v mit Knoten u, sondern führt* von v nach u*: v ist der* Anfangsknoten *der Kante, bezeichnet mit $\mathbf{i}(e)$, und u ist der* Endknoten *der Kante, bezeichnet mit $\mathbf{t}(e)$. Der* Eingangsgrad *(englisch:* in–degree*) eines Knoten v ist die Anzahl der Kanten e mit $\mathbf{t}(e) = v$ (die also* nach v *führen), und der* Ausgangsgrad *(englisch:* out–degree*) ist die Anzahl der Kanten e mit $\mathbf{i}(e) = v$ (die also* von v *zu anderen Knoten führen).*

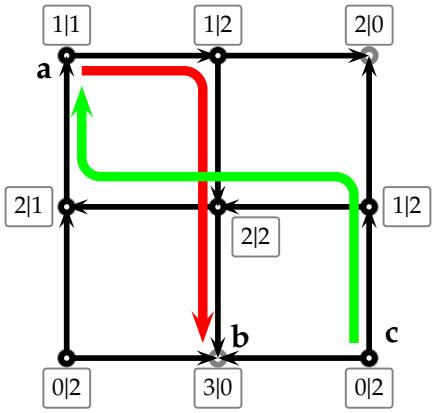
Wanderungen und Wege in gerichteten Graphen sind genauso definiert wie für "normale" Graphen — nur daß die Kanten "in der richtigen Richtung benutzt" werden müssen. D.h., wenn

$$v_0, v_1, \ldots, v_n$$

eine Wanderung in $\mathbf{D}$ ist, dann müssen die geordneten Paare (v_{i-1}, v_i) *für $i = 1, \ldots, n$ Kanten aus E sein.*

Wenn man in einem Digraphen $\mathbf{D}$ die Orientierung "vergißt", also jede gerichtete Kante (v, w) durch eine "normale" Kante $\{v, w\}$ ersetzt, dann erhält man einen "normalen" Graphen $\mathbf{G}$ (um den Gegensatz zu einem gerichteten Graphen zu betonen, spricht man auch von einem ungerichteten Graphen*): Dieser wird der* zugrundeliegende Graph *von $\mathbf{D}$ genannt.*

In der folgenden Graphik wird die Orientierung der Kanten durch Pfeile angedeutet, und für jeden Knoten sind in einem kleinen Kästchen Eingangsgrad|Ausgangsgrad angegeben. Vom Knoten c führt eine orientierte Wanderung zum Knoten a, und vom Knoten a führt eine orientierte Wanderung zum Knoten b — aber nicht in die Gegenrichtung!



Aufgabe 44 ($\star\star$)**:** *Sei $\mathbf{G}(V, E)$ ein Graph, in dem jeder Knoten geraden Grad hat. Zeige, daß man den Kanten von $\mathbf{G}$ eine Orientierung aufprägen kann, sodaß für jeden Knoten der Ausgangsgrad gleich dem Eingangsgrad ist.*

Aufgabe 45 ($\star\star$)**:** *Beweise die folgende Variante des Satzes von Euler:*

Ein Digraph $\mathbf{D}$ ohne isolierte Knoten hat eine (orientierte) geschlossene Eulersche Wanderung genau dann, wenn sein zugrundeliegender Graph $\mathbf{G}$ zusammenhängend ist und für jeden Knoten der Eingangsgrad gleich dem Ausgangsgrad ist.

DEFINITION 3.5.2. *Ein* Netzwerk *ist ein Digraph* $\mathbf{N}(V, E)$ *mit zwei ausgezeichneten Knoten, einer* Quelle $\mathbf{q}$ *und einer* Senke $\mathbf{s}$, $\mathbf{q} \neq \mathbf{s}$, *und mit einer Gewichtsfunktion* $\mathbf{c} : E \to \mathbb{R}^+$ *(die also nur* nichtnegative *Werte annimmt) und die in diesem Zusammenhang* Kapazität *heißt.*

Die Idee hinter dieser Definition ist ein Netzwerk von miteinander verbundenen Röhren: In der Quelle $\mathbf{q}$ wird Wasser eingepumpt, das in der Senke $\mathbf{s}$ das Netzwerk wieder verläßt; die Kapazität $\mathbf{c}$ entspricht dem maximal möglichen Durchfluß durch die einzelnen Röhren.

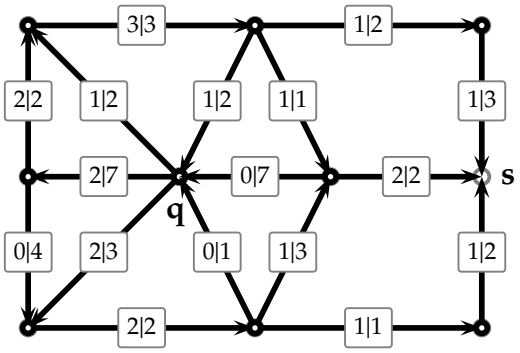
DEFINITION 3.5.3. *Ein* Fluß *(englisch:* Flow*) in einem Netzwerk* $\mathbf{N}(V, E)$ *(mit Quelle* $\mathbf{q}$*, Senke* $\mathbf{s}$ *und Kapazität* $\mathbf{c}$*) ist eine Funktion* $f : E \to \mathbb{R}$ *mit den Eigenschaften*

- $0 \leq f(e) \leq \mathbf{c}(e)$ *für alle Kanten* $e \in E$,
- $\sum_{\mathbf{i}(e)=v} f(e) = \sum_{\mathbf{t}(e)=v} f(e)$ *für alle Knoten* $\neq \mathbf{q}, \mathbf{s}$.

Die Stärke $val(f)$ *eines Flusses* f *ist definiert als*

$$val(f) = \sum_{\mathbf{i}(e)=\mathbf{q}} f(e) - \sum_{\mathbf{t}(e)=\mathbf{q}} f(e).$$

Die folgende Graphik zeigt ein kleines Netzwerk mit Quelle $\mathbf{q}$ und Senke $\mathbf{s}$, Fluß|Kapazität der Kanten sind in kleinen Kästchen eingetragen: Ersichtlich hat der Fluß Stärke 4.



Für eine beliebige Teilmenge $S \subseteq V$ von Knoten eines Netzwerks $\mathbf{N}(V, E)$ führen wir folgende Notation ein:

- $S^{\rightarrow} := \{e \in E : \mathbf{i}(e) \in S, \mathbf{t}(e) \notin S\}$ ("Netto–Output"),
- $S^{\leftarrow} := \{e \in E : \mathbf{t}(e) \in S, \mathbf{i}(e) \notin S\}$ ("Netto–Input").

LEMMA 3.5.4. *Sei* f *ein Fluß in einem Netzwerk* $\mathbf{N}(V, E)$ *mit Quelle* $\mathbf{q}$ *und Senke* $\mathbf{s}$. *Sei* S *eine beliebige Teilmenge von* V*, die* $\mathbf{q}$ *enthält, aber nicht* $\mathbf{s}$. *Dann gilt:*

$$\sum_{e \in S^{\rightarrow}} f(e) - \sum_{e \in S^{\leftarrow}} f(e) = val(f).$$

BEWEIS. Wir betrachten

$$\sum_{v \in S} \left(\sum_{\mathbf{i}(e)=v} f(e) - \sum_{\mathbf{t}(e)=v} f(e) \right).$$

Einerseits ergibt diese Summe $\mathrm{val}(f)$, denn alle Summanden für $v \neq \mathbf{q}$ sind Null nach Definition eines Flusses, und der Summand $v = \mathbf{q}$ liefert genau $\mathrm{val}(f)$.
Andrerseits können wir die Summe auch als Summe über Kanten interpretieren: Sei $e = (v, w)$ eine Kante. Wenn $v \in S$, dann kommt $+f(e)$ in der Summe vor; wenn auch $w \in S$, dann kommt $-f(e)$ in der Summe vor — diese Terme heben sich also gegenseitig auf. Daher tragen nur solche Kanten etwas zur Summe bei, die *genau einen* Knoten in S haben, das sind genau jene in $S^{\rightarrow}$ (die entsprechenden Terme werden *addiert*) bzw. in $S^{\leftarrow}$ (die entsprechenden Terme werden *subtrahiert*). □

Natürlich ist die Frage, die man stellen wird: "Was ist die *maximale* Stärke eines Flusses in einem gegebenen Netzwerk?"

Definition 3.5.5. *Ein* Schnitt *(englisch:* Cut*) C in einem Netzwerk $\mathbf{N}(V, E)$ ist eine Teilmenge $C \subseteq E$ von Kanten, sodaß* jeder *Weg von der Quelle* $\mathbf{q}$ *zur Senke* $\mathbf{s}$ *mindestens eine Kante aus C enthält. Die* Kapazität $\mathbf{c}(C)$ *des Schnitts ist die Summe der Kapazitäten der Kanten in C, also*

$$\mathbf{c}(C) = \sum_{e \in C} \mathbf{c}(e).$$

Das folgende ist "intuitiv klar":

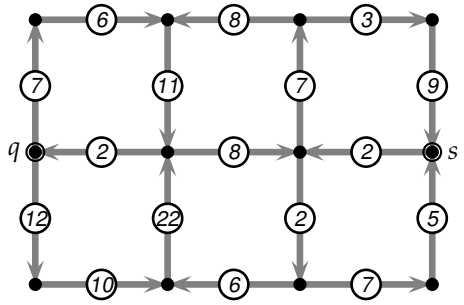
Lemma 3.5.6. *Sei $\mathbf{N}(V, E)$ ein Netzwerk mit Quelle $\mathbf{q}$, Senke $\mathbf{s}$ und Kapazitätsfunktion $\mathbf{c}$. Dann ist die Stärke eines beliebigen Flusses kleiner oder gleich der Kapazität eines beliebigen Schnitts.*

Beweis. Sei C ein Schnitt, und sei S die Menge der Knoten in $\mathbf{N}$, die von der Quelle $\mathbf{q}$ aus durch Wege erreichbar sind, die *keine* Kanten aus C enthalten. Dann ist $S^{\rightarrow} \subseteq C$.
Nach Lemma 3.5.4 gilt für einen beliebigen Fluß f:

$$\mathrm{val}(f) = \sum_{e \in S^{\rightarrow}} f(e) - \sum_{e \in S^{\leftarrow}} f(e) \leq \sum_{e \in S^{\rightarrow}} \mathbf{c}(e) \leq \sum_{e \in C} \mathbf{c}(e) = \mathbf{c}(C).$$

□

Aufgabe 46 (⋆)**:** *Betrachte das folgende Netzwerk: q bezeichnet die Quelle, s die Senke, die Kapazitäten der gerichteten Kanten sind in die kleinen Kreise eingetragen.*



Finde einen maximalen Fluß in diesem Netzwerk und begründe (kurz), warum dieser maximal ist.

Es gilt aber stärker der folgende Satz:

SATZ 3.5.7 (Max–Flow–Min–Cut–Theorem, Satz von Ford–Fulkerson). *Sei* $\mathbf{N}(V, E)$ *ein Netzwerk mit Quelle* $\mathbf{q}$, *Senke* $\mathbf{s}$ *und Kapazitätsfunktion* $\mathbf{c}$. *Dann ist die maximale Stärke eines Flusses* gleich *der minimalen Kapazität eines Schnitts.*

Wir verschieben den allgemeinen Beweis dieses Satzes und beweisen zunächst:

LEMMA 3.5.8. *Sei* $\mathbf{N}(V, E)$ *ein Netzwerk mit Quelle* $\mathbf{q}$, *Senke* $\mathbf{s}$ *und Kapazitätsfunktion* $\mathbf{c} : E \to \mathbb{Z}^+$ *(d.h., alle Kapazitäten sind* ganze *nichtnegative Zahlen). Dann gibt es einen Fluß* f *in* $\mathbf{N}$, *der in jeder Kante ganzzahlig ist (d.h.,* $f(e) \in \mathbb{Z}^+$ *für alle* $e \in E$*: Wir sagen,* f *ist ein* ganzzahliger Fluß*), und einen Schnitt* C, *sodaß*

$$val(f) = \mathbf{c}(C).$$

Insbesondere ist f ein Fluß maximaler Stärke und C ein Schnitt minimaler Kapazität. (Satz 3.5.7 ist damit also für *ganzzahlige* Kapazitätsfunktionen gezeigt)

BEWEIS. Das Kernstück unseres Beweises ist die Behauptung: Für einen ganzzahligen Fluß f gibt es

- entweder einen ganzzahligen Fluß f' mit $\text{val}(f') = \text{val}(f) + 1$
- oder einen Schnitt C mit $\mathbf{c}(C) = \text{val}(f)$.

Wenn wir das zeigen können, können wir algorithmisch vorgehen und mit dem "Nullfluß" $f \equiv 0$ starten, den wir sukzessive "verstärken" (solange die erste Alternative der Behauptung zutrifft), bis die zweite Alternative der Behauptung zutrifft und wir einen *maximalen Fluß* konstruiert haben.

Zum Beweis dieser Behauptung konstruieren wir algorithmisch zwei Mengen $S \subseteq V$ und $E_S \subseteq E$:

`/* Initialisierung: */`

$S \leftarrow \{\mathbf{q}\}$, $E_S \leftarrow \emptyset$.

`/* Schleife: Wird wiederholt, solange die Bedingung erfüllt ist. */`

while (Bedingung: $\mathbf{s} \notin S$ *und* es existiert eine Kante $e = (v, w)$, für die *entweder* $f(e) < \mathbf{c}(e)$ und $v \in S$, aber $w \notin S$ (i.e.: $e \in S^{\rightarrow}$) *oder* $f(e) > 0$ und $v \notin S$, aber $w \in S$ (i.e.: $e \in S^{\leftarrow}$)) **do**

$S \leftarrow S \cup \{v, w\}$ (i.e.: gib den Knoten von e, der noch nicht in S enthalten ist (also v oder w), zu S dazu.)

$E_S \leftarrow E_S \cup \{e\}$ (i.e.: gib die Kante e zu E_S dazu.)

end while

Die so konstruierte Knotenmenge S ergibt zusammen mit der Kantenmenge E_S einen (gerichteten) Teilgraphen $\mathbf{N}'$ von $\mathbf{N}$, dessen zugrundeliegender (*ungerichteter*) Graph (in dem man also "die Orientierung der Kanten vergißt") ein *Baum* ist.

Es gibt nun zwei Möglichkeiten:

Fall 1: $\mathbf{s} \in S$. Dann gibt es eine Folge von *paarweise verschiedenen* Knoten $\mathbf{q} = v_0, v_1, \ldots, v_n = \mathbf{s}$, sodaß für alle $i = 1, \ldots, n$

(a) entweder $(v_{i-1}, v_i) =: e_i \in E_S$ ist eine der Kanten mit $f(e_i) < \mathbf{c}(e_i)$,
(b) oder $(v_i, v_{i-1}) =: e_i \in E_S$ ist eine der Kanten mit $f(e_i) > 0$

gilt[6]. Die Menge dieser Kanten $\{e_i\colon\ 1 \le i \le n\}$ zerfällt also in zwei disjunkte Teilmengen

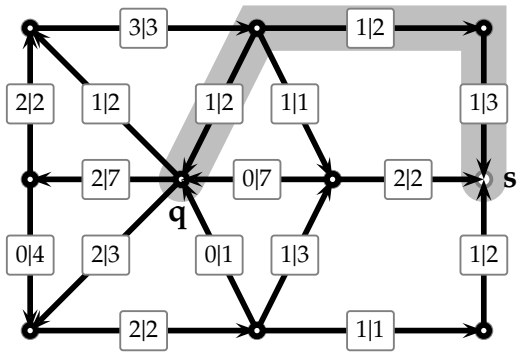
- $A \subseteq E_S$: für $e_i \in A$ trifft Alternative (a) zu,
- $B \subseteq E_S$: für $e_i \in B$ trifft Alternative (b) zu.

Nun definieren wir einen Fluß f' wie folgt:

$$f'(e) = \begin{cases} f(e) + 1 & \text{falls } e \in A, \\ f(e) - 1 & \text{falls } e \in B, \\ f(e) & \text{sonst.} \end{cases}$$

Es ist leicht zu sehen, daß $0 \le f'(e) \le \mathbf{c}(e)$ für alle Kanten $e \in E$ gilt, und daß für alle Knoten v_i, $i = 1, \ldots, n-1$ (andere Knoten — außer $\mathbf{q}$ und $\mathbf{s}$ — sind von der Änderung ja gar nicht betroffen!) nach wie vor $\sum_{\mathbf{i}(e)=v_i} f'(e) = \sum_{\mathbf{t}(e)=v_i} f'(e)$ gilt: f' ist also tatsächlich ein Fluß. Ebenso ist leicht zu sehen, daß $\mathrm{val}(f') = \mathrm{val}(f) + 1$.

Beispiel 3.5.9. *Die folgende Graphik zeigt eine Menge S (grau unterlegt), die sich mit diesem Schritt ergeben würde: Die Senke* $\mathbf{s}$ *gehört zu S, daher läßt sich der Fluß um* 1 *erhöhen.*



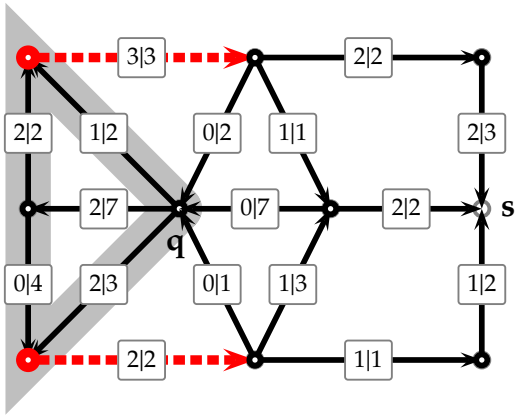
Fall 2: $\mathbf{s} \notin S$. Dann ist aber $S^{\rightarrow}$ ein Schnitt, und nach Konstruktion von S gilt für jede Kante $e \in S^{\rightarrow}$: $f(e) = \mathbf{c}(e)$, und es gilt für jede Kante $e \in S^{\leftarrow}$: $f(e) = 0$. Daher ist

$$\mathrm{val}(f) = \sum_{e \in S^{\rightarrow}} f(e) - \sum_{e \in S^{\leftarrow}} f(e) = \sum_{e \in S^{\rightarrow}} \mathbf{c}(e) = \mathbf{c}(S^{\rightarrow}).$$

Beispiel 3.5.10. *Die folgende Graphik zeigt die Situation, die sich nach der Erhöhung des Flusses aus der vorigen Graphik ergibt: Die Menge S (wieder grau unterlegt) enthält nun die Senke* $\mathbf{s}$ nicht, *und die beiden aus S herausführenden Kanten (die strichlierten Kanten links oben und links unten[7]) bilden einen Schnitt.*

[6] Im *zugrundeliegenden Graphen* von $\mathbf{N}'$ (wo also "auf die Orientierung der Kanten vergessen wird") entspricht diese Folge dem *eindeutigen Weg* von $\mathbf{q}$ nach $\mathbf{s}$.

[7] In der farbigen Version dieses Skriptums: Die roten Kanten.



Damit ist die obige Behauptung (und unser Lemma) gezeigt. □

Beweis von Satz 3.5.7. Nach Lemma 3.5.8 ist die Behauptung für ganzzahlige Kapazitätsfunktionen richtig. Dann gilt sie aber auch für Kapazitätsfunktionen $\mathbf{c} : E \to \mathbb{Q}^+$: Dazu multiplizieren wir alle Kapazitäten $\mathbf{c}(e)$ mit dem gemeinsamen Nenner m und erhalten so ein Netzwerk mit ganzzahligen Kapazitäten, für dieses gilt der Satz, und durch "Division aller Kapazitäten und Flüsse durch m" sehen wir die Gültigkeit des Satzes im ursprünglichen Netzwerk $\mathbf{N}$.

Für reellwertige Kapazitätsfunktionen können wir alle Kapazitäten $\mathbf{c}(e)$ beliebig genau von unten durch rationale Zahlen approximieren, und durch Anwendung unseres Satzes für *rational–wertige* Kapazitätsfunktionen finden wir Flüsse, die der Kapazität eines minimalen Schnittes beliebig nahe kommen: Die Aussage folgt dann durch Übergang zum Grenzwert[8] □

3.6. Die Sätze von Menger, König und Hall

Aus dem Max–Flow–Min–Cut–Theorem kann man verschiedene wichtige Resultate herleiten. Wir geben hier drei prominente Beispiele.

3.6.1. Der Satz von Menger.

Definition 3.6.1. *Sei* $\mathbf{D}(V, E)$ *ein Digraph, und seien* s, t *zwei verschiedene Knoten in* $\mathbf{D}$. *Dann heißt eine Teilmenge* $C \subseteq E$ *von Kanten mit der Eigenschaft, daß* jeder *Weg von* s *nach* t *(mindestens) eine Kante aus* C *enthält, eine* s–t–trennende Kantenmenge.

Satz 3.6.2 (Satz von Menger). *Sei* $\mathbf{D}$ *ein Digraph und seien* s, t *zwei verschiedene Knoten in* $\mathbf{D}$. *Dann ist die* maximale *Anzahl von* paarweise kantendisjunkten Wegen *(d.h., keine zwei Wege haben eine Kante gemeinsam) von* s *nach* t *gleich der* minimalen *Kardinalität einer* s–t–*trennenden Kantenmenge.*

[8] Strenggenommen ist dieses Argument noch nicht ausreichend — wir müssen ja "konvergente Flüsse und Schnitte" haben, nicht nur konvergente Stärken und Kapazitäten. Dazu müßten wir folgendermaßen vorgehen: Unsere Konstruktion liefert ja eine Folge von Flüssen/Schnitten, deren Stärken/Kapazitäten konvergieren. Nun betrachten wir eine Kante k_1: Die Fluß–Werte auf dieser Kante müssen nicht konvergieren, da sie aber beschränkt sind, muß es einen Häufungspunkt und somit eine konvergente Teilfolge von Flüssen/Schnitten geben. Danach wendet man dasselbe Argument für diese Teilfolge und Kante k_2 an, u.s.w: Da wir einen *endlichen* Graphen haben, bricht dieses Verfahren ab.

