D-MATH ETH Zürich

Ruedi Suter

Diskrete Mathematik

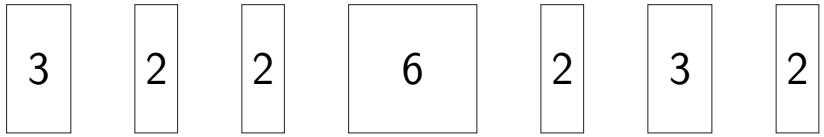
Wintersemester 2002/03

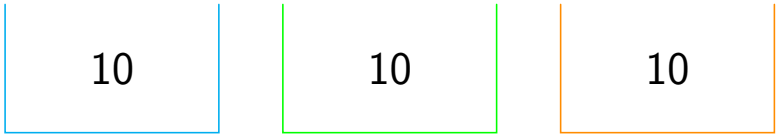
(3. Semester ITET)

Eine Zusammenstellung der Folien und Materialien, aber kein Skript.

Ein Verpackungsproblem

Stellen Sie sich vor, Sie haben eine Kollektion von Utensilien und Schachteln mit gegebenem Fassungsvermögen.
Welche passende/n Aufgabe/n können Sie dazu stellen? Welche Verfahren (Algorithmen) zum Verpacken der Utensilien in die Schachteln kommen Ihnen in den Sinn?





Diskutieren Sie zu zweit! Halten Sie sich nicht zu stark an das vorgegebene Beispiel, sondern formulieren Sie Ihren Algorithmus allgemein!

In ca. 8 Minuten werde ich Sie fragen, was Sie gefunden haben.

Gesucht ist eine optimale Verpackung.

Definition Optimale Verpackung = Verpackung, welche mit möglichst wenigen Schachteln auskommt.

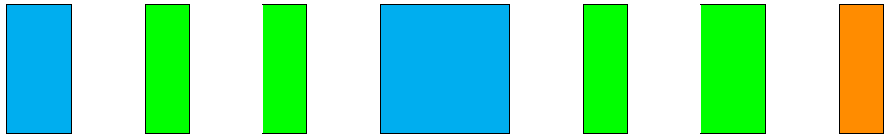
(Auch andere Szenarien sind vorstellbar.)

Unterschiedliche Ansätze:

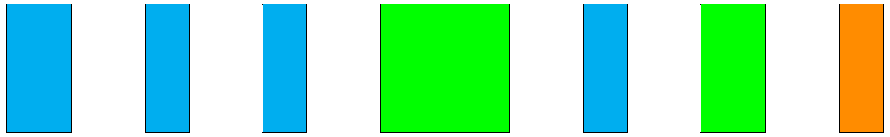
1. Packe die Schachteln der Reihe nach.
2. Packe die Utensilien der Reihe nach
   2.1 in der gegebenen Reihenfolge.
   2.2 und ordne sie zuerst nach absteigender Grösse.
3. „Mischung“.

Beispiele: (Packe gleich gefärbte Utensilien in die entsprechende Schachtel.)

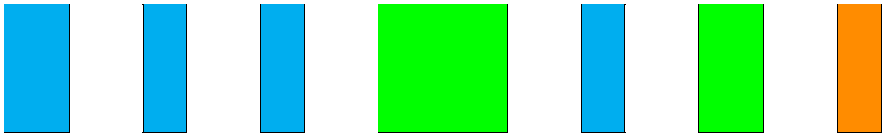
1.1 Nimm immer grösstes Utensil, das noch Platz hat.



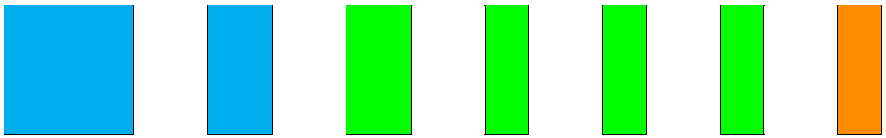
2.1.1 First Fit (nächstes Utensil in erste Schachtel, die passt)



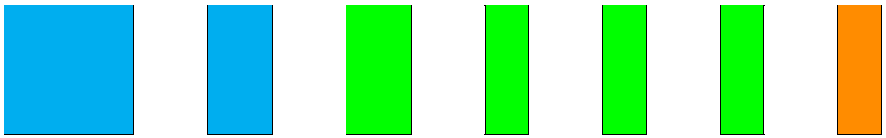
2.1.2 Best Fit (nächstes Utensil in diejenige Schachtel, die dadurch möglichst gut gefüllt wird)



2.2.1 First Fit (nächstes Utensil in erste Schachtel, die passt)

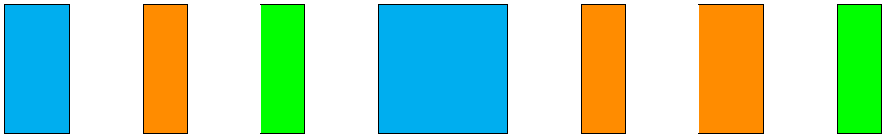


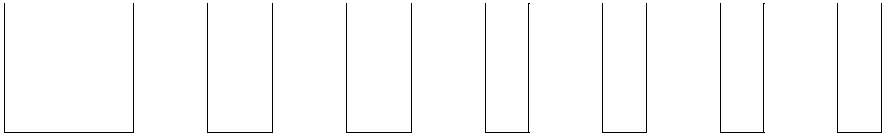
2.2.2 Best Fit (nächstes Utensil in diejenige Schachtel, die dadurch möglichst gut gefüllt wird)

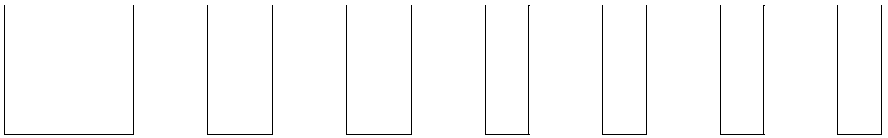


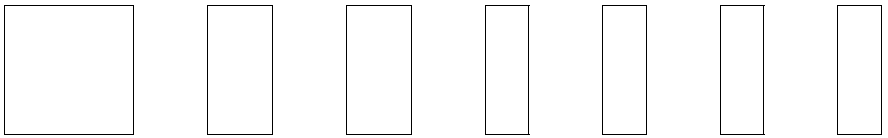
3.1 Bis jetzt waren immer alle drei Schachteln nötig. Die Verpackungen waren nicht optimal, denn es gibt eine Verpackung, die nur zwei Schachteln benötigt.

3.2 Zufällige Verpackung.









Fragen

1. Wieviele Schachteln werden schlimmstenfalls benötigt?
   [Beispiel: Wenn wie oben alle Utensilien nicht grösser als 10 sind und die Gesamtgrösse aller Utensilien 20 ist, reichen dann immer 3 Schachteln der Grösse 10?]
2. Wie findet man eine optimale Verpackung?
3. Gibt es einen Algorithmus, der eine optimale Verpackung in „kurzer Laufzeit“ findet?
4. Wie weit weichen die Verpackungen aus den Greedy-Algorithmen First Fit oder Best Fit von einer optimalen Verpackung schlimmstenfalls ab?
5. ...

Als Greedy-Algorithmen (greedy = gierig) werden Algorithmen bezeichnet, die nicht voraus schauend sind, sondern bloss lokal die beste Wahl treffen. In unserem Verpackungsproblem taugten die angegebenen Greedy-Algorithmen nicht zum Auffinden einer optimalen Verpackung. Wir werden später (Kapitel Graphentheorie) Greedy-Algorithmen kennen lernen, die (für andere Probleme) optimale Lösungen liefern.

Einige Antworten

1. Ja, 3 Schachteln reichen, und oft sind auch 3 Schachteln nötig, z. B. für vier Utensilien der Grössen 6, 6, 5, 3.
2. Wir nehmen an, es sind endlich viele Utensilien gegeben. Diese auf eine gegebene Anzahl Schachteln zu verteilen, ist nur auf endlich viele Arten möglich, die man im Prinzip alle aufzählen kann. Problematisch ist dabei aber, dass die Anzahl dieser Möglichkeiten schnell mit der Anzahl der Utensilien wächst.
3. Vielleicht erstaunt es Sie zu erfahren, dass das – wenn die Frage präzis gestellt wird – eine noch ungelöste Frage ist, für deren Lösung ein Preis von USD 1 000 000 in Aussicht gestellt ist.
   (`http://www.claymath.org/prizeproblems/pvsnp.htm`)
4. Das ist bekannt. Referenz: D. S. Johnson et al. *Worst-case performance bounds for simple one-dimensional packing algorithms.* SIAM J. Comput. **3** (1974), 299–325.
5. ...

Vgl. N. L. Seel: Psychologie des Lernens. München 2000
(korrigiert und an Schweizer Verhältnisse angepasst)

In einem nostalgischen Zug arbeiten ein Lokführer, ein Heizer und ein Kondukteur. Die drei heissen Keller, Müller und Schmid, aber nicht notwendigerweise in dieser Reihenfolge. Im Zug fahren drei Akademiker, ein Dr. Keller, ein Dr. Müller und ein Dr. Schmid.

1. Dr. Keller wohnt in Zürich.
2. Der Heizer wohnt in der Mitte zwischen Basel und Zürich.
3. Dr. Müller verdient genau CHF 8000 pro Monat.
4. Jener der drei Passagiere, der zufälligerweise Nachbar des Heizers ist, verdient genau dreimal soviel wie der Heizer.
5. Herr Schmid vom Fahrpersonal schlug kürzlich den Kondukteur im Schach.
6. Der Namensvetter des Heizers wohnt in Basel.

Wie heisst der Lokführer?

Klassische Aussagenlogik

(Die klassische Aussagenlogik wurde bereits in anderen Lehrveranstaltungen behandelt. Wir können uns deshalb kurz fassen.)

Alle zweistelligen Junktoren $\{1,0\}^2 \to \{1,0\}$

P	Q	äquivalent zu	Bezeichnung	Umgangssprache
1	1		Tautologie	wahr
0	0		Kontradiktion	falsch
P	P		Identität	P
Q	Q		Identität	Q
$\neg Q$	$\neg Q$		Negation	nicht Q
$\neg P$	$\neg P$		Negation	nicht P
$P \vee Q$	1 1 1 0		Disjunktion, Alternative, Adjunktion	P oder Q
$P \leftarrow Q$	1 1 0 1	$P \vee \neg Q$	Replikation, Subjunktion, Konditional	nur wenn P, dann Q
$P \to Q$	1 0 1 1	$\neg P \vee Q$	Implikation, Subjunktion, Konditional	wenn P, dann Q
$P \mid Q$	0 1 1 1	$\neg P \vee \neg Q$	Sheffer-Strich, Antikonjunktion	nicht beide P und Q
$P \leftrightarrow Q$	1 0 0 1	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$	Äquivalenz, Äquijunktion, Bijunktion	P genau dann, wenn Q
$P \oplus Q$	0 1 1 0	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$	Antivalenz, Disvalenz	entweder P oder Q
$P \wedge Q$	1 0 0 0		Konjunktion	P und Q
$\neg(P \to Q)$	0 1 0 0	$P \wedge \neg Q$	Inhibition	P und nicht Q
$\neg(P \leftarrow Q)$	0 0 1 0	$\neg P \wedge Q$	Inhibition	nicht P und Q
$P \downarrow Q$	0 0 0 1	$\neg P \wedge \neg Q$	Peirce-Pfeil, Antialternative, Nicodscher Junktor	weder P noch Q

Formeln (mit Junktoren $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$)

- Jede Aussagenvariable ist eine Formel.
- Sind F und G Formeln, so auch:

  $\neg F$
  $(F \wedge G)$
  $(F \vee G)$
  $(F \rightarrow G)$
  $(F \leftrightarrow G)$

Klammern gemäss üblichen Regeln weglassen,
Bindungsstärke der Junktoren:

$\neg$ bindet stärker als $\wedge$
$\wedge$ bindet stärker als $\vee$
$\vee$ bindet stärker als $\rightarrow$
$\rightarrow$ bindet stärker als $\leftrightarrow$

Beispiele

$F \wedge G \rightarrow H \vee I$ Abkürzung für $((F \wedge G) \rightarrow (H \vee I))$

$F \wedge G \vee H$ Abkürzung für $((F \wedge G) \vee H)$
[wird oft geschrieben als $(F \wedge G) \vee H$;
analog schreibt man meistens $F \leftrightarrow (G \rightarrow H)$
statt nur $F \leftrightarrow G \rightarrow H$]

Die Junktoren $\wedge$ und $\vee$ sind assoziativ, also schreibt man $F \wedge G \wedge H$ statt $(F \wedge G) \wedge H$ oder $F \wedge (G \wedge H)$;
analog für $\vee$ und für Verknüpfungen mit mehr als drei Aussagenvariablen.

Achtung: In $(F \rightarrow G) \rightarrow H$ und $F \rightarrow (G \rightarrow H)$ darf man die Klammern nicht weglassen.

Definition Eine Formel F heisst

eine Tautologie oder allgemeingültig oder auch wahr, wenn F für alle möglichen Belegungen der Aussagenvariablen wahr ist (Notation: $\models F$);

eine Kontradiktion oder unerfüllbar oder auch falsch, wenn $\neg F$ eine Tautologie ist;

erfüllbar, wenn F nicht unerfüllbar ist.

Mengenlehre

Notationen:

$\varnothing$ (auch $\{\,\}$)	leere Menge
$a \in A$	a ist Element von A
$B \subseteq A \;\; (a \in B \to a \in A)$	B ist Teilmenge von A
$A \cap B = \{x \,\vert\, x \in A \wedge x \in B\}$	Durchschnitt
$A \cup B = \{x \,\vert\, x \in A \vee x \in B\}$	Vereinigung
$A - B = \{a \,\vert\, a \in A \wedge a \notin B\}$	Differenz
$A \times B = \{(a,b) \,\vert\, a \in A \wedge b \in B\}$	Produkt
$A \triangle B = (A \cup B) - (A \cap B)$	symmetrische Differenz

Durchschnitt, Vereinigung, Produkt (Menge der n-Tupel) von n Mengen $A_1, \ldots, A_n$:

$$A_1 \cap \cdots \cap A_n \qquad A_1 \cup \cdots \cup A_n \qquad A_1 \times \cdots \times A_n$$

Durchschnitt, Vereinigung, Produkt von einer Familie $(A_i)_{i \in I}$ von Mengen:

$$\bigcap_{i \in I} A_i \qquad \bigcup_{i \in I} A_i \qquad \prod_{i \in I} A_i$$

Bsp. Jede Menge ist die Vereinigungsmenge ihrer Elemente:

$$A = \bigcup_{a \in A} \{a\}$$

Die Kardinalität einer Menge A, geschrieben $|A|$ oder $\#A$, ist die Anzahl ihrer Elemente. (Für endliche Mengen ist klar, wie das geht. Hier sind ein paar Beispiele von Kardinalitäten unendlicher Mengen: $|\mathbb{N}| = \aleph_0$, $|\mathbb{Q}| = \aleph_0$, $|\mathbb{R}| = 2^{\aleph_0}$.)

Prädikatenlogik (1. Stufe)

Erweiterung der Aussagenlogik: neu hinzu kommen Prädikatensymbole und Quantoren. (Zusätzlich kann man auch noch Funktionssymbole betrachten.)

