

Kombinatorische und diskrete Mathematik

Ulrich Faigle



Download free books at

bookboon.com

Ulrich Faigle

Kombinatorische und diskrete Mathematik

Kombinatorische und diskrete Mathematik
© 2012 Ulrich Faigle & Ventus Publishing ApS
ISBN 978-87-403-0130-4

Inhalt

	Vorwort	6
1	Elementares Zählen	8
1	Die natürlichen Zahlen	8
2	Die fundamentalen Zählprinzipien	10
2	Polynomalgebra	34
1	Der Binomialsatz	34
2	Division mit Rest	41
3	Ringe	44
1	Halbgruppen und Ringe	44
2	Restklassen und endliche Körper	50
4	Potenzreihen	58
1	Formale Potenzreihen	58
2	Erzeugende Funktionen	62
3	Rekursionen	64
4	Asymptotische Eigenschaften	76

Wenn ein **Server** für Sie kein Wassersportler ist...

IT-Jobs bei Lidl
it-bei-lidl.com

trendence
2015
DEUTSCHLANDS
100
Top-Arbeitgeber IT

LIDL



5	Inzidenzalgebra	81
1	Möbiusfunktion und -Funktion	83
2	Möbiusinversion und Siebformel	88
3	Eulercharakteristik und Kettenkomplexe	93
4	Planare Graphen	95
6	Netzwerke	102
1	Der Algorithmus von Ford und Fulkerson	105
2	Anwendungen	110
7	Der Greedy-Algorithmus	122
	Literaturverzeichnis	131

EY
Building a better working world

**So müsste er
aussehen: unser
Firmenwagen
für Einsteiger.**

www.de.ey.com/karriere
[#BuildersWanted](https://twitter.com/BuildersWanted)

„EY“ und „wir“ beziehen sich auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited, einer Gesellschaft mit beschränkter Haftung nach englischem Recht. ED None.



Vorwort

*Weisst du, wieviel Sternlein stehen
an dem blauen Himmelszelt?
Weisst du, wieviel Wolken gehen
weit hinüber alle Welt?
Gott, der Herr, hat sie gezählet,
dass ihm auch nicht eines fehlet
an der ganzen grossen Zahl.*

Kinderlied¹

*Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk*

Grundlage der Mathematik²

Das Zählen von Gegenständen gleicher Art, die Suche also nach der Anzahl von Objekten eines bestimmten Typs, ist die elementarste mathematische Tätigkeit. Gezählt wird grundsätzlich mit natürlichen und ganzen Zahlen, auch wenn die Mathematik den Zahlbegriff zu allgemeineren algebraischen Strukturen erweitert hat, um Typen von Objekten unter vereinheitlichenden Gesichtspunkten behandeln zu können. Es gibt viele Zählprobleme, die auch heute noch nicht befriedigend gelöst werden können. Der momentane Entwicklungsstand der Mathematik und Informatik, so gewaltig er sein mag, reicht nicht aus, um alle kombinatorischen Probleme zu beherrschen. Dennoch hat sich inzwischen ein Grundkanon von Zähltechniken mit Hilfe von Gruppen, Ringen, Polynomen, Potenzreihen und Inzidenzalgebren herauskristallisiert, in den hier eingeführt werden soll.

Die klassische Kombinatorik ist motiviert durch die Frage, wieviele Objekte man erhalten kann, wenn man gewisse gegebene Grundbausteine in zulässiger Weise miteinander "kombiniert". Bei ihr steht deshalb die Frage nach der *Anzahl* im Vordergrund, die am liebsten aus einer geschickten Formel zu gewinnen wäre. Es hat sich jedoch immer mehr gezeigt, dass schon die Frage nach der *Existenz* oder der *Konstruktion* von (mindestens) einem Objekt mit vorgegebenen kombinatorischen Eigenschaften alles andere als trivial ist. Dieser Aspekt hat zur Entwicklung einer neuen Disziplin, der *kombinatorischen* (oder *diskreten*) *Optimierung* geführt, die neben die traditionelle Kombinatorik getreten ist, diese ergänzt und erweitert. Die beiden letzten Kapitel behandeln diskrete algorithmische Grundstrukturen auf der Basis des Modells von sog. *Flüssen* in Graphen (oder Netzwerken) und dem sog. *Greedy-Algorithmus*, den beiden grundlegenden algorithmischen Prinzipien der diskreten Mathematik und Informatik schlechthin.