Beweis. Wir machen aus dem Digraphen ein Netzwerk, indem wir s und t als Quelle und Senke auffassen und für die Kanten die ganzzahlige Kapazitätsfunktion $\mathbf{c} \equiv 1$ wählen.
Eine s–t–trennende Kantenmenge ist dann ein Schnitt in diesem Netzwerk, und die Kapazität eines solchen Schnittes ist gleich seiner Kardinalität. Sei m also die Kapazität eines minimalen Schnittes $=$ die minimale Anzahl einer s–t–trennenden Kantenmenge.
Es gibt also einen maximalen Fluß f der Stärke m in diesem Netzwerk. Der Fluß f ist ganzzahlig (nach Lemma 3.5.8), er nimmt also nur die Werte 0 oder 1 an[9].
Wenn es aber einen Fluß der Stärke m gibt, dann gibt es auch m kantendiskjunkte Wege von s nach t, die nur Kanten e mit $f(e) = 1$ benutzen: Dies zeigen wir mit Induktion nach m.
Für $m = 0$ ist die Behauptung klar.
Für den Schritt $m-1$ auf m konstruieren wir mithilfe von f zunächst einen Weg von s nach t: Dazu starten wir in s, verwenden nur Kanten e mit $f(e) = 1$, ohne jemals eine Kante zweimal zu benutzen, und gelangen so schließlich nach t. Damit haben wir zunächst eine Wanderung erhalten, in der Knoten wiederholt auftreten könnten: Zwischen je zwei wiederholten Knoten schneiden wir die dazwischenliegende geschlossene Wanderung heraus und erhalten so schließlich einen Weg p. Für alle Kanten von p reduzieren wir den Fluß um 1, damit reduziert sich die Stärke des verbleibenden Flusses auf $m-1$. Nach Induktion finden wir nun $m-1$ kantendisjunkte Wege, und der Weg p hat nach Konstruktion keine Kante mit diesen Wegen gemeinsam. □

Das geht wegen der "Flußeigenschaft"!

3.6.2. Der Satz von König.

Definition 3.6.3. *Sei* $\mathbf{G}(V, E)$ *ein Graph. Ein* Matching *in* $\mathbf{G}$ *ist eine Familie von paarweise disjunkten Kanten (d.h., keine zwei Kanten im Matching haben einen Knoten gemeinsam).*
Ein Edge–Cover *(eine* Kantenüberdeckung*) in* $\mathbf{G}$ *ist eine Menge von Knoten mit der Eigenschaft, daß* jede *Kante in* $\mathbf{G}$ *einen Knoten aus dem Edge–Cover enthält.*
Ein Graph $\mathbf{G}(V, E)$ *heißt* bipartiter Graph*, wenn seine Knotenmenge in zwei disjunkte Teilmengen A und B zerfällt (eine sogenannte* Bipartition*: $V = A \dot\cup B$, also $V = A \cup B$ und $A \cap B = \emptyset$), sodaß jede Kante einen Knoten aus A und einen Knoten aus B enthält.*

Aufgabe 47 ($\star$)**:** *Zeige: Ein Graph* $\mathbf{G}$ *ist genau dann bipartit, wenn jede geschlossene Wanderung in* $\mathbf{G}$ *gerade Länge hat.*

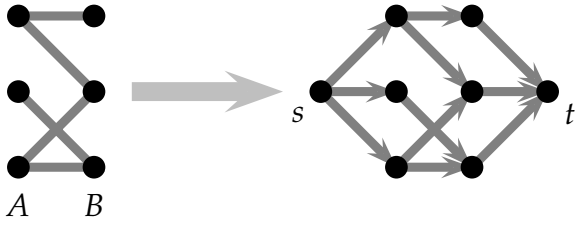
Satz 3.6.4 (Satz von König). *Sei* $\mathbf{G}(A \dot\cup B, E)$ *ein bipartiter Graph. Die maximale Kardinalität eines Matchings in* $\mathbf{G}$ *ist gleich der minimalen Kardinalität eines Edge–Cover in* $\mathbf{G}$.

Beweis. Wir konstruieren aus $\mathbf{G}$ einen Digraphen $\mathbf{D}$: Die Knoten von $\mathbf{D}$ seien $A \cup B \cup \{s, t\}$, und die gerichteten Kanten von $\mathbf{D}$ seien

- alle Paare (s, a) für $a \in A$,
- alle Paare (a, b) mit $\{a, b\} \in E$, $a \in A$ und $b \in B$,

[9] Wenn wir f als charakteristische Funktion deuten, dann entspricht er einfach einer Teilmenge von Kanten (nämlich jenen mit $f(e) = 1$).

- alle Paare (b, t) für $b \in B$.



Jeder Weg in **D** von s nach t ist von der Form (s, a, b, t), wobei $a \in A$, $b \in B$ und $\{a, b\} \in E$. Daher entspricht eine Familie von kantendisjunkten Wegen (s, a_i, b_i, t) in **D** eindeutig einem Matching in **G**, das aus den Kanten $\{a_i, b_i\}$ besteht.

Jedem Edge–Cover S in **G** entspricht eine s–t–trennende Kantenmenge in **D**, die aus den Kanten (s, a) für $a \in A \cap S$ und aus den Kanten (b, t) für $b \in B \cap S$ besteht, und umgekehrt entspricht jeder s–t–trennenden Kantenmenge, die nur Kanten enthält, die entweder mit s oder mit t inzident sind, ein Edge–Cover.

Es kann zwar klarerweise noch andere s–t–trennende Kantenmenge in **D** geben, aber keine davon kann weniger Kanten enthalten als eine *minimale* s–t–trennende Kantenmenge von obigem Typ (denn wenn eine s–t–trennende Kantenmenge die Kante (a, b) enthält, können wir sie durch (s, a) ersetzen).

Die Behauptung folgt also aus dem Satz von Menger. □

3.6.3. Der Satz von Hall.

Definition 3.6.5. *Seien $A_1, \ldots, A_n$ Mengen. Ein* Repräsentantensystem *von $A_1, \ldots, A_n$ ist ein n–Tupel $(x_1, \ldots, x_n)$ mit den Eigenschaften*

- $x_i \in A_i$ *für* $i = 1, \ldots, n$,
- $x_i \neq x_j$ *für* $i \neq j$.

Eine anschauliche Interpretation wäre die folgende: Es seien n Frauen gegeben, die jeweils eine gewisse Menge von Männern für heiratsfähig erachten; sei A_i die Menge der Männer, die von der i–ten Frau als heiratsfähig erachtet werden. Ein Repräsentantensystem entspricht dann einer Wahl von Männern, mit denen eine n–fache Heirat (ohne Bigamie) möglich wäre: Darum heißt der folgende Satz auch *Heiratssatz*.

Satz 3.6.6 (Satz von Hall). *Seien $A_1, \ldots, A_n$ endliche Mengen. Es existiert genau dann ein Repräsentantensystem von $A_1, \ldots, A_n$, wenn für alle Indexmengen $J \subseteq [n]$ gilt:*

$$\left| \bigcup_{j \in J} A_j \right| \geq |J| \,.$$

Beweis. Die Notwendigkeit der Bedingung ist klar — in der anschaulichen Interpretation: Jede Menge J von Frauen muß insgesamt zumindest $|J|$ Männer als heiratsfähig erachten, sonst kann es keine n–fache Heirat geben.

Wir konstruieren einen bipartiten Graphen **G**, dessen Knotenmenge V in A und B zerfällt, wobei $B = [n]$ und $A = \bigcup_{i=1}^{n} A_i$, und dessen Kanten Knoten $i \in A$ und $j \in B$ genau dann verbinden, wenn $i \in A_j$.

Ein Matching in **G** ist eine Menge paarweise disjunkter Kanten $\{i, j\}$, d.h., jeder Knoten i liegt in A_j, und die Knoten i sind alle verschieden. Ein Repräsentantensystem entspricht also einem Matching der Größe n in **G**.

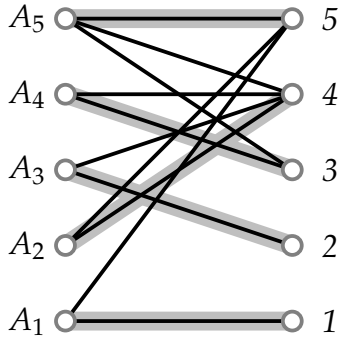
Die Menge B ist (natürlich) ein Edge–Cover mit $|B| = n$. Wir wollen zeigen: *Jedes* Edge–Cover S hat mindestens n Elemente.

Sei also S *irgendein* Edge–Cover; und sei $J := B \setminus S$. Jeder Knoten in $A(J) := \bigcup_{j \in J} A_j$ ist mit einem Knoten von J durch eine Kante verbunden, daher muß $A(J) \subseteq S$ gelten (sonst wäre S ja kein Edge–Cover). Daher gilt nach Voraussetzung:

$$|S| \geq |B| - |J| + \underbrace{\left|A(J)\right|}_{\geq |J|} \geq n.$$

Die Behauptung folgt also aus dem Satz von König. □

Beispiel 3.6.7. *Die folgende Graphik zeigt die Situation für die Mengen* $A_1 = \{1, 5\}$, $A_2 = \{4, 5\}$, $A_3 = \{2, 3\}$, $A_4 = \{3, 4\}$, *und* $A_5 = \{3, 4, 5\}$. *Die Kanten eines Matchings der Größe* 5 *sind grau unterlegt.*



3.7. Planare Graphen, Polyedersatz und 5–Farbensatz

Die abstrakt–mengentheoretische Definition von Graphen ist sehr nützlich, um Mißverständnisse auszuschließen — in der Praxis wird man sich Graphen aber meist als "Punkte, die durch Kurven verbunden sind" vorstellen (die *in der "Zeichenebene"* liegen).

Unter "Kurve" wollen wir hier eine stückweise stetig differenzierbare Abbildung von $[0, 1] \to M$ verstehen, wobei M der Raum ist, in dem wir unseren Graphen "zeichnen" (meist die Ebene $\mathbb{R}^2$, aber auch andere Mannigfaltigkeiten wären hier denkbar).

Definition 3.7.1. *Sei M eine* Mannigfaltigkeit[10] *und* **G** *ein Graph. Eine Abbildung μ, die jedem Knoten v* injektiv *einen Punkt $\mu(v)$ in M zurordnet, und jeder Kante $e = \{v, w\}$ eine Kurve $\gamma : [0, 1] \to M$ mit $\gamma(0) = \mu(v)$, $\gamma(1) = \mu(w)$, sodaß die zwei verschiedenen Kanten e_1, e_2 zugeordneten Kurven γ_1, γ_2 höchstens Anfangs– oder Endpunkte gemeinsam haben, heißt eine* Einbettung *von* **G** *in M.*

[10] Ein Begriff der Differentialgeometrie: Für unsere Zwecke brauchen wir nur die Ebene $\mathbb{R}^2$, den Raum $\mathbb{R}^3$ sowie die Oberfläche einer Kugel im Raum (Sphäre) und die Oberfläche eines Fahrradschlauchs (Torus).

Etwas weniger kompliziert[11] ausgedrückt: Wenn wir den Graphen $\mathbf{G}$ in M so zeichnen können, daß sich Kanten höchstens in ihren Endpunkten schneiden, dann ist diese Zeichnung des Graphen eine Einbettung.

PROPOSITION 3.7.2. *Jeder Graph* $\mathbf{G}$ *kann in* $\mathbb{R}^3$ *eingebettet werden.*

BEWEIS. Wir betrachen eine beliebige Gerade g in $\mathbb{R}^3$ und stellen die Knoten von $\mathbf{G}$ als verschiedene Punkte auf g dar. Für jede Kante wählen wir eine Ebene e, die durch g geht (die Ebenen sollen paarweise verschieden sein), und stellen die Kante durch einen Halbkreis in der Ebene dar. □

Aufgabe 48 ($\star\ \star\ \star$)**:** *Zeige: Jeder Graph* $\mathbf{G}$ *kann in* $\mathbb{R}^3$ *so eingebettet werden, daß jeder Kante ein* Geradenstück *entspricht.*

(Hinweis: Ordne den Knoten von $\mathbf{G}$ *Punkte auf der Kurve* $\left(t, t^2, t^3\right)$ *zu.)*

In der Ebene $\mathbb{R}^2$ ist die Situation nicht so einfach.

DEFINITION 3.7.3. *Ein Graph* $\mathbf{G}$*, der in die Ebene* $\mathbb{R}^2$ *eingebettet werden kann, heißt* planarer Graph.

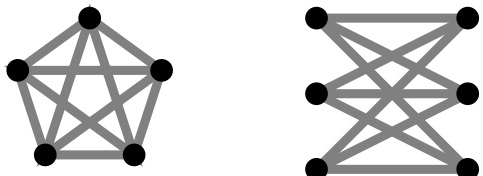
BEMERKUNG 3.7.4. *Einbettung in die Ebene ist übrigens äquivalent mit Einbettung in die Sphäre (Kugeloberfläche)*

$$\left\{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\right\},$$

Denn die stereographische Projektion *liefert eine differenzierbare Bijektion zwischen der Sphäre ohne den "Nordpol"* $(0, 0, 1)$ *und dem* $\mathbb{R}^2$*.*

DEFINITION 3.7.5. *Sei* $A \dot\cup B$ *eine Bipartition von* V *mit* $|A| = n$*,* $|B| = m$*. Der* vollständige bipartite Graph $\mathbf{K}_{n,m}$ *ist der* einfache bipartite *Graph auf* $V = A \dot\cup B$*, der dadurch definiert ist, daß er* alle *Kanten besitzt, die möglich sind; es gilt also* $E\left(\mathbf{K}_{n,m}\right) = \{\{a, b\} : a \in A, b \in B\}$.

Nach ein bißchen Herumprobieren hat man sich schnell überzeugt: Der vollständige Graph $\mathbf{K}_5$ und der vollständige bipartite Graph $\mathbf{K}_{3,3}$ sind *nicht* planar (siehe dazu auch Korollar 3.7.11).



$\mathbf{K}_5$ $\mathbf{K}_{3,3}$

DEFINITION 3.7.6. *Wenn man in einem Graphen* $\mathbf{G}$ *beliebig oft Kanten durch einen neuen Knoten unterteilt (d.h., aus der ursprünglichen Kante* $\{v_1, v_2\}$ *werden zwei neue* $\{v_1, v_{neu}\}$*,* $\{v_{neu}, v_2\}$*; alles andre bleibt unverändert), so nennt man das Ergebnis eine* Unterteilung *(englisch:* Subdivision*) von* $\mathbf{G}$*.*

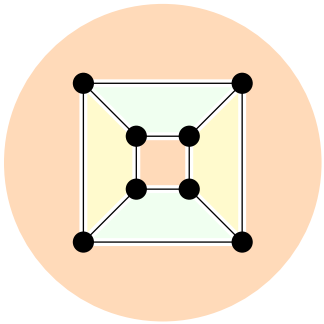
Klarerweise ist jede Unterteilung eines Graphen $\mathbf{G}$ genau dann planar, wenn $\mathbf{G}$ selbst planar ist.

[11] . . . aber nicht ganz exakt.

Satz 3.7.7 (Satz von Kuratowski). *Ein Graph ist genau dann planar ist, wenn er* keine *Unterteilung von* $\mathbf{K}_5$ *oder* $\mathbf{K}_{3,3}$ *als Teilgraph hat.*

Definition 3.7.8. *Sei* $\mathbf{G}$ *ein zusammenhängender planarer Graph mit einer Einbettung* μ *in die Ebene* $\mathbb{R}^2$*: Wenn diese Einbettung aus der Ebene entfernt wird (d.h., man betrachtet* $\mathbb{R}^2 \setminus \mu(\mathbf{G})$*), bleibt eine endliche Menge von zusammenhängenden "Stücken" über; eines davon ist unbeschränkt, alle anderen sind* topologisch äquivalent *zu einer Kreisscheibe: Diese "Stücke" werden* Flächen *genannt.*

Die folgende Graphik zeigt die Einbettung eines Graphs mit 8 Knoten und 12 Kanten; die Einbettung hat 6 Flächen (die unbeschränkte Fläche ist "alles außerhalb des äußeren Quadrats").



Satz 3.7.9 (Eulerscher Polyedersatz). *Sei* $\mathbf{G}$ (V, E) *ein zusammenhängender planarer Graph, und sei eine Einbettung von* $\mathbf{G}$ *in die Ebene mit genau* F *Flächen gegeben. Dann gilt:*

$$|V| - |E| + F = 2. \tag{3.1}$$

Beweis. Wir zeigen die Behauptung mit Induktion nach $n := |E|$. Ein *zusammenhängender* Graph mit $n = 0$ Kanten hat 1 Knoten und 1 Fläche, die Aussage ist also für $n = 0$ richtig.

Beim Induktionsschritt $(n-1) \to n$ unterscheiden wir zwei Fälle:

Fall 1: Es gibt eine Kante e, sodaß der Graph $\mathbf{G} - \mathbf{e}$ noch immer zusammenhängend ist. Dann hat $\mathbf{G} - \mathbf{e}$ noch immer $|V|$ Knoten, aber um eine Kante weniger (also $n-1$ Kanten) und um eine Fläche weniger (weil die beiden Flächen "links und rechts" von e zu einer Fläche verschmolzen sind) als $\mathbf{G}$.

Fall 2: Wenn es keine solche Kante gibt, ist $\mathbf{G}$ ein Baum, hat also $|E|+1$ Knoten und eine Fläche. □

Bemerkung 3.7.10. *Wir haben den Beweis hier sehr glatt und "effizient" geführt: Allen philosophisch Interessierten sei das ausgezeichnete Buch "Proofs and Refutations"* **[5]** *von Imre Lakatos wärmstens empfohlen, das anhand des Eulerschen Polyedersatzes die Schwierigkeiten mathematischer Intuition und ihrer Präzisierung darstellt.*

Aufgabe 49 $(\star\star)$**:** *Finde einen Eulerschen Polyedersatz für unzusammenhängende planare Graphen.*

(Hinweis: In der entsprechenden Gleichung wird die Anzahl der Komponenten des Graphen eine Rolle spielen.)

Aufgabe 50 (⋆ ⋆ ⋆)**:** *Angenommen, sämtliche Flächen eines (endlichen) zusammenhängenden planaren Graphen* **G** *sind durch Kreise (also geschlossene Wege) mit derselben Anzahl* n *von Kanten begrenzt, und alle Knoten haben denselben Grad* d*.*

Drücke die Anzahl der Flächen von **G** *durch* d *und* n *aus. Wieviele Graphen mit diesen Eigenschaften gibt es? (Hinweis: Platonische Körper!)*

Korollar 3.7.11. *Die Graphen* $\mathbf{K}_5$ *und* $\mathbf{K}_{3,3}$ *sind nicht planar.*

Beweis. $\mathbf{K}_5$ hat 5 Knoten und 10 Kanten, eine Einbettung in die Ebene müßte nach (3.1) also 7 Flächen haben. Jede Fläche wird aber von mindestens 3 Kanten begrenzt (denn wenn eine Fläche nur von einer bzw. nur von zwei Kanten begrenzt würde, hätten wir ja eine Schlinge bzw. eine mehrfache Kante), während jede Kante höchstens 2 Flächen begrenzt. Doppelte Abzählung[12] liefert für die Anzahl F der Flächen daher

$$3F \leq 2\,|E| \implies F \leq \frac{10\times 2}{3} = 6\frac{2}{3},$$

ein Widerspruch.

$\mathbf{K}_{3,3}$ hat 6 Knoten und 9 Kanten, also müßte eine Einbettung in die Ebene nach (3.1) 5 Flächen haben. Hier wird aber jede Fläche von mindestens 4 Kanten begrenzt, denn in einem *bipartiten* Graphen gibt es keine geschlossene Wanderung ungerader Länge. Mit doppelter Abzählung wie zuvor erhalten wir also für die Anzahl F der Flächen

$$4F \leq 2\,|E| \implies F \leq \frac{9\times 2}{4} = 4\frac{1}{2},$$

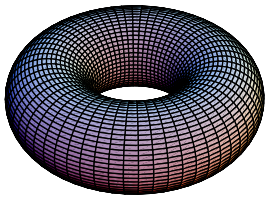
ein Widerspruch. □

Aufgabe 51 (⋆ ⋆)**:** *Zeige:* $\mathbf{K}_5$ *und* $\mathbf{K}_{3,3}$ *kann man auf dem* Torus *— das ist die* 2*–dimensionale Mannigfaltigkeit, die duch die Gleichung*

$$\left(c - \sqrt{x^2+y^2}\right)^2 + z^2 = a^2$$

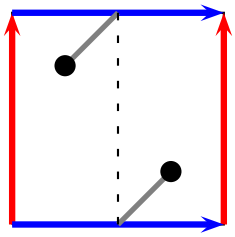
mit $c > a$ *beschrieben ist — einbetten.*

Hinweis: Den Torus kann man sich als "Fahrradschlauch" (ohne Ventilöffnung) vorstellen.



In der Topologie stellt man sich das auch so vor: Durch zwei kreisförmige Schnitte wird der Torus zu einem Rechteck — um ihn wieder zusammenzusetzen, müßte man gegenüberliegende Seiten des Rechtecks "gleichsinnig" miteinander verkleben (also so, daß die verklebten Pfeile in der folgenden Graphik in dieselbe Richtung zeigen). Die hier gezeichnete Kante ist durch den "waagrechten" Schnitt durchtrennt; im zusammengeklebten Torus verbindet sie die beiden Knoten.

[12] $\sum_F \left|\text{Kanten, die } F \text{ begrenzen}\right| = \sum_E \left|\text{Flächen, die } E \text{ begrenzt}\right|$.