$P(x)$	1-stelliges Prädikatensymbol
$Q(x_1, \ldots, x_n)$	n-stelliges Prädikatensymbol
R	0-stelliges Prädikatensymbol, Aussagenvariable
$\forall\, x$	Allquantor (für alle x)
$\exists\, x$	Existenzquantor (es existiert x)

$$\left(\begin{array}{ll} f(x) & \text{1-stelliges Funktionssymbol} \\ g(x_1, \ldots, x_n) & n\text{-stelliges Funktionssymbol} \\ c & \text{0-stelliges Funktionssymbol, Konstante} \end{array}\right)$$

Klammern: Bindungsstärke der Quantoren ist so stark wie diejenige des Negationsjunktors $\neg$.

Schreibweise: $\forall\, x \;\, P(x)$ oder $\forall\, x : P(x)$ oder $\forall\, x \,\big(P(x)\big)$.

Gebundene/freie Variable: Bsp. $\forall\, x \,\big(P(x,y) \to \exists\, z\, Q(y,z)\big)$ die Variablen x und z sind gebunden, y ist frei.

Bsp. $\forall\, x \,\big(P(x) \wedge Q(x)\big) \;\leftrightarrow\; \forall\, x\, P(x) \wedge \forall\, x\, Q(x)$ ist eine Tautologie.
Bsp. $\exists\, x \;\, P(x) \wedge \exists\, x \;\, Q(x) \to \exists\, x \,\big(P(x) \wedge Q(x)\big)$ ist keine Tautologie.

Korrektheitssatz/Vollständigkeitssatz wie in Aussagenlogik.
Aber: kein Entscheidungsverfahren.

Prädikate

Ein Prädikat kann man auffassen als Funktion auf einer Menge A mit Wertebereich $\{1, 0\} = \{\text{wahr}, \text{falsch}\}$, also

$$P : A \to \{1, 0\}.$$

Bsp. Auf $A = \mathbb{Z}_{>0}$ hat man das Prädikat

$$\mathrm{Prim}(x) :\Longleftrightarrow \text{„}x \text{ ist eine Primzahl“}.$$

Einsetzen von positiven ganzen Zahlen für die Variable x gibt dann Aussagen wie $\mathrm{Prim}(11)$ (wahr) oder $\mathrm{Prim}(18)$ (falsch).

Allgemeiner kann man n-stellige Prädikate anschauen,

$$P : A_1 \times \cdots \times A_n \to \{1, 0\}.$$

Bsp. $A_1 = \{\text{Geraden in der Ebene}\}$ und
$A_2 = A_3 = \{\text{Punkte in der Ebene}\}$

$$P(g, p, q) :\Longleftrightarrow \text{„}p \text{ und } q \text{ liegen auf } g\text{“}.$$

Bsp. $\forall\, y \big(y > 2 \wedge \mathrm{Prim}(y) \;\to\; \neg\, \mathrm{Prim}(y + 1)\big)$ ist eine (wahre) Aussage. Hingegen ist etwa in $z > 1 \to \neg\, \mathrm{Prim}(12)$ die Variable z frei und der obige Ausdruck keine Aussage.

Gebräuchliche Abkürzung: $\exists!\, x$ (es existiert genau ein x).

Sei $P(x)$ ein Prädikat auf einer Menge A und $B \subseteq A$ eine Teilmenge. Man schreibt dann oft etwa

$\forall\, x \in B :\; P(x)$ als Abkürzung für $\forall\, x \big(x \in B \to P(x)\big)$.

Ebenso ist

$\exists\, x \in B :\; P(x)$ Abkürzung für $\exists\, x \big(x \in B \wedge P(x)\big)$.

Negationen:

$$\begin{aligned} \neg \forall\, x :\; P(x) &\iff \exists\, x :\; \neg P(x) \\ \nexists\, x :\; P(x) &\iff \forall\, x :\; \neg P(x) \end{aligned}$$

Relationen

Eine n-stellige Relation in $A_1 \times \cdots \times A_n$ ist eine Teilmenge von $A_1 \times \cdots \times A_n$.

Ist bloss andere Bezeichnung für n-stelliges Prädikat:

$$\begin{gathered} P : A_1 \times \cdots \times A_n \to \{1, 0\} \\ \downarrow \\ \big\{(a_1, \ldots, a_n) \;\big|\; P(a_1, \ldots, a_n)\big\} \subseteq A_1 \times \cdots \times A_n \end{gathered}$$

Und in die andere Richtung:

$$\begin{gathered} R \subseteq A_1 \times \cdots \times A_n \\ \downarrow \\ P(a_1, \ldots, a_n) = \begin{cases} 1 & \text{falls } (a_1, \ldots, a_n) \in R, \\ 0 & \text{falls } (a_1, \ldots, a_n) \notin R. \end{cases} \end{gathered}$$

Funktionen „sind“ Spezialfälle von Relationen. Ist eine Funktion $f : A \to B$ gegeben, so hat man ihren Graphen $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$, also eine Relation in $A \times B$. Eine Relation $R \subseteq A \times B$ ist genau dann Graph einer Funktion $f : A \to B$, wenn $\forall\, a \in A\, \exists!\, b \in B : (a, b) \in R$.

Besonders wichtig sind 2-stellige Relationen in $A_1 \times A_2$ mit $A = A_1 = A_2$. Man spricht dann von einer 2-stelligen (oder binären) Relation auf A.

Statt $(a, b) \in R$ schreibt man auch $a\, R\, b$.

Bsp. einer 2-stelligen Relation auf $\mathbb{R}$

$$R = \{(x, y) \in \mathbb{R}^2 \mid x \leqslant y\}$$

Wie üblich schreibt man dann für $x\, R\, y$ einfach $x \leqslant y$.

Eine binäre Relation R auf A heisst

reflexiv	$:\Longleftrightarrow \forall\, a\ (a\, R\, a)$
symmetrisch	$:\Longleftrightarrow \forall\, a\, \forall\, b\ (a\, R\, b \to b\, R\, a)$
antisymmetrisch	$:\Longleftrightarrow \forall\, a\, \forall\, b\ (a\, R\, b \wedge b\, R\, a \to a = b)$
transitiv	$:\Longleftrightarrow \forall\, a\, \forall\, b\, \forall\, c\ (a\, R\, b \wedge b\, R\, c \to a\, R\, c)$

Zwei wichtige Klassen von binären Relationen:

Äquivalenzrelationen (oft bezeichnet mit $\sim, \approx, \simeq, \cong, \equiv, \backsim$ usw.) sind reflexive, symmetrische und transitive Relationen.

Ordnungsrelationen (oft bezeichnet mit $\leq, \leqslant, \preceq$ usw.) sind reflexive, antisymmetrische und transitive Relationen.

Sei $(L, \leqslant)$ eine Menge mit einer Ordnungsrelation, also eine partiell geordnete Menge.
Seien $a, b \in L$. Ein Element $c \in L$ heisst kleinste obere Schranke von a und b oder Supremum von a und b, falls $a \leqslant c$ und $b \leqslant c$ und für alle $d \in L$ mit $a \leqslant d$ und $b \leqslant d$ gilt $c \leqslant d$. Falls so ein c existiert, so ist es eindeutig bestimmt (warum?), und man bezeichnet es mit $a \vee b$.
Seien $a, b \in L$. Ein Element $c \in L$ heisst grösste untere Schranke von a und b oder Infimum von a und b, falls $c \leqslant a$ und $c \leqslant b$ und für alle $d \in L$ mit $d \leqslant a$ und $d \leqslant b$ gilt $d \leqslant c$. Falls so ein c existiert, so ist es eindeutig bestimmt, und man bezeichnet es mit $a \wedge b$.

Ein Verband ist eine partiell geordnete Menge, in der jedes Paar von Elementen sowohl ein Supremum als auch ein Infimum besitzt.

In einem Verband gelten die folgenden Beziehungen zwischen der Ordnungsrelation und den Operationen $\wedge$ und $\vee$: $\forall\, a \forall\, b : a \leqslant b \leftrightarrow a \wedge b = a \leftrightarrow a \vee b = b$.

Ein distributiver Verband L ist ein Verband, in dem die Distributivitätsaxiome gelten:
$\forall a \forall b \forall c : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ und
$\forall a \forall b \forall c : a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.
(Bem. Es genügt, ein Distributivgesetz zu fordern, das andere lässt sich daraus herleiten.)

Eine Boolesche Algebra B ist ein distributiver Verband, in dem zusätzlich noch zwei Elemente $0, 1 \in B$ ausgezeichnet sind sowie eine Operation $\overline{\ } : B \to B$, so dass folgende Axiome gelten: $\forall a : a \wedge \overline{a} = 0$ und $\forall a : a \vee \overline{a} = 1$.

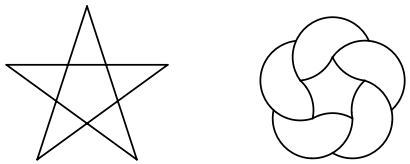
In jeder Booleschen Algebra gelten die Gesetze von De Morgan[1] : $\forall a \forall b : \overline{a \wedge b} = \overline{a} \vee \overline{b}$ und $\forall a \forall b : \overline{a \vee b} = \overline{a} \wedge \overline{b}$.

[1] De Morgan, Augustus (1806 - 1871): I was x years old in the year x^2.

ALGEBRA

Gruppen

$\mathrm{Aut}(X) = \{S : X \to X \mid S$ Symmetrie (genau: Isometrie)$\}$ von $X =$ Pentagramm bzw. $X =$ Kranz:



Aut(Kranz) $= \{$Drehungen um ganzzahlige Vielfache von $72°$ um dem Mittelpunkt$\}$. $|\mathrm{Aut}(\text{Kranz})| = 5$.

Aut(Pentagramm) $= \{$Drehungen um ganzzahlige Vielfache von $72°$ um dem Mittelpunkt, Spiegelungen an den Symmetrieachsen$\}$. $|\mathrm{Aut}(\text{Pentagramm})| = 10$.

Beobachtungen:

0) Die Zusammensetzung zweier Symmetrien ist wieder eine Symmetrie, d. h. man hat
$$\circ : \mathrm{Aut}(X) \times \mathrm{Aut}(X) \to \mathrm{Aut}(X).$$

1) Für $S, T, U \in \mathrm{Aut}(X)$ gilt $(S \circ T) \circ U = S \circ (T \circ U)$.

2) Die Identität $X \to X$ ist eine Symmetrie.

3) Zu jeder Symmetrie gibt es eine inverse Symmetrie.

Abstraktion dieser Beobachtungen $\rightsquigarrow$ Gruppe (was vorher $\mathrm{Aut}(X)$ war, wird nun G, und statt $\circ$ schreiben wir $*$).

Def. Eine Gruppe ist eine Menge G zusammen mit einer binären Operation (Verknüpfungsvorschrift)

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\longmapsto g * h \end{aligned}$$

welche den Axiomen der Assoziativität, der Existenz eines Neutralelementes und der Existenz der Inversen genügt.

1) Assoziativität
$\forall\, g,h,k \in G : (g*h)*k = g*(h*k)$

2) Neutralelement
$\exists\, e \in G\ \forall\, g \in G : e*g = g = g*e$

3) Inverse
$\forall\, g \in G\ \exists\, h \in G : g*h = e = h*g$

Bemerkungen:

- Das Neutralelement ist eindeutig bestimmt. Oft schreibt man dafür auch 1 statt e.
- Jedes Gruppenelement $g \in G$ hat ein eindeutig bestimmtes Inverses, das man als g^{-1} schreibt.
- Das Verknüpfungsgesetz schreibt man oft als $\cdot$, und meistens lässt man dann sogar den Punkt weg und schreibt gh. Weil das Assoziativgesetz gilt, schreibt man dann ghk für $(gh)k = g(hk)$.

Def. Eine abelsche Gruppe ist eine Gruppe G, welche noch das Axiom der Kommutativität erfüllt.

4) Kommutativität
$\forall\, g,h \in G : g*h = h*g$

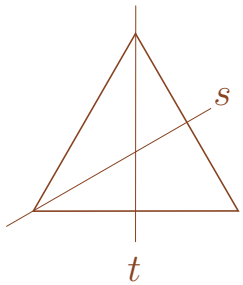
Bis jetzt haben wir Gruppen multiplikativ geschrieben, also Notationen wie gh, g^{-1}, $e = 1$ verwendet.
Abelsche Gruppen schreibt man oft additiv, also mit Notationen wie $u+v$, $-u$, $e = 0$.

Def. Man nennt die Kardinalität $|G|$ einer Gruppe G ihre Ordnung. Die Ordnung eines Elementes $g \in G$ ist definiert als die kleinste positive ganze Zahl n so, dass $g^n = e$, falls es so ein n gibt, und als ∞, falls $g^n \neq e$ für alle $n \in \mathbb{Z}_{>0}$. Notation: $|g|$.

Gruppentafel

	$\dots$	h	$\dots$
$\vdots$			
g		gh	
$\vdots$			

Bsp. Symmetriegruppe des gleichseitigen Dreiecks: s und t bezeichnen Achsenspiegelungen



	1	s	t	ts	st	sts
1	1	s	t	ts	st	sts
s	s	1	st	sts	t	ts
t	t	ts	1	s	sts	st
ts	ts	t	sts	st	1	s
st	st	sts	s	1	ts	t
sts	sts	st	ts	t	s	1

Def. Seien G und H Gruppen. Eine Abbildung $\varphi : G \to H$ heisst Homomorphismus, falls gilt

$$\forall g_1, g_2 \in G : \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2).$$

Ein Isomorphismus ist ein bijektiver Homomorphismus.

[„Besser“: Ein Homomorphismus $\varphi : G \to H$ heisst Isomorphismus, falls ein Homomorphismus $\psi : H \to G$ existiert, so dass $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_H$.]

Ein Automorphismus ist ein Isomorphismus einer Gruppe auf sich (also oben mit $G = H$).

Def. Eine Untergruppe einer Gruppe G ist eine Teilmenge $U \subseteq G$ so, dass folgende beiden Eigenschaften gelten:

- $U \neq \varnothing$,
- $\forall\, g, h \in U : g^{-1}h \in U$.

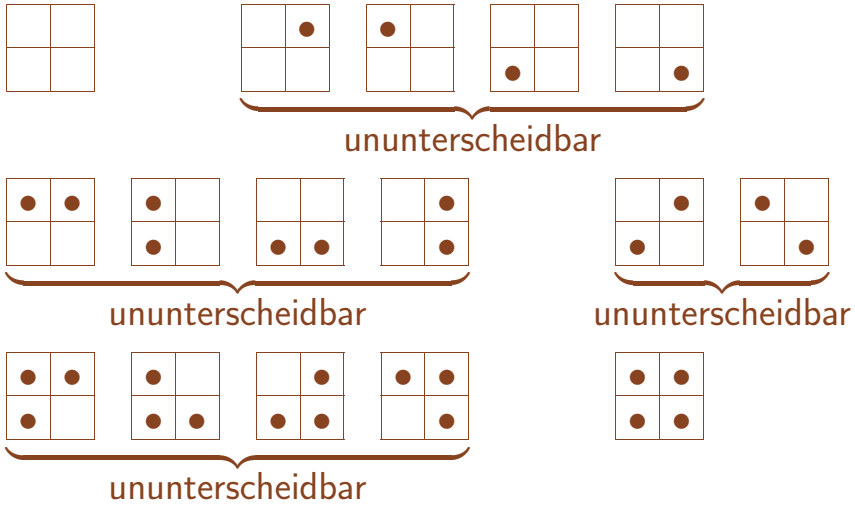
Bsp. Für $g \in G$ ist $\langle g \rangle := \left\{ g^n \;\middle|\; n \in \mathbb{Z} \right\}$ eine abelsche Untergruppe von G, und es gilt $|\langle g \rangle| = |g|$.