Ein Wort zum Thema Graphen in der Kombinatorik. Viele Kombinatoriker betreiben *Graphentheorie*, d.h. sie untersuchen Eigenschaften abstrakter Graphen *an sich*. In der vorliegenden Einführung liefern Graphen vor allem eine mathematische

1 W. HEY (1789-1854)

2 L. KRONECKER (1823-1891)

Modellsprache, um kombinatorische Strukturen zu untersuchen. "Reine Graphentheorie" wird deshalb hier stiefmütterlich behandelt. Den diesbezüglich interessierten Leser verweisen wir auf die Fülle spezieller Lehrbücher zur Graphentheorie (z.B. die im Literaturverzeichnis genannten Texte [2] und [5]).

Beim Leser werden keine speziellen kombinatorischen Vorkenntnisse erwartet. Allerdings sollten mathematische Grundkenntnisse in der linearen Algebra und der reellen Analysis vorhanden sein. Ebenso sollte der Leser mit der mathematischen Standardnotation der Mengenlehre und der Vektor- und Matrixrechnung vertraut sein, da diese nicht extra erklärt wird.

Die mit "EX." gekennzeichneten Abschnitte haben den Charakter von Übungen *und* von Beispielen. Sie dienen dazu, den Stoff inhaltlich zu verdeutlichen und zu vertiefen. Generell ist die Darstellung in dieser Einführung so gehalten, dass sie vom Leser aktive Mitarbeit verlangt. Alle Argumente sind zwar (hoffentlich) vollständig. Die Ausarbeitung von Details wird aber oft dem Leser überlassen. Wer mehr (auch ausgearbeitete) Übungsaufgaben sucht, der sei insbesondere auf das schöne Buch von Lovász [8] hingewiesen, das eine detaillierte und breite Einführung in die Kombinatorik zum aktiven Selbststudium bietet.

Vom Stoffumfang her entspricht diese Einführung einer einsemestrigen, vierstündigen mathematischen Vorlesung mit Übungen, wie sie vom Autor an der Universität zu Köln angeboten wird.

Köln, Frühjahr 2012

Ulrich Faigle

1 Elementares Zählen

Obwohl das Rechnen mit reellen und insbesondere rationalen und ganzen Zahlen dem Leser als bekannt voraussetzt wird, wird nochmals auf die natürlichen und ganzen Zahlen eingegangen, die nicht nur die Grundlage aller Zahlbereiche und allen Zählens sondern auch allen mathematischen Argumentierens und Konstruierens schlechthin sind.

1 Die natürlichen Zahlen

1.1. Natürliche Induktion und Rekursion. Die Mathematik geht davon aus, dass es (mindestens) eine *induktive Menge* gibt, d.h. eine Menge U mit den Eigenschaften

- (A) $\emptyset \in U$;
 (S) Für jede Menge x gilt: $x \in U \implies x \cup \{x\} \in U$.

Das Element \emptyset ist die *leere Menge*. Das Element $\text{succ}(x) := x \cup \{x\}$ ist der sog. *Nachfolger* des Elements x in der induktiven Menge U . Die beiden Eigenschaften (A) („Induktionsanfang“) und (S) („Induktionsschritt“) formulieren das Prinzip der natürlichen Induktion. Jede induktive Menge U enthält zumindest die Elemente

$$\emptyset, \text{succ}(\emptyset) = \emptyset \cup \{\emptyset\}, \text{succ}(\text{succ}(\emptyset)) = \emptyset \cup \{\emptyset\} \cup \{\emptyset \cup \{\emptyset\}\}, \dots$$

Man definiert nun induktiv die *natürlichen Zahlen*

$$\begin{aligned} 0 &:= \emptyset \\ n + 1 &:= \text{succ}(n) \end{aligned}$$

Deren Menge $\mathbb{N} := \{0, 1, \dots, n, n + 1, \dots\}$ ist somit die kleinste induktiv geordnete Menge, die es gibt.