DEFINITION 3.7.12. *Sei* $\mathbf{G}(V,E)$ *ein Graph. Zwei Knoten* v_1, v_2 *heißen* benachbart, *wenn sie durch eine Kante verbunden sind (also wenn* $\{v_1,v_2\} \in E$*). Die Menge aller Knoten, die mit einem fixen Knoten* v *benachbart sind, nennen wir die* Nachbarn *von* v*.*
Wir stellen uns vor, daß wir die Knoten von $\mathbf{G}$ *mit (endlich vielen) verschiedenen Farben färben: Wir sprechen von einer* Knotenfärbung, *wenn keine zwei benachbarten Knoten mit derselben Farbe gefärbt sind.*
(Wenn wir die Farben der Einfachheit halber mit den Zahlen $1,2,\ldots,n$ *bezeichnen, dann ist eine Knotenfärbung also eine Funktion* $c : V(\mathbf{G}) \to [n]$ *mit der Eigenschaft* $c(v_1) \neq c(v_2)$*, falls* $\{v_1,v_2\} \in E(\mathbf{G})$*.)*

SATZ 3.7.13. *Jeder* planare *Graph ohne Schlingen hat eine Knotenfärbung mit* 5 *Farben.*

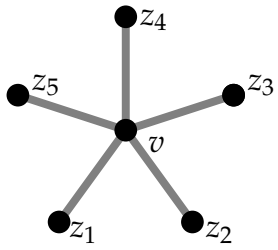
BEWEIS. Wir zeigen das mit Induktion nach der Anzahl der Knoten $n = |V|$. Die Aussage ist natürlich klar für $n \leq 5$.
Sei die Behauptung also für alle Graphen mit weniger als n Knoten gezeigt. Sei $\mathbf{G}(V,E)$ ein Graph mit n Knoten; o.B.d.A. können wir annehmen, daß $\mathbf{G}$ keine mehrfachen Kanten hat (denn das spielt für eine zulässige Färbung ja keine Rolle). Wir stellen uns $\mathbf{G}$ eingebettet in die Ebene vor. Sei n_i die Anzahl der Knoten von $\mathbf{G}$, die Grad i haben (also $n = \sum_{i\geq 1} n_i$), bezeichne F die Anzahl der Flächen (der Einbettung) von $\mathbf{G}$. Wie im Beweis von Korollar 3.7.11 sehen wir $2\cdot|E| \geq 3\cdot F$. Durch doppelte Abzählung erhalten wir $\sum i\cdot n_i = 2\cdot|E|$ (siehe Proposition 1.4.2). Fassen wir dies und (3.1) nochmal zusammen:

$$\begin{aligned} \sum n_i &= |V|\,, \\ \sum i\cdot n_i &= 2\cdot|E|\,, \\ 4\cdot|E| &\geq 6\cdot F, \\ 6|V| - 6|E| + 6F &= 12. \end{aligned}$$

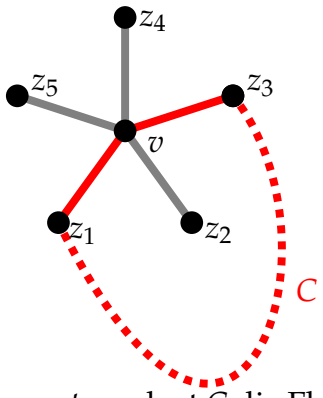
Daraus folgern wir:

$$6|V| - 2|E| \geq 12 \implies \sum (6-i)\, n_i \geq 12.$$

Da mindestens ein Summand der linken Seite positiv sein muß, können wir folgern, daß ein $n_i > 0$ sein muß für $i < 6$: $\mathbf{G}$ enthält also einen Knoten vom Grad ≤ 5. Sei v ein solcher Knoten. Wir betrachten den Teilgraphen $\mathbf{H} = \mathbf{G} - \mathbf{v}$, der von den Knoten $V \setminus \{v\}$ induziert wird. Nach Induktion hat $\mathbf{H}$ eine Knotenfärbung mit 5 Farben $1,2,3,4,5$: Wenn für die Nachbarn (in $\mathbf{G}$) von v nicht alle Farben aufgebraucht wurden, können wir die "freie" Farbe für v verwenden und sind fertig. Also können wir annehmen: v hat Grad 5, und alle Nachbarn von v haben verschiedene Farben. Seien diese Nachbarn $z_1,\ldots,z_5$ im Gegenuhrzeigersinn (in der Einbettung von $\mathbf{G}$) numeriert; o.B.d.A. sei i die Farbe von z_i.



Sei S die Menge aller Knoten, die von z_1 durch Wege erreicht werden können, die *nur* Knoten der Farben 1 oder 3 enthalten. In der Menge S können wir die Farben 1 und 3 vertauschen, ohne daß zwei Knoten, die durch eine Kante verbunden sind, die gleiche Farbe erhalten.
Wenn $z_3 \notin S$, dann vertauschen wir die Farben in S: Danach hat kein Nachbar von v mehr die Farbe 1 (z_1 hat ja nun Farbe 3), daher können wir Farbe 1 für v verwenden.
Also müssen wir annehmen, daß $z_3 \in S$. Es gibt dann also einen Weg $z_1, x_1, \ldots, x_k, z_3$, der nur Knoten mit Farben 1 oder 3 enthält; wenn wir den Knoten v dazugeben, wird daraus ein Kreis C.



Nach dem *Jordanschen Kurvensatz* zerlegt C die Ebene in zwei Teile, klarerweise liegen die Knoten z_2 und z_4 nicht im selben Teil. O.B.d.A. soll z_2 im Inneren von C liegen. Sei T die Menge der Knoten, die von z_2 durch Wege erreicht werden können, die *nur* Knoten der Farben 2 oder 4 enthalten. Kein solcher Weg kann den Kreis C kreuzen, also ist $z_4 \notin T$. Also können wir in der Menge T die Farben 2 und 4 vertauschen, wodurch Farbe 2 für v "frei wird". □

Bemerkung 3.7.14. *Tatsächlich gilt: Jeder planare Graph hat eine Knotenfärbung mit 4 Farben. Dieser berühmte "Vier–Farben–Satz" ist aber sehr viel schwerer zu beweisen.*

KAPITEL 4

Suchen und Sortieren

4.1. Analyse von Algorithmen: Wurzelbäume

Das Wort *Algorithmus* kommt aus dem Arabischen[1] und bedeutet allgemein eine genau definierte Handlungsvorschrift zur Lösung einer Problemstellung. Für Mathematiker genügt es meist, daß es *überhaupt* einen Algorithmus zur Lösung gibt — wir hatten ja in einigen Beweise "Konstruktionsalgorithmen" angegeben —, für praktische Anwendungen, wie sie z.B. bei der Programmierung von Computern laufend auftreten, ist aber natürlich auch entscheidend, daß der Algorithmus

- schnell
- und platzsparend

ist, also z.B. in der Sprache der Computerprogramme

- möglichst wenig Rechenschritte
- und möglichst wenig Speicherplatz

braucht.

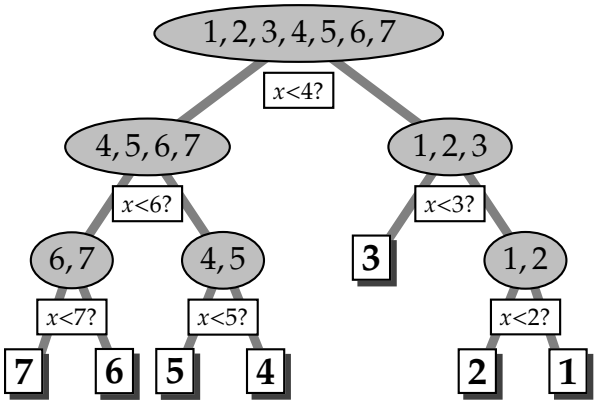
Wir werden uns im folgenden nur mit dem "Effizienzkriterium Geschwindigkeit" befassen. Dabei kann man untersuchen,

- wie lange der Algorithmus im *schlechtest möglichen Fall* dauert (englisch: *Worst case analysis*),
- oder wie lange der Algorithmus im *Durchschnitt* dauert (englisch: *Average case analysis*).

Anstatt an einer exakten allgemeinen Definition von "Algorithmus", "Worst Case" und "Average Case" zu scheitern, betrachten wir im folgenden typische Beispiele, die alle in der Programmierung von Computern eine Rolle spielen.

BEISPIEL 4.1.1. *Sei der Suchbereich $S = [7]$ gegeben. Die Aufgabe lautet, eine unbekannte Zahl $x \in S$ durch (möglichst wenige) Fragen des Typs "$x < i$?" für irgendein $i \in [7]$ zu erraten. Einen Algorithmus zur Bestimmung der gesuchten Zahl x kann man sehr einfach durch einen* Entscheidungsbaum *beschreiben:*

[1] Das Wort ist tatsächlich die Verballhornung eines Namens: Muhammed Al Chwarizmi war ein arabischer Mathematiker des 8. Jahrhunderts nach Christus, dessen Lehrbuch in der lateinischen Übersetzung mit den Worten "Dixit Algorismi" begann. Das Wort hat also nichts mit den Wörtern "Arithmetik" oder "Rhythmus" zu tun, die griechischen Ursprungs sind.



Es ist offensichtlich: Im schlechtesten Fall *(*Worst case*) führt dieser Algorithmus in 3 Schritten zum Ziel (im besten Fall braucht man 2 Schritte), und im* Durchschnitt *(*Average case*) braucht man* $\frac{1\cdot 2+6\cdot 3}{7} = \frac{20}{7}$ *Schritte.*

Unser Beispiel zeigt zweierlei:

- Ein (Such–)Algorithmus läßt sich zweckmäßig durch einen *(Entscheidungs–)Baum* beschreiben,
- Die *Effizienz eines (Such–)Algorithmus* kann man durch Analyse des entsprechenden (Entscheidungs–)Baumes ermitteln.

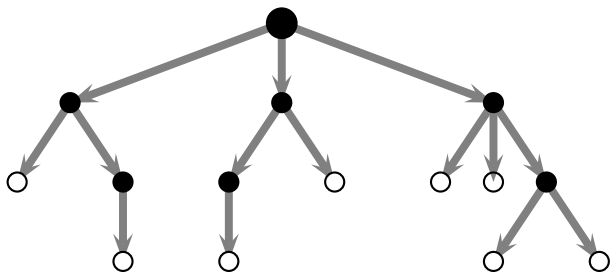
DEFINITION 4.1.2. *Ein* Wurzelbaum *ist ein Baum mit einem ausgezeichneten Knoten, der sogenannten* Wurzel. *(In einem Entscheidungsbaum ist die Wurzel der Knoten "ganz oben", von dem aus sich alles verzweigt.)*

In einem Wurzelbaum gibt es eine implizite Orientierung *der Kanten "von der Wurzel weg", in folgendem Sinn: Sei w die Wurzel und sei $e = \{v_1, v_2\}$ eine Kante. Wenn die Länge des Weges von w nach v_1 k ist, dann ist die Länge des Weges von w nach v_2 $k \pm 1$ — o.B.d.A. nehmen wir $k+1$ an und orientieren die Kante dann: $\vec{e} := (v_1, v_2)$.*

In einem Wurzelbaum (mit der impliziten Orientierung) unterscheiden wir dann die sogenannten

- inneren Knoten*, die Ausgangsgrad > 0 haben,*
- *und die* Blätter *(manchmal auch* Endknoten *oder* äußere Knoten *genannt), die Ausgangsgrad $= 0$ haben. (Die Wurzel kann selbst ein Blatt sein — wenn der Wurzelbaum nur aus einem einzigen Knoten besteht.)*

Im folgenden Wurzelbaum sind die inneren Knoten als schwarze Punkte und die Blätter durch weiße Kreis markiert; die Wurzel ist etwas dicker gezeichnet und die implizite Orientierung der Kanten ist durch Pfeile angedeutet.



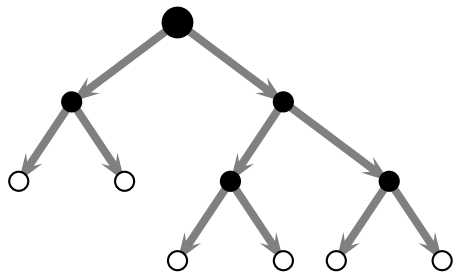
Im Entscheidungsbaum eines Suchalgorithmus bedeutet

- ein *Blatt*, daß der Algorithmus zu einem Ergebnis gekommen ist,
- und der maximale Ausgangsgrad eines inneren Knotens die größte Anzahl der Teile, in die der Suchraum nach einer Frage zerfallen kann.

Dies motiviert die folgende Definition:

Definition 4.1.3. *Sei* **W** *ein Wurzelbaum mit Wurzel w, und sei v ein Knoten in* **W**. *Die Länge des (eindeutigen!) Weges von der Wurzel w zum Knoten v heißt* Länge *des Knotens und wird mit* $\ell(v)$ *bezeichnet. Die Menge der Knoten der Länge k nennen wir das* Niveau *k in* **W**.
Wenn der maximale Ausgangsgrad eines inneren Knotens von **W** *kleinergleich q ist, dann nennen wir* **W** *einen q*–Baum. **W** *heißt ein* vollständiger *q*–Baum, *wenn* jeder *innere Knoten von* **W** *Ausgangsgrad q hat.*
Ein innerer Knoten in einem q–Baum **W** *heißt* gesättigt, *wenn sein Ausgangsgrad gleich q ist. (Ein vollständiger q–Baum hat also nur gesättigte innere Knoten.)*

Z.B. ist der obige Wurzelbaum ein nicht–vollständiger 3–Baum (aber auch ein 4–Baum, 5–Baum, etc.); sein rechtestes Blatt hat die Länge 3, sein linkestes Blatt hat die Länge 2. Der folgende Wurzelbaum ist ein vollständiger 2–Baum:



Lemma 4.1.4. *Sei* $q \geq 2$, *und sei* **W** *ein vollständiger q–Baum mit genau n Blättern. Dann gilt die folgende Teilbarkeitsrelation:*

$$(q-1) \mid (n-1) \tag{4.1}$$

Beweis. Das sieht man leicht mit Induktion nach der Blattanzahl n: Für den (einzigen) q–Baum mit nur *einem* Blatt (das dann zugleich die Wurzel ist!) ist die Behauptung richtig.
In einem beliebigen vollständigen q–Baum mit $n > 1$ Blättern gibt es also einen inneren Knoten v, an dem q Blätter $b_1, \ldots, b_q$ "hängen"[2]. Wenn wir diese Blätter entfernen (also den Teilgraphen betrachten, der durch $V(\mathbf{W}) \setminus \{b_1, \ldots, b_q\}$ induziert wird), dann hat der entstehende Wurzelbaum genau $n - q + 1$ Blätter (v ist ja nun zu einem Blatt geworden), und er ist wieder ein vollständiger q–Baum: Nach Induktionsvoraussetzung gilt $(q-1) \mid (n-q)$; daraus folgt $(q-1) \mid (n-1)$. □

Aufgabe 52 (⋆): *Sei T ein vollständiger 2–Baum mit n Blättern, $e(T)$ bezeichne die Summe der Längen der Blätter, $i(T)$ die Summe der Längen der inneren Knoten. Zeige:*

$$e(T) = i(T) + 2(n-1).$$

[2] v kann als ein innerer Knoten maximaler Länge gewählt werden.

4.2. Suchalgorithmen

Wir wollen nun das "allgemeine Suchproblem" beschreiben, für das wir schon zwei Beispiele (Beispiele 1.5.1 und 4.2.3) gesehen haben.
Gegeben sei eine gewisser Suchraum, also eine Menge S von möglichen Ereignissen (im Wägeproblem aus Beispiel 1.5.1 war das $\left\{\underline{1}, \overline{1}, \ldots, \underline{c}, \overline{c}\right\}$; in Beispiel 4.2.3 war das $[7]$). Weiters seien gewisse "Tests" gegeben, mit denen der Suchraum in Teilmengen partitioniert wird (im Wägeproblem waren die Tests die Wägungen, und im Beispiel 4.2.3 waren das die Fragen "$x < i$?"): Das allgemeine *Suchproblem* besteht darin, ein bestimmtes (aber zunächst unbekanntes) Element in $x \in S$ durch eine Kombination der verfügbaren Tests zu identifizieren. Unter einem *Suchalgorithmus* verstehen wir eine derartige "Kombination der verfügbaren Tests", die *in jedem Fall* (d.h., unabhängig vom Element x) zum Ziel führt. Es ist klar, daß wir einen Suchalgorithmus durch einen *Entscheidungsbaum* beschreiben können: Das ist ein q–Baum, wobei q die größte Anzahl von Blöcken ist, in die ein Test den Suchraum partitioniert.

Aufgabe 53 ($\star\star$)**:** *Löse das Wägeproblem für n Münzen, wenn bekannt ist, daß die falsche Münze schwerer ist.*

4.2.1. Worst–Case Analyse: Informationstheoretische Schranke. Die *Worst–Case Analyse* eines Algorithmus stellt fest, wie lange der Algorithmus im *schlechtesten Fall* braucht. Für Suchalgorithmen ist das also die *maximale* Länge eines Blattes im entsprechenden Entscheidungsbaum $\mathbf{W}$; wir nennen dies die *Länge des Wurzelbaumes* $\mathbf{W}$ und bezeichnen sie mit $L(\mathbf{W})$:

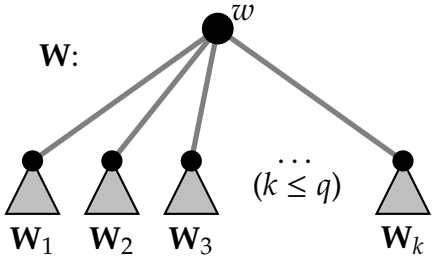
$$L(\mathbf{W}) := \max_{b \text{ Blatt in } \mathbf{W}} \ell(b).$$

Satz 4.2.1. *Sei $q \geq 2$ und $\mathbf{W}$ ein q–Baum mit n Blättern. Dann gilt*

$$L(\mathbf{W}) \geq \left\lceil \log_q n \right\rceil,$$

wo $\log_q n$ der Logarithmus von n zur Basis q ist.

Beweis. Die Behauptung ist klarerweise äquivalent zu $L := L(\mathbf{W}) \geq \log_q n$ oder $q^L = q^{L(\mathbf{W})} \geq n$. Letzteres zeigen wir durch Induktion nach L.
Ist $L = 0$, dann besteht der Baum nur aus der Wurzel, die dann gleichzeitig das einzige Blatt ist, und wir haben in diesem Fall $q^0 \geq 1$.
Für den Induktionsschritt bemerken wir, daß ein typischer q–Baum $\mathbf{W}$ folgendermaßen aussieht:



Von der Wurzel w weg führen $k \leq q$ Kanten; an den anderen Enden dieser Kanten hängt ein Teilgraph $\mathbf{W}_i$, der wieder die Struktur eines q–Baumes hat (symbolisiert durch die Dreiecke im obigen Bild). Wegen $L > 0$ befinden sich alle n Blätter in diesen Teilbäumen, einer dieser Teilbäume muß daher mindestens $n/k \geq n/q$ Blätter enthalten. Bezeichnen wir diesen Teilbaum mit $\mathbf{W}'$. Klarerweise gilt $L(\mathbf{W}') \leq L(\mathbf{W}) - 1$, somit können wir auf $\mathbf{W}'$ die Induktionsvoraussetzung anwenden:

$$q^{L(\mathbf{W}')} \geq \text{Anzahl der Blätter in } \mathbf{W}' \geq \frac{n}{q}.$$

Somit folgt:

$$q^{L(\mathbf{W})} \geq q^{L(\mathbf{W}')+1} = q^{L(\mathbf{W}')} \cdot q \geq \frac{n}{q} q = n.$$

□

Der Wert $\left\lceil \log_q n \right\rceil$ heißt *informationstheoretische Schranke*. Es ist klar, daß wir für unser zuvor beschriebenes "allgemeines Suchproblem" keinen Algorithmus angeben können, der *immer* (also auch im *worst case*) weniger Tests benötigt als $\left\lceil \log_q n \right\rceil$.
Als "Faustregel" für die Konstruktion eines Suchalgorithmus kann man offenbar ansehen: "Zerlege den Suchraum mit jedem Test in möglichst gleich große Teile". Diese simple Heuristik hatten wir auch in Beispiel 1.5.1 verwendet: Dort haben wir tatsächlich einen Algorithmus gefunden, der immer in $3 = \left\lceil \log_3 24 \right\rceil$ zum Ziel führt. Es ist aber *keineswegs immer* möglich, einen Algorithmus zu konstruieren, der mit der theoretisch möglichen unteren Schranke für die Anzahl der Tests auskommt: Typischerweise gelingt das nicht, wenn die Tests die Suchräume nicht "hinreichend gleichförmig" partitionieren können. Das folgende Beispiel illustriert diesen Sachverhalt.

Beispiel 4.2.2. *Betrachten wir nochmals das Wägeproblem aus Beispiel 1.5.1 — diesmal aber mit 13 statt mit 12 Münzen: Hier ist wieder $q = 3$, aber für den Suchraum S gilt nun $|S| = n = 26$. Die informationstheoretische Schranke ist $\left\lceil \log_3 26 \right\rceil = 3$. Es ist aber unmöglich, diese Schranke tatsächlich zu erreichen:*
Bei der ersten Wägung müssen wir ja sowohl in die rechte als auch die linke Waagschale je k Münzen legen. Durch diese Wägung wird der Suchraum in 3 Blöcke partitioniert:

- *linke Waagschale leichter: Restlicher Suchraum hat $2k$ Elemente,*
- *rechte Waagschale leichter: Restlicher Suchraum hat $2k$ Elemente,*
- *beide Waagschalen gleich schwer: Restlicher Suchraum hat $26 - 4k$ Elemente.*

Mindestens einer dieser neuen Suchräume muß also mindestens $\frac{26}{3}$ Elemente haben (denn $2k + 2k + (26 - 4k) = 26$): Diese Zahl muß aber (natürlich) ganz *sein, also ≥ 9, und überdies* gerade, *also ≥ 10. Insbesondere kann es also nicht gelingen, die "möglichst gleichförmige Partitionierung" des Suchraumes in Blöcke der Größe 9, 9 und 8 zu erreichen, und deshalb wird hier die informationstheoretische Schranke verfehlt: Denn der in einem (oder zwei, falls $k = 5$) Fällen nach der ersten Wägung verbleibende Suchraum hat (mindestens) 10 Elemente, und wir brauchen dafür* mindestens *weitere $\left\lceil \log_3 10 \right\rceil = 3$ weitere Wägungen; insgesamt benötigen wir also mindestens 4 Wägungen.*

Wie in Satz A.1.1 im Appendix ausgeführt ist, benötigt ein optimaler Algorithmus für das "allgemeine Münzwägeproblem" mit $n \geq 3$ Münzen $\left\lceil \log_3(2n+2) \right\rceil$ Wägungen.

Beispiel 4.2.3 (Binary search). *Der klassische Algorithmus für das Einordnen eines neuen Elements x in eine bereits geordnete* Liste $a_1 \leq a_2 \leq \cdots \leq a_n$ *ist* Binary Search*: Der Suchraum ist hier die Menge der möglichen Stellen, wo x eingeordnet werden könnte, er umfaßt also $n+1$ Elemente. Der Algorithmus funktioniert so:*

> Sei $L = (a_1, a_2, \ldots, a_n)$ eine der Größe nach geordnete Liste von n reellen Zahlen (entspricht einem Suchraum von $n+1$ möglichen Stellen), bei der wir möglicherweise bereits die Relation $x \leq a_n$ kennen (entspricht einem Suchraum von nur mehr n möglichen Stellen).
>
> Wenn der der Liste L entsprechende Suchraum nur mehr ein Element enthält, sind wir fertig; d.h.: Wenn $n = 0$ *oder* wenn $n = 1$ ist *und* wir die Relation $a_2 = a_{n+1} \leq a_n = a_1$ bereits kennen, dann schreiben wir a_{n+1} an die erste Stelle.
>
> Ansonsten vergleichen wir a_{n+1} mit jenem Element x der Liste, das den Suchraum S möglichst gleichmäßig zerteilt (für $m = |S|$ ist $x = a_{\lceil m/2 \rceil}$). Gilt $a_{n+1} > x$, dann setzen wir $L = \left(a_{\lceil m/2 \rceil + 1}, \ldots, a_n\right)$; gilt $a_{n+1} \leq x$, dann setzen wir $L = \left(a_1, \ldots, a_{\lceil m/2 \rceil}\right)$ (hier kennen wir nun die Relation $x \leq a_{\lceil m/2 \rceil}$); in jedem Fall beginnen wir wieder von vorne.