Gruppenwirkungen

Ziel: Ein allgemeines Verfahren verstehen und anwenden können, um gewisse Abzählprobleme zu lösen.

Dazu müssen noch einige Begriffe eingeführt werden: Gruppenwirkungen, Orbits, Stabilisatoren, Fixpunktmengen.

Bsp. Ein 2×2-Quadrat kann durch Ausstanzen von Löchern je in der Mitte der vier 1×1-Teilquadrate mit 0 bis 4 Löchern versehen werden. Wieviele unterscheidbare solche 2×2-Quadrate gibt es?

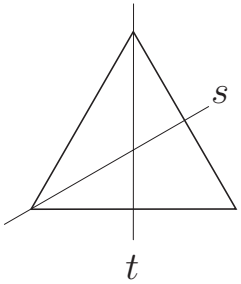


Es gibt nur 6 Arten von unterscheidbaren 2×2-Quadraten.

Stellen Sie sich vor, Sie wollen die Anzahl der zweimal gelochten 5×5-Quadrate bestimmen. Würden Sie das analog wie oben machen wollen, alle $\binom{25}{2} = 300$ Positionen aufzeichnen und dann in Haufen ununterscheidbarer Quadrate aufteilen?

Repetition

Symmetriegruppe $G = \mathrm{Dih}_3$ des gleichseitigen Dreiecks



	1	s	t	ts	st	sts
1	1	s	t	ts	st	sts
s	s	1	st	sts	t	ts
t	t	ts	1	s	sts	st
ts	ts	t	sts	st	1	s
st	st	sts	s	1	ts	t
sts	sts	st	ts	t	s	1

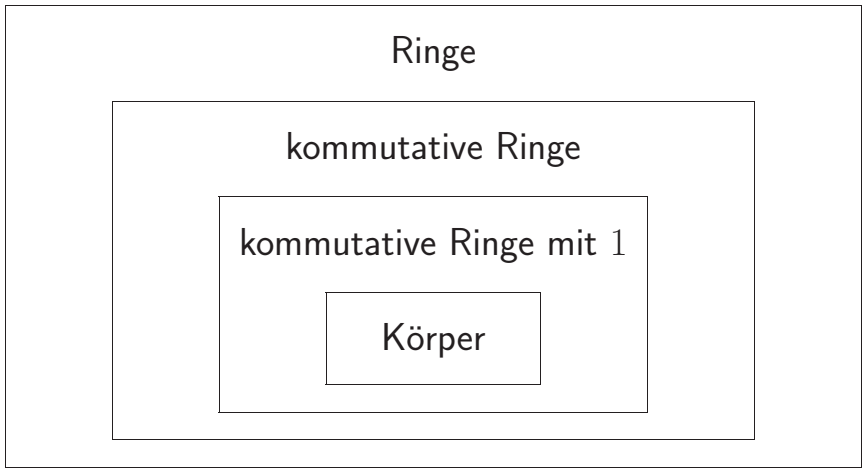
1	Identität
s	Geradenspiegelung
t	Geradenspiegelung
ts	Drehung um $120°$
st	Drehung um $240°$
sts	Geradenspiegelung

Es gelten die folgenden Relationen:

$$s^2 = 1$$
$$t^2 = 1$$
$$sts = tst$$

Ringe und Körper

1. Definitionen und Beispiele
2. Endliche Körper
   2.1 Primkörper $\mathbb{F}_p$, kleiner Satz von Fermat
   2.2 Endliche Körper $\mathbb{F}_{p^n}$



Def. Ein Ring ist eine Menge R zusammen mit zwei binären Operationen, einer Addition

$$\begin{aligned} R \times R &\longrightarrow R \\ (r, s) &\longmapsto r + s \end{aligned}$$

und einer Multiplikation

$$\begin{aligned} R \times R &\longrightarrow R \\ (r, s) &\longmapsto r \cdot s \end{aligned}$$ (oft als rs geschrieben),

so dass folgende Axiome erfüllt sind:

1) Additive abelsche Gruppe
$(R, +)$ ist eine abelsche Gruppe.

2) Assoziativität der Multiplikation
$\forall\, r, s, t \in R : (rs)t = r(st)$ (schreibe also rst).

3) Distributivität
$\forall\, r, s, t \in R : r\big(s + t\big) = rs + rt,$
$\forall\, r, s, t \in R : \big(r + s\big)t = rt + st.$

Ein kommutativer Ring ist ein Ring, in welchem die Multiplikation kommutativ ist, also

4) Kommutativität der Multiplikation
$\forall\, r, s \in R : rs = sr.$

Ein kommutativer Ring mit 1 ist ein kommutativer Ring, in dem ein Neutralelement für die Multiplikation existiert, also

5) Neutralelement 1 für die Multiplikation
$\exists\, 1 \in R \forall\, r \in R : 1r = r.$

Ein Körper ist ein kommutativer Ring mit 1, so dass $1 \neq 0$ (0 ist das Neutralelement für die Addition) und so dass jedes von 0 verschiedene Element ein multiplikatives Inverses hat, also

6) Multiplikative Inverse
$\forall\, r \in R - \{0\}\, \exists\, s \in R : rs = 1 \neq 0.$

Mit anderen Worten: Ein Körper ist eine Menge R zusammen mit zwei binären Operationen, einer Addition $+$ und einer Multiplikation $\cdot$, so dass folgende Axiome erfüllt sind:

1) Additive abelsche Gruppe
$(R, +)$ ist eine abelsche Gruppe.

2) Multiplikative abelsche Gruppe
$(R - \{0\}, \cdot\,)$ ist eine abelsche Gruppe (dabei ist 0 das Neutralelement für die Addition).

3) Distributivität
$\forall\, r, s, t \in R : r\big(s + t\big) = rs + rt.$

Endliche Körper

Satz $\mathbb{Z}_n$ (Ring der Restklassen modulo n) ist genau dann ein Körper, wenn $n = p$ eine Primzahl ist. Notation: $\mathbb{F}_p = \mathbb{Z}_p$.

Satz (Kleiner Satz von Fermat) Ist p eine Primzahl und $a \in \mathbb{Z}$ nicht durch p teilbar, so gilt $a^{p-1} \equiv 1 \pmod{p}$.

Satz Ist $\mathbb{F}$ ein endlicher Körper, so gilt $|\mathbb{F}| = p^n$ für eine Primzahl p und eine positive ganze Zahl n.

Satz Ist $q = p^n > 1$ eine Primzahlpotenz, so gibt es bis auf Isomorphie genau einen Körper mit q Elementen. Bezeichnung: $\mathbb{F}_q$.

Satz Die multiplikative Gruppe $\mathbb{F}_q^\times$ ist eine zyklische Gruppe der Ordnung $q - 1$.

Erzeugende Funktionen II

0. Wann existiert $\frac{1}{a(x)}$?

Sei R ein kommutativer Ring mit 1. Mit $R^\times$ wird die multiplikative Gruppe der in R invertierbaren Elemente bezeichnet.

Bsp. Falls K ein Körper ist, so ist $K^\times = K - \{0\}$.
Bsp. $\mathbb{Z}^\times = \{\pm 1\}$.

Satz $\big(R[\![x]\!]\big)^\times = \left\{ \sum_{n=0}^{\infty} a_n x^n \in R[\![x]\!] \,\middle|\, a_0 \in R^\times \right\}$.

Beweis. Sei $b(x) = \sum_{n=0}^{\infty} b_n x^n \in R[\![x]\!]$. Die Frage ist, wann sich die Koeffizienten $b_0, b_1, \ldots$ so bestimmen lassen, dass $a(x)b(x) = 1 = 1 \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + \cdots$ gilt. Wir erinnern zuerst an die Potenzreihenentwicklung des Produktes.

$$a(x)b(x) = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) x^n.$$

„$\Longrightarrow$“ Sei $a(x)b(x) = 1$. Dann ist insbesondere der Koeffizient von x^0 gleich 1, also $a_0 b_0 = 1$. D. h. $a_0 \in R^\times$.

„$\Longleftarrow$“ Sei $a_0 \in R^\times$. Dann können wir die Folge $b_0, b_1, \ldots$ rekursiv bestimmen: Zuerst ist $b_0 = \frac{1}{a_0}$. Für $n > 0$ soll $[x^n]a(x)b(x) = 0$ gelten, also

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

■

1. Mengenpartitionen

Repetition: Eine Partition $\mathcal{P}$ einer Menge M besteht aus einer Menge von Teilmengen von M mit

- $\varnothing \notin \mathcal{P}$,
- $B_1, B_2 \in \mathcal{P} \implies B_1 = B_2$ oder $B_1 \cap B_2 = \varnothing$,
- $\bigcup_{B \in \mathcal{P}} B = M$.

(Partition von M $\leftrightsquigarrow$ Äquivalenzrelation auf M. Die Blöcke $B \in \mathcal{P}$ sind genau die Äquivalenzklassen.)

Problem Wieviele Partitionen von $\{1, \ldots, n\}$ in k Blöcke gibt es? Bezeichung für diese Anzahl: $\left\{ {n \atop k} \right\}$ oder $S_{n,k}$ heisst Stirlingzahl zweiter Art (nach James Stirling (1692–1770)).

Bsp. Aus

$\left\{ {3 \atop 1} \right\} = 1$	$\mathcal{P} = \{\{1,2,3\}\}$
$\left\{ {3 \atop 2} \right\} = 3$	$\mathcal{P}_1 = \{\{1,2\},\{3\}\}$
	$\mathcal{P}_2 = \{\{1,3\},\{2\}\}$
	$\mathcal{P}_3 = \{\{2,3\},\{1\}\}$

erhält man alle Partitionen von $\{1,2,3,4\}$ in 2 Blöcke: Die neu hinzu gekommene Zahl 4 bildet einen eigenen Block:

$$\mathcal{P} \rightsquigarrow \{\{1,2,3\},\{4\}\},$$

oder 4 kommt zu einem schon vorhandenen Block hinzu:

$$\begin{aligned}
\mathcal{P}_1 &\rightsquigarrow \{\{1,2,4\},\{3\}\},\ \{\{1,2\},\{3,4\}\},\\
\mathcal{P}_2 &\rightsquigarrow \{\{1,3,4\},\{2\}\},\ \{\{1,3\},\{2,4\}\},\\
\mathcal{P}_3 &\rightsquigarrow \{\{2,3,4\},\{1\}\},\ \{\{2,3\},\{1,4\}\}.
\end{aligned}$$

Dieselbe Idee liefert allgemein die folgende Rekursion.

$$\left\{ n \atop k \right\} = \left\{ n-1 \atop k-1 \right\} + k \left\{ n-1 \atop k \right\} \qquad (n \geqslant 1)$$

$$\left\{ 0 \atop 0 \right\} = 1, \quad \left\{ n \atop 0 \right\} = 0 \text{ für } k \neq 0.$$

Wir betrachten die erzeugende Funktion

$$S_k(x) := \sum_{n=0}^{\infty} \left\{ n \atop k \right\} x^n.$$

Es ist also $S_0(x) = 1$ und für $k \geqslant 1$ haben wir

$$\begin{aligned} S_k(x) &= 0 + \sum_{n=1}^{\infty} \left(\left\{ n-1 \atop k-1 \right\} + k \left\{ n-1 \atop k \right\} \right) x^n \\ &= x \sum_{n=1}^{\infty} \left\{ n-1 \atop k-1 \right\} x^{n-1} + kx \sum_{n=1}^{\infty} \left\{ n-1 \atop k \right\} x^{n-1} \\ &= x S_{k-1}(x) + kx S_k(x), \end{aligned}$$

also

$$S_k(x) = \frac{x}{1-kx} S_{k-1}(x) \quad (k \geqslant 1).$$

Mit $S_0(x) = 1$ erhalten wir also

$$S_k(x) = \frac{x^k}{(1-x)(1-2x)\cdots(1-kx)}.$$

Die Partialbruchzerlegung ist von der Form

$$\frac{1}{(1-x)(1-2x)\cdots(1-kx)} = \sum_{j=1}^{k} \frac{u_j}{1-jx}. \qquad (*)$$

Die Konstanten $u_1, \ldots, u_k$ lassen sich so ausrechnen: wir fixieren h $(1 \leqslant h \leqslant k)$, multiplizieren den Ansatz $(*)$ mit $1-hx$ und setzen $x = 1/h$ ein:

$$\begin{aligned} u_h &= \frac{1}{(1-1/h)(1-2/h)\cdots(1-(h-1)/h)(1-(h+1)/h)\cdots(1-k/h)} \\ &= (-1)^{k-h} \frac{h^{k-1}}{(h-1)!\,(k-h)!} \end{aligned}$$

Für $k \geqslant 1$ haben wir also

$$S_k(x) = \sum_{h=1}^{k} (-1)^{k-h} \frac{h^{k-1}}{(h-1)!\,(k-h)!} \cdot \frac{x^k}{(1-hx)}$$

und somit

$$\begin{aligned} \left\{ n \atop k \right\} &= [x^n] S_k(x) \\ &= \sum_{h=1}^{k} (-1)^{k-h} \frac{h^{k-1}}{(h-1)!\,(k-h)!} \cdot h^{n-k} \\ &= \sum_{h=1}^{k} (-1)^{k-h} \frac{h^n}{h!\,(k-h)!}. \end{aligned}$$

Damit ist das Problem gelöst.

$$\left\{ n \atop k \right\} = S_{n,k} = \begin{cases} \displaystyle\sum_{h=1}^{k} \frac{(-1)^{k-h} h^n}{h!\,(k-h)!} & (k \geqslant 1), \\ 1 & (n = k = 0), \\ 0 & (n \neq 0,\ k = 0). \end{cases}$$

Bsp. $\left\{ 4 \atop 2 \right\} = -\frac{1}{1} + \frac{16}{2} = 7.$

Problem Wieviele Partitionen von $\{1, \ldots, n\}$ gibt es? Mit anderen Worten: Wieviele Äquivalenzrelationen gibt es auf einer n-elementigen Menge? Bezeichung für diese Anzahl: Bell_n heisst Bellzahl.

Einige Zitate von Eric Temple Bell (1883–1960):

- Euclid taught me that without assumptions there is no proof. Therefore, in any argument, examine the assumptions.
- It is the perennial youthfulness of mathematics itself which marks it off with a disconcerting immortality from the other sciences.
- Abstractness, sometimes hurled as a reproach at mathematics, is its chief glory and its surest title to practical usefulness. It is also the source of such beauty as may spring from mathematics.
- The longer mathematics lives the more abstract—and therefore, possibly also the more practical—it becomes.
- "Obvious" is the most dangerous word in mathematics.