Induktionsbeweise. Die natürliche Induktion ist ein Beweisprinzip für die Gültigkeit einer Aussage A über natürliche Zahlen³:

$$\boxed{A(0) \wedge (A(n) \implies A(n + 1)) \implies \{x \in \mathbb{N} \mid A(x)\} = \mathbb{N} .}$$

Das heisst in Worten:

- *Trifft die Aussage A auf die natürliche Zahl 0 zu („ $A(0)$ “) und folgt allgemein $A(n+1)$ aus $A(n)$, dann trifft die Aussage A auf sämtliche natürlichen Zahlen zu.*

Ein *Induktionsbeweis* bzgl. einer Aussage A geht deshalb so vor:

³ das Symbol „ \wedge “ bezeichnet hier den logischen Operator „und“

- (0) Man beweist die Richtigkeit von A für die natürliche Zahl 0, d.h. man verifiziert die Aussage $A(0)$.
- (i) Dann zeigt man, dass aus der Gültigkeit von A für eine Zahl n notwendigerweise auch die Gültigkeit von A für ihren Nachfolger $n + 1$ folgen würde (d.h. $A(n) \Rightarrow A(n + 1)$).
- (ii) Man schliesst dann, dass die Aussage A auf jede natürliche Zahl zutrifft.

Rekursion. Mit dem Induktionsprinzip lassen sich Aussagen über natürliche Zahlen beweisen. Ebenso lassen sich mit dem Induktionsprinzip mathematische Operationen und Ausdrücke *rekursiv* definieren. Jede rekursive Definition ist von ihrer Natur her konstruktiv und gestattet es, einen so definierten Ausdruck in endlich vielen Rechenschritten explizit auszuwerten.

Zum Beispiel ist die Addition einer Zahl $m \in \mathbb{N}$ mit einer Zahl $n \in \mathbb{N}$ rekursiv folgendermassen erklärt:

$$\begin{aligned} \text{(A)} \quad m + 0 &:= m. \\ \text{(S)} \quad m + (n + 1) &:= (m + n) + 1. \end{aligned}$$

Nach der Addition kann auch die *Multiplikation* rekursiv eingeführt werden:

$$\begin{aligned} \text{(A)} \quad m \cdot 0 &:= 0. \\ \text{(S)} \quad m \cdot (n + 1) &:= (m \cdot n) + m. \end{aligned}$$

BEMERKUNG. Aus diesen Definitionen ergeben sich die üblichen Regeln für das Rechnen mit natürlichen Zahlen. Diese setzen wir allerdings, wie oben schon gesagt, als bekannt voraus und leiten sie deshalb hier nicht nochmals ab.

Der Ausdruck $n!$ (ausgesprochen: „*n* faktät“) ist so definiert:

$$\begin{aligned} \text{(A)} \quad 0! &:= 1. \\ \text{(S)} \quad n! &:= n \cdot (n - 1)!. \end{aligned}$$

Diese rekursive Definition beinhaltet die Rechenanweisung

$$n! = 1 \cdot 2 \cdot \dots \cdot (n - 1)n \quad (\text{für } n \geq 1).$$

Rekursiv lassen sich ebenso Ausdrücke definieren, die von mehreren Parametern abhängen. Die *Binomialkoeffizienten* $\binom{n}{k}$ sind z.B. rekursiv so definiert:

$$\begin{aligned} \text{(P}_1\text{)} \quad \binom{n}{0} &:= 1 \quad \text{und} \quad \binom{n}{n} := 1 \quad \text{für alle } n = 0, 1, 2, \dots \\ \text{(P}_2\text{)} \quad \binom{n}{k} &:= \binom{n-1}{k-1} + \binom{n-1}{k} \quad \text{für } 1 \leq k \leq n - 1. \end{aligned}$$

Die in (P_1) und (P_2) implizierte Rechenanweisung besagt, dass man zeilenweise das folgende *Pascal'sche Dreieck* aufbaut, bis man zu dem gewünschten Term $\binom{n}{k}$ gekommen ist. Der Term in einer Zeile ergibt sich „gema“ss (P_2) als die Summe der beiden Terme direkt in der Zeile darüber:

4 B. PASCAL (1623-1662)

der Vereinigungsmenge fortsetzen, indem wir einfach weiterzählen. Für endliche Mengen M und K ergibt sich also das (wichtige!) Zählprinzip

$$(2) \quad \boxed{M \cap K = \emptyset \implies |M \cup K| = |M| + |K|.$$

Das *direkte Produkt* der Menge M mit einer (nichtleeren) endlichen Menge ist rekursiv so definiert:

$$(A) \quad M \times \{k_1\} := \{(m, k_1) \mid m \in M\}.$$

$$(S) \quad M \times \{k_1, k_2\} := (M \times \{k_1\}) \cup (M \times \{k_2\}).$$

Aus (2) ergibt sich nun

$$|M \times \{k_1, k_2\}| = |M \times \{k_1\}| + |M \times \{k_2\}| = |M| \cdot 2$$

und allgemein das Zählprinzip

$$(3) \quad \boxed{|M \times K| = |M| \cdot |K|,$$

da die Rekursion des direkten Produkts ja mit der rekursiven Definition der Multiplikation natürlicher Zahlen übereinstimmt (vgl. Lemma 1.1).