Die informationstheoretische Schranke besagt, daß wir im worst case mindestens $\left\lceil \log_2(n+1) \right\rceil$ Tests "$a_{n+1} > x$?" brauchen. Und mit Induktion sehen wir, daß der obige Algorithmus diese Schranke tatsächlich erreicht:

Für $n = 0$ brauchen wir $0 = \log_2(1)$ Tests.

Falls $n > 0$, brauchen wir einen ersten Test und haben dann einen Liste vor uns, deren entsprechender Suchraum maximal $\lceil (n+1)/2 \rceil$ Elemente enthält (denn der ursprüngliche Suchraum ist in zwei Blöcke $n+1 = \lceil (n+1)/2 \rceil + \lfloor (n+1)/2 \rfloor$ partitioniert worden). Nach Induktion brauchen wir dafür $\left\lceil \log_2(\lceil (n+1)/2 \rceil) \right\rceil$ Tests. Die Anzahl der benötigten Tests ist also tatsächlich

$$\begin{aligned} 1 + \lceil \log_2 \underbrace{\lceil (n+1)/2 \rceil}_{= \frac{n+1}{2} + \frac{[n \equiv 0\ (2)]}{2}} \rceil &= \left\lceil 1 + \log_2 \frac{n+1}{2} + \log_2 \left(1 + \frac{[n \equiv 0\ (2)]}{n+1} \right) \right\rceil \\ &= \left\lceil \log_2(n+1) + \log_2 \left(1 + \frac{[n \equiv 0\ (2)]}{n+1} \right) \right\rceil \\ &= \left\lceil \log_2(n+1 + [n \equiv 0\ (2)]) \right\rceil \\ &= \left\lceil \log_2(n+1) \right\rceil. \end{aligned} \tag{4.2}$$

$n = 2^r - 2 \mapsto r$,
$n = 2^r - 1 \mapsto r$,
$n = 2^r \mapsto r+1$.

(Die letzte Gleichung folgt aus einer Betrachtung der Sprungstellen von $\left\lceil \log_2(x) \right\rceil$ bei 2^m, $m = 0, 1, \ldots$.)

4.2.2. Average–Case Analyse: Hauptsatz der Informationstheorie. Für praktische Anwendungen ist es meist von größerer Bedeutung, die *durchschnittliche* Dauer eines Algorithmus zu bestimmen: Im Fachjargon heißt das *Average–Case Analyse* eines Algorithmus.

Übersetzt in die "Sprache der Entscheidungsbäume" stehen wir also vor folgender Situation: Gegeben ist ein q–Baum $\mathbf{W}$ mit n Blättern, die mit $1, 2, \ldots, n$ numeriert sind. Jedem Blatt i ist eine bestimmte *Wahrscheinlichkeit* $\mathbf{P}(i)$ zugeordnet; mit $0 \leq \mathbf{P}(i) \leq 1$ und $\sum_{i=1}^{n} \mathbf{P}(i) = 1$. Sei $\ell(i)$ die Länge des Blattes i, dann interessiert uns die *erwartete Länge* der Blätter des Baumes $\mathbf{W}$, die wir mit $\overline{L}(\mathbf{W})$ bezeichnen:

$$\overline{L}(\mathbf{W}) = \sum_{i=1}^{n} \mathbf{P}(i)\, \ell(i).$$

Unsere Frage lautet also: Wie klein kann $\overline{L}(\mathbf{W})$ werden, wenn $\mathbf{W}$ alle möglichen q–Bäume mit n Blättern durchläuft?

Aufgabe 54 ($\star$)**:** *Es seien $m \cdot n$ Leute in einem $m \times n$-Rechteck angeordnet. Wir sollen die unbekannte Person X durch Fragen der Art „Ist X in der i-ten Zeile?", beziehungsweise „Ist X in der j-ten Spalte?" finden. Wieviele Fragen benötigen wir im Durchschnitt?*

Satz 4.2.4 (Kraftsche Ungleichung). *(1) Sei $\mathbf{W}$ ein q–Baum mit n Blättern $1, 2, \ldots, n$, deren Längen durch $\ell(1), \ell(2), \ldots, \ell(n)$ gegeben sind. Dann ist*

$$\sum_{i=1}^{n} q^{-\ell(i)} \leq 1,$$

und Gleichheit gilt genau dann, wenn $\mathbf{W}$ ein vollständiger *q–Baum ist.*

(2) *Seien $\ell(1), \ell(2), \ldots, \ell(n)$ in $\mathbb{Z}^+$ gegeben mit $\sum_{i=1}^{n} q^{-\ell(i)} \leq 1$. Dann existiert ein q–Baum $\mathbf{W}$ mit n Blättern, deren Längen $\ell(1), \ldots, \ell(n)$ sind.*

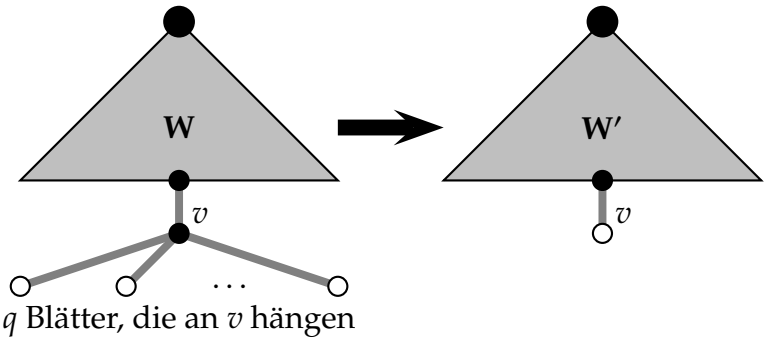
Beweis. Für $q = 1$ sind alle diese Aussagen trivial. Sei also $q \geq 2$.

ad (1): Wenn wir einen q–Baum $\mathbf{W}$ gegeben haben, der nicht vollständig sein sollte, dann können wir ihn durch Anhängen von weiteren Blättern an ungesättigte innere Knoten zu einem vollständigen Baum $\mathbf{W}'$ machen. Dieser hat dann n' Blätter mit $n' \geq n$. Da die Summe $\sum_{i \geq 1} q^{-\ell(i)}$ dabei sicher zunimmt, genügt es zu zeigen, daß für einen *vollständigen* q–Baum die Gleichheit gilt.

Das beweisen wir mit Induktion nach der Anzahl der Blätter n.

Falls $n = 1$ ist, dann besteht der q–Baum nur aus der Wurzel, die gleichzeitig ein Blatt ist (denn $q \geq 2$); für diesen Baum gilt $\sum_{i=1}^{1} q^{-\ell(i)} = q^0 = 1$.

Für den Induktionsschritt sei $\mathbf{W}$ ein vollständiger q–Baum mit n Blättern. Wir betrachten einen Knoten in $v \in \mathbf{W}$, an dem nur Blätter hängen (einen solchen Knoten muß es geben: Wähle z.B. einen inneren Knoten maximaler Länge). Da $\mathbf{W}$ vollständig ist, hängen an v q Blätter $v_1, \ldots, v_q$, die wir alle entfernen; d.h., wir betrachten den Teilgraphen $\mathbf{W}'$, der durch $V(\mathbf{W}) \setminus \{v_1, \ldots, v_q\}$ induziert wird.



W' ist wieder ein vollständiger q–Baum, in dem der Knoten v nun ein Blatt ist; er hat also $n-q+1$ Blätter. Sei $\ell = \ell(v_1) = \cdots = \ell\left(v_q\right)$ die Länge der entfernten Blätter in **W**. Dann gilt in **W**:

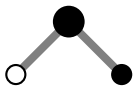
$$\sum_{i=1}^{n} q^{-\ell(i)} = \sum_{i\in[n]\setminus\{v_1,\ldots,v_q\}} q^{-\ell(i)} + q\cdot q^{-\ell}. \tag{4.3}$$

Die rechte Summe in (4.3) ist aber einfach die Summe über die $n-q+1$ Blätter von **W'**, also gleich 1 nach Induktion.

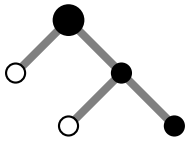
ad (2): Der gesuchte q–Baum kann sukzessive konstruiert werden: Wir illustrieren die Vorgangsweise anhand eines Beispiels. Sei $q=2$, $n=6$, $\ell(1)=1$, $\ell(2)=2$, $\ell(3)=3$, $\ell(4)=\ell(5)=5$, $\ell(6)=6$. Es gilt in der Tat

$$2^{-1}+2^{-2}+2^{-3}+2\cdot 2^{-5}+2^{-6} = \frac{61}{64} \leq 1.$$

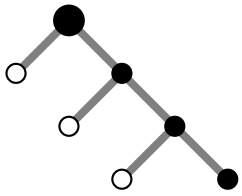
Wir beginnen mit einer Wurzel und zeichnen $q=2$ Kanten nach unten, an denen jeweils ein Knoten hängt. Da eines der Blätter die Länge 1 haben soll, machen wir einen dieser Knoten zu einem Blatt:



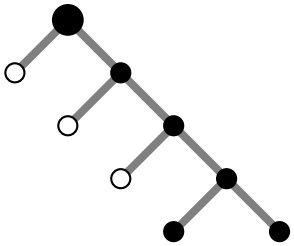
Beim anderen Knoten können wir weiter verzweigen. Da ein Blatt die Länge zwei haben soll, machen wir einen der neuen Knoten zu einem Blatt:



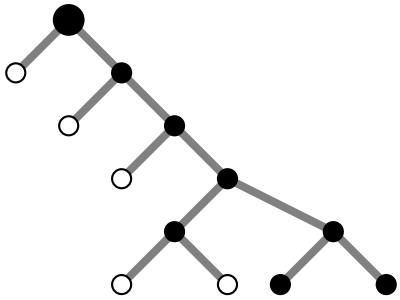
Beim anderen Knoten können wir wieder verzweigen. Ein Blatt soll die Länge 3 haben, also machen wir einen der neuen Knoten zu einem Blatt:



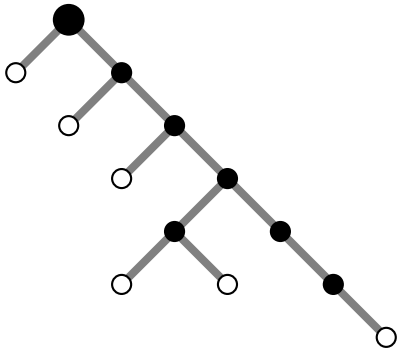
Beim anderen Knoten können wir wieder verzweigen. Da es kein Blatt der Länge 4 geben soll, belassen wir die beiden neuen Knoten als innere Knoten:



Wir können nun bei beiden noch Knoten verzweigen. Es soll zwei Blätter der Länge 5 geben, daher machen wir die ersten beiden durch die Verzweigungen entstandenen Knoten zu Blättern:



Wir müssen jetzt nur noch ein Blatt der Länge 6 realisieren: Wir hängen es an einen der freien Knoten an; eine Verzweigung ist nun überflüssig und kann wieder entfernt werden:



Die Vorgangsweise ist an sich klar. Die einzige Frage ist: Könnte es nicht passieren, daß an irgendeiner Stelle *mehr* Blätter einer bestimmten Länge erzeugt werden müssen als "freie" Knoten zur Verfügung stehen?
Wenn wir die Anzahl der Blätter mit Länge k mit $w(k)$ bezeichnen (d.h., wir wollen einen q–Baum mit $w(k)$ Blättern der Länge k konstruieren, mit $k = 0, 1, \ldots, L$, wobei L die maximale Länge eines Blatts ist), dann können wir die Voraussetzung $\sum_{i=1}^{n} q^{-\ell(i)} \leq 1$ so schreiben:

$$\sum_{k=0}^{L} w(k)\, q^{-k} \leq 1,$$

oder äquivalent

$$w(0)\, q^{L} + w(1)\, q^{L-1} + \cdots + w(L-1)\, q + w(L) \leq q^{L}. \tag{4.4}$$

Angenommen, wir sind mit der oben illustrierten Vorgangsweise soweit gekommen, daß alle Blätter der Längen $0, 1, \ldots, k$ bereits erzeugt wurden; nun müßten wir also $w(k+1)$ Blätter der Länge $k+1$ anhängen.

Durch "vollständiges Verzweigen" von der Wurzel aus bis zum "Niveau" $k+1$ wären an sich q^{k+1} "freie" Knoten vorhanden. Einige dieser Äste stehen aber nicht mehr zur Verfügung, denn wir haben bereits Blätter kürzerer Länge eingetragen; genauer gesagt: Wenn ein Blatt der Länge m eingetragen wurde, dann verringert dies die Anzahl der "freien" Knoten auf Niveau $k+1$ um q^{k+1-m}. Insgesamt stehen uns also nur mehr

$$q^{k+1} - w(0)\, q^{k+1} - w(1)\, q^k - \cdots - w(k)\, q$$

freie Knoten auf Niveau $k+1$ zur Verfügung, und wenn wir mit unserer Prozedur fortfahren wollen, müßte

$$w(k+1) \leq q^{k+1} - w(0)\, q^{k+1} - w(1)\, q^k - \cdots - w(k)\, q$$

gelten. Dies ist aber äquivalent mit

$$w(0)\, q^L + w(1)\, q^{L-1} + \cdots + w(k)\, q^{L-k} + w(k+1)\, q^{L-k-1} \leq q^L,$$

und diese Ungleichung ist nach Voraussetzung (4.4) richtig. □

Wir benötigen noch einen Hilfssatz aus der Analysis:

LEMMA 4.2.5. *Es seien $s_1, s_2, \ldots, s_n$ und $y_1, y_2, \ldots, y_n$ positive reelle Zahlen mit $\sum_{i=1}^n s_i \leq \sum_{i=1}^n y_i$. Für $q > 1$ gilt dann*

$$\sum_{i=1}^{n} y_i \log_q \frac{y_i}{s_i} \geq 0,$$

und Gleichheit gilt genau dann, wenn $s_i = y_i$ für alle i gilt.

BEWEIS. Wegen $\log_q x = \frac{\log x}{\log q}$ genügt es, die Behauptung für den natürlichen Logarithmus log zu zeigen.
Aus der Analysis kennen wir die folgende Ungleichung für den Logarithmus

$$\log x \leq x - 1 \text{ für } x > 0,$$

wobei Gleichheit nur für $x = 1$ gilt. Daraus folgt zunächst

$$\sum_{i=1}^{n} y_i \log \frac{s_i}{y_i} \leq \sum_{i=1}^{n} y_i \left(\frac{s_i}{y_i} - 1 \right) = \sum_{i=1}^{n} s_i - \sum_{i=1}^{n} y_i \leq 0$$

nach Voraussetzung. Wegen $\log \frac{s_i}{y_i} = -\log \frac{y_i}{s_i}$ folgt dann die behauptete Ungleichung.
Gleichheit kann nur gelten, wenn $\log(s_i/y_i) = (s_i/y_i - 1)$ für alle i gilt. Dies gilt aber nur für $s_i/y_i = 1$, also für $s_i = y_i$. □

Damit können wir nun den *Hauptsatz der Informationstheorie* beweisen.

SATZ 4.2.6 (Hauptsatz der Informationstheorie). *Sei $n \geq 1$, $q \geq 2$, und sei $(p_1, p_2, \ldots, p_n)$ mit $p_i < 1$ für alle i eine Wahrscheinlichkeitsverteilung auf den Blättern von q–Bäumen $\mathbf{W}$ mit n Blättern. Dann gilt*

$$-\sum_{i=1}^{n} p_i \log_q p_i \leq \min_{\mathbf{W}} \overline{L}(\mathbf{W}) < -\sum_{i=1}^{n} p_i \log_q p_i + 1,$$

wobei $0 \log_q 0$ *als* 0 *zu interpretieren ist.*

BEWEIS. Wir nehmen zunächst $1 > p_i > 0$ für alle i an. Sei $\mathbf{W}$ irgendein q–Baum mit n Blättern, und seien die Blattlängen $\ell(1), \ell(2), \ldots, \ell(n)$. Aus der Kraftschen Ungleichung wissen wir, daß

$$\sum_{i=1}^{n} q^{-\ell(i)} \leq 1 = p_1 + p_2 + \cdots + p_n$$

gilt. Wir wählen nun in Lemma 4.2.5 $s_i = q^{-\ell(i)}$ und $y_i = p_i$. Das liefert

$$\sum_{i=1}^{n} p_i \log_q \frac{p_i}{q^{-\ell(i)}} \geq 0$$

oder nach Umformung

$$\sum_{i=1}^{n} p_i (\log_q p_i + \ell(i)) \geq 0.$$

Das impliziert $\overline{L}(\mathbf{W}) = \sum_{i=1}^{n} p_i \ell(i) \geq -\sum_{i=1}^{n} p_i \log_q p_i$. Damit ist die linke Ungleichung bewiesen.

Um die rechte Ungleichung zu beweisen, müssen wir *einen* q–Baum $\mathbf{W}$ mit n Blättern finden, der

$$\overline{L}(\mathbf{W}) < -\sum_{i=1}^{n} p_i \log_q p_i + 1$$

erfüllt.

Dazu definieren wir natürliche Zahlen $\ell(i)$ durch $-\log_q p_i \leq \ell(i) < -\log_q p_i + 1$. (Diese sind wegen $0 < p_i \leq 1$ tatsächlich wohldefiniert.)

Es gilt also $q^{-\ell(i)} \leq p_i$ für alle i und somit $\sum_{i=1}^{n} q^{-\ell(i)} \leq \sum_{i=1}^{n} p_i = 1$.

Nach dem zweiten Teil der Kraftschen Ungleichung wissen wir, daß es dann einen q–Baum $\mathbf{W}$ mit n Blättern geben muß, dessen Blätter die Längen $\ell(1), \ell(2), \ldots, \ell(n)$ haben. Für diesen Baum gilt dann:

$$\begin{aligned}
\overline{L}(\mathbf{W}) = \sum_{i=1}^{n} p_i \ell(i) &< \sum_{i=1}^{n} p_i (-\log_q p_i + 1) \\
&= -\sum_{i=1}^{n} p_i \log_q p_i + \sum_{i=1}^{n} p_i \\
&= -\sum_{i=1}^{n} p_i \log_q p_i + 1.
\end{aligned}$$

Schließlich kann man überlegen, daß mit der Konvention $0 \log_q 0 = 0$ die obigen Argumente auch für den Fall modifiziert werden können, daß eine oder mehrere Wahrscheinlichkeiten gleich 0 sind. □

Der Satz besagt, daß die minimal mögliche durchschnittliche Laufzeit eines Suchalgorithmus, der durch einen q–Baum beschrieben werden kann, ziemlich genau gleich $-\sum_{i=1}^{n} p_i \log_q p_i$ ist: Diese Größe ist daher sehr wichtig für die Analyse von Suchalgorithmen. Im Fall der *Gleichverteilung* (also für $p_1 = p_2 = \cdots = p_n = 1/n$) erhalten wir

$$-\sum_{i=1}^{n} \frac{1}{n} \log_q \frac{1}{n} = -\log_q \frac{1}{n} = \log_q n.$$

Das ist "im wesentlichen" derselbe Wert wie in Satz 4.2.1: Im Fall der Gleichverteilung gibt es also "praktisch keinen" Unterschied zwischen der *worst case analysis* und der *average case analysis*.

Für $q = 2$ nennt man die Größe

$$-\sum_{i=1}^{n} p_i \log_2 p_i,$$

die *Entropie* der Wahrscheinlichkeitsverteilung $(p_1, p_2, \ldots, p_n)$: Sie gibt die durchschnittliche Anzahl an Ja/Nein–Fragen an, die man stellen muß, um die volle Information zu erhalten.

4.2.3. Der Huffman–Algorithmus. Der Hauptsatz der Informationstheorie gibt eine untere Schranke für die erwartete Laufzeit eines Suchalgorithmus; nun wollen wir noch den eleganten *Huffman–Algorithmus* kennenlernen, mit dem ein q–Baum konstruiert wird, der einem Suchalgorithmus mit der minimalen erwarteten Laufzeit entspricht. Bevor wir ihn beschreiben, stellen wir einige Hilfsüberlegungen an.

Sei $(p_1, p_2, \ldots, p_n)$ eine Wahrscheinlichkeitsverteilung, wobei ohne Beschränkung der Allgemeinheit $p_1 \geq p_2 \geq \cdots \geq p_n \geq 0$ sei. Bezeichnen wir das Minimum über alle möglichen q–Bäume $\mathbf{W}$ mit n Blättern, die die Wahrscheinlichkeiten $p_1, p_2, \ldots, p_n$ haben, mit $\overline{L}(p_1, p_2, \ldots, p_n)$, also

$$\overline{L}(p_1, p_2, \ldots, p_n) := \min_{\mathbf{W}} \overline{L}\,(\mathbf{W})\,.$$

Wir suchen einen q–Baum $\mathbf{W}_0$, der dieses Minimum erreicht, das heißt

$$\overline{L}(\mathbf{W}_0) = \sum_{i=1}^{n} p_i \ell\,(i) = \overline{L}(p_1, p_2, \ldots, p_n).$$

Wir sagen dann, daß $\mathbf{W}_0$ optimal für $(p_1, p_2, \ldots, p_n)$ ist.

(1) Wir können uns auf den Fall beschränken, daß $(q-1) \mid (n-1)$ gilt: Denn wenn $n - 1 = k(q-1) - a$ ist $1 \leq a < q - 1$, dann hängt man a Blätter, denen die Wahrscheinlichkeit 0 zugeordnet ist, an innere Knoten des Baumes $\mathbf{W}_0$ an. Das ist möglich, denn wenn $(q-1) \nmid (n-1)$ gilt, dann kann gemäß (4.1) der q–Baum nicht vollständig sein, und es gibt also ungesättigte innere Knoten, wo die Blätter angehängt werden können. (Der so entstehende erweiterte q–Baum $\mathbf{W}_1$ muß aber keineswegs schon vollständig sein.)