$\mathrm{Bell}_0 = 1$ und für $n \geqslant 1$ müssen wir einfach die Stirlingzahlen aufsummieren. Wegen $\left\{ {n \atop k} \right\} = 0$ für $k > n$ haben wir also

$$\begin{aligned}
\mathrm{Bell}_n &= \sum_{k=1}^{n} \left\{ {n \atop k} \right\} = \sum_{k=1}^{N} \left\{ {n \atop k} \right\} \quad (\text{für } N \geqslant n) \\
&= \sum_{k=1}^{N} \sum_{h=1}^{k} (-1)^{k-h} \frac{h^n}{h!\,(k-h)!} \\
&= \sum_{h=1}^{N} \frac{h^n}{h!} \sum_{k=h}^{N} \frac{(-1)^{k-h}}{(k-h)!} \\
&= \sum_{h=1}^{N} \frac{h^{n-1}}{(h-1)!} \sum_{l=0}^{N-h} \frac{(-1)^l}{l!} = \frac{1}{e} \sum_{h=0}^{\infty} \frac{h^n}{h!}\,.
\end{aligned}$$

Aus der Formel

$$\mathrm{Bell}_n = \frac{1}{e} \sum_{h=0}^{\infty} \frac{h^n}{h!}$$

(Dobiński (1877)), die auch für $n = 0$ richtig ist, wenn wir $0^0 := 1$ setzen, können wir nun die exponentielle erzeugende Funktion der Bellzahlen bestimmen.

$$\begin{aligned}
\mathrm{Bell}(x) &= \sum_{n=0}^{\infty} \mathrm{Bell}_n \frac{x^n}{n!} = \frac{1}{e} \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{h=0}^{\infty} \frac{h^n}{h!} \\
&= \frac{1}{e} \sum_{h=0}^{\infty} \frac{1}{h!} \sum_{n=0}^{\infty} \frac{(hx)^n}{n!} = \frac{1}{e} \sum_{h=0}^{\infty} \frac{1}{h!}\, e^{hx} \\
&= \frac{1}{e}\, e^{e^x} = e^{e^x - 1}
\end{aligned}$$

Hier haben wir ein Beispiel, wo eine Potenzreihe ohne konstanten Term (nämlich die Potenzreihe für $e^x - 1$) in eine Potenzreihe (nämlich die Potenzreihe für e^x) eingesetzt wird.

Aus der Reihenentwicklung $e^{e^x - 1} = 1 + x + x^2 + \frac{5}{6}\,x^3 + \frac{5}{8}\,x^4 + \frac{13}{30}\,x^5 + \frac{203}{720} + \cdots$ lesen wir ab: $\mathrm{Bell}_0 = \mathrm{Bell}_1 = 1$, $\mathrm{Bell}_2 = 2$, $\mathrm{Bell}_3 = 5$, $\mathrm{Bell}_4 = 15$, $\mathrm{Bell}_5 = 52$, $\mathrm{Bell}_6 = 203$. (Zur Erinnerung: Bell_2, Bell_3 und Bell_4 waren in der Serie 2 Aufgabe 5 zu bestimmen.)

Vorher hatten wir aus einer Rekursionsformel eine erzeugende Funktion berechnet. Nun wollen wir sehen, wie wir aus der (exponentiellen) erzeugenden Funktion $\mathrm{Bell}(x)$ eine Rekursionsformel für die Bellzahlen erhalten. Dazu leiten wir die Formel $\mathrm{Bell}(x) = e^{e^x - 1}$ ab:

$$\mathrm{Bell}'(x) = \mathrm{Bell}(x)\, e^x.$$

Der Koeffizient von x^n ist

$$\frac{n+1}{(n+1)!}\,\mathrm{Bell}_{n+1} = \sum_{k=0}^{n} \frac{1}{k!}\,\mathrm{Bell}_k \cdot \frac{1}{(n-k)!}$$

d. h. es gilt die Rekursionsformel

$$\mathrm{Bell}_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \mathrm{Bell}_k \quad (n \geqslant 0)$$

mit dem Anfangswert $\mathrm{Bell}_0 = 1$.

2. Nochmals Fibonaccizahlen

(nach Leonardo Pisano Fibonacci (ca. 1170–1250))

Letztes Mal hatten wir die erzeugende Funktion der Fibonaccizahlen bestimmt, nämlich $\frac{x}{1-x-x^2}$, und dann mithilfe der Partialbruchzerlegung eine Formel für die Fibonaccizahlen erhalten.

Repetition: Die Fibonaccizahlen $F_0, F_1, F_2, \ldots$ sind definiert durch

$$\boxed{\begin{aligned} F_{n+2} &= F_{n+1} + F_n \quad (n \geqslant 0) \\ F_0 &= 0,\ F_1 = 1. \end{aligned}}$$

Wir betrachten nun die exponentielle erzeugende Funktion der Fibonaccizahlen, also

$$f(x) := \sum_{n=0}^{\infty} F_n \frac{x^n}{n!}.$$

Es ist nahe liegend, die ersten beiden Ableitungen von $f(x)$ zu betrachten.

$$f'(x) = \sum_{n=1}^{\infty} F_n \frac{x^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} F_{n+1} \frac{x^n}{n!}$$
$$f''(x) = \sum_{n=2}^{\infty} F_n \frac{x^{n-2}}{(n-2)!} = \sum_{n=0}^{\infty} F_{n+2} \frac{x^n}{n!}$$

Mit der Rekursionsformel folgt sofort

$$f''(x) = f'(x) + f(x).$$

Die allgemeine Lösung dieser homogenen linearen Differentialgleichung mit konstanten Koeffizienten lautet

$$f(x) = ce^{\tau x} + \tilde{c}e^{\tilde{\tau} x},$$

wobei $\tau = \frac{1+\sqrt{5}}{2}$ und $\tilde{\tau} = \frac{1-\sqrt{5}}{2}$. Aus den Anfangswerten $F_0 = 0$, $F_1 = 1$ oder $f(0) = 0$, $f'(0) = 1$ berechnen wir $c = \frac{1}{\sqrt{5}} = -\tilde{c}$. Damit haben wir die bekannte Formel

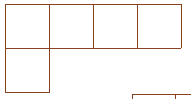
$$F_n = n! \cdot [x^n] \frac{1}{\sqrt{5}} \left(e^{\tau x} - e^{\tilde{\tau} x}\right) = \frac{1}{\sqrt{5}} \left(\tau^n - \tilde{\tau}^n\right)$$

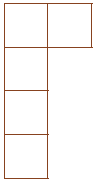
erneut hergeleitet.

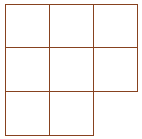
3. Zahlpartitionen I

Problem Auf wieviele Arten lässt sich die natürliche Zahl n als Summe von k positiven ganzen Zahlen schreiben, wenn die Reihenfolge der Summanden irrelevant ist? Bezeichung für diese Anzahl: $P_{n,k}$.

Zahlpartitionen lassen sich anhand von Youngdiagrammen veranschaulichen.

Bsp. $4+1$  $(4,1) \vdash 5$

Bsp. $2+1+1+1$  $(2,1,1,1) \vdash 5$

Bsp. $3+3+2$  $(3,3,2) \vdash 8$

Eine Partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ ist gegeben durch positive ganze Zahlen $\lambda_1 \geqslant \cdots \geqslant \lambda_k > 0$, die Längen der Zeilen im Youngdiagramm für λ. Die Anzahl der Zeilen, also die Länge der ersten Spalte, ist die Länge der Partition. Die Anzahl der Zellen im Youngdiagramm ist $n = \sum_{h=1}^{k} \lambda_h$. Wir schreiben auch $\lambda \vdash n$ und sagen λ ist eine Partition von n. Für $\lambda \vdash n$ bezeichnet λ' die konjugierte Partition von n. Das Youngdiagramm von λ' erhält man aus demjenigen von λ durch Spiegeln an der Diagonalen. Z. B. $(4,1)' = (2,1,1,1)$ und $(3,3,2)' = (3,3,2)$. Es ist nun auch klar, dass $P_{n,k}$ auch die Anzahl der Partitionen von n mit grösstem Teil k ist.

Rekursion für $P_{n,k}$:

$$\boxed{\begin{array}{l} P_{n,k} = P_{n-1,k-1} + P_{n-k,k} \quad (n \geqslant k > 0) \\ P_{n,0} = \delta_{n,0}, P_{0,k} = \delta_{k,0} \\ P_{n,k} = 0 \ (n < k) \end{array}}$$

Das folgt aus der Summenregel: für $\lambda = (\lambda_1, \ldots, \lambda_k)$ zählt $P_{n-1,k-1}$ die Partitionen $\lambda \vdash n$ mit $\lambda_k = 1$ und $P_{n-k,k}$ jene mit $\lambda_k > 1$.

Hier ist eine Notation für Partitionen, die oft nützlich ist: $[1^{m_1}\, 2^{m_2}\, 3^{m_3}\, \cdots]$, wobei dann noch die evidenten Abkürzungen vorgenommen werden. Hier gibt m_i an, wie oft die Zahl i in der gegebenen Partition vorkommt.

Bsp. $(7,7,5,4,3,1,1) = [1^2\, 2^0\, 3^1\, 4^1\, 5^1\, 6^0\, 7^2] = [1^2\, 3\, 4\, 5\, 7^2]$.

Bsp. Alle Partitionen $\lambda \vdash 6$: $[6]$, $[1\,5]$, $[2\,4]$, $[1^2\,4]$, $[3^2]$, $[1\,2\,3]$, $[1^3\,3]$, $[2^3]$, $[1^2\,2^2]$, $[1^4\,2]$, $[1^6]$.

4. Nochmals Permutationen

Bsp. Die Permutation

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

ist eine Permutation vom Typ $[1^2\,2\,5]$ (zwei 1-Zykel (Fixpunkte), ein 2-Zykel und ein 5-Zykel).

Kombinatorisches Problem Wieviele Permutationen vom Typ $[1^{m_1}\,2^{m_2}\,\ldots\,k^{m_k}] \vdash n = \sum_{j=1}^{k} j\,m_j$ gibt es?

Antwort: $\dfrac{n!}{1^{m_1}\,\ldots\,k^{m_k}\,m_1!\,\ldots\,m_k!}$

Bsp. Permutationen vom Grad 6

Typ	Beispiel	Anzahl
$[1^6]$	$\mathrm{id} = (1)(2)(3)(4)(5)(6)$	1
$[1^4\,2]$	$(1\,2) = (1\,2)(3)(4)(5)(6)$	15
$[1^2\,2^2]$	$(1\,2)(3\,4) = (1\,2)(3\,4)(5)(6)$	45
$[2^3]$	$(1\,2)(3\,4)(5\,6)$	15
$[1^3\,3]$	$(1\,2\,3) = (1\,2\,3)(4)(5)(6)$	40
$[1\,2\,3]$	$(1\,2\,3)(4\,5) = (1\,2\,3)(4\,5)(6)$	120
$[3^2]$	$(1\,2\,3)(4\,5\,6)$	40
$[1^2\,4]$	$(1\,2\,3\,4) = (1\,2\,3\,4)(5)(6)$	90
$[2\,4]$	$(1\,2\,3\,4)(5\,6)$	90
$[1\,5]$	$(1\,2\,3\,4\,5) = (1\,2\,3\,4\,5)(6)$	144
$[6]$	$(1\,2\,3\,4\,5\,6)$	120
		720

5. Tabelle für Zählprobleme

Anzahl Möglichkeiten, n Bälle in m Fächern zu platzieren.

	beliebig	$\leqslant 1$ Ball pro Fach	$\geqslant 1$ Ball pro Fach	1 Ball pro Fach
Bälle unterscheidbar Fächer unterscheidbar	m^n	$m^{\underline{n}}$	$m!\left\{ {n \atop m} \right\}$	$m!\,\delta_{n,m}$
Bälle nicht unterscheidbar Fächer unterscheidbar	$\binom{n+m-1}{m-1}$	$\binom{m}{n}$	$\binom{n-1}{m-1}$	$\delta_{n,m}$
Bälle unterscheidbar Fächer nicht unterscheidbar	$\sum_{k=0}^{m} \left\{ {n \atop k} \right\}$	$\begin{cases} 1 & \text{falls } m \geqslant n \\ 0 & \text{falls } m < n \end{cases}$	$\left\{ {n \atop m} \right\}$	$\delta_{n,m}$
Bälle nicht unterscheidbar Fächer nicht unterscheidbar	$\sum_{k=0}^{m} P_{n,k}$	$\begin{cases} 1 & \text{falls } m \geqslant n \\ 0 & \text{falls } m < n \end{cases}$	$P_{n,m}$	$\delta_{n,m}$

Zu $m!\left\{{n \atop m}\right\}$. Teile die Menge der Bälle in m (nichtleere) Blöcke und verteile die Blöcke auf die Fächer.

Zu $\binom{n+m-1}{m-1}$. Der Nikolaus verteilt n Orangen an m Kinder, wobei auch Kinder leer ausgehen können.

Zu $\binom{n-1}{m-1}$. Der Nikolaus verteilt n Orangen an m Kinder, wobei jedes Kind mindestens eine Orange erhält.

Nochmals zu $\binom{n-1}{m-1}$. Es geht darum, m-Tupel $(\lambda_1, \ldots, \lambda_m)$ von positiven ganzen Zahlen mit $\sum_{k=1}^{m} \lambda_k = n$ zu zählen. Gesucht ist eine Bijektion

$$\left\{(\lambda_1, \ldots, \lambda_m) \in (\mathbb{Z}_{>0})^m \;\middle|\; \sum_{k=1}^{m} \lambda_k = n\right\} \longrightarrow \binom{\{1, \ldots, n-1\}}{m-1}.$$

Das m-Tupel $(\lambda_1, \ldots, \lambda_m)$ wird auf die $(m-1)$-elementige Menge $\{\lambda_1, \lambda_1 + \lambda_2, \ldots, \lambda_1 + \cdots + \lambda_{m-1}\}$ abgebildet. Die Umkehrabbildung ordnet $\{\mu_1 < \cdots < \mu_{m-1}\}$ das m-Tupel $(\mu_1, \mu_2 - \mu_1, \ldots, \mu_{m-1} - \mu_{m-2}, n - \mu_{m-1})$ zu.

Zu $\sum_{k=0}^{m} \left\{{n \atop k}\right\}$ und $\sum_{k=0}^{m} P_{n,k}$. Für $n > 0$ ist $\left\{{n \atop 0}\right\} = P_{n,0} = 0$, und wir können dann die Summe von $k = 1$ bis $k = m$ laufen lassen.

Die Unterscheidung „unterscheidbar / nicht unterscheidbar“ wird bei den Bällen bzw. den Fächern für $n \leqslant 1$ bzw. $m \leqslant 1$ hinfällig.

6. Zahlpartitionen II

Problem Auf wieviele Arten lassen sich 5-, 10- und 20-Räppler zu 1 Franken addieren?

Allgemeiner: Welche Beträge lassen sich auf wieviele Arten durch 5-, 10- und 20-Räppler addieren?

$$\begin{aligned} a &= \text{Anzahl } 5\text{-Räppler} \\ b &= \text{Anzahl } 10\text{-Räppler} \\ c &= \text{Anzahl } 20\text{-Räppler} \\ \hline 5a + 10b + 20c &= \text{Gesamtbetrag in Rappen} \end{aligned}$$

Wir schreiben nun den Gesamtbetrag in den Exponenten und bilden die erzeugende Funktion.

$$\begin{aligned} \sum_{a=0}^{\infty}\sum_{b=0}^{\infty}\sum_{c=0}^{\infty} x^{5a+10b+20c} &= \sum_{a=0}(x^5)^a \sum_{b=0}(x^{10})^b \sum_{c=0}(x^{20})^c \\ &= \frac{1}{(1-x^5)(1-x^{10})(1-x^{20})} = \frac{(1+x^5)(1+x^{10})^2}{(1-x^{20})^3} \\ &= (1 + x^5 + 2x^{10} + 2x^{15} + x^{20} + x^{25}) \sum_{n=0}^{\infty} \binom{n+2}{2} x^{20n} \end{aligned}$$

Die gesuchte Anzahl für 1 Franken ist der Koeffizient von x^{100} in der obigen erzeugenden Funktion, also

$$\begin{aligned} &[x^{100}] \frac{1}{(1-x^5)(1-x^{10})(1-x^{20})} \\ &\quad = \binom{7}{2} + \binom{6}{2} = 21 + 15 = 36. \end{aligned}$$

Wie lautet die Antwort, wenn höchstens 10 5-Räppler verwendet werden dürfen? Der Faktor $\frac{1}{1-x^5} = \sum_{a=0}^{\infty}(x^5)^a$ ist dann durch $\sum_{a=0}^{10}(x^5)^a = \frac{1-(x^5)^{11}}{1-x^5}$ zu ersetzen.

$$[x^{100}]\frac{1-(x^5)^{11}}{(1-x^5)(1-x^{10})(1-x^{20})} = 27$$

Definition der Partitionsfunktion: $p(n) = \sum_{k=0}^{n} P_{n,k}$ ist die Anzahl aller Partitionen von n.