MEINE TO DO'S

- Wohnung suchen
- Mit Mama zu IKEA fahren
- Stundenplan erstellen
- Nebenjob auf Jobmensa.de finden

Entdecke jetzt deutschland's größtes Jobportal für Studenten

Per Induktion lassen sich diese Argumente ohne Mühe auf disjunkte Vereinigungen oder direkte Produkte mehrerer Mengen verallgemeinern. Wir kommen auf diese Weise zu den *fundamentalen Zählprinzipien*:

(FZP₁) Sind M_1, \dots, M_n endliche disjunkte Mengen, dann gilt:
 $|M_1 \cup M_2 \cup \dots \cup M_n| = |M_1| + |M_2| + \dots + |M_n|.$
 (FZP₂) Sind M_1, \dots, M_n beliebige endliche Mengen, dann gilt:
 $|M_1 \times M_2 \times \dots \times M_n| = |M_1| \times |M_2| \times \dots \times |M_n|.$

Aus (FZP₁) gewinnt man sofort ein abgeschwächtes (aber oft nützliches) Zählprinzip in folgender Situation: Wir nehmen an, dass eine Menge M von $|M| \geq 1$ Objekten in $r \geq 1$ nichtleere und paarweise disjunkte Teilmengen M_1, \dots, M_r aufgeteilt wird. Dann gilt:

(4) Mindestens ein M_i ist so gross, dass $r \cdot |M_i| \geq |M|$ erfüllt ist.

In der Tat erhielten wir ja sonst den Widerspruch

$$r|M| = r(|M_1| + \dots + |M_r|) = r|M_1| + \dots + r|M_r| < r|M|.$$

BEMERKUNG. Die Regel (4) ist als *Schubfachprinzip* bekannt. Man stellt sich vor, dass n Objekte in r Schubfächer abgelegt werden. Dann muss eines der Fächer mindestens n/r Objekte enthalten.

2.1. Gewichtetes und doppeltes Zählen. Die fundamentalen Zählprinzipien (FZP₁) und (FZP₂) lassen sich auf gewichtete Mengen erweitern. Dabei verstehen wir unter einer *Gewichtung* der Menge M eine reellwertige Funktion

$$w : M \rightarrow \mathbb{R},$$

die jedem $i \in M$ ein *Gewicht* $w(i)$ zuweist. Um (FZP₁) zu verallgemeinern, definieren wir

$$w(S) := \sum_{i \in S} w(i) \quad \text{für jede Teilmenge } S \subseteq M.$$

Dann beobachtet man für beliebige $S, T \subseteq M$ die sog. *modulare Gleichung*

(5) $w(S) + w(T) = w(S \cup T) + w(S \cap T).$

Man macht sich nämlich z.B.

$$w(S) = \sum_{i \in S} w(i) = \sum_{j \in S \setminus T} w(j) + \sum_{k \in S \cap T} w(k) = w(S \setminus T) + w(S \cap T)$$

leicht klar, da $S \setminus T$ und $S \cap T$ disjunkte Mengen sind. Daraus folgt dann

$$w(S) + w(T) - w(S \cap T) = w(S \setminus T) + w(T) = w(S \cup T)$$

und somit die Gleichung (5). Bzgl. (FZP₂) betrachten wir $M = M_1 \times M_2$ und eine Gewichtung $w : M \rightarrow \mathbb{R}$. Da bei endlichen Summen die Summanden in beliebiger Reihenfolge addiert werden dürfen, ergibt sich

$$(6) \quad \boxed{\sum_{i \in M_1} \left(\sum_{j \in M_2} w(i, j) \right) = \sum_{(i, j) \in M} w(i, j) = \sum_{j \in M_2} \left(\sum_{i \in M_1} w(i, j) \right)}$$

BEMERKUNG. In (6) wird die Summe $w(M)$ aller Gewichte auf zwei verschiedene Arten ermittelt. Deshalb verkörpert (6) das sog. *Prinzip des doppelten Zählens*.