Es ist $\mathbf{W}_0$ genau dann optimal für $(p_1, p_2, \ldots, p_n)$, wenn $\mathbf{W}_1$ optimal für $(p_1, p_2, \ldots, p_n, \underbrace{0, \ldots, 0}_{a \text{ Nullen}})$

ist. Denn sei $\mathbf{W}_0$ optimal für $(p_1, p_2, \ldots, p_n)$. Dann gilt einerseits:

$$\overline{L}(p_1, p_2, \ldots, p_n) = \overline{L}(\mathbf{W}_0) = \overline{L}(\mathbf{W}_1) \geq \overline{L}(p_1, p_2, \ldots, p_n, 0, \ldots, 0).$$

Nun sei $\mathbf{W}_2$ ein Baum, der optimal für $(p_1, p_2, \ldots, p_n, 0, \ldots, 0)$ sei. Sei $\mathbf{W}_3$ der Baum, der aus $\mathbf{W}_2$ durch Entfernen der a Blätter mit Wahrscheinlichkeit 0 entsteht. Dann gilt also andrerseits

$$\overline{L}(p_1, p_2, \ldots, p_n, 0, \ldots, 0) = \overline{L}(\mathbf{W}_2) = \overline{L}(\mathbf{W}_3) \geq \overline{L}(p_1, p_2, \ldots, p_n).$$

Die beiden Ungleichungen besagen zusammen

$$\overline{L}(p_1, p_2, \ldots, p_n) = \overline{L}(p_1, p_2, \ldots, p_n, 0, \ldots, 0), \tag{4.5}$$

d.h., $\mathbf{W}_1$ ist optimal für $(p_1, p_2, \ldots, p_n, 0, \ldots, 0)$.
Falls nun umgekehrt $\mathbf{W}_1$ optimal für $(p_1, p_2, \ldots, p_n, 0, \ldots, 0)$ ist, dann gilt

$$\overline{L}(p_1, p_2, \ldots, p_n, 0, \ldots, 0) = \overline{L}(\mathbf{W}_1) = \overline{L}(\mathbf{W}_0) \geq \overline{L}(p_1, p_2, \ldots, p_n).$$

Wegen (4.5) folgt aber dann, daß $\mathbf{W}_0$ optimal für $(p_1, p_2, \ldots, p_n)$ ist.
(2) Sei $\ell(i)$ die Länge des Blattes, das Wahrscheinlichkeit p_i hat. Wenn $\mathbf{W}_0$ optimal ist, dann muß $\ell(1) \leq \ell(2) \leq \cdots \leq \ell(n)$ gelten. Denn wenn es Indices $i < j$ gibt mit $\ell(i) > \ell(j)$ und $p_i > p_j$, dann betrachten wir den q–Baum $\mathbf{W}_1$, der genauso wie $\mathbf{W}_0$ aussieht, wo aber die Wahrscheinlichkeiten p_i und p_j vertauscht wurden. Dann gilt

$$\begin{aligned}
\overline{L}(\mathbf{W}_1) &= p_i \ell(j) + p_j \ell(i) + \sum_{\substack{k=1 \\ k \neq i,j}}^{n} p_k \ell(k) \\
&= -p_i \ell(i) - p_j \ell(j) + p_i \ell(j) + p_j \ell(i) + \sum_{k=1}^{n} p_k \ell(k) \\
&= \overline{L}(\mathbf{W}_0) - \big(p_i - p_j\big)\big(\ell(i) - \ell(j)\big) \\
&< \overline{L}(\mathbf{W}_0),
\end{aligned}$$

und somit wäre $\mathbf{W}_0$ nicht optimal, ein Widerspruch.
(3) Wir können uns darauf beschränken, daß $\mathbf{W}_0$ vollständig ist. Denn sei L die maximale Blattlänge in $\mathbf{W}_0$.
Angenommen, es gibt in $\mathbf{W}_0$ einen inneren Knoten u mit $\ell(u) \leq L - 2$, von dem *weniger* als q Kanten "nach unten" verzweigen. Dann können wir *irgendein* Blatt mit Länge L samt der zugehörigen Kante nehmen und an u anhängen. Wir erhalten so einen Baum $\mathbf{W}_1$ mit $\overline{L}(\mathbf{W}_1) \leq \overline{L}(\mathbf{W}_0)$.
Also können wir voraussetzen, daß alle inneren Knoten in Niveaux $\leq L - 2$ gesättigt sind. Sei I die Menge der (sämtlich gesättigten) inneren Knoten u mit $\ell(u) \leq L - 2$, und sei J die Menge der inneren Knoten u mit $\ell(u) = L - 1$.
Die Gesamtzahl der Knoten ist dann einerseits $|I| + |J| + n$.
Andrerseits können wir die Anzahl der Knoten auch so bestimmen: Alle Knoten in I haben je q unmittelbare "Nachfolger" (das sind die anderen Endknoten der

q Kanten, die nach unten verzweigen), für die Knoten $j \in J$ bezeichne n_j die Anzahl der entsprechenden Nachfolger. Die Gesamtzahl der Knoten ist daher auch $1 + q\,|I| + \sum_{j\in J} n_j$. (Der Term 1 zählt die Wurzel.)

Wenn wir die beiden Abzählformeln gleichsetzen erhalten wir

$$(n-1) - |I|\,(q-1) = \sum_{j\in J}(n_j - 1).$$

Aus $(q-1) \mid (n-1)$ folgt

$$(q-1) \Big| \sum_{j\in J}(n_j - 1). \tag{4.6}$$

Wir verteilen nun die Blätter der Länge L so um, daß *möglichst viele* innere Knoten im Niveau $L-1$ gesättigt sind. Das heißt, wir nehmen Blätter der Länge L von ungesättigten inneren Knoten der Länge $L-1$ weg und hängen sie an andere solche Knoten an (ohne allerdings neue Blätter zu erzeugen; d.h., jeder innere Knoten vom Niveau $L-1$ muß mindestens ein Blatt behalten). Es ist klar, daß wir so folgende Situation erreichen können: Im Niveau $L-1$ gibt es

- eine gewisse Anzahl von *gesättigten* inneren Knoten,
- möglicherweise *einen* inneren Knoten, an dem a Blätter hängen; $2 \le a < q$,
- und an allen weiteren inneren Knoten hängt *genau ein* Blatt.

Aus der Teilbarkeitsrelation (4.6) folgt aber sofort, daß es *keinen* inneren Knoten im Nivau $L-1$ geben kann, an dem $2 \le a < q$ Blätter hängen.

Somit hängen an allen inneren Knoten im Niveau $L-1$ entweder genau q Blätter oder genau ein Blatt.

Nun entfernen wir für jeden inneren Knoten im Niveau $L-1$, an dem nur ein Blatt hängt, eben dieses Blatt, und machen ihn dadurch selbst zu einem neuen Blatt, dem wir dieselbe Wahrscheinlichkeit geben wie dem gerade entfernten Blatt: Entweder sinkt die durchschnittliche Blattlänge oder sie bleibt gleich (falls die zugehörigen Wahrscheinlichkeit gleich 0). Der neue, nunmehr *vollständige* q–Baum ist daher mindestens ebenso "gut" wie der ursprüngliche $\mathbf{W}_0$.

Unsere Zwischenbilanz sieht also so aus: Bei der Suche nach einem optimalen q–Baum für $(p_1, p_2, \ldots, p_n)$

- können wir uns auf *vollständige* q–Bäume beschränken;
- wenn wir die Wahrscheinlichkeiten absteigend anordnen,

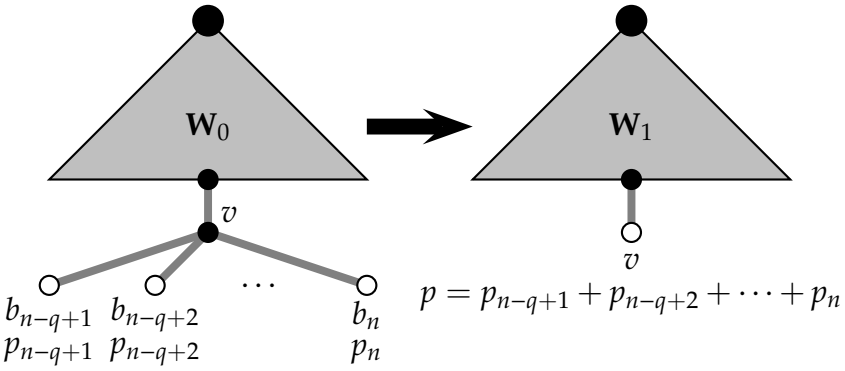
  $$p_1 \ge p_2 \ge \cdots \ge p_n \ge 0,$$

  und das Blatt mit Wahrscheinlichkeit p_i mit b_i bezeichnen, dann gilt in einem optimalen Baum

  $$\ell(b_1) \le \ell(b_2) \le \cdots \le \ell(b_n).$$

  Insbesondere müssen die "letzten" Blätter $b_{n-q+1}, \ldots, b_{n-1}, b_n$ allesamt die maximale Blattlänge L haben.

Nach diesen Vorarbeiten können wir nun den *Reduktionsschritt* formulieren, der die Grundlage für den Huffman–Algorithmus ist: Sei $\mathbf{W}_0$ ein vollständiger Baum, der optimal für $(p_1, p_2, \ldots, p_n)$ ist, und sei v der Knoten, an dem die "letzten" Blätter $b_{n-q+1}, \ldots, b_{n-1}, b_n$ (mit maximaler Länge L) hängen. Wir bilden nun den neuen Baum $\mathbf{W}_1$, der aus $\mathbf{W}_0$ durch Entfernen dieser q Blätter entsteht. Durch das Entfernen der q Blätter wird v zu einem neuen Blatt in $\mathbf{W}_1$; wir teilen diesem die Wahrscheinlichkeit $p = p_{n-q+1} + \cdots + p_{n-1} + p_n$ zu.



Es gilt

$$\begin{aligned}\overline{L}(p_1, p_2, \ldots, p_{n-q}, p) &\le \overline{L}(\mathbf{W}_1) \\ &= \overline{L}(\mathbf{W}_0) - pL + p(L-1) \\ &= \overline{L}(p_1, p_2, \ldots, p_n) - p. \end{aligned} \tag{4.7}$$

Sei umgekehrt $\mathbf{U}_1$ ein vollständiger q–Baum mit $n - q + 1$ Blättern, der optimal für $(p_1, p_2, \ldots, p_{n-q}, p)$ ist. Sei u das Blatt, dessen Wahrscheinlichkeit p ist. Wir hängen an dieses q neue Knoten an und geben ihnen die Wahrscheinlichkeiten $p_{n-q+1}, \ldots, p_{n-1}, p_n$. Dadurch entsteht der neue Baum $\mathbf{U}_0$. (Wir lesen also gewissermaßen die obige Graphik "von rechts nach links".)
Wenn wir die Länge von u in $\mathbf{U}_1$ mit $\ell(u)$ bezeichnen, dann gilt

$$\begin{aligned}\overline{L}(p_1, p_2, \ldots, p_n) &\le \overline{L}(\mathbf{U}_0) \\ &= \overline{L}(\mathbf{U}_1) - p\,\ell(u) + p(\ell(u) + 1) \\ &= \overline{L}(p_1, p_2, \ldots, p_{n-q}, p) + p. \end{aligned} \tag{4.8}$$

Durch Kombination von (4.7) und (4.8) folgt

$$\overline{L}(p_1, p_2, \ldots, p_n) = \overline{L}(p_1, p_2, \ldots, p_{n-q}, p) + p,$$

außerdem gilt in den obigen Ungleichungen überall Gleichheit. Insbesondere ist $\mathbf{W}_0$ genau dann optimal für $(p_1, p_2, \ldots, p_n)$, wenn $\mathbf{W}_1$ optimal für $(p_1, p_2, \ldots, p_{n-q}, p)$ ist.

Der *Algorithmus von Huffman* funktioniert nun so: Gegeben ist die Wahrscheinlichkeitsverteilung $(p_1, p_2, \ldots, p_n)$; o.B.d.A. können wir $p_1 \ge \cdots \ge p_n$ annehmen. Wenn $n - 1$ nicht durch $q - 1$ teilbar ist, also $n - 1 = (q-1)k + r$ für $1 \le r < q$, dann ergänzen wir $q - r - 1$ Wahrscheinlichkeiten 0 und können also ab jetzt $(q-1) \mid (n-1)$ annehmen. Nun fassen wir die q kleinsten Wahrscheinlichkeiten

$p_{n-q+1}, \ldots, p_{n-1}, p_n$ zu $p = p_{n-q+1} + \cdots + p_{n-1} + p_n$ zusammen und erhalten so die neue Wahrscheinlichkeitsverteilung $(p_1, p_2, \ldots, p_{n-q}, p)$, die wir absteigend ordnen. Diesen Schritt wiederholen wir solange, bis "alles zusammengefaßt" ist (d.h., wir sind bei der trivialen Wahrscheinlichkeitsverteilung $(p_1 = 1)$ angelangt). Wenn wir die Schritte in umgekehrter Reihenfolge ansehen, ergibt sich ein q–Baum. Jene Blätter, die den möglicherweise am Anfang hinzugefügten Wahrscheinlichkeiten 0 entsprechen, werden zum Schluß wieder entfernt. Der so erhaltene Baum ist ein optimaler Baum für $(p_1, p_2, \ldots, p_n)$.

An Hand eines Beispiels wird der Algorithmus sofort klar werden.

Beispiel 4.2.7. *Es sei $n = 8$, $q = 3$, und die Wahrscheinlichkeitsverteilung sei*

$$\left(\tfrac{22}{100}, \tfrac{22}{100}, \tfrac{17}{100}, \tfrac{16}{100}, \tfrac{15}{100}, \tfrac{3}{100}, \tfrac{3}{100}, \tfrac{2}{100}\right).$$

Wir werden der Einfachheit halber die Nenner meist nicht anschreiben.

Zunächst überprüfen wir, ob die Bedingung $(q-1) \mid (n-1)$ erfüllt ist: 2 teilt 7 nicht, daher ergänzen wir eine 0, sodaß die neue Verteilung $(22, 22, 17, 16, 15, 3, 3, 2, 0)$ ist.

Die $q = 3$ kleinsten Wahrscheinlichkeiten werden nun zusammengefasst. Ihre Summe ist $0 + 2 + 3 = 5$.

Die reduzierte Verteilung (wieder absteigend geordnet) ist also

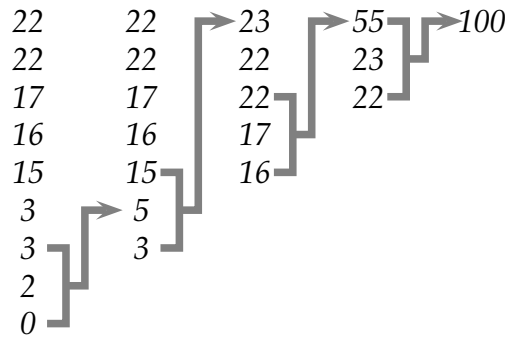
$$(22, 22, 17, 16, 15, 5, 3).$$

Wir fassen wieder die drei kleinsten Wahrscheinlichkeiten zusammen. Ihre Summe ist $3 + 5 + 15 = 23$.

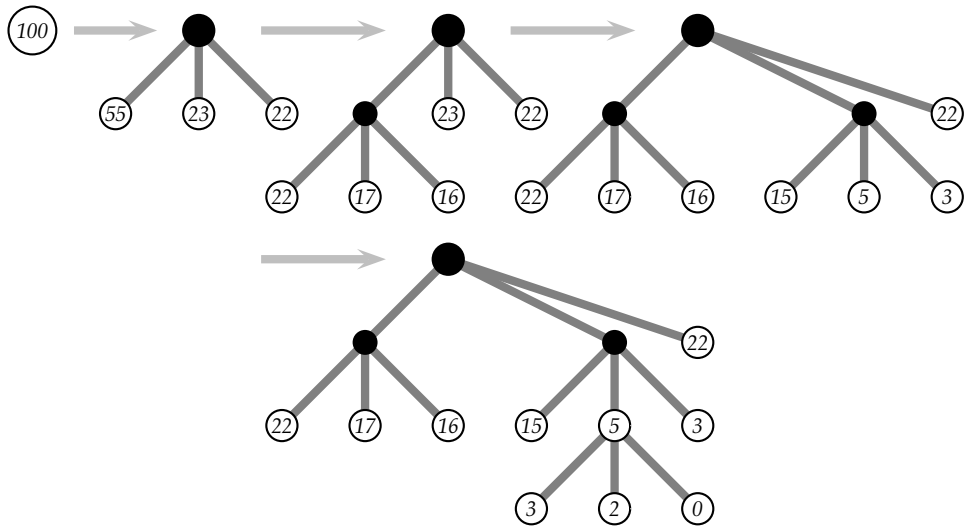
Die reduzierte Verteilung ist dann $(23, 22, 22, 17, 16)$.

Die nächste Reduktion ergibt $(55, 23, 22)$.

Nun bleibt nur noch eine Reduktion, die zu der trivialen Verteilung (100) führt.



Liest man diese Graphik von rechts nach links, dann baut sich der folgende Baum auf:



Die minimal mögliche erwartete Blattlänge ist daher im vorliegenden Fall

$$\overline{L} = \frac{1}{100}(1 \cdot 22 + 2 \cdot (22 + 17 + 16 + 15 + 3) + 3 \cdot (3 + 2)) = \frac{183}{100} = 1.83\,.$$

Die untere Schranke aus dem Hauptsatz der Informationstheorie ist dagegen

$$-\frac{22}{100}\log_3\frac{22}{100} - \frac{22}{100}\log_3\frac{22}{100} - \frac{17}{100}\log_3\frac{17}{100} - \frac{16}{100}\log_3\frac{16}{100}$$
$$-\frac{15}{100}\log_3\frac{15}{100} - \frac{3}{100}\log_3\frac{3}{100} - \frac{3}{100}\log_3\frac{3}{100} - \frac{2}{100}\log_3\frac{2}{100} \sim 1.67\ldots\,.$$

Man beachte weiters, daß die Länge des 3*–Baumes, den wir eben ermittelt haben, gleich* 3 *ist — der* 3*–Baum ist also nicht optimal im Sinne der worst case analysis, denn* $\lceil \log_3 8 \rceil = 2$.

Aufgabe 55 (⋆)**:** *Gegeben ist die Verteilung* $(\frac{30}{100}, \frac{20}{100}, \frac{15}{100}, \frac{14}{100}, \frac{11}{100}, \frac{10}{100})$ *für die Blätter* $1, 2, \ldots, 6$. *Zeige, daß die folgenden binären Suchbäume (*2*–Bäume) optimal sind. Nur einer ist ein Huffman–Baum, welcher?*

Bemerkung 4.2.8. *Beim "Aufbau des Baumes" kann im Huffman–Algorithmus die Situation eintreten, daß für einen Teilbaum zwei oder mehr Möglichkeiten bestehen, ihn "einzuhängen": In solchen Fällen können wir den Teilbaum "möglichst nahe bei der Wurzel" einhängen. Die folgende Übungsaufgabe illustriert diesen Fall.*

Aufgabe 56 (⋆)**:** *Gegeben sei der Suchraum* $\{1, 2, \ldots, 10\}$, *in dem ein (zunächst unbekanntes) Element zu suchen ist. Für die Suche stehen Tests zur Verfügung, die den Suchraum* immer *in drei* beliebige *Teile zerlegen können. Weiters ist von vornherein bekannt, daß Element* i *mit Wahrscheinlichkeit* p_i *das Gesuchte ist:*

i	1	2	3	4	5	6	7	8	9	10
p_i (in %)	30	22	14	12	9	4	4	2	2	1

Konstruiere in dieser Situation einen optimalen Suchalgorithmus (Suchbaum) im Sinne der Average–Case–Analysis. Achtung beim Aufbauen des Baumes: Siehe die Bemerkung dazu in der Vorlesung!

4.3. Sortieralgorithmen

Eine wichtige Anwendung unserer theoretischen Resultate ist die folgende allgemeine Aufgabe, die für die Programmierung von Computern große Bedeutung hat:

> Gegeben sei eine Liste von n verschiedene reellen Zahlen
>
> $$(a_1, a_2, \ldots, a_n)\,.$$
>
> Man ordne diese Zahlen der Größe nach auf möglichst effiziente Weise, und zwar unter Verwendung der Tests "$a_i > a_j$?".

Wenn wir die der Größe nach geordnete Liste mit $\left(a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}\right)$ bezeichnen, dann wird klar, daß das Sortieren der Liste gleichbedeutend damit ist, die Permutation π^{-1} (also die Anordnung der ursprünglichen Liste $(a_1, a_2, \ldots, a_n)$) zu bestimmen. Wir nehmen der Einfachheit halber an, daß alle möglichen Anordnungen der Elemente $a_1, a_2, \ldots, a_n$ gleich wahrscheinlich sind.

Der Suchraum umfaßt hier alle $n!$ Permutationen von $a_1, a_2, \ldots, a_n$, und q ist hier 2. Nach Satz 4.2.1 ist die Anzahl der notwendigen Tests durch die informationstheoretische Schranke

$$\left\lceil \log_2 n! \right\rceil$$

nach unten begrenzt. Um eine Vorstellung von der Größenordnung zu erhalten, verwenden wir die aus der Analysis bekannte *Stirlingsche Formel*

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

und erhalten damit

$$\left\lceil \log_2 n! \right\rceil \sim \log_2 \left(\left(\frac{n}{e}\right)^n \sqrt{2\pi n}\right) = n \log_2 n - n \log_2 e + \frac{1}{2} \log_2 (2\pi n).$$

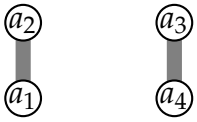
Für unsere Zwecke ignorieren wir den letzten Term und schreiben also

$$\left\lceil \log_2 n! \right\rceil \sim n \log_2 n - n \log_2 e. \tag{4.9}$$

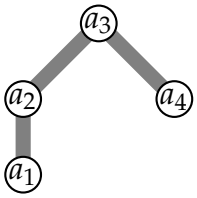
Beispiel 4.3.1. *Sei $n = 4$. Die informationstheoretische Schranke liefert $\left\lceil \log_2 24 \right\rceil = 5$: Theoretisch ist es also möglich, einen Algorithmus zu finden, der immer nach 5 Fragen die Reihenfolge der vier Elemente a_1, a_2, a_3, a_4 herausgefunden hat.*

Am Anfang ist es sicherlich egal, welche zwei Elemente wir vergleichen; beginnen wir also mit a_1 und a_2: O.B.d.A. können wir $a_1 < a_2$ annehmen (der andere Fall ist symmetrisch). Wir notieren diese Information in einem sogenannten Hasse–Diagramm, *das die bisher bekannten Ordnungsrelationen in einem (von oben nach unten orientierten) Wald zeigt: Ein Element x im Hasse–Diagramm ist größer als ein anderes Element y, wenn x mit y durch einen Weg "von oben nach unten" verbunden ist.*

Nun vergleichen wir a_3 und a_4, wieder nehmen wir o.B.d.A. $a_3 > a_4$ an (der andere Fall ist symmetrisch):



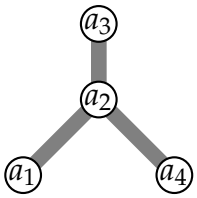
Nun vergleichen wir a_2 und a_3, sei o.B.d.A. $a_2 < a_3$ (der andere Fall ist symmetrisch):



Wenn wir jetzt a_2 und a_4 vergleichen, dann gibt es zwei (nicht–symmetrische) Möglichkeiten: Falls $a_2 < a_4$ ist, dann kennen wir bereits die vollständige Ordnung

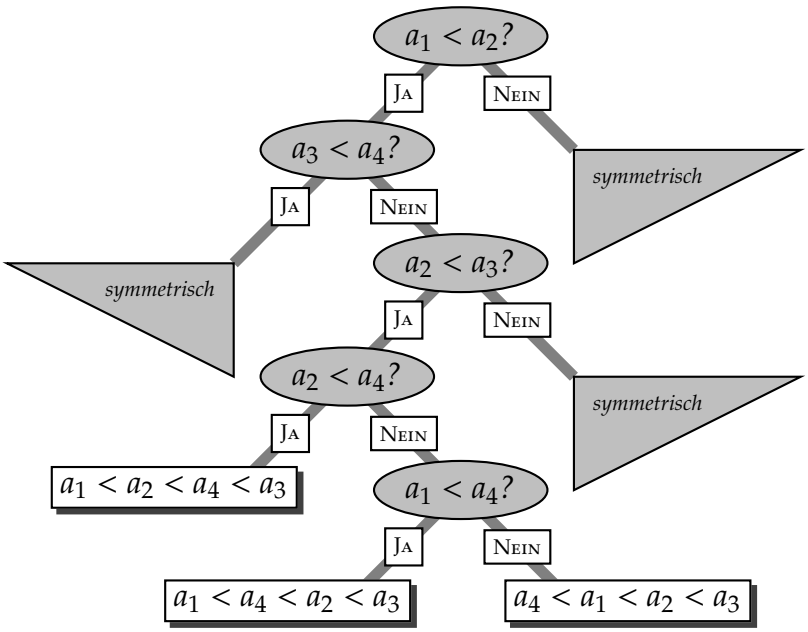
$$a_1 < a_2 < a_4 < a_3.$$

Andernfalls sieht unser Informationsstand im Hasse–Diagramm so aus:



Wenn wir jetzt noch a_1 und a_4 vergleichen, sind wir fertig: Tatsächlich haben wir höchstens 5 Tests gebraucht.