Nach dem vorherigen Beispiel sollte klar sein, dass sich die erzeugende Funktion

$$P(x) = \sum_{n=0}^{\infty} p(n)\, x^n$$

als das folgende unendliche Produkt schreiben lässt:

$$P(x) = \prod_{m=1}^{\infty} \frac{1}{1-x^m}\,.$$

Dieses unendliche Produkt ist eine wohlbestimmte Potenzreihe, denn $[x^n] \prod_{m=1}^{\infty} \frac{1}{1-x^m} = [x^n] \prod_{m=1}^{n} \frac{1}{1-x^m}$.

Wir wollen nun Partitionen betrachten, die gewissen Restriktionen genügen. Zum Beispiel können wir Partitionen von n mit lauter verschiedenen Teilen betrachten. Für $n = 6$ sind dies die vier Partitionen 6, $5+1$, $4+2$ und $3+2+1$. Die erzeugende Funktion ist

$$Q(x) = \prod_{m=1}^{\infty}(1+x^m).$$

Andrerseits wollen wir Partitionen von n mit lauter ungeraden Teilen betrachten. Für $n = 6$ sind dies die vier Partitionen $5+1$, $3+3$, $3+1+1+1$ und $1+1+1+1+1+1$. Die erzeugende Funktion lautet

$$\widetilde{Q}(x) = \prod_{l=0}^{\infty} \frac{1}{1-x^{2l+1}}\,.$$

Nun rechnen wir

$$\begin{aligned} Q(x) = \prod_{m=1}^{\infty}(1+x^m) &= \prod_{m=1}^{\infty} \frac{(1+x^m)(1-x^m)}{1-x^m} \\ &= \prod_{m=1}^{\infty} \frac{1-x^{2m}}{1-x^m} = \prod_{l=0}^{\infty} \frac{1}{1-x^{2l+1}} = \widetilde{Q}(x). \end{aligned}$$

Damit haben wir die folgende Proposition bewiesen.

Proposition Die Anzahl der Partitionen von n mit lauter verschiedenen Teilen ist gleich der Anzahl der Partitionen von n mit lauter ungeraden Teilen.

Ganz analog beweisen wir das folgende Beispiel.
Bsp. Die Anzahl der Partitionen von n, wo alle geraden Teile verschieden sind, ist gleich der Anzahl der Partitionen von n, wo kein Teil mehr als dreimal vorkommt. (Für $n = 6$ sind das alle Partitionen ausser $2+2+2$ und $2+2+1+1$ bzw. $2+1+1+1+1$ und $1+1+1+1+1+1$.)
Beweis.

$$\prod_{m=1}^{\infty} \frac{1+x^{2m}}{1-x^{2m-1}} = \prod_{m=1}^{\infty} \frac{(1+x^{2m})(1-x^{2m})}{(1-x^{2m-1})(1-x^{2m})}$$
$$= \prod_{k=1}^{\infty} \frac{1-x^{4k}}{1-x^{k}}\,.$$

■

Schliesslich soll noch eine Rekursionsformel zur Berechnung von $p(n)$ angegeben werden. Dazu benützen wir folgenden Satz von Euler (1707–1783), den wir hier nicht beweisen.
Satz (Eulerscher Pentagonalzahlsatz)

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{m=-\infty}^{\infty} (-1)^m x^{m(3m-1)/2}$$
$$= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots\,.$$

Da dieses unendliche Produkt gerade der Reziprokwert der erzeugenden Funktion $P(x) = \sum_{n=0}^{\infty} p(n)\,x^n$ ist, erhalten wir folgende unendliche Rekursionsformel:

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + \cdots$$

für $n > 0$ mit $p(0) = 1$ und $p(m) = 0$ für $m < 0$. Für fixiertes n kommen natürlich nur endlich viele Summanden vor.

Mit dieser Formel ist es problemlos möglich, beispielsweise $p(200) = 3\,972\,999\,029\,388$ zu finden. Es gibt eine einfache approximative Formel für $p(n)$ von Hardy (1877–1947) und Ramanujan (1887–1920), nämlich

$$p(n) \approx \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}\,.$$

Es gibt eine (komplizierte) exakte Formel von Rademacher (1892–1969).

7. Anhang: Einige Potenzreihenentwicklungen

$$\sum_{n=0}^{\infty} \binom{r+n-1}{n} x^n = (1-x)^{-r} \qquad (r \in \mathbb{C})$$

insbesondere:

$$\sum_{n=0}^{\infty} \binom{n+m}{m} x^n = \frac{1}{(1-x)^{m+1}} \qquad (m \in \mathbb{N})$$

insbesondere:

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$
$$\sum_{n=0}^{\infty} n\,x^n = \frac{x}{(1-x)^2}$$
$$\sum_{n=0}^{\infty} n^2\,x^n = \frac{x+x^2}{(1-x)^3}$$

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x$$

$$\sum_{n=1}^{\infty} \frac{x^n}{n} = -\ln(1-x)$$

Graphentheorie

1. Einige Grundbegriffe

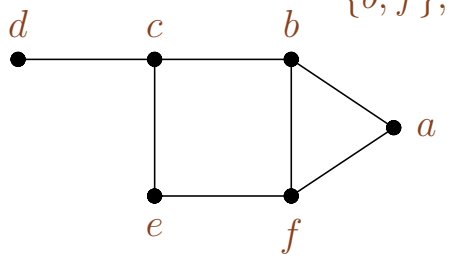
Definition Ein (endlicher) Graph ist ein Paar $G = (V, E)$, bestehend aus einer (endlichen) Menge V und einer Teilmenge $E \subseteq \binom{V}{2}$ der zweielementigen Teilmengen von V. Die Elemente von V heissen Ecken (engl. vertices) oder Knoten und jene von E Kanten (engl. edges).

Vereinbarung Unter einem Graphen wollen wir in dieser Lehrveranstaltung stillschweigend einen endlichen Graphen verstehen.

Diese Bezeichnungen sind klar, wenn wir uns einen Graphen anhand seiner geometrischen Realisierung vorstellen.

Bsp. $G = (V, E)$ mit $V = \{a, b, c, d, e, f\}$,

$$E = \big\{\{a,b\},\{a,f\},\{b,c\},\{b,f\},\{c,d\},\{c,e\},\{e,f\}\big\}$$



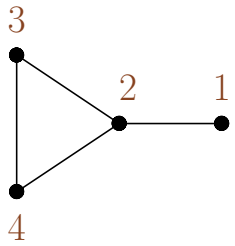
Unter einer Abbildung $G \to G'$ zwischen zwei Graphen $G = (V, E)$ und $G' = (V', E')$ versteht man eine Abbildung der entsprechenden Eckenmengen $\varphi : V \to V'$ so, dass gilt

$$\{v, w\} \in E \Longrightarrow \{\varphi(v), \varphi(w)\} \in E'.$$

Wir schreiben dann auch $\varphi : G \to G'$ und erweitern φ auf

E, durch $\varphi(e) := \{\varphi(v), \varphi(w)\} \in E'$ für $e = \{v, w\} \in E$.

Bsp. Sei H der Graph



Eine Abbildung $H \to G$ ist zum Beispiel

$$\begin{aligned} \alpha : \{1,2,3,4\} &\longrightarrow \{a,b,c,d,e,f\} \\ 1 &\longmapsto c \\ 2 &\longmapsto b \\ 3 &\longmapsto a \\ 4 &\longmapsto f \end{aligned}$$

Eine andere Abbildung $H \to G$ ist zum Beispiel

$$\begin{aligned} \beta : \{1,2,3,4\} &\longrightarrow \{a,b,c,d,e,f\} \\ 1 &\longmapsto f \\ 2 &\longmapsto a \\ 3 &\longmapsto b \\ 4 &\longmapsto f \end{aligned}$$

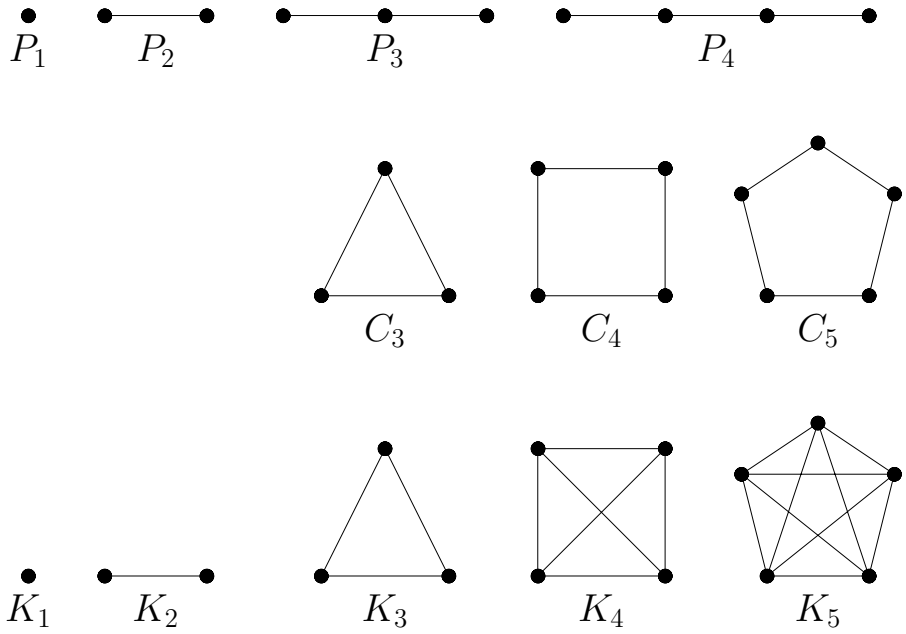
Isomorphismus Eine Abbildung $\varphi : G \to G'$ zwischen zwei Graphen $G = (V, E)$ und $G' = (V', E')$, also $\varphi : V \to V'$, heisst Isomorphismus, wenn φ bijektiv ist und die Umkehrabbildung $\varphi^{-1} : V' \to V$ auch eine Abbildung zwischen Graphen ist. Mit anderen Worten, φ ist bijektiv und

$$\{v, w\} \in E \iff \{\varphi(v), \varphi(w)\} \in E'.$$

Die Graphen G und G' heissen dann isomorph. Ein Isomorphismus $G \to G$ heisst Automorphismus von G. Die Menge aller Automorphismen von G ist eine Gruppe, die Automorphismengruppe von G, geschrieben $\mathrm{Aut}(G)$.

Untergraph $G' = (V', E')$ heisst ein Untergraph von $G = (V, E)$, falls $V' \subseteq V$ und $E' \subseteq E$. Notation: $G' \subseteq G$. Gilt sogar $E' = E \cap \binom{V'}{2}$, so heisst G' ein induzierter Untergraph von G. Gilt $V' = V$, so heisst G' ein aufspannender Untergraph von G.

2. Einige spezielle Graphen, Wege und Kreise in Graphen, Zusammenhang



Weg P_n der Länge $n-1$ ($n = 1, 2, \ldots$).

Kreis C_n der Länge n ($n = 3, 4, \ldots$).

Vollständiger Graph K_n mit n Ecken und $\binom{n}{2}$ Kanten ($n = 0, 1, 2, \ldots$, K_0 ist der leere Graph).

Varianten des Konzepts „Graph“:
Graph mit Schlingen: hier sind Kanten von einer Ecke zu sich selber erlaubt. Z. B. der Kreis C_1.
Multigraph: hier sind nebst Schlingen auch Mehrfachkanten erlaubt. Z. B. der Kreis C_2.

Sei G ein Graph. Ein Weg in G der Länge n ist ein Untergraph von G, der isomorph zu P_{n+1} ist. Die Begriffe „Anfangsecke“, „Endecke“, „Weg von u nach v“, „Weg zwischen u und v“ haben die evidenten Bedeutungen. Der Abstand zweier Ecken u und v, geschrieben $\mathrm{dist}(u, v)$, ist die Länge des kürzesten Weges zwischen u und v bzw. ∞, falls es keinen solchen Weg gibt.

Die Relation

$$u \sim v \;:\Longleftrightarrow\; \mathrm{dist}(u, v) \neq \infty$$

ist eine Äquivalenzrelation auf V. Ihre Äquivalenzklassen heissen Zusammenhangskomponenten von G (oder genauer heissen die von diesen Eckenmengen induzierten Untergraphen von G die Zusammenhangskomponenten von G). Ein Graph G heisst zusammenhängend, wenn er aus 1 Zusammenhangskomponente besteht. (Insbesondere ist dann also G nicht der leere Graph.)

3. Weitere Grundbegriffe, Beschreibung von Graphen mittels Matrizen

Sei $G = (V, E)$ ein Graph mit n Ecken, $V = \{v_1, \ldots, v_n\}$, und m Kanten, $E = \{e_1, \ldots, e_m\}$.

Die Adjazenzmatrix $A = (a_{ij})_{i,j=1,\ldots,n}$ ist gegeben durch

$$a_{ij} = \begin{cases} 1 & \text{falls } \{v_i, v_j\} \in E, \\ 0 & \text{sonst.} \end{cases}$$

Die Inzidenzmatrix $B = (b_{ih})_{\substack{i=1,\ldots,n \\ h=1,\ldots,m}}$ ist gegeben durch

$$b_{ih} = \begin{cases} 1 & \text{falls } v_i \in e_h, \\ 0 & \text{sonst.} \end{cases}$$

Zwei Ecken u und v von G heissen benachbart oder adjazent, falls $\{u, v\}$ eine Kante in G ist.

Der Grad einer Ecke $v \in V$ ist die Anzahl der zu v benachbarten Ecken in G. Notation: $d(v)$.

Unter der Gradfolge von G verstehen wir die aufsteigend geordnete Liste der Grade aller Ecken von G.
Isomorphe Graphen haben dieselbe Gradfolge, denn ein Isomorphismus bildet jede Ecke auf eine Ecke mit demselben Grad ab. Die Umkehrung gilt nicht (siehe Übung).

Bem. Die Zeilensummen der Inzidenzmatrix sind die Grade der Ecken. (Die Spaltensummen der Inzidenzmatrix sind immer 2, denn zu jeder Kante gehören zwei Ecken.)

Satz $\sum_{v \in V} d(v) = 2\,|E|$.

Beweis. (Doppeltes Abzählen) Die linke Seite summiert die Zeilensummen der Inzidenzmatrix, die rechte Seite die Spaltensummen. ■

4. Färbungen

Eine Färbung (genauer: eine Eckenfärbung) eines Graphen $G = (V, E)$ ist eine Abbildung $c : V \to S$ (S ist eine Menge von „Farben“) so, dass $c(u) \neq c(v)$ für alle benachbarten Ecken u, v gilt.
Die chromatische Zahl $\chi(G)$ von G ist die kleinste Zahl k so, dass eine Färbung $c : V \to \{1, \ldots, k\}$ existiert. Der Graph G heisst k-färbbar, wenn $\chi(G) \leqslant k$ gilt.