EX. 1.1. Man zeige:

- a) Unter der speziellen Gewichtung $w : M \cup K \rightarrow \mathbb{R}$ mit $w(i) = 1$ für alle $i \in M \cup K$, erhält man (2) aus (5).
- b) Unter der speziellen Gewichtung $w : M \times K \rightarrow \mathbb{R}$ mit $w(i, j) = 1$ für alle $(i, j) \in M \times K$ erhält man (3) aus (6).

2.2. Anwendungen der Zählprinzipien. Wir wollen die Zählprinzipien nun auf einige kombinatorische Grundstrukturen anwenden.

Abbildungen. Es seien R und M (beliebige) Mengen. Jede Abbildung (Funktion) $f : M \rightarrow R$ kann man als einen (möglicherweise unendlichen) Parametervektor mit den Komponenten $f_i = f(i)$ auffassen:

$$f \longleftrightarrow (f_i \mid i \in M).$$

Deshalb notiert man die Menge dieser Abbildungen auch als

$$R^M := \{f : M \rightarrow R\}.$$

Im Fall $r = |R| < \infty$ und $n = |M| < \infty$ hat man somit die Entsprechung

$$f \in R^M \longleftrightarrow (f_i \mid i \in M) \in R \times \dots \times R = R^n$$

und folgert mit dem Zählprinzip (FZP₂):

$$(7) \quad |R^M| = |R|^{|M|} = r^n .$$

Indikatorfunktionen. Im Fall $R = \{0, 1\}$ entspricht jede Funktion $f \in R^M$ eindeutig einer Teilmenge von M :

$$f \in \{0, 1\}^M \iff F = \{i \in M \mid f(i) = 1\}.$$

Man nennt f dann die Indikator- oder Inzidenzfunktion der Teilmenge $F \subseteq M$. Ist $n = |M| < \infty$, so besagt (7), dass es 2^n Indikatorfunktionen gibt. Also findet man:

LEMMA 1.2. Eine endliche Menge M besitzt genau $2^{|M|}$ Teilmengen.

Permutationen. Eine *Permutation*⁷ der Menge M ist eine bijektive Abbildung $\pi : M \rightarrow M$. Im endlichen Fall $M = \{m_1, \dots, m_n\}$ schreiben wir abkürzend auch $\pi_i = \pi(m_i)$ und stellen π durch seine (abgekürzte) Wertetafel dar:

$$(8) \quad \begin{array}{c|c|c|c|c} \pi & m_1 & m_2 & \dots & m_n \\ \hline & \pi_1 & \pi_2 & \dots & \pi_n \end{array} \iff \pi = \pi_1 \pi_2 \dots \pi_n .$$

Eine Permutation π bringt also die Elemente von M in eine andere Reihenfolge.

⁷ *permutare* (lat.) vertauschen

strategy&

Bewirb Dich bis zum 18. Oktober 2015.

DATA EMERGENCY

&

7.-9. November 2015, Berlin

Gesundheitsbranche in der Datenkrise!
Deine innovativen Ideen und Strategien zum Thema e-Health sind gefragt.
Entwickle gemeinsam mit Strategy&-Beratern Hightech-Strategien für eine gesunde Zukunft.

Mehr Informationen unter www.strategyand.pwc.com/DBTAcademy

pwc

© 2015 PwC. All rights reserved.
PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.
Please see www.pwc.com/structure for further details.



Diese Definition ist vielleicht intuitiv einleuchtend – *aber nicht rekursiv!* Rekursiv kann man Permutationen endlicher Mengen so definieren:

- (1) Im Fall $M = \emptyset$ ist $\pi = \emptyset$ eine Permutation.
- (2) Im Fall $|M| \geq 1$ ist das Paar $\pi = (a, \pi')$ eine Permutation, wenn a ein (beliebiges) Element von M und π' eine Permutation von $M' = M \setminus \{a\}$ ist.

Aus der rekursiven Definition erhalten wir sofort die Anzahl $P(n)$ aller Permutationen einer n -elementigen Menge über die Rekursion

- (1) $P(0) = 1$ für $n = 0$.
- (2) $P(n) = nP(n - 1)$ für $n = 1, 2, \dots$

Diese stimmt mit der Rekursion der Fakultäten überein. Also gilt:

$$P(n) = n! \quad \text{für alle } n \in \mathbb{N}.$$

NOTATION. Die Permutation $\pi = (a, \emptyset)$ schreibt man $\pi = a$. Auch allgemeiner lässt man Klammern weg und schreibt statt $\pi = (a, \pi')$ einfach $\pi = a\pi'$ und kommt dann zu einer Darstellung wie in (8).