Der entsprechende Entscheidungsbaum sieht so aus:



Für $n = 5$ ergibt die informationstheoretische Schranke $\lceil \log_2 120 \rceil = 7$: Es ist gar nicht so einfach, einen Algorithmus zu konstruieren, der tatsächlich immer nach höchstens 7 Vergleichen die richtige Ordnung ermittelt (siehe Abschnitt A.4 im Anhang).

Aufgabe 57 ($\star\ \star\ \star$)**:** *Bestimme die optimalen Sortieralgorithmen für $n = 6, 7, 8$. (Hinweis: Setze voraus, daß es einen Sortieralgorithmus für $n = 5$ gibt, der immer mit höchstens 7 Vergleichen auskommt.) Was sind die optimalen Suchlängen?*

Nun wollen wir drei gängige Algorithmen zum Sortieren einer Liste betrachten.

4.3.1. Sortieren durch Einfügen. *Sortieren durch Einfügen* ist wohl die nächstliegende Methode: Wir beginnen mit dem ersten Element der Liste, das (natürlich) eine geordnete Liste (a_1) darstellt. Wenn wir die ersten i Elemente in die richtige Ordnung

$$b_1 < b_2 < \cdots < b_i$$

gebracht haben, dann fügen wir im folgenden Schritt a_{i+1} mit *binary search* (siehe Beispiel 4.2.3) in die richtige Stelle ein.

Im schlechtesten Fall ist also die Gesamtzahl $B(n)$ der benötigten Vergleiche gemäß (4.2)

$$B(n) = \sum_{i=2}^{n} \lceil \log_2 i \rceil.$$

Diese Summe kann man explizit ausrechnen: Schreiben wir n als $n = 2^m + r$ für natürliche Zahlen m und r, sodaß $0 < r \leq 2^m$. Es gilt

$$\lceil \log_2 i \rceil = k \iff 2^{k-1} < i \leq 2^k.$$

Wir partitionieren also den Summationsbereich, den i durchläuft, in die Blöcke $\{2\}$, $\{3, 4\}$, $\{5, 6, 7, 8\}$, $\ldots$, $\{2^m + 1, \ldots, n\}$. Im Bereich $\{2^{k-1} + 1, \ldots, 2^k\}$ ist $\lceil \log_2 i \rceil$ konstant gleich k. Der Beitrag den dieser Bereich für die Summe liefert ist daher $2^{k-1} \cdot k$. Insgesamt erhalten wir

$$B(n) = \sum_{k=1}^{m} k \cdot 2^{k-1} + (n - 2^m)(m + 1).$$

Wenn wir die (abbrechende) geometrischen Reihe

$$\sum_{k=0}^{m} x^k = \frac{1 - x^{m+1}}{1 - x}$$

differenzieren, erhalten wir

$$\sum_{k=0}^{m} k \cdot x^{k-1} = \frac{1 - (m + 1)x^m + mx^{m+1}}{(1 - x)^2}.$$

Wenn wir in dieser Formel $x = 2$ setzen, erhalten wir also zunächst

$$\sum_{k=1}^{m} k \cdot 2^{k-1} = 1 + (m - 1)\, 2^m,$$

und damit schließlich für $B(n)$

$$B(n) = n(m+1) - 2^{m+1} + 1$$

oder, wenn wir m wieder durch n ausdrücken,

$$B(n) = n\left\lceil \log_2 n \right\rceil - 2^{\lceil \log_2 n \rceil} + 1.$$

Im Vergleich mit der (Größenordnung der) informationstheoretischen Schranke (4.9) ist das nicht schlecht: Der führende Term $n\left\lceil \log_2 n \right\rceil$ ist gleich, nur der nächste Term ist kleiner, denn $-2^{\lceil \log_2 n \rceil}$ ist ungefähr $-n$, während $-n \log_2 e$ ungefähr $-1.44\,n$ ist.

4.3.2. Mergesort. Eine andere Idee besteht darin, das Sortieren *rekursiv* aufzubauen: Wir teilen die n Elemente $a_1, a_2, \ldots, a_n$ in zwei ungefähr gleich große Hälften, sortieren beide Hälften (rekursiv) nach derselben Methode, und fügen am Schluß die beiden (dann geordneten) Listen zusammen. Dieser Algorithmus heißt *Sortieren durch Zusammenlegen* (englisch: *Merge-Sort*).

Das Zusammenlegen erfordert aber einige Vergleiche: Seien die Listen $b_1 < b_2 < \cdots < b_m$ und $c_1 < c_2 < \cdots < c_n$ gegeben, die wir in der richtigen Reihenfolge zusammenfügen sollen. Das Zusammenfügen können wir "reißverschlußartig" durchführen, also durch folgenden Algorithmus:

`/* Initialisierung: */`

$b \leftarrow (b_1, b_2, \ldots, b_m)$, $c \leftarrow (c_1, c_2, \ldots, c_k)$ und $l \leftarrow \big()$ (l ist die leere Liste).

`/* Schleife: Wird wiederholt, solange die Bedingung erfüllt ist. */`

while (Bedingung: *Beide* Listen b und c sind nicht leer.) **do**

Vergleiche die ersten Elemente b' und c' von b und c; sei x das kleinere der beiden.

Füge x hinten an die Liste l an `/* Bemerke, daß` l `stets richtig geordnet ist! */`

Entferne x aus seiner "alten" Liste (d.h., wenn $x = b'$, dann setze $b \leftarrow b \setminus x$.

end while`/* Zum Schluß */`

Falls eine der Listen b, c nicht leer ist, füge sie an l hinten an: l ist dann die aus den ursprünglichen Listen b und c zusammengefügte geordnete Liste.

Es ist klar, daß wir für dieses Zusammenfügen im schlechtesten Fall $m + k - 1$ Vergleiche brauchen.

Bezeichnen wir nun die Gesamtzahl der Vergleiche, die Mergesort im schlechtesten Fall für die Liste $(a_1, a_2, \ldots, a_n)$ benötigt, mit $M(n)$. Dann erhalten wir die Rekursion[3]

$$M(n) = M(\lfloor n/2 \rfloor) + M(\lceil n/2 \rceil) + n - 1.$$

(Denn wir müssen zuerst die beiden Hälften mit $\lfloor n/2 \rfloor$ und $\lceil n/2 \rceil$ Elementen ordnen und brauchen dann schlimmstenfalls noch weitere $n-1$ Vergleiche, um die beiden geordneten Hälften zusammenzufügen.)

[3]Kurzes Nachdenken zeigt: Das ist nicht "nur" eine obere Schranke für den worst–case, sondern der "echte" worst–case!

BEMERKUNG 4.3.2. *Man kann mit Induktion leicht nachweisen, daß $M(n) = B(n)$ für alle n gilt. Die folgende Tabelle gibt die ersten Werte von $M(n) = B(n)$ wieder und vergleicht sie mit der informationstheoretischen Schranke $\lceil \log_2 n! \rceil$:*

n	2	3	4	5	6	7	8	9	10	11	12
$\lceil \log_2 n! \rceil$	1	3	5	7	10	13	16	19	22	26	29
$B(n) = M(n)$	1	3	5	8	11	14	17	21	25	29	33

Für $n \leq 11$ kann man tatsächlich Algorithmen konstruieren, die mit $\lceil \log_2 n! \rceil$ Vergleichen auskommen. Für $n = 12$ hat eine Computer–Suche ergeben, daß die Minimalzahl 30 ist, also um 1 größer als die informationstheoretische Schranke.

4.3.3. Quicksort. Die wahrscheinlich gängigste Sortiermethode ist der sogenannte *Quicksort*–Algorithmus, der ebenfalls rekursiv vorgeht. Dabei teilen wir die n Elemente wieder in zwei Teile, diesmal aber so, daß die Elemente in einem Teil *alle* kleiner sind als die Elemente im anderen Teil; ordnen jeden der Teile (rekursiv) nach derselben Methode; und fügen die Teile dann (ohne zusätzliche Arbeit wie bei Mergesort) wieder aneinander.

Wenn wir annehmen, daß die Liste im Computer als Vektor

$$a = (a_1, \ldots, a_n)$$

gespeichert ist (daß wir also insbesondere zwei Komponenten des Vektors vertauschen können und zu jeder Komponente des Vektors den linken bzw. rechten Nachbarn — sofern vorhanden — bestimmen können), dann können wir diese Aufteilung algorithmisch so vornehmen, daß kein zusätzlicher Speicherplatz für die zwei Teile benötigt wird:

`/* Initialisierung: */`

Markiere die *letzte* Koordinate (i.e.: a_n) des Vektors..
`/* Schleife: Wird wiederholt, solange die Bedingung erfüllt ist. */`
while (Bedingung: Die Koordinate a_1 ist nicht markiert.) **do**
  Sei x das markierte Element.
  if (a_1 steht links von x UND $a_1 > x$) ODER (a_1 steht rechts von x UND $a_1 \leq x$
  then
    vertausche a_1 und x (die Markierung "wandert dabei mit")
  end if
  Bewege die Markierung um eine Stelle in Richtung von Element a_1 (nach rechts, wenn a_1 rechts von x steht, sonst nach links).
end while

Wir verdeutlichen uns dieses Verfahren an einem Beispiel mit $n = 9$; $a_1 = 4$ wird hier graphisch durch einen Kreis gekennzeichnet, die Markierung durch ein kleines Dreieck:

4	8	9	5	2	1	6	7	3
3	8	9	5	2	1	6	7	4
3	4	9	5	2	1	6	7	8
3	4	9	5	2	1	6	7	8
3	4	9	5	2	1	6	7	8
3	1	9	5	2	4	6	7	8
3	1	4	5	2	9	6	7	8
3	1	2	5	4	9	6	7	8
3	1	2	4	5	9	6	7	8

Es ist klar, daß dieser Algorithmus nach $n-1$ Schritten abbricht. Wenn wir a_1 und das markierte Element x als "Grenzen" (also als erstes/letztes Element) eines "Intervalls" (oder Teilvektors) I von a betrachten, dann ist klar, daß nach jedem Schritt des Algorithmus *links* von I nur Elemente kleiner a_1 stehen und *rechts* von I nur Elemente größergleich a_1 (denn zu Beginn ist dies leererweise richtig, und in jedem Wiederholungsschritt wird dieser Zustand aufrechterhalten). Damit ist weiters klar, daß nach Abbruch des Algorithmus

- alle Elemente, die links von a_1 stehen, kleiner sind als a_1 — diese bilden also den *einen* Teil der Liste,
- alle Elemente, die rechts von a_1 stehen, größergleich sind als a_1 — diese bilden also den *anderen* Teil der Liste).

Auf diese beiden Teil–Listen wird dann dasselbe Verfahren rekursiv angewendet (wenn sie mehr als ein Element beinhalten), bis die ganze Liste richtig geordnet ist.
Die worst case analysis von Quicksort fällt sehr schlecht aus: Wenn die Liste a zufälligerweise bereits total geordnet sein sollte, also

$$a_1 < a_2 < \cdots < a_n,$$

dann wird die Liste in jedem rekursiven Schritt stets

- in die *leere* Liste (die Teil–Liste der Elemente kleiner als das erste Element),
- und in die ursprüngliche Liste ohne ihr erstes Element (die Teil–Liste der Elemente größergleich dem ersten Element, ohne das erste Element selbst)

zerlegt. In diesem Fall benötigen wir also

$$(n-1) + (n-2) + \cdots + 1 = \binom{n}{2}$$

Vergleiche — das sind *alle* Vergleiche von 2 Elementen aus a!
Die average case analysis ist hingegen sehr viel freundlicher: Sei $Q(n)$ die durchschnittliche Anzahl von Vergleichen, die Quicksort für eine Liste a der

Länge n benötigt. Das erste Element a_1 ist jeweils mit Wahrscheinlichkeit $1/n$ das kleinste, das zweitkleinste, ..., oder das größte Element. Wenn a_1 das s–kleinste Element in a ist, dann erhalten wir eine Aufteilung in $s-1$ (die kleineren) und $n-s$ (die größeren) Elemente; für jeden der Teile wiederholen wir rekursiv die Prozedur. Zusammen mit den $n-1$ Vergleichen mit a_1 erhalten wir also die Rekursion

$$Q(n) = n - 1 + \frac{1}{n}\sum_{s=1}^{n}\left(Q(s-1) + Q(n-s)\right)$$

mit dem Anfangswert $Q(0) = 0$. Die rechte Seite können wir vereinfachen:

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

Wir multiplizieren beide Seiten mit n ...

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

... und schreiben dieselbe Gleichung mit $n-1$ statt n nochmals an:

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

Nun subtrahieren wir die beiden obigen Gleichungen und erhalten

$$nQ(n) - (n-1)Q(n-1) = 2(n-1) + 2Q(n-1),$$

oder vereinfacht

$$Q(n) = \frac{n+1}{n}Q(n-1) + 2\frac{n-1}{n}.$$

Das ist eine lineare Rekursion, die aber keine konstanten Koeffizienten hat. Durch Iteration erraten wir eine Summendarstellung für $Q(n)$,

$$Q(n) = 2(n+1)\sum_{k=0}^{n-1}\frac{k}{(k+1)(k+2)},$$

die man mit Induktion nach n leicht nachprüfen kann.
Wenn wir die folgende "Partialbruchzerlegung"

$$\begin{aligned}\frac{k}{(k+1)(k+2)} &= \frac{k+2-2}{(k+1)(k+2)}\\ &= \frac{1}{k+1} - \frac{2}{(k+1)(k+2)}\\ &= \frac{1}{k+1} - \left(\frac{2}{k+1} - \frac{2}{k+2}\right)\end{aligned}$$

verwenden, dann vereinfacht sich die obige Summe (Teleskopsumme!) zu

$$Q(n) = 2(n+1)\left(\sum_{k=1}^{n}\frac{1}{k} - 2 + \frac{2}{n+1}\right).$$

Die Summe auf der rechten Seite ist die *harmonische Zahl* $H_n := \sum_{k=1}^{n} 1/k$ (siehe auch Definition 1.2.3); wir erhalten also

$$Q(n) = 2(n+1)H_n - 4n.$$

Da $H_n \sim \log n$, gelangen wir schließlich zu

$$Q(n) \sim 2n \log n = 2n \log_2 n / \log_2 e \approx 1.38\, n \log_2 n.$$

Wenn wir dieses Resultat wieder mit der informationstheoretischen Schranke $\lceil \log_2 n! \rceil$ vergleichen, dann sehen wir aus (4.9): Die Größenordnung $n \log_2 n$ ist "optimal", nur haben wir hier noch die multiplikative Konstante von ≈ 1.38.

BEMERKUNG 4.3.3. *Wir halten abschließend fest, daß die "Effizienz" eines Algorithmus in der Praxis der Computerprogrammierung nicht allein mit der Anzahl der benötigten (abstrakten) Schritte (Tests) gemessen wird.*
Es ist z.B. ein Nacheil des Sortierens durch Einfügen, daß man jedes Mal, wenn man den richtigen Platz für das neue Element a_{i+1} in der bereits geordneten Liste gefunden hat, alle größeren Elemente verschieben muß, um für a_{i+1} Platz zu schaffen.
Das Sortieren durch Zusammenlegen hat einen anderen Nachteil: Die Teillisten müssen der rekursiv aufgerufenen Funktion immer als Argument übergeben werden, dafür muß also stets neuer Speicherplatz verwendet werden. Insgesamt entsteht dadurch ein sehr großer Speicherbedarf.

ANHANG A

Ausgewählte Zusatzinformationen

Dieser Anhang enthält zusätzliches Material zum Thema, das in der zweistündigen Vorlesung keinen Platz mehr fand.

A.1. Das allgemeine Münzwägeproblem

SATZ A.1.1. *Sei $n \geq 3$. Gegeben seien n Münzen, von denen eine schwerer oder leichter ist. Dann gibt es einen Algorithmus, der* immer *nach $\lceil \log_3(2n+2) \rceil$ Wägungen herausfindet, welche der Münzen falsch ist, und ob sie schwerer oder leichter ist. Diese Zahl von Wägungen ist optimal.*

BEWEIS. Es ist klar, daß man $n \geq 3$ voraussetzen muß.
Die Zahl $\lceil \log_3(2n+2) \rceil$ erfassen wir durch eine Fallunterscheidung:

$$\lceil \log_3(2n+2) \rceil = \begin{cases} \lceil \log_3(2n) \rceil + 1 & \text{falls } 2n = 3^e - 1 \text{ für ein } e \in \mathbb{N}, \\ \lceil \log_3(2n) \rceil & \text{sonst.} \end{cases}$$

In anderen Worten: Die Zahl $\lceil \log_3(2n+2) \rceil$ ist immer gleich der informationstheoretischen Schranke; außer wenn $n = (3^e - 1)/2$ für ein e ist — dann ist sie um 1 größer.
Es sind daher zwei Dinge zu zeigen:

(1) Es gibt *keinen* Algorithmus, der immer nach höchstens
$$\lceil \log_3(2n+2) \rceil - 1$$
Wägungen fertig wird.
(2) Wir müssen hingegen einen Algorithmus angeben, der tatsächlich *immer* nach höchstens
$$\lceil \log_3(2n+2) \rceil$$
Wägungen fertig wird.

Punkt (1) haben wir uns im wesentlichen bereits überlegt: Unter die informationstheoretische Schranke $\lceil \log_3(2n) \rceil$ kommen wir keinesfalls, damit ist Punkt (1) für $n \neq (3^e - 1)/2$ klar.
Falls $n = (3^e - 1)/2$ für ein $e \in \mathbb{N}$ ist, argumentieren wir so wie im Fall $n = 13$: Angenommen, wir legen bei der ersten Wägung jeweils ℓ Münzen in die beiden Waagschalen. Abhängig vom Ausgang der Wägung bleiben uns dann 2ℓ, 2ℓ oder $2n - 4\ell$ Möglichkeiten. Eine dieser Größen muß mindestens $2n/3$ sein, und daher — da es sich um natürliche Zahlen handelt — mindestens $(2n+1)/3$.
Andrerseits sind alle diese Größen auch gerade, aber $(2n+1)/3$ ist eine ungerade Zahl. Daher muß eine dieser Größen mindestens $(2n+2)/3$ sein. (Sogar min-

Denn $n = (3^e - 1)/2$.

Für $n = (3^e - 1)/2$ ist $(2n+1)/3 = 3^{e-1}$, also ungerade.

destens $(2n+4)/3$, aber das brauchen wir gar nicht.) Einer der verbleibenden Suchräume enthält also mindestens $(2n+2)/3$ Möglichkeiten. Gemäß informationstheoretischer Schranke brauchen wir dann noch mindestens $\left\lceil \log_3((2n+2)/3) \right\rceil = \left\lceil \log_3(2n+2) \right\rceil - 1$ weitere Wägungen (in zumindest einem Fall). Zusammen mit der ersten Wägung sind das $\left\lceil \log_3(2n+2) \right\rceil$ Wägungen.

Für Punkt (2) müssen wir einen Algorithmus konstruieren, der das Wägeproblem in der angegebenen Anzahl von Wägungen erledigt. Wir behaupten, daß die folgende Strategie zum Ziel führt:

(A) Falls zu irgendeinem Zeitpunkt der Suchraum gleich

$$\{\overline{1}, \overline{2}, \ldots, \overline{N}, \underline{1}, \underline{2}, \ldots, \underline{N}\}$$

ist, dann führt man die Wägung

$$1, 2, \ldots, \left\lceil \tfrac{N}{3} \right\rceil : \left\lceil \tfrac{N}{3} \right\rceil + 1, \left\lceil \tfrac{N}{3} \right\rceil + 2, \ldots, 2\left\lceil \tfrac{N}{3} \right\rceil \tag{A.1}$$

durch. Sollte jedoch $N = (3^e - 1)/2$ für ein $e \in \mathbb{N}$ sein, und eine andere Münze, sagen wir R, schon als richtig identifiziert sein, dann führt man die Wägung

$$1, 2, \ldots, \left\lceil \tfrac{N}{3} \right\rceil : \left\lceil \tfrac{N}{3} \right\rceil + 1, \left\lceil \tfrac{N}{3} \right\rceil + 2, \ldots, \left\lceil 2\tfrac{N}{3} \right\rceil, R \tag{A.2}$$

durch.