Bem. Ist $\varphi : G \to G'$ eine Abbildung zwischen Graphen, so gilt $\chi(G) \leqslant \chi(G')$, denn aus einer Färbung von G' erhalten wir durch Zusammensetzen mit φ eine Färbung von G. Es ist nun leicht einzusehen, dass gilt

$$\chi(G) = \min\{k \mid G \to K_k\},$$

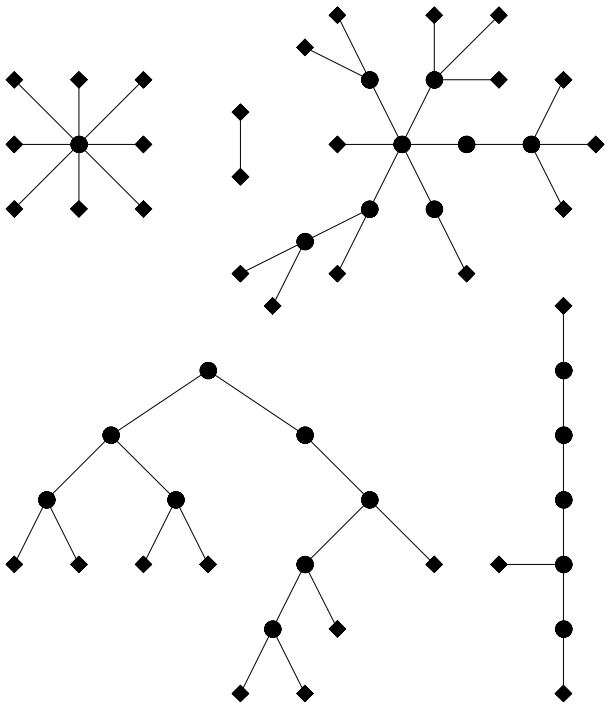
d. h. die chromatische Zahl von G ist die kleinste Zahl k so, dass eine Abbildung von G in den vollständigen Graphen mit k Ecken existiert.

Bäume

1. Definition und Charakterisierung

Definition Ein Graph $T = (V, E)$ heisst Baum, wenn T zusammenhängend ist und kein Untergraph von T ein Kreis ist.
Ein Wald ist ein Graph, dessen Zusammenhangskomponenten Bäume sind.
Ein Blatt eines Baumes ist eine Ecke vom Grad 1.

Bsp. eines Waldes (die Blätter der Zusammenhangskomponenten sind durch Quadrate gekennzeichnet)



Satz Für einen Graphen $T = (V, E)$ sind die folgenden Aussagen äquivalent.

(1) T ist ein Baum.

(2) Zwischen je zwei Ecken gibt es genau einen Weg.

(3) T ist zusammenhängend und $|V| - |E| = 1$.

Satz von Cayley Im vollständigen Graphen mit n Ecken ($n \geqslant 1$) gibt es genau n^{n-2} aufspannende Bäume.

Für diesen Satz gibt es inzwischen zahlreiche Beweise. Der bis anhin eleganteste verwendet doppeltes Abzählen.

Schwieriger: Wieviele nichtisomorphe Bäume mit n Ecken gibt es?

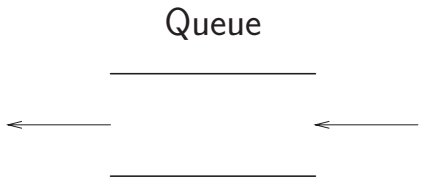
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Anzahl	1	1	1	2	3	6	11	23	47	106	235	551	1301	3159

2. Breitensuche und Tiefensuche

Input: nichtleerer Graph G,
Liste der Ecken von G: $v_1, \ldots, v_n$.

Output: aufspannender Baum $T = (V_T, E_T)$ der Zusammenhangskomponente von v_1.

Breitensuche (Breadth First Search)



$\text{Queue} := v_1 \; [V_T := \{v_1\}, E_T := \varnothing]$

while Queue **nicht leer do**

begin

$u :=$ vorderste Ecke der Queue

if u **benachbart zu neuer Ecke** v

then füge v zuhinterst in die Queue ein
$[V_T := V_T \cup \{v\}, E_T := E_T \cup \{\{u, v\}\}]$

else lösche u von der Queue

end

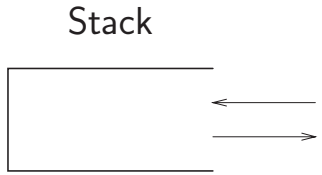
Nach Konstruktion ist (V_T, E_T) ein Baum. Es bleibt noch einzusehen, dass V_T alle Ecken der Zusammenhangskomponente von v_1 in G enthält. Wäre $w \in V - V_T$ in der Zusammenhangskomponente von v_1, so gäbe es einen Weg zwischen v_1 und w. Längs dieses Weges gäbe es dann eine Kante $\{u, u'\}$ mit $u \in V_T$ und $u' \notin V_T$. Irgendwann wäre u die vorderste Ecke der Queue gewesen und u' als neue Ecke hinzugekommen. Widerspruch.

Bsp. für den BFS-Algorithmus
Ein Graph mit den acht Ecken $a, \ldots, h$ ist gegeben durch die Angabe der Nachbarecken jeder Ecke.

Ecken	a	b	c	d	e	f	g	h
Nachbar-	b	a	a	a	b	a	d	e
ecken	c	c	b	b	d		e	g
	d	d		e	g		h	
	f	e		g	h			

Queue	neue Kante	Queue	neue Kante
a		dfe	
ab	$\{a, b\}$	$dfeg$	$\{d, g\}$
abc	$\{a, c\}$	feg	
$abcd$	$\{a, d\}$	eg	
$abcdf$	$\{a, f\}$	egh	$\{e, h\}$
$bcdf$		gh	
$bcdfe$	$\{b, e\}$	h	
$cdfe$			

Tiefensuche (Depth First Search)



siehe Übung

Netzwerke

In diesem Abschnitt geht es um die Modellierung von Flüssen, welche einem Netzwerkknoten s entspringen und in einem anderen Netzwerkknoten t versickern.

Nach den Definitionen (auf Folien) werden wir (an der Wandtafel) den klassischen Satz von Ford und Fulkerson (1956) beweisen, das Max-Flow Min-Cut Theorem, und ihren Algorithmus zur Bestimmung maximaler Flüsse angeben. Anschliessend folgen Anwendungen.

1. Definitionen

Wir benötigen zuerst den Begriff eines gerichteten Graphen oder Digraphen ("directed graph"). Ein gerichteter Graph ist ein Paar $\vec{G} = (V, A)$, bestehend aus einer Menge V und einer Teilmenge $A \subseteq V^2 - \{(v, v) \mid v \in V\}$.

Die Elemente von V heissen Ecken (engl. vertices) oder Knoten und jene von A Bögen (engl. arcs).

Für einen Bogen $a \in A$ schreiben wir $a = (a^-, a^+)$, d. h. a^- ist die Anfangsecke von a und a^+ seine Endecke.

Wie wir das schon bei den Graphen vereinbart hatten, wollen wir auch hier stillschweigend $|V| < \infty$ voraussetzen.

Ein gerichteter Graph lässt sich anhand seiner geometrischen Realisierung anschaulich vorstellen.

Ein Netzwerk $N = (\vec{G}, c, s, t)$ besteht aus einem gerichteten Graphen $\vec{G} = (V, A)$, einer Kapazitätsfunktion

$$\begin{aligned} c : A &\longrightarrow \mathbb{N} \\ a &\longmapsto c(a) = \text{Kapazität von } a \end{aligned}$$

und zwei verschiedenen Ecken $s, t \in V$, der Quelle s und der Senke t.

Für eine Funktion $f : A \to \mathbb{R}$ definieren wir den Einfluss in einer Ecke v und den Ausfluss in v als

$$\operatorname{in}_v(f) := \sum_{\substack{a \in A \\ a^+ = v}} f(a) \quad \text{und} \quad \operatorname{out}_v(f) := \sum_{\substack{a \in A \\ a^- = v}} f(a).$$

Ein Fluss in N ist eine Funktion

$$f : A \longrightarrow \mathbb{N}$$

mit folgenden Eigenschaften:

1. $\forall\, a \in A$: $0 \leqslant f(a) \leqslant c(a)$,
2. $\forall\, v \in V - \{s, t\}$: $\operatorname{in}_v(f) = \operatorname{out}_v(f)$.

Der Wert eines Flusses f, geschrieben $\operatorname{val}(f)$, ist

$$\operatorname{val}(f) := \operatorname{out}_s(f) - \operatorname{in}_s(f) = \operatorname{in}_t(f) - \operatorname{out}_t(f).$$

Ein Schnitt in N ist eine Partition (S, T) der Eckenmenge V mit $s \in S$ und $t \in T$, also $V = S \cup T$ und $S \cap T = \varnothing$ (und $s \in S$, $t \in T$). Die Kapazität eines Schnittes (S, T), geschrieben $\operatorname{cap}(S, T)$, ist

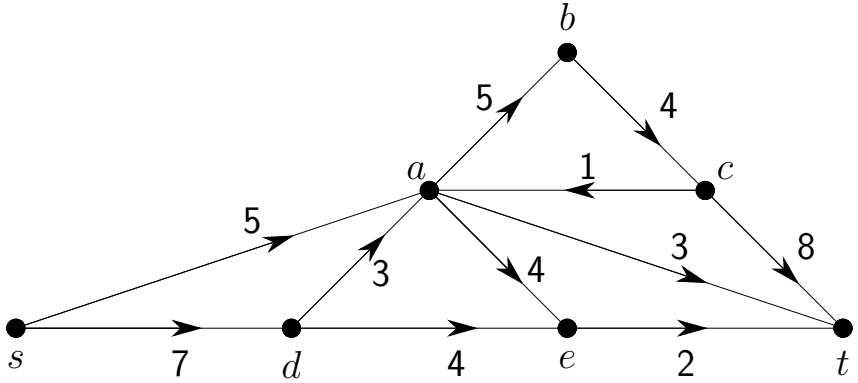
$$\operatorname{cap}(S, T) := \sum_{\substack{a \in A \\ a^- \in S \\ a^+ \in T}} c(a).$$

Beispiel zur Konstruktion eines maximalen Flusses von der Quelle s zur Senke t. Die angeschriebenen Zahlen sind die Kapazitäten der Bögen.

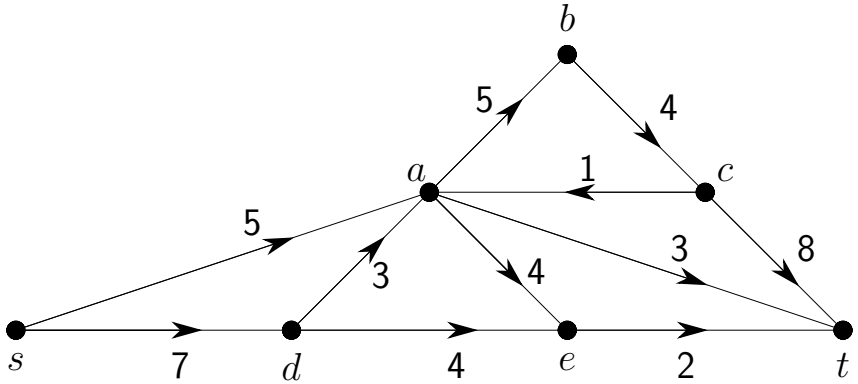
Fluss f (0 auf nicht beschrifteten Bögen)

Markierung: Vorgängerecke, Richtung, zusätzlicher Fluss

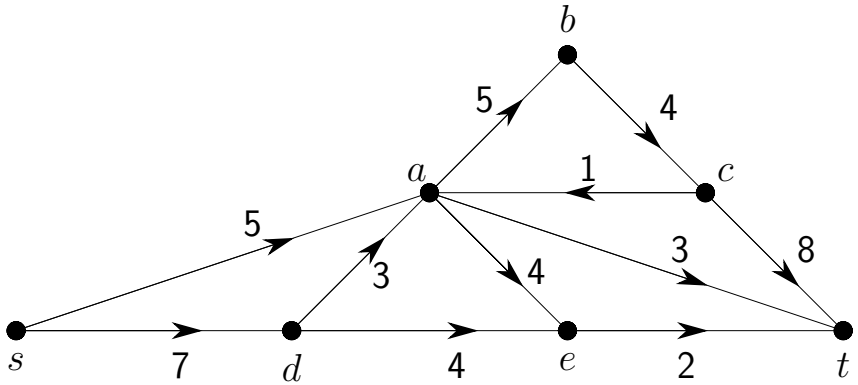
zunehmender Weg bzgl. f



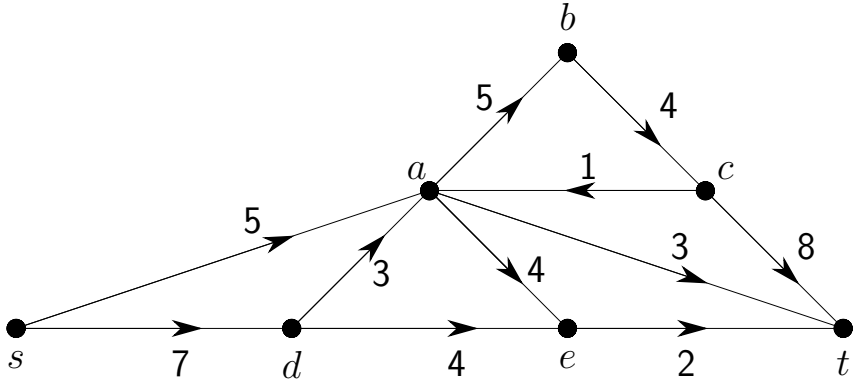
$\mathrm{val}(f) =$



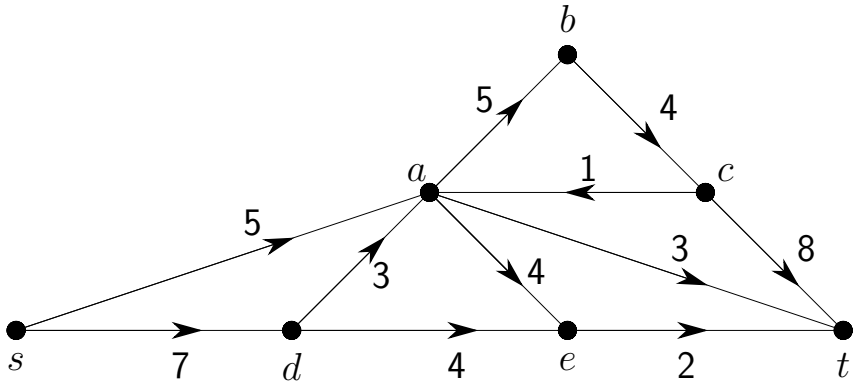
$\mathrm{val}(f) =$



$\mathrm{val}(f) =$



$\mathrm{val}(f) =$



$\mathrm{val}(f) =$

Chromatisches Polynom

Schon definiert: chromatische Zahl eines Graphen. Nun soll diese Invariante etwas verfeinert und das chromatische Polynom eines Graphen definiert werden.

Analogie: A, B $n\times n$-Matrizen. Zur Erinnerung: A, B sind ähnlich, falls es eine invertierbare $n\times n$-Matrix S gibt mit $A = SBS^{-1}$.

$$\det A \neq \det B \implies A \text{ und } B \text{ sind nicht ähnlich.}$$

Feinere Invariante: charakteristisches Polynom.

$$p_A(z) \neq p_B(z) \implies A \text{ und } B \text{ sind nicht ähnlich.}$$

Sei $G = (V, E)$ ein Graph. Wir setzen

$$P(G, z) := \text{Anzahl Färbungen der Ecken von } G \text{ mit } z > 0 \text{ Farben.}$$

D. h. für $z \in \mathbb{Z}_{>0}$ ist $P(G, z)$ die Anzahl der Funktionen

$$f : V \longrightarrow \{1, \ldots, z\} \text{ mit } \{v, w\} \in E \implies f(v) \neq f(w).$$

Die chromatische Zahl ist dann

$$\chi(G) = \min\big\{k \in \mathbb{N} \;\big|\; P(G, k) > 0\big\}.$$

Klar: $P(K_n, z) = z^{\underline{n}} = z(z-1)(z-2)\ldots(z-n+1)$.

Zur Berechnung von $P(G, z)$: Seien $v, w \in V$, $v \neq w$, $\{v, w\} \notin E$. Wir definieren zwei neue Graphen:

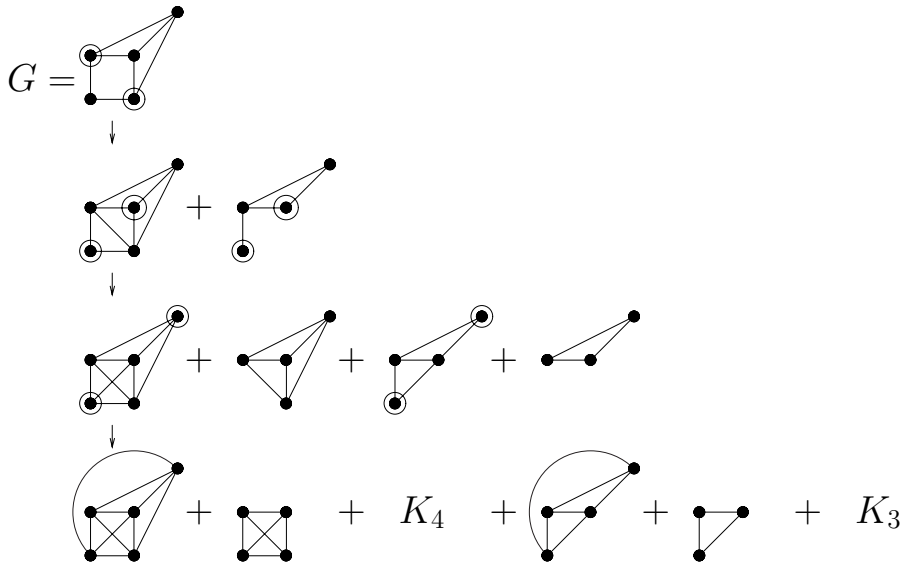
$G_{\{v,w\}}$ „G mit zusätzlicher Kante $\{v, w\}$“

$G_{v=w}$ „G mit den Ecken v und w identifiziert“ (Entferne in G die Ecken v und w samt allen Kanten $\{v, .\}$, $\{w, .\}$. Füge eine neue Ecke hinzu und verbinde sie mit allen Ecken, welche in G zu v oder w benachbart sind.)

Die beiden Graphen $G_{\{v,w\}}$ und $G_{v=w}$ haben je mindestens ein nicht verbundenes Paar von Ecken weniger als G. Eine Iteration führt schliesslich zu lauter vollständigen Graphen. Und hier ist die wesentliche Beobachtung:

$$P(G, z) = \underbrace{P(G_{\{v,w\}}, z)}_{\substack{\text{zählt Färbungen } f \\ \text{mit } f(v) \neq f(w)}} + \underbrace{P(G_{v=w}, z)}_{\substack{\text{zählt Färbungen } f \\ \text{mit } f(v) = f(w)}}. \qquad (*)$$

Bsp. Die v und w entsprechenden Ecken in der Rekursion $(*)$ sind eingekreist.



Es gilt also

$$\begin{aligned} P(G, z) &= P(K_5, z) + 3\,P(K_4, z) + 2\,P(K_3, z) \\ &= z^5 - 7\,z^4 + 19\,z^3 - 23\,z^2 + 10\,z. \end{aligned}$$

Wir gehen ganz naiv vor, indem wir in 4. und 6. alle möglichen Fälle anschauen. Das ist eine gute Übung, um sich zu vergegenwärtigen, was unter der Implikation $P \to Q$ (falls P, dann Q) zu verstehen ist. Antwort: $P \to Q$ ist wahr, ausser wenn P wahr ist und Q falsch. Wenn also P falsch ist, so ist $P \to Q$ immer wahr, unabhängig von Q. Und wenn P wahr ist, so stimmt der Wahrheitswert (wahr/falsch) von $P \to Q$ mit dem Wahrheitswert von Q überein.

Mit den evidenten Abkürzungen haben wir das folgende System von Bedingungen, die *alle* erfüllt sein müssen. (Dabei haben wir Bedingungen wie Lokführer $\neq$ Heizer oder Basel $\neq$ Zürich usw. nicht explizit aufgeführt.)

0. $\{\text{Lokführer, Heizer, Kondukteur}\} = \{\text{K, M, S}\}$
1. $\text{W(Dr. K)} = \text{Z}$
2. $\text{W(Heizer)} = \text{H}$ [Herznach liegt in der Mitte zwischen Basel und Zürich]
3. $\text{L(Dr. M)} = \text{CHF 8000}$
4. $\text{W(Dr. K)} = \text{W(Heizer)} \vee \text{W(Dr. M)} = \text{W(Heizer)} \vee \text{W(Dr. S)} = \text{W(Heizer)}$
   $\text{W(Dr. K)} = \text{W(Heizer)} \to \text{L(Dr. K)} = 3 \cdot \text{ L(Heizer)}$
   $\text{W(Dr. M)} = \text{W(Heizer)} \to \text{L(Dr. M)} = 3 \cdot \text{ L(Heizer)}$
   $\text{W(Dr. S)} = \text{W(Heizer)} \to \text{L(Dr. S)} = 3 \cdot \text{ L(Heizer)}$
5. $\text{Kondukteur} \neq \text{S}$
6. $\text{Heizer} = \text{K} \to \text{W(Dr. K)} = \text{B}$
   $\text{Heizer} = \text{M} \to \text{W(Dr. M)} = \text{B}$
   $\text{Heizer} = \text{S} \to \text{W(Dr. S)} = \text{B}$

Einsetzen von 1., 2. und 3. in 4. liefert die Bedingungen

4. $\text{Z} = \text{H} \vee \text{W(Dr. M)} = \text{H} \vee \text{W(Dr. S)} = \text{H}$
   $\text{Z} = \text{H} \to \text{L(Dr. K)} = 3 \cdot \text{ L(Heizer)}$
   $\text{W(Dr. M)} = \text{H} \to \text{CHF 8000} = 3 \cdot \text{ L(Heizer)}$ [aber 3 teilt CHF 8000 nicht]
   $\text{W(Dr. S)} = \text{H} \to \text{L(Dr. S)} = 3 \cdot \text{ L(Heizer)}$.
   Es folgt: $\text{W(Dr. S)} = \text{H}$.

Einsetzen von 1. und der eben gefundenen Bedingung $\text{W(Dr. S)} = \text{H}$ in 6. gibt

6. $\text{Heizer} = \text{K} \to \text{Z} = \text{B}$
   $\text{Heizer} = \text{M} \to \text{W(Dr. M)} = \text{B}$
   $\text{Heizer} = \text{S} \to \text{H} = \text{B}$.
   Es folgt: $\text{Heizer} = \text{M}$.

Zusammen mit der Bedingung 5. folgen $\text{Kondukteur} = \text{K}$ und $\text{Lokführer} = \text{S}$.

Nun sind wir aber noch nicht ganz fertig, denn es könnte ja sein, dass die sechs Bedingungen in sich widersprüchlich sind. Das ist nicht so, wie das folgende Modell zeigt.

Name	Beruf	Wohnort	Lohn
Keller	Kondukteur		
Müller	Heizer	Herznach	CHF 3000
Schmid	Lokführer		
Dr. Keller		Zürich	
Dr. Müller		Basel	CHF 8000
Dr. Schmid		Herznach	CHF 9000

Seien G eine Gruppe und X eine G-Menge.

Satz Jeder Stabilisator G_x eines Punktes $x \in X$ ist eine Untergruppe von G.

Beweis. Zu zeigen sind die folgenden beiden Punkte.

- $G_x \neq \varnothing$
- $\forall\, g, h \in G_x : g^{-1}h \in G_x$

$G_x \neq \varnothing$, denn $1x = x$, also $1 \in G_x$.
Seien $g, h \in G_x$, also $gx = x$ und $hx = x$. Lassen wir g^{-1} auf $gx = x$ wirken, so erhalten wir $g^{-1}gx = g^{-1}x$, also $1x = g^{-1}x$, d. h. $x = g^{-1}x$.
Nun setzen wir alles zusammen: $g^{-1}hx = g^{-1}x = x$, also $g^{-1}h \in G_x$. ■

Satz Zwischen Stabilisatoren von Punkten x und gx (also im selben Orbit) gibt es folgende Beziehung:

$$G_{gx} = gG_xg^{-1} := \left\{ghg^{-1} \;\middle|\; h \in G_x\right\}.$$

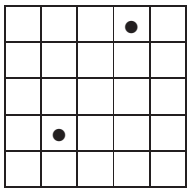
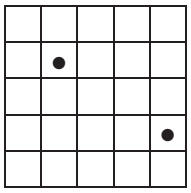
Beweis. Wir beachten zuerst, dass folgende Gleichheit besteht:

$$\left\{ghg^{-1} \;\middle|\; h \in G_x\right\} = \left\{\ell \;\middle|\; g^{-1}\ell g \in G_x\right\}.$$

Wegen $\ell \in G_{gx} \Leftrightarrow \ell gx = gx \Leftrightarrow g^{-1}\ell gx = x \Leftrightarrow g^{-1}\ell g \in G_x$ ist also $G_{gx} = \left\{\ell \;\middle|\; g^{-1}\ell g \in G_x\right\}$, wie behauptet. ■

Auf der nächsten Seite finden Sie ein Beispiel zum Lemma von Cauchy-Frobenius.

Frage Wieviele zweimal gelochte unterscheidbare 5×5-Quadrate gibt es?

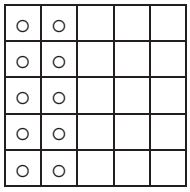
Beispiel:  und  sind ununterscheidbar.

Hier ist $G = \mathrm{Dih}_4$ die Symmetriegruppe des Quadrates. Und X ist die Menge aller Konfigurationen von 5×5-Quadraten mit zwei Löchern. Aus den 25 Feldern müssen also 2 Felder ausgewählt werden, was auf $\binom{25}{2} = 300$ Arten möglich ist, also $|X| = 300$.

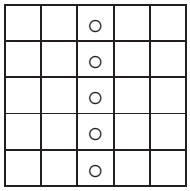
Wir gehen nun alle 8 Gruppenelemente durch und bestimmen jeweils die Anzahl Elemente in der Fixpunktmenge des betreffenden Gruppenelementes.

Die Fixpunktmenge der Identität ist die ganze Menge X, $|X| = 300$.

Als nächstes Gruppenelement betrachten wir die Spiegelung s an der vertikalen Achse. Ein zweifach gelochtes Quadrat gehört genau dann zur Fixpunktmenge X^s, wenn entweder ein Loch im linken 2×5-Block



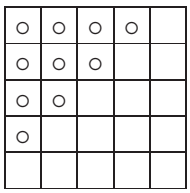
gewählt wird (10 Möglichkeiten) und das zweite Loch symmetrisch bzgl. der vertikalen Achse dazu, oder wenn beide Löcher auf der Achse



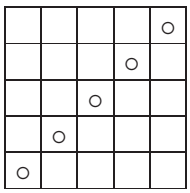
gewählt werden ($\binom{5}{2} = 10$ Möglichkeiten). Also $|X^s| = 10 + 10 = 20$.

Die Fixpunktmenge der Spiegelung an der horizontalen Achse besteht auch aus 20 Elementen.

Als nächstes Gruppenelement betrachten wir die Spiegelung an der SW-NE-Diagonalen. Auch die Fixpunktmenge dieses Gruppenelementes besteht aus $10 + \binom{5}{2} = 20$ Elementen:



Wähle ein Loch in einer der Positionen ∘ und das zweite symmetrisch bzgl. der SW-NE-Diagonalen dazu.



Wähle beide Löcher auf der Diagonalen.

Die Fixpunktmenge der Spiegelung an der NW-SE-Diagonalen besteht auch aus 20 Elementen.

Die Drehungen d_1, d_2 um $90°$ bzw. $270°$ haben keine Fixpunkte, $|X^{d_1}| = |X^{d_2}| = |\varnothing| = 0$.

Schliesslich bleibt die Drehung um $180°$, was dasselbe ist wie die Punktspiegelung im Zentrum. Die Fixpunktmenge dieser Punktspiegelung hat 12 Elemente: man wähle ein Loch irgendwo, aber nicht in der Mitte, und das zweite symmetrisch dazu.

Gemäss dem Lemma von Cauchy-Frobenius gibt es also

$$\frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{1}{8}\big(300 + 20 + 20 + 20 + 20 + 0 + 0 + 12\big) = 49$$

Orbits. Es gibt also 49 unterscheidbare 5×5-Quadrate mit 2 Löchern.

Repetition: Elementare Kombinatorik

Fakultäten: für $r \in \mathbb{Z}_{\geqslant 0}$ setzt man

$$r! := \prod_{k=1}^{r} k\,.$$

Fallende und steigende Faktorielle: für $n \in \mathbb{C}$ und $r \in \mathbb{Z}_{\geqslant 0}$ setzt man

$$n^{\underline{r}} := \prod_{k=0}^{r-1} (n-k),$$
$$n^{\overline{r}} := \prod_{k=0}^{r-1} (n+k).$$

Binomialkoeffizienten: für $n \in \mathbb{C}$ und $r \in \mathbb{Z}_{\geqslant 0}$ setzt man

$$\binom{n}{r} := \frac{n^{\underline{r}}}{r!}\,.$$

Ein Produkt über eine leere Indexmenge ist dabei als 1 zu verstehen, also $0! = n^{\underline{0}} = n^{\overline{0}} = 1$.

Frage: Auf wieviele Arten lassen sich r Elemente aus einer n-elementigen Menge auswählen (hier sind natürlich beide Zahlen n und r natürliche Zahlen)? Die Frage ist zu wenig präzis gestellt. Wir unterscheiden vier Fälle. Ist die Reihenfolge der ausgewählten Elemente zu beachten, oder ist die Ordnung irrelevant? Darf jedes Element höchstens einmal gewählt werden, oder sind Wiederholungen gestattet?

r* aus *n (Beispiel $r = 2$, $n = |\{\odot, \ominus, \otimes\}| = 3$)

	mit Wiederholungen	ohne Wiederholungen
geordnet	$(\odot,\odot), (\odot,\ominus), (\odot,\otimes),$ $(\ominus,\odot), (\ominus,\ominus), (\ominus,\otimes),$ $(\otimes,\odot), (\otimes,\ominus), (\otimes,\otimes)$ $\boldsymbol{n^r}$	$(\odot,\ominus), (\odot,\otimes), (\ominus,\odot),$ $(\ominus,\otimes), (\otimes,\odot), (\otimes,\ominus)$ $\boldsymbol{\frac{n!}{(n-r)!} = n^{\underline{r}}}$
ungeordnet	$\{\odot,\odot\}, \{\odot,\ominus\}, \{\odot,\otimes\},$ $\{\ominus,\ominus\}, \{\ominus,\otimes\}, \{\otimes,\otimes\}$ $\boldsymbol{\binom{n+r-1}{r} = \frac{n^{\overline{r}}}{r!}}$	$\{\odot,\ominus\}, \{\odot,\otimes\}, \{\ominus,\otimes\}$ $\boldsymbol{\binom{n}{r} = \frac{n^{\underline{r}}}{r!}}$

Bemerkungen: im Feld ungeordnet / mit Wiederholungen sind mit $\{\ldots\}$ nicht Mengen gemeint, sondern **Multimengen** (d. h. Elemente können mit Multiplizitäten in $\mathbb{Z}_{\geqslant 0}$ auftreten).
Hier ist noch eine gebräuchliche Notation: $\left(\!\binom{n}{r}\!\right) := \binom{n+r-1}{r}$.