(B) Falls zu irgendeinem Zeitpunkt der Suchraum gleich

$$\{\overline{1}, \overline{2}, \ldots, \overline{m}, \underline{m+1}, \ldots, \underline{N}\}$$

ist, dann führt man im Falle $m \geq 2\left\lceil \frac{N}{3} \right\rceil$ die Wägung

$$1, 2, \ldots, \left\lceil \tfrac{N}{3} \right\rceil : \left\lceil \tfrac{N}{3} \right\rceil + 1, \left\lceil \tfrac{N}{3} \right\rceil + 2, \ldots, 2\left\lceil \tfrac{N}{3} \right\rceil \tag{A.3}$$

durch, und im Falle $m < 2\left\lceil \frac{N}{3} \right\rceil$ die Wägung

$$1, 2, \ldots, \tfrac{x}{2}, m+1, \ldots, m+\tfrac{y}{2} : \tfrac{x}{2}+1, \ldots, x, m+\tfrac{y}{2}+1, \ldots, m+y, \tag{A.4}$$

wo

$$x := \begin{cases} m & \text{falls } m \text{ gerade,} \\ m-1 & \text{falls } m \text{ ungerade,} \end{cases}$$

und $y = 2\lceil N/3 \rceil - x$.

Zunächst überlegen wir uns, daß das überhaupt ein wohldefinierter Algorithmus ist. Was zu zeigen ist, daß man sich nach jeder Wägung wieder in einem der beiden Fälle (A) oder (B), für irgendein N befindet. Dies ist in der Tat leicht für jeden einzelnen Fall nachzuprüfen. Führen wir im Fall (B) etwa die Wägung (A.4) durch, dann ist im Falle, daß die linke Seite leichter gewesen sein sollte, der neue Suchraum gleich

$$\{\overline{1}, \overline{2}, \ldots, \overline{\tfrac{x}{2}}, \underline{m+\tfrac{y}{2}+1}, \ldots, \underline{m+y}\},$$

im Falle, daß die rechte Seite leichter gewesen sein sollte, gleich

$$\{\underline{m+1}, \ldots, \underline{m+\tfrac{y}{2}}, \overline{\tfrac{x}{2}+1}, \ldots, \overline{x}\},$$

im Falle, daß beide Seiten gleich schwer gewesen sein sollten, gleich

$$\{\overline{x+1},\ldots,\overline{m},\underline{m+y+1},\ldots,\underline{N}\}.$$

Somit ergibt sich in jedem der drei Fälle ein Suchraum vom Typ (B), und der Algorithmus kann fortgesetzt werden. Für die anderen Wägungen gelten analoge Überlegungen.

Dass dieser Algorithmus tatsächlich zum Ziel führt, beweisen wir nun mit Induktion nach N. Die Induktionsvoraussetzung sei, daß wir im Fall (A) immer in $\log_3(2N+2)$ Wägungen die falsche Münze aufspüren, falls jedoch schon eine Münze als richtig indentifiziert wurde, dann sogar in $\log_3(2N)$ Wägungen, und daß wir im Fall (B) immer in $\log_3 N$ Wägungen die falsche Münze aufspüren.

Wir kommen zum Induktionsschritt. Wir beginnen mit Fall (A). Falls wir die Wägung (A.1) durchführen, dann bleibt nach erfolgter Wägung entweder der Suchraum

$$\{\overline{\underline{1}},\overline{\underline{2}},\ldots,\overline{\left\lceil\tfrac{N}{3}\right\rceil},\underline{\left\lceil\tfrac{N}{3}\right\rceil+1},\underline{\left\lceil\tfrac{N}{3}\right\rceil+2},\ldots,\underline{2\left\lceil\tfrac{N}{3}\right\rceil}\}$$

oder

$$\{\underline{\underline{1}},\underline{\underline{2}},\ldots,\underline{\left\lceil\tfrac{N}{3}\right\rceil},\overline{\left\lceil\tfrac{N}{3}\right\rceil+1},\overline{\left\lceil\tfrac{N}{3}\right\rceil+2},\ldots,\overline{2\left\lceil\tfrac{N}{3}\right\rceil}\}$$

oder

$$\{\overline{2\left\lceil\tfrac{N}{3}\right\rceil+1},\ldots,\overline{N},\underline{2\left\lceil\tfrac{N}{3}\right\rceil+1},\ldots,\underline{N}\}.$$

In den ersten beiden Fällen handelt es sich um Suchräume vom Typ (B) der Größe $2\left\lceil\frac{N}{3}\right\rceil$, im dritten Fall um einen Suchraum vom Typ (A) der Größe $2N-4\left\lceil\frac{N}{3}\right\rceil\le 2\left\lceil\frac{N}{3}\right\rceil$. Gemäß Induktionsvoraussetzung brauchen wir also in allen Fällen noch (höchstens) $\left\lceil\log_3(2\left\lceil\frac{N}{3}\right\rceil)\right\rceil$ weitere Wägungen. Zweckmäßigerweise schreiben wir $2N=3^e-a$, mit $0\le a<3^e-3^{e-1}$ und a ungerade. Zusammen mit der eingangs durchgeführten Wägung (A.1) ist die Gesamtanzahl der Wägungen im betrachteten Fall gleich

$$1+\left\lceil\log_3(2\left\lceil\tfrac{N}{3}\right\rceil)\right\rceil=1+\left\lceil\log_3(2\left\lceil\tfrac{3^e-a}{6}\right\rceil)\right\rceil.$$

Falls $a\ge 3$, dann gilt

$$\begin{aligned}1+\left\lceil\log_3(2\left\lceil\tfrac{3^e-a}{6}\right\rceil)\right\rceil&\le 1+\left\lceil\log_3(2\left\lceil\tfrac{3^e-3}{6}\right\rceil)\right\rceil\\&\le 1+\left\lceil\log_3(3^{e-1}-1)\right\rceil\\&\le 1+(e-1)=e=\left\lceil\log_3 2N\right\rceil.\end{aligned}$$

Ist hingegen $a=1$, dann ergibt sich

$$\begin{aligned}1+\left\lceil\log_3(2\left\lceil\tfrac{3^e-a}{6}\right\rceil)\right\rceil&=1+\left\lceil\log_3(2\left\lceil\tfrac{3^e-1}{6}\right\rceil)\right\rceil\\&\le 1+\left\lceil\log_3(2\left\lceil\tfrac{3^e+3}{6}\right\rceil)\right\rceil\\&\le 1+\left\lceil\log_3(3^{e-1}+1)\right\rceil\\&\le 1+e=\left\lceil\log_3(2N+2)\right\rceil.\end{aligned}$$

Falls wir hingegen die Wägung (A.2) durchführen (und das kann nur dann der Fall sein, wenn $N = (3^e - 1)/2$), dann bleibt uns nach dieser Wägung entweder ein Suchraum vom Typ (B) der Größe $\lceil 2N/3 \rceil = 3^{e-1}$ oder ein Suchraum vom Typ (A) der Größe $2N - 2 \cdot 3^{e-1} = 3^{e-1} - 1 \leq 3^{e-1}$. Gemäß Induktionsvoraussetzung brauchen wir noch (höchstens) $\left\lceil \log_3 3^{e-1} \right\rceil = e - 1$ weitere Wägungen. Zusammen mit der eingangs ausgeführten Wägung (A.2) ergibt das $1 + (e-1) = e = \left\lceil \log_3 2N \right\rceil$ Wägungen.
Zusammenfassend: Falls N nicht die Form $(3^e - 1)/2$ hat, dann wird man *immer* in $\left\lceil \log_3 2N \right\rceil$ Wägungen fertig, und ebenso wenn schon eine richtige Münze identifiziert wurde. Nur wenn $N = (3^e - 1)/2$ für ein e ist und noch keine richtige Münze identifiziert wurde (das kann aber nur ganz am Anfang passieren, das heißt wenn $N = n$ und $n = (3^e - 1)/2$), dann benötigt man (höchstens) $\left\lceil \log_3 (2N + 2) \right\rceil$ Wägungen. Dies ist exakt das, was für Fall (A) behauptet wurde.
Nun wenden wir uns Fall (B) zu. Egal ob wir die Wägung (A.3) oder (A.4) durchführen, es bleibt uns nach der Wägung ein Suchraum vom Typ (B) der Größe $\lceil N/3 \rceil$ oder der Größe $N - 2\lceil N/3 \rceil \leq \lceil N/3 \rceil$. Gemäß Induktionsvoraussetzung brauchen wir (höchstens) noch $\left\lceil \log_3 \lceil N/3 \rceil \right\rceil$ weitere Wägungen. Wenn wir $N = 3^e - a$, mit $0 \leq a < 3^e - 3^{e-1}$ schreiben, dann sind das zusammen mit der eingangs durchgeführten Wägung (A.4)

$$1 + \left\lceil \log_3 \lceil N/3 \rceil \right\rceil \leq 1 + \left\lceil \log_3 3^{e-1} \right\rceil = 1 + (e-1) = e = \left\lceil \log_3 N \right\rceil$$

Wägungen, wie behauptet. □

A.2. Diskrete Wahrscheinlichkeitsrechnung

Viele Abzählungsfragen stammen ursprünglich von wahrscheinlichkeitstheoretischen Fragestellungen.
Wir geben hier nur eine ganz kurze Skizze (Wahrscheinlichkeitstheorie ist ein eigenes, sehr interessantes Gebiet!) und mischen die relevanten abstrakten Definitionen mit (einfachen) illustrierenden Beispielen:

Definition A.2.1. *Sei Ω eine endliche Menge und $\mathbf{P}$ eine Abbildung $\Omega \to [0,1]$, die jedem $\omega \in \Omega$ eine* Wahrscheinlichkeit $\mathbf{P}(\omega)$ *zwischen 0 und 1 zuordnet, sodaß gilt:*

$$\sum_{\omega \in \Omega} \mathbf{P}(\omega) = 1. \tag{A.5}$$

Das Paar $(\Omega, \mathbf{P})$ nennt man Wahrscheinlichkeitsraum*; die Elemente von ω werden auch als* Elementarereignisse *bezeichnet; $\mathbf{P}$ heißt die* Verteilung *auf Ω. Ist $\mathbf{P}$ konstant auf Ω (d.h., alle Elemente aus Ω haben* dieselbe *Wahrscheinlichkeit, gemäß* (A.5) *also $\mathbf{P}(\omega) = \frac{1}{|\Omega|}$ für alle $\omega \in \Omega$), dann spricht man von* Gleichverteilung.

Beispiel A.2.2. *Beim Werfen eines normalen Spielwürfels gibt es 6 mögliche Ausgänge, die wir naheliegenderweise mit den entsprechenden Augenzahlen bezeichnen. In diesem Fall ist also $\Omega = \{1,2,3,4,5,6\}$, und $\mathbf{P}(\omega)$ ist die Wahrscheinlichkeit, daß Augenzahl ω erreicht wird. Einen Würfel werden wir genau dann als* fair *ansehen, wenn die Augenzahlen gleichverteilt sind, also $\mathbf{P}(\omega) = \frac{1}{6}$ für alle $\omega \in \Omega$.*

Definition A.2.3. *Sei* $(\Omega, \mathbf{P})$ *ein Wahrscheinlichkeitsraum. Eine beliebige Teilmenge* $E \subseteq \Omega$ *heißt ein* Ereignis. *Die Wahrscheinlichkeit von Ereignis E definieren wir als*

$$\mathbf{P}(E) := \sum_{\omega \in E} \mathbf{P}(\omega). \tag{A.6}$$

Beispiel A.2.4. *Beim Würfeln könnte man auch nach der Wahrscheinlichkeit fragen, daß eine* gerade *Augenzahl gewürfelt wird: Das entsprechende Ereignis wäre dann* $\{2, 4, 6\}$*, und die Wahrscheinlichkeit dieses Ereignisses ist bei einem fairen Würfel* $\frac{1}{2}$.

Definition A.2.5. *Sei* $(\Omega, \mathbf{P})$ *ein Wahrscheinlichkeitsraum. Eine (beliebige) Funktion* $X : \Omega \to \mathbb{R}$ *heißt* Zufallsvariable. *Auf dem Bild* $X(\Omega) \subset \mathbb{R}$ *von X existiert die* von X induzierte Verteilung $\mathbf{P}_X$*,*

$$\mathbf{P}_X(x) := \sum_{X(\omega)=x} \mathbf{P}(\omega) \tag{A.7}$$

Beispiel A.2.6. *Beim zweimaligen Würfeln ist der Raum der Elementarereignisse die Menge* $[6] \times [6]$ *aller Paare von Zahlen aus* $[6]$*; für ein Würfelspiel ist aber vielleicht nur die* Summe der Augenzahlen *relevant: Die entsprechende Zufallsvariable X ist dann die Abbildung*

$$X : [6] \times [6] \to \{2, 3, \ldots, 12\}, \; X((i,j)) := i + j.$$

Die induzierte Verteilung auf $\{2, 3, \ldots, 12\}$ *ist*

$$\left(\frac{1}{36}, \frac{2}{36}, \frac{3}{36}, \frac{4}{36}, \frac{5}{36}, \frac{6}{36}, \frac{5}{36}, \frac{4}{36}, \frac{3}{36}, \frac{2}{36}, \frac{1}{36}\right).$$

Definition A.2.7. *Sei* $(\Omega, \mathbf{P})$ *ein Wahrscheinlichkeitsraum. Zwei Ereignisse* E_1, E_2 *aus* Ω *heißen* unabhängig, *wenn* $\mathbf{P}(E_1 \cap E_2) = \mathbf{P}(E_1) \cdot \mathbf{P}(E_2)$ *gilt.*
Seien $X : \Omega \to \mathbb{R}$ *und* $Y : \Omega \to \mathbb{R}$ *zwei Zufallsvariable mit den induzierten Verteilungen* $\mathbf{P}_X$ *auf* $T := X(\Omega)$ *und* $\mathbf{P}_Y$ *auf* $U := Y(\Omega)$*. Die* gemeinsame Verteilung *auf* $T \times U$ *ist dann gegeben durch*

$$\mathbf{P}(x, y) := \sum_{X(\omega)=x, Y(\omega)=y} \mathbf{P}(\omega). \tag{A.8}$$

X und Y heißen unabhängig, *wenn für die gemeinsame Verteilung gilt:*

$$\forall x, y : \; \mathbf{P}(x, y) = \mathbf{P}_X(x) \cdot \mathbf{P}_Y(y). \tag{A.9}$$

Unabhängigkeit von zwei *Ereignissen bzw. von* zwei *Zufallsvariablen kann man in offensichtlicher Weise auf m Ereignisse bzw. m Zufallsvariablen verallgemeinern.*

Beispiel A.2.8. *Beim zweimaligen Würfeln sind die Ereignisse* $(i, .)$ *(d.h., beim ersten Würfeln kommt Augenzahl i) und* $(., j)$ *(d.h., beim zweiten Würfeln kommt Augenzahl j) unabhängig; die Zufallsvariablen* $X : (i, j) \mapsto i$ *und* $Y : (i, j) \mapsto j$ *sind es daher auch.*
Nicht unabhängig *sind hingegen die Zufallsvariablen* $U : (i, j) \mapsto i + j$ *und* $V : (i, j) \mapsto i \cdot j$*, denn z.B. gilt für die gemeinsame Verteilung*

$$\mathbf{P}(2, 1) = \frac{1}{36} > \mathbf{P}_U(2) \cdot \mathbf{P}_V(1) = \frac{1}{36^2}.$$

DEFINITION A.2.9. *Sei* $(\Omega, \mathbf{P})$ *ein Wahrscheinlichkeitsraum und* X *eine Zufallsvariable. Der* Erwartungswert $\mathrm{E}(X)$ *ist definiert als*

$$\mathrm{E}(X) := \sum_{\omega \in \Omega} \mathbf{P}(\omega)\, X(\omega). \tag{A.10}$$

Ersichtlich ist der Erwartungswert $\mathrm{E}(.)$ *ein* lineares Funktional *auf dem Raum aller Zufallsvariablen:*

$$\mathrm{E}(\lambda \cdot X + \mu \cdot Y) = \lambda \cdot \mathrm{E}(X) + \mu \cdot \mathrm{E}(Y) \tag{A.11}$$

für beliebige Zufallsvariable X, Y *und Skalare* λ, μ.

Die Varianz $\mathrm{var}(X)$ *ist definiert als*

$$\mathrm{var}(X) := \mathrm{E}\Big((X - \mathrm{E}(X))^2\Big). \tag{A.12}$$

Es ist leicht zu sehen:

$$\mathrm{var}(X) = \mathrm{E}\left(X^2\right) - \mathrm{E}(X)^2. \tag{A.13}$$

BEISPIEL A.2.10. *Sei* Ω *die Menge aller Permutation von* $[n]$*, und sei die Gleichverteilung auf* Ω *gegeben. Wir fragen uns, wieviele Fixpunkte eine Permutation von* n *Elementen* im Erwartungswert *hat, d.h., uns interessiert der Erwartungswert der Zufallsvariable* F*, die jeder Permutation die Anzahl ihrer Fixpunkte zuordnet.*

Dazu betrachten wir die n *Zufallsvariablen* $F_i : \Omega \to \{0,1\}$; $F_i(\pi) = 1 \Leftrightarrow \pi(i) = i$. *Ersichtlich ist* $\mathrm{E}(F_i) = \frac{(n-1)!}{n!} = \frac{1}{n}$*, also erhalten wir*

$$\mathrm{E}(F) = \mathrm{E}\left(\sum_{i=1}^{n} F_i\right) = \sum_{i=1}^{n} \mathrm{E}(F_i) = 1.$$

Für die Varianz von F *müssen wir gemäß* (A.13) *nur* $\mathrm{E}\left(F^2\right)$ *ausrechnen:*

$$\begin{aligned}\mathrm{E}\left(F^2\right) &= \mathrm{E}\left(\left(\sum_{i=1}^{n} F_i\right)^2\right) \\ &= \sum_{i=1}^{n} \mathrm{E}\left(F_i^2\right) + 2 \sum_{1 \le i < j \le n} \mathrm{E}\left(F_i \cdot F_j\right).\end{aligned}$$

Es ist aber $F_i^2 = F_i$ *und daher* $\mathrm{E}\left(F_i^2\right) = \frac{1}{n}$*, außerdem ist*

$$\mathrm{E}\left(F_i \cdot F_j\right) = \sum_{\pi:\, \pi(i)=i, \pi(j)=j} \frac{1}{n!} = \frac{(n-2)!}{n!} = \frac{1}{n(n-1)}.$$

Also ist $\mathrm{E}\left(F^2\right) = 1 + \binom{n}{2} \frac{2}{n(n-1)} = 2$ *und daher*

$$\mathrm{var}(F) = \mathrm{E}\left(F^2\right) - \mathrm{E}(F)^2 = 1.$$

Aufgabe 58 ($\star$)**:** *Betrachte die Gleichverteilung auf* $\mathfrak{S}_n$ *und bestimme die Wahrscheinlichkeit, daß eine Permutation* $\pi \in \mathfrak{S}_n$ genau $k \le n$ *Fixpunkte hat.*

DEFINITION A.2.11. *Sei* $(\Omega, \mathbf{P})$ *ein Wahrscheinlichkeitsraum und* X *eine Zufallsvariable. Dann ist die* wahrscheinlichkeitserzeugende Funktion $\mathbf{EP}_X$ *von* X *definiert als*

$$\mathbf{EP}_X(z) := \sum_{\omega\in\Omega} \mathbf{P}(\omega)\, z^{X(\omega)} = \sum_{x\in X(\Omega)} \mathbf{P}_X(x)\, z^x. \tag{A.14}$$

PROPOSITION A.2.12. *Sei* $(\Omega, \mathbf{P})$ *ein Wahrscheinlichkeitsraum und* X *eine Zufallsvariable. Dann gilt für die fallenden Faktoriellen von* X*, also für die Zufallsvariable* $X^{\underline{n}} = X\cdot(X-1)\cdots(X-n+1)$*:*

$$\mathrm{E}\left(X^{\underline{n}}\right) = \frac{\mathbf{d}^n}{\mathbf{d}z^n}\mathbf{EP}_X(z)\bigg|_{z=1}. \tag{A.15}$$

Insbesondere ist

$$\mathrm{E}(X) = \frac{\mathbf{d}}{\mathbf{d}z}\mathbf{EP}_X(z)\bigg|_{z=1} \text{ und } \mathrm{E}\left(X^2\right) = \frac{\mathbf{d}^2}{\mathbf{d}z^2}\mathbf{EP}_X(z)\bigg|_{z=1} + \mathrm{E}(X). \tag{A.16}$$

BEWEIS. Ergibt sich durch einfache Rechnung. □

BEISPIEL A.2.13 (Binomialverteilung). *Wir betrachten eine Münze, deren Wurf mit Wahrscheinlichkeit* p *Kopf liefert und mit Wahrscheinlichkeite* $q = (1-p)$ *Zahl. (Abstrakt also:* $\Omega = \{Kopf, Zahl\}$ *mit* $\mathbf{P}(Kopf) = p$, $\mathbf{P}(Zahl) = q = 1-p$.*)*
Weiters betrachten wir die Zufallsvariable X*:* $X(Kopf) = 1$, $X(Zahl) = 0$*. Wenn wir den Wurf der Münze* n *mal wiederholen, dann sind die entsprechenden Zufallsvariablen* $X_1, \dots X_n$ *unabhängig, und die Zufallsvariable* $S = X_1 + \cdots + X_n$ *(sie ist definiert auf dem Raum der* n*–fachen Münzwürfe* $\{Kopf, Zahl\}^n$ *und zählt die Anzahl des Auftretens von Kopf) hat die sogenannte* Binomialverteilung*:*

$$\mathbf{P}(S = k) = \binom{n}{k} p^k q^{n-k}. \tag{A.17}$$

Wir sehen auf einen Blick: Die wahrscheinlichkeitserzeugende Funktion der binomialverteilten Zufallsvariable S *ist* $\mathbf{EP}_S(z) = (pz+q)^n$*. Die Ableitung* $\frac{\mathbf{d}}{\mathbf{d}z}\mathbf{EP}_S(z) = np(pz+q)^{n-1}$*, also ist gemäß* (A.16)[1]

$$\mathrm{E}(S) = np.$$

Weiters ist $\frac{\mathbf{d}^2}{\mathbf{d}z^2}\mathbf{EP}_S(z) = n(n-1)p^2(pz+q)^{n-2}$*, also ist gemäß*(A.16)

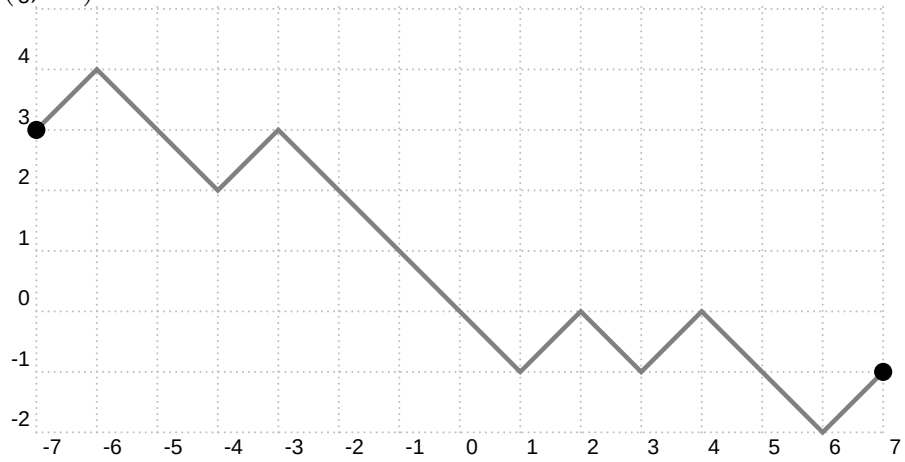
$$\mathrm{var}(S) = \mathrm{E}\left(S^2\right) - \mathrm{E}(S)^2 = n(n-1)p^2 + np - n^2p^2 = n\left(p - p^2\right) = npq.$$

A.2.1. Gitterpunktwege.