Inklusion-Exklusion

Satz Seien $A_1, \ldots, A_n$ endliche Mengen. Für $\varnothing \neq I \subseteq [n] := \{1, \ldots, n\}$ setzen wir

$$N(I) := \left| \bigcap_{i \in I} A_i \right|.$$

Für $k \in [n]$ setzen wir

$$\alpha_k := \sum_{I \in \binom{[n]}{k}} N(I).$$

[Zur Erinnerung: $\binom{[n]}{k}$ ist die Menge der k-elementigen Teilmengen von $\{1, \ldots, n\}$.] Dann gilt

$$\left|A_1 \cup \cdots \cup A_n\right| = \alpha_1 - \alpha_2 + \alpha_3 - + \cdots + (-1)^{n+1}\alpha_n. \qquad (*)$$

Beweis Sei $a \in A_1 \cup \cdots \cup A_n$. Wir setzen $I_a := \left\{ i \in [n] \;\middle|\; a \in A_i \right\}$. Aus der Definition ist sofort klar, dass für $\varnothing \neq I \subseteq [n]$ gilt

$$a \in \bigcap_{i \in I} A_i \iff I \subseteq I_a. \qquad (**)$$

Wir zeigen nun, dass der Beitrag von a zur rechten Seite von $(*)$, welche ausgeschrieben

$$\sum_{k=1}^{n} (-1)^{k+1} \sum_{I \in \binom{[n]}{k}} \left| \bigcap_{i \in I} A_i \right| \qquad (***)$$

lautet, gleich 1 ist. Der Beitrag von a zu $\left| \bigcap_{i \in I} A_i \right|$ ist gleich 1, falls $a \in \bigcap_{i \in I} A_i$, und 0 sonst, also wegen $(**)$ ist der Beitrag 1 für $I \subseteq I_a$ und 0 sonst. Der Gesamtbeitrag von a zu $(***)$ ist also

$$\sum_{k=1}^{n} (-1)^{k+1} \sum_{I \in \binom{I_a}{k}} 1 = \sum_{k=1}^{n} (-1)^{k+1} \left| \binom{I_a}{k} \right| = 1 - \underbrace{\sum_{k=0}^{n} (-1)^k \binom{|I_a|}{k}}_{= (1-1)^{|I_a|} = 0, \text{ da } |I_a| > 0} = 1.$$

■

Korollar Seien $A_1, \ldots, A_n \subseteq X$, X eine endliche Menge. Dann ist

$$\left|X - (A_1 \cup \cdots \cup A_n)\right| = |X| - \alpha_1 + \alpha_2 - + \cdots + (-1)^n \alpha_n$$

($\alpha_1, \ldots, \alpha_n$ wie im Satz).

Wie lässt sich die Potenzreihenentwicklung einer in $x = 0$ definierten rationalen Funktion bestimmen?

Gegeben sei also eine rationale Funktion der Form $\dfrac{p(x)}{q(x)}$ mit $p(x), q(x) \in \mathbb{C}[x]$ und $q(0) \neq 0$. Ausserdem sei o. B. d. A. $q(0) = 1$ (wegen $q(0) \neq 0$ können wir sonst das Zähler- und das Nennerpolynom mit $1/q(0)$ multiplizieren).

Beispiel: $\dfrac{p(x)}{q(x)} = \dfrac{90x^4 - 159x^3 + 71x^2 - 13x + 2}{18x^3 - 21x^2 + 8x - 1} = \dfrac{-90x^4 + 159x^3 - 71x^2 + 13x - 2}{-18x^3 + 21x^2 - 8x + 1}$.

- Polynomdivision $\rightsquigarrow \dfrac{p(x)}{q(x)} = r(x) + \dfrac{s(x)}{q(x)}$ wobei $r(x), s(x) \in \mathbb{C}[x]$ mit $\deg s(x) < \deg q(x)$.

  Beispiel: $\dfrac{p(x)}{q(x)} = \dfrac{-90x^4 + 159x^3 - 71x^2 + 13x - 2}{-18x^3 + 21x^2 - 8x + 1} = 5x - 3 + \dfrac{1 - 16x + 32x^2}{1 - 8x + 21x^2 - 18x^3}$.

- Faktorisierung von $q(x)$:

  $$q(x) = (1 - \alpha_1 x)^{m_1} \ \ldots \ (1 - \alpha_l x)^{m_l},$$

  wobei $\alpha_1, \ldots, \alpha_l \in \mathbb{C}^\times$ paarweise verschieden sind ($\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_l}$ sind die Nullstellen von $q(x)$ mit Vielfachheiten $m_1, \ldots, m_l$).

  Beispiel: $1 - 8x + 21x^2 - 18x^3 = (1 - 2x)(1 - 3x)^2$.

- Ansatz

  $$\frac{s(x)}{q(x)} = \frac{u_1(x)}{(1 - \alpha_1 x)^{m_1}} + \cdots + \frac{u_l(x)}{(1 - \alpha_l x)^{m_l}}, \qquad (*)$$

  wobei $u_1(x), \ldots, u_l(x) \in \mathbb{C}[x]$ mit $\deg u_i(x) < m_i$ $(i = 1, \ldots, l)$. Wie lassen sich die Polynome $u_1(x), \ldots, u_l(x)$ bestimmen? Antwort: Multipliziere $(*)$ mit $q(x)$ und mache Koeffizientenvergleich.

  Beispiel: $\dfrac{1 - 16x + 32x^2}{1 - 8x + 21x^2 - 18x^3} = \dfrac{A}{1 - 2x} + \dfrac{Bx + C}{(1 - 3x)^2}$

  $\rightsquigarrow \ 1 - 16x + 32x^2 = (A + C) + (-6A + B - 2C)x + (9A - 2B)x^2$

  $$\rightsquigarrow \left|\begin{array}{rrrr} 1 = & A & + & C \\ -16 = & -6A + & B & - 2C \\ 32 = & 9A & - 2B & \end{array}\right| \rightsquigarrow \ (A, B, C) = (4, 2, -3).$$

- Aus der bekannten Formel

  $$\frac{1}{(1 - \alpha x)^m} = \sum_{n=0}^{\infty} \binom{m + n - 1}{m - 1} \alpha^n x^n$$

  erhalten wir die gesuchte Potenzreihenentwicklung:

  $$\frac{p(x)}{q(x)} = r(x) + u_1(x) \sum_{n=0}^{\infty} \binom{m_1 + n - 1}{m_1 - 1} {\alpha_1}^n x^n + \cdots + u_l(x) \sum_{n=0}^{\infty} \binom{m_l + n - 1}{m_l - 1} {\alpha_l}^n x^n,$$

  woraus sich nun die Koeffizienten a_n in $\dfrac{p(x)}{q(x)} = \displaystyle\sum_{n=0}^{\infty} a_n x^n$ ablesen lassen.

  Beispiel: $\dfrac{90x^4 - 159x^3 + 71x^2 - 13x + 2}{18x^3 - 21x^2 + 8x - 1} = 5x - 3 + \dfrac{4}{1 - 2x} + \dfrac{2x - 3}{(1 - 3x)^2}$

  $$= 5x - 3 + 4 \sum_{n=0}^{\infty} \binom{n}{0} 2^n x^n + (2x - 3) \sum_{n=0}^{\infty} \binom{n + 1}{1} 3^n x^n$$

  $$= 5x - 3 + \sum_{n=0}^{\infty} \big(2^{n+2} x^n + 2 \cdot 3^n (n + 1) x^{n+1} - 3^{n+1} (n + 1) x^n\big).$$

  Wir lesen ab:

  $$a_n = \begin{cases} -2 & \text{für } n = 0, \\ -3 & \text{für } n = 1, \\ 2^{n+2} + 2 \cdot 3^{n-1} n - 3^{n+1}(n + 1) & \text{für } n \geqslant 2. \end{cases}$$

3. Bipartite Graphen, Sätze von König und Hall

Eine Teilmenge $M \subseteq E$ der Kantenmenge eines Graphen $G = (V, E)$ heisst Matching, wenn keine zwei Kanten aus M eine gemeinsame Ecke haben.

Eine Teilmenge $C \subseteq V$ der Eckenmenge eines Graphen $G = (V, E)$ heisst überdeckende Eckenmenge, wenn für jede Kante $e = \{v_1, v_2\} \in E$ gilt $v_1 \in C$ oder $v_2 \in C$ (oder beide in C).

Klar: $|M| \leqslant |C|$.

Bipartite Graphen auf einer Eckenmenge $V = P \dot\cup Q$ sind so, dass alle Kanten von der Form $\{p, q\}$ mit $p \in P$ und $q \in Q$ sind.

Bemerkung: Für einen Graphen G sind die folgenden Aussagen äquivalent.

- G ist bipartit.
- G ist 2-färbbar.
- G enthält keinen Kreis ungerader Länge.

Satz [König 1931] Gegeben sei ein bipartiter Graph G. Seien M ein Matching in G mit $|M|$ maximal und C eine überdeckende Eckenmenge in G mit $|C|$ minimal. Dann gilt $|M| = |C|$.

Beweis. Mit Max-Flow Min-Cut Theorem.

Satz [Hall 1935 „Heiratssatz“] Ein bipartiter Graph $G = (P \dot\cup Q, E)$ hat genau dann ein Matching M mit $|M| = |P|$, wenn jede Teilmenge $U \subseteq P$ die Bedingung $|U| \leqslant |N(U)|$ erfüllt, wobei $N(U) \subseteq Q$ die Menge der Ecken bezeichnet, welche zu (mindestens) einer Ecke in U benachbart sind. (Wie immer ist G endlich.)

Beweis. „$\Rightarrow$“ klar.
„$\Leftarrow$“ (Kontraposition) Sei M ein Matching mit $|M|$ maximal, aber $|M| < |P|$. Nach dem Satz von König gibt es eine überdeckende Eckenmenge $C = P' \cup Q'$, wobei $P' \subseteq P$ und $Q' \subseteq Q$, mit $|C| = |M| < |P|$.
Die Endecken der in $P - P'$ beginnenden Kanten sind alle in Q' enthalten, weil C eine überdeckende Eckenmenge ist. In Formeln: $N(P - P') \subseteq Q'$. Es folgt

$$|P - P'| = |P| - |P'| > |C| - |P'| = |P' \cup Q'| - |P'| = |Q'| \geqslant |N(P - P')|.$$

Für $U = P - P'$ ist also die Bedingung $|U| \leqslant |N(U)|$ nicht erfüllt. ■

Zuerst noch eine Erläuterung zum Beweis des Satzes von König. Ich habe Ihnen vorgeführt, wie sich ein Matching M in einem bipartiten Graphen $G = (P \dot\cup Q, E)$ mit $|M|$ maximal finden lässt. Das geht nämlich so: Man betrachtet das Netzwerk $N = (\vec{G}, c, s, t)$. Dabei ist $\vec{G} = \big(\{s\} \dot\cup P \dot\cup Q \dot\cup \{t\}, A\big)$ der gerichtete Graph mit der Menge der Bögen

$$A = \big\{(s,p) \bigm| p \in P\big\} \cup \big\{(p,q) \bigm| p \in P,\, q \in Q,\, \{p,q\} \in E\big\} \cup \big\{(q,t) \bigm| q \in Q\big\}$$

und der konstanten Kapazitätsfunktion $c(a) = 1$ für alle $a \in A$. Sei nun f ein Fluss mit $\mathrm{val}(f)$ maximal. (So einen Fluss können Sie mit dem Markierungsalgorithmus konstruieren.) Das zugehörige Matching ist

$$M = \big\{\{p,q\} \bigm| p \in P,\, q \in Q,\, f\big((p,q)\big) = 1\big\}.$$

Ich habe Ihnen dann gesagt, dass sich eine überdeckende Eckenmenge C mit $|C|$ minimal aus dem Schnitt (S_f, T_f) zum Fluss f ablesen lässt. Das soll hier noch etwas ausführlicher erklärt werden.

Wir setzen $C := (P - S_f) \cup (Q \cap S_f)$. Sei nun $\{p,q\} \in E$ mit $p \in P \cap S_f$ und $q \in Q$. Gemäss der Definition von S_f gibt es also einen unvollständigen zunehmenden Weg bezüglich f von der Quelle s zur Ecke p.

- Falls $f\big((p,q)\big) = 0$, so lässt sich dieser unvollständige zunehmende Weg bezüglich f bis zur Ecke q verlängern, d. h. es gilt $q \in S_f$.
- Falls $f\big((p,q)\big) = 1$, so wird p bei der Konstruktion von S_f auf einem Rückwärtsbogen erreicht, und zwar auf dem Bogen (p,q), denn das ist der einzige von p ausgehende Bogen mit Fluss 1. Es gilt also auch hier $q \in S_f$.

Fazit: $\{p,q\} \in E$ mit $p \in P \cap S_f$ und $q \in Q \Rightarrow q \in Q \cap S_f$.
Deshalb ist $C = (P - S_f) \cup (Q \cap S_f)$ eine überdeckende Eckenmenge des ursprünglich gegebenen bipartiten Graphen G.

Schliesslich soll noch $|C| = |M|$ nachgewiesen werden. Wir müssen bloss $|C| \leqslant |M|$ zeigen, da sowieso $|M| \leqslant |C|$ gilt.

- Für jede Ecke $p \in P - S_f$ gilt (wegen $s \in S_f$) $f\big((s,p)\big) = 1$. Da in der Ecke p die Kirchhoff-Regel erfüllt sein muss, gibt es genau einen von p ausgehenden Bogen (p,q) mit $f\big((p,q)\big) = 1$, also $\{p,q\} \in M$. Für die Endecke $q \in Q$ gilt $q \in Q - S_f$, denn wäre $q \in Q \cap S_f$, so könnten wir wegen $f\big((p,q)\big) = 1$ einen unvollständigen zunehmenden Weg bezüglich f von der Quelle s zur Ecke q bis p verlängern; aber $p \notin S_f$.
- Für jede Ecke $q \in Q \cap S_f$ gilt (wegen $t \notin S_f$) $f\big((q,t)\big) = 1$. Da in der Ecke q die Kirchhoff-Regel erfüllt sein muss, gibt es genau einen in q ankommenden Bogen (p,q) mit $f\big((p,q)\big) = 1$, also $\{p,q\} \in M$. (Für die Anfangsecke $p \in P$ gilt $p \in P \cap S_f$.)

Damit haben wir eine injektive Abbildung $C \to M$ gefunden und $|C| \leqslant |M|$ gezeigt.