DEFINITION A.2.14. *Wir betrachten das* Gitter $\mathbb{Z}^2$ *der Punkte mit ganzzahligen Koordinaten in der Ebene* $\mathbb{R}^2$ *und dazu "zulässige Schritte", die Punkt* (i,j) *entweder mit* $(i+1, j+1)$ *verbinden (ein "Aufwärtsschritt") oder mit* $(i+1, j-1)$ *(ein "Abwärtsschritt").*
Eine Folge von Gitterpunkten $(p_0, p_1, \dots, p_n)$ *heißt* Gitterpunktweg *der Länge* n*, der in* p_0 *beginnt und in* p_n *endet, wenn für* $i = 1, \dots, n$ *immer* p_{i-1} *mit* p_i *durch einen zulässigen Schritte verbunden ist. (Abbildung 1 illustriert diesen Begriff.)*

[1] Es ist ja $p + q = 1$.

ABBILDUNG 1. Ein Gitterpunktweg, der in $(-7,3)$ startet und in $(7,-1)$ endet



Jedem Aufwärtsschritt ordnen wir die Wahrscheinichkeit p zu, jedem Abwärtsschritt die Wahrscheinlichkeit $q = 1 - p$; die Wahrscheinlichkeit eines Gitterpunktweges sei dann das Produkt der Wahrscheinlichkeiten seiner Schritte.

BEISPIEL A.2.15. *Sei Ω die Familie aller Gitterpunktwege der Länge n, die im Ursprung $(0,0)$ starten. Sei X die Zufallsvariable, die jedem Gitterpunktweg aus Ω die y–Koordinate seines Endpunktes zuordnet (X nimmt also Werte aus $\{-n, -n+2, \ldots, n-2, n\}$ an).*
Es ist offensichtlich, daß für die wahrscheinlichkeitserzeugende Funktion gilt:

$$\mathbf{EP}_X(z) = \left(p \cdot z + q\frac{1}{z}\right)^n.$$

Analog zu Beispiel A.2.13 erhalten wir:

$$\mathrm{E}(X) = n(p-q), \ \mathrm{var}(X) = 4npq.$$

A.2.2. Dyck–Pfade: Das Spiegelungsprinzip und die Catalan–Zahlen. Sei Ω die Familie aller Gitterpunktwege der Länge $2n$, die in $(0,0)$ beginnen und in $(2n,0)$ enden. Ersichtlich ist $|\Omega| = \binom{2n}{n}$ und alle Gitterpunktwege in Ω sind gleich wahrscheinlich. Wir stellen die Frage:

Wie wahrscheinlich ist es, daß ein Gitterpunktweg von $(0,0)$ nach $(2n,0)$ niemals unter die x–Achse gerät (daß also die y–Koordinaten aller seiner Punkte stets ≥ 0 sind)?

Klarerweise ist die Frage äquivalent zu einem Abzählungsproblem:

DEFINITION A.2.16. *Ein Gitterpunktweg, der in $(0,0)$ beginnt und in $(2n,0)$ endet, und der niemals unter die x–Achse gerät, heißt* Dyck–Pfad *der Länge $2n$.*

SATZ A.2.17 (Spiegelungsprinzip). *Die Anzahl der Dyck–Pfade der Länge $2n$ ist*

$$C_n := \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}. \tag{A.18}$$

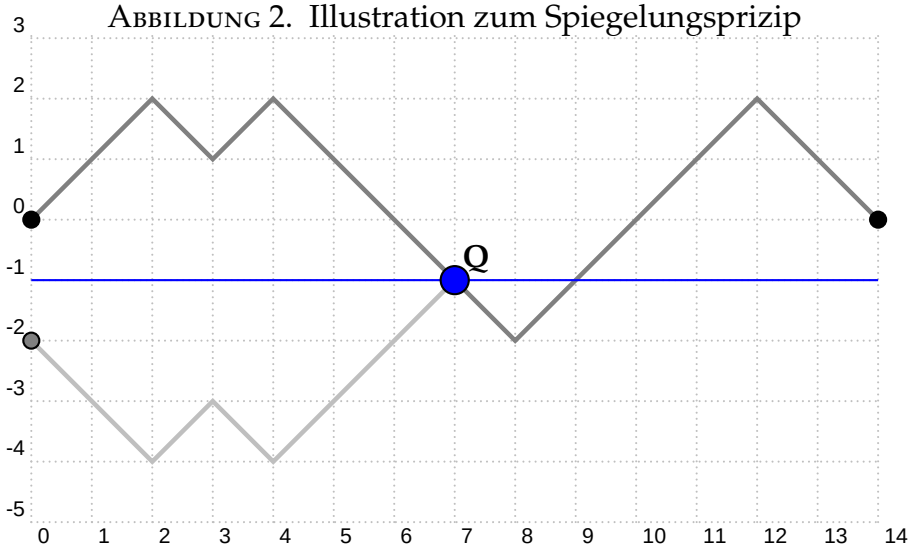


ABBILDUNG 2. Illustration zum Spiegelungsprizip

BEWEIS. Die gesuchte Anzahl ist natürlich die Anzahl $\binom{2n}{n}$ *aller* Gitterpunktwege von $(0,0)$ nach $(2n,0)$ *minus* der Anzahl jener "schlechten" Gitterpunktwege von $(0,0)$ nach $(2n,0)$, die unter die x–Achse geraten.

Ein "schlechter" Gitterpunktweg p muß notwendigerweise ein erstes Mal die Gerade $y \equiv -1$ treffen, nenne diesen ersten Treffpunkt Q. Spiegle nun den Anfangsabschnitt von p, der in $(0,0)$ beginnt und in Q endet, an der Geraden $y \equiv -1$, und setze ab dem Punkt Q mit dem Endabschnitt von p fort: Es entsteht ein Gitterpunktweg, der in $(0,-2)$ beginnt und in $(2n,0)$ endet. (Abbildung 2 illustriert das Verfahren.)

Diese "Spiegelungsabbildung" definiert aber eine *Bijektion* zwischen der Familie der "schlechten" Gitterpunktwege und der Familie aller Gitterpunktwege, die in $(0,-2)$ beginnen und in $(2n,0)$ enden: Deren Anzahl ist $\binom{2n}{n+1}$. □

Aufgabe 59 ($\star\,\star$)**:** *Zeige, daß die Anzahlen*

- *der Dyck–Pfade der Länge* $2n$
- *und der Triangulierungen des* $(n+2)$*–Ecks*

dieselbe Rekursion erfüllen.

Aufgabe 60 ($\star\,\star$)**:** *Für zwei ganze Zahlen* $h_1 > h_2$ *betrachten wir die Familie aller Paare von Gitterpunktwegen* (P_1, P_2)*, wo* P_i *in* $(0, 2h_i)$ *beginnt und in* $(2n, 2h_i)$ *endet, und wo* P_1 *und* P_2 *keinen Gitterpunkt gemeinsam haben (man nennt das* nichtüberschneidende Gitterpunktwege*). Zeige, daß die Anzahl dieser nichtüberschneidenden Gitterpunktwege durch die* 2×2*–Determinante*

$$\det \begin{vmatrix} \binom{2n}{n} & \binom{2n}{n-h_1+h_2} \\ \binom{2n}{n+h_1-h_2} & \binom{2n}{n} \end{vmatrix}$$

gegeben ist.

(Hinweis: Versuche die Idee des Spiegelungsprinzips geeignet zu adaptieren!)

Aufgabe 61 ($\star\,\star\,\star$)**:** *Seien* i*,* j *und* h *ganze Zahlen, sodaß* $0 \le 2i, 2j \le h$*. Zeige: Die Anzahl aller Gitterpunktwege von* $(0, 2i)$ *nach* $(2n, 2j)$*, die* zwischen *den Geraden* $y = 0$ *und* $y = h \ge 0$

liegen (d.h., diese Gitterpunktwege gehen nie unter die x–Achse und nie über die "Höhe" h), ist

$$\sum_{k\in\mathbb{Z}}\left(\binom{2n}{n-i+j-k\,(h+2)}-\binom{2n}{n+i+j-k\,(h+2)+1}\right).$$

(Hinweis: Kombiniere das Spiegelungsprinzip mit dem Prinzip der Inklusion–Exklusion.)

A.3. Die Lagrangesche Inversionsformel

Gegeben sei eine formale Potenzreihe $f(z)$ mit verschwindendem konstanten Term: Dann existiert, wie wir aus Satz 2.2.10 wissen, die zusammensetzungsinverse Reihe $F(z)$; für die Koeffizienten von $F(z)$ wollen wir nun eine allgemeine Formel angeben. Dazu ist es nützlich, ein etwas allgemeineres Problem zu betrachten.

Zunächst brauchen wir aber eine Erweiterung unseres Kalküls der formalen Potenzreihen.

Definition A.3.1. *Eine (formale)* Laurentreihe *ist eine formale Reihe*

$$\sum_{n\geq N} a_n z^n$$

für ein $N\in\mathbb{Z}$ (N kann kleiner Null sein, d.h., es können negative Potenzen von z auftreten); die a_n sind hier irgendwelche Koeffizienten in $\mathbb{C}$.

Wir bezeichnen die Menge aller formalen Laurentreihen mit $\mathbb{C}((z))$.

Man kann nun auch für Laurentreihen Addition, Multiplikation, Skalarmultiplikation und Zusammensetzung genau wie bei den formalen Potenzreihen definieren. Es bleiben auch alle Sätze (mit geringfügigen Modifikationen) gültig. Ein wesentlicher Unterschied besteht darin, daß der Satz über das multiplikative Inverse für Laurentreihen einfacher lautet:

Satz A.3.2. *Eine formale Laurentreihe $a(z)$ besitzt genau dann eine bezüglich der Multiplikation inverse Laurentreihe, wenn $a(z)\neq 0$. Die inverse Reihe ist in diesem Fall* eindeutig *bestimmt.*

Das bedeutet, daß die formalen Laurentreihen sogar einen *Körper* bilden.

In der Folge werden wir nur den Fall betrachten, daß die formale Potenzreihe $f(z)$ "mit z^1 beginnt", also von der Gestalt

$$f(z)=f_1\cdot z^1+f_2\cdot z^2+\cdots$$

ist mit $f_1\neq 0$ (der allgemeinere Fall $f=f_m\cdot z^m+\cdots$ für $m>1$ läßt sich darauf leicht zurückführen.) Wir beweisen zuerst ein vorbereitendes Lemma.

Lemma A.3.3. *Gegeben sei die formale Potenzreihe $f(z)=f_1z+f_2z^2+\cdots$ mit $f_1\neq 0$. Dann gilt für alle ganzen Zahlen n die Gleichung*

$$\left[\!\left[z^{-1}\right]\!\right] f^{n-1}(z)f'(z)=[n=0]\,.$$

BEWEIS. Es ist klar, daß der Koeffizient von z^{-1} in jeder abgeleiteten Reihe gleich 0 ist, also insbesondere in $Df^n(z)$. Das bedeutet, daß $n\left[\!\left[z^{-1}\right]\!\right] f^{n-1}(z)f'(z) = 0$. Somit ist die Behauptung bereits für alle $n \neq 0$ gezeigt. Für $n = 0$ wiederum kann man das direkt nachrechnen:

$$\begin{aligned}
\left[\!\left[z^{-1}\right]\!\right] f^{-1}(z)f'(z) &= \left[\!\left[z^{-1}\right]\!\right] \frac{f_1 + 2f_2z + \cdots}{f_1z + f_2z^2 + \cdots} \\
&= \left[\!\left[z^{-1}\right]\!\right] \frac{1}{z} \frac{f_1 + 2f_2z + \cdots}{f_1 + f_2z + \cdots} \\
&= \left[\!\left[z^{-1}\right]\!\right] \frac{1}{z} \frac{1 + 2\frac{f_2}{f_1}z + \cdots}{1 - \underbrace{z\left(-\frac{f_2}{f_1} - \cdots\right)}_{=:h(z)}} \\
&= \left[\!\left[z^{-1}\right]\!\right] \frac{1}{z} \left(1 + 2\frac{f_2}{f_1}z + \cdots\right)\left(1 + h\left(z\right) + h\left(z\right)^2 + \cdots\right) \\
&= 1.
\end{aligned}$$

□

SATZ A.3.4. *Sei $g(z)$ eine formale Laurentreihe und $f(z) = f_1z + f_2z^2 + \cdots$ mit $f_1 \neq 0$. Angenommen, es gibt eine Entwicklung von $g(z)$ in Potenzen von $f(z)$, also*

$$g(z) = \sum_k c_k f^k(z).$$

Dann sind die Koeffizienten c_n gegeben durch

$$c_n = \frac{1}{n}\left[\!\left[z^{-1}\right]\!\right] g'(z)f^{-n}(z) \quad \textit{für } n \neq 0, \tag{A.19}$$

oder alternativ durch

$$c_n = \left[\!\left[z^{-1}\right]\!\right] g(z)f'(z)f^{-n-1}(z). \tag{A.20}$$

BEWEIS. Für die erste Behauptung differenzieren wir die Voraussetzung:

$$g'(z) = \sum_k kc_k f'(z)f^{k-1}(z).$$

Nun multiplizieren wir beide Seiten mit $f^{-n}(z)$:

$$g'(z)f^{-n}(z) = \sum_k kc_k f'(z)f^{k-n-1}(z).$$

Wenn wir nun auf beiden Seiten den Koeffizienten von z^{-1} ablesen, dann erhalten wir gemäß Lemma A.3.3 auf der rechten Seite nc_n. Also ergibt sich die Behauptung durch Koeffizientenvergleich (nach Division durch n).
Für die zweite Behauptung multiplizieren wir die Voraussetzung mit $f'(z)f^{-n-1}(z)$, sodaß wir

$$g(z)f^{-n-1}(z)f'(z) = \sum_k c_k f^{k-n-1}(z)f'(z)$$

erhalten, und argumentieren genau wie zuvor. □

Die *Lagrangesche Inversionsformel* ergibt sich nun als Spezialfall.

KOROLLAR A.3.5 (Lagrangesche Inversionsformel). *Sei $f(z)$ eine formale Potenzreihe der Gestalt $f(z) = f_1 z + f_2 z^2 + \cdots$ mit $f_1 \neq 0$, sei $F(z)$ die bezüglich der Zusammensetzung inverse Reihe. Dann gilt*

$$[\![z^n]\!]\, F^k(z) = \frac{k}{n}[\![z^{-k}]\!]\, f^{-n}(z) \quad \textit{für } n \neq 0, \tag{A.21}$$

oder

$$[\![z^n]\!]\, F^k(z) = [\![z^{-k-1}]\!]\, f'(z) f^{-n-1}(z). \tag{A.22}$$

BEWEIS. Wenn $F(z)$ zusammensetzungsinvers zu $f(z)$ ist, dann gilt insbesondere $F^k(f(z)) = z^k$. Ausführlich geschrieben bedeutet das

$$\sum_n F_n^{(k)} f(z)^n = z^k,$$

wobei $F^k(z) = \sum_n F_n^{(k)} z^n$. Wenn wir nun (A.19) aus Satz A.3.4 auf $g(z) = z^k$ anwenden, erhalten wir

$$F_n^{(k)} = \frac{1}{n}[\![z^{-1}]\!]\, k z^{k-1} f^{-n}(z) = \frac{k}{n}[\![z^{-k}]\!]\, f^{-n}(z),$$

und wenn wir (A.20) anwenden, erhalten wir die zweite Behauptung. □

BEISPIEL A.3.6. *Wir hatten bei der Aufgabe, die Triangulierungen eines n–Ecks zu zählen, die folgende Gleichung für die erzeugende Funktion der gesuchten Zahlen hergeleitet:*

$$zF(z)^2 - F(z) + 1 = 0.$$

Wenn wir beide Seiten mit z multiplizieren und die Schreibweise $G(z) := zF(z)$ einführen, dann schreibt sich die Gleichung in der Form

$$z = G(z) - G^2(z).$$

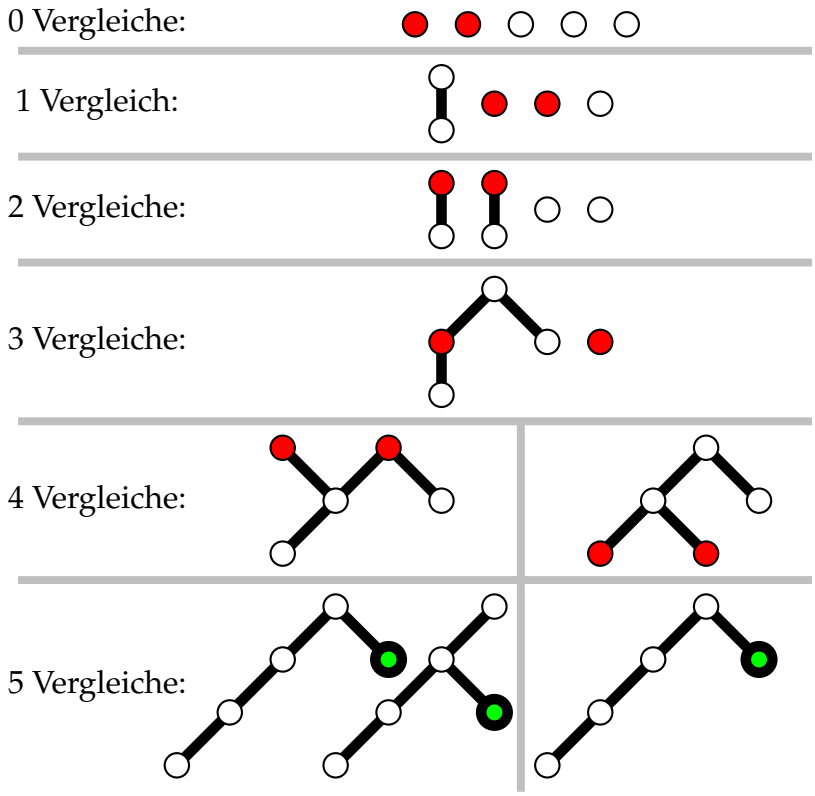
Mit anderen Worten: $G(z)$ ist die bezüglich der Zusammensetzung inverse Reihe zu $z - z^2$. Wenn wir nun die Lagrangesche Inversionsformel in der Form (A.21) *auf $f(z) = z - z^2$ (mit $k = 1$) anwenden, dann erhalten wir:*

$$\begin{aligned}
[\![z^n]\!]\, G(z) &= \frac{1}{n}[\![z^{-1}]\!]\, (z - z^2)^{-n} \\
&= \frac{1}{n}[\![z^{-1}]\!]\, z^{-n}(1 - z)^{-n} \\
&= \frac{1}{n}[\![z^{n-1}]\!]\, (1 - z)^{-n} \\
&= \frac{1}{n}\binom{-n}{n-1}(-1)^{n-1} \\
&= \frac{1}{n}\binom{2n-2}{n-1},
\end{aligned}$$

was mit unserem früheren Ergebnis äquivalent ist.

A.4. Optimaler Sortieralgorithmus für $n = 5$

Es ist eine ganz unterhaltsame Tüftelei, den optimalen Sortieralgorithmus für $n = 5$ zu konstruieren. Die folgende Graphik illustriert die ersten fünf Vergleiche und die daraus schrittweise gewonnenen Informationen (in Form von Hasse–Diagrammen): Die zwei Elemente, die jeweils verglichen werden, sind als ausgefüllte Kreise[2] dargestellt.



Nach fünf Vergleichen bleiben (bis auf Isomorphie) zwei Hasse-Diagramme über; bei beiden kann man die richtige Position des mit einem dicken Kreis[3] markierten Elements durch Binary Search ermitteln: Dies bedeutet zwei weitere Vergleiche, sodaß die Ordnung der 5 Element immer mit 7 Vergleichen ermittelt werden kann. Das ist optimal, weil

$$\left\lceil \log_2 (5!) \right\rceil = \left\lceil \log_2 (120) \right\rceil = \log_2 (128) = 7.$$

[2] In der farbigen Version dieses Skriptums: als rote Kreise.

[3] In der farbigen Version dieses Skriptums: mit einem grünen Kreis.

Literaturverzeichnis

[1] M. Aigner. *Diskrete Mathematik*. Vieweg, 4. edition, 2001.
[2] G. Andrews. *The Theory of Partitions*. Cambridge University Press, 1984.
[3] N. Biggs. *Algebraic Graph Theory*. Cambridge University Press, 2nd edition, 1993.
[4] P.J. Cameron. *Combinatorics — Topics, Techniques, Algorithms*. Cambridge University Press, 1994.
[5] I. Lakatos. *Beweise und Widerlegungen*. Friedr. Vieweg & Sohn Verlagsges.m.b.H., 1979.
[6] S. Roman. *The Umbral Calculus*. Dover Publications Inc., 2005.

Index

Verzeichnis von Symbolen und Abkürzungen

$\dot{\bigcup}$: disjunkte Vereinigung. 7

$\mathbb{C}$: Körper der komplexen Zahlen. 1
$\lceil x \rceil$: Nächstgrößere ganze Zahl an x. 4
$[\![z^n]\!]\, f(z)$: Koeffizient von z^n in der Potenzreihe $f(z)$. 43

deg: Grad des Polynoms p. 13
$\dot{\cup}$: disjunkte Vereinigung. 7

$\mathrm{E}(X)$: Erwartungswert von X. 116

$\lfloor x \rfloor$: Nächstkleinere ganze Zahl an x. 4

$\mathbb{N}$: Menge der natürlichen Zahlen $\{1, 2, 3, \dots\}$. 1

$\mathbb{Q}$: Körper der rationalen Zahlen. 1

$\mathbb{R}$: Körper der reellen Zahlen. 1
$[n]$: Menge der ersten n natürlichen Zahlen: $\{1, 2, \dots, n\}$. 2

$\mathrm{var}(X)$: Varianz von X. 116

$\mathbb{Z}$: Ring der ganzen Zahlen $\{\dots, -2, -2, -1, 0, 1, 2, \dots\}$. 1