BEMERKUNG. Permutationen unendlicher Mengen kann man nicht so einfach rekursiv definieren (und deshalb auch nicht so einfach zählen).

Zykeln. Eine Permutation π der (endlichen) n -elementigen Menge M heisst *zyklisch*, wenn zu jedem $a \in M$ die Elemente

$$a, \pi(a), \pi^2(a) = \pi(\pi(a)), \dots, \pi^{n-1}(a) = \pi(\pi^{n-2}(a))$$

alle verschieden sind. Ist z.B. für ein gewisses k die Zahl $m > k$ minimal mit der Eigenschaft $\pi^m(a) = \pi^k(a)$, dann ist

$$\zeta = \pi^k(a)\pi^{k+1}(a) \dots \pi^{m-1}(a)$$

eine zyklische Permutation der Menge

$$M_\zeta = \{\pi^k(a), \dots, \pi^{m-1}(a)\}$$

und heisst *Zykel* von π . Die Zahl $\ell(\zeta) = |M_\zeta| = m - k$ ist die sog. Länge des Zyklus ζ .

Die Einschränkung von π auf das Komplement $M \setminus M_\zeta$ ist wieder eine Permutation (von $M \setminus M_\zeta$). Wenn man darauf wieder die obige Konstruktion anwendet und so fortfährt, findet man schliesslich:

LEMMA 1.3. Sei π eine Permutation der endlichen Menge $M \neq \emptyset$. Dann zerfällt M in paarweise disjunkte nichtleere Teilmengen M_1, \dots, M_k derart, dass die Einschränkung von π auf M_i eine zyklische Permutation von M_i (d.h. ein Zykel von π) ist für alle $i = 1, \dots, k$.

BEMERKUNG. Ein Element $a \in M$ mit $\pi(a) = a$ heisst *Fixpunkt* von π . Fixpunkte bilden also Zykeln der Länge 1.

Stirlingzahlen erster Art. Der Parameter $s(n, k)$ bezeichnet die Anzahl aller Permutationen einer n -elementigen Menge mit genau k Zykeln und heisst *Stirlingzahl 1. Art*⁸. Wir erhalten (nach Definition und dem Zählprinzip (FZP₁)):

$$n! = P(n) = \sum_{k=1}^n s(n, k) \quad (n \geq 1).$$

Allgemein hat man $s(n, k) = 0$ im Fall $k > n$ (da eine n -elementige Menge nicht in mehr als n paarweise disjunkte nichtleere Teilmengen zerfallen kann). Daraus ergibt sich eine rekursive Berechnung dieser Stirlingzahlen analog zur Art des Pascalschen Dreiecks:

- (1) $s(0, 0) = 1$.
- (2) $s(n, 0) = 0$, wenn $n \geq 1$.
- (3) $s(n, k) = s(n-1, k-1) + (n-1)s(n-1, k)$, wenn $n, k \geq 1$.

Die ersten beiden dieser Regeln sind klar. Zum Beweis der dritten hält man ein $a \in M$ fest und unterscheidet zwischen der Menge aller Permutationen bei denen a ein Fixpunkt ist und der Menge aller Permutationen, bei denen a kein Fixpunkt ist.

Dann gibt es in der ersten Menge $s(n-1, k-1)$ Permutationen mit genau k Zykeln (inklusive a). Permutationen mit k Zykeln vom zweiten Typ konstruiert man so: Man wählt eine Permutation π' mit k Zykeln bzgl. der Grundmenge $M' = M \setminus \{a\}$ und fügt nun a in einen Zyklus ein, indem man es vor ein Element des Zyklus stellt. Dafür gibt es $|M'| = n-1$ Möglichkeiten. Die Summe dieser Möglichkeiten kommt in (3) zum Ausdruck.

k -Permutationen. Wir verallgemeinern Permutationen und definieren *k -Permutationen* von Mengen M rekursiv so:

- (1) $\pi = \emptyset$ ist eine 0-Permutation von M .
- (2) Im Fall $k \geq 1$ ist $\pi = a\pi'$ eine k -Permutation von M , wenn $a \in M$ gilt und π' eine $(k-1)$ -Permutation von $M' = M \setminus \{a\}$ ist.

Analog zur Notation von Permutationen schreiben wir k -Permutationen in der Form

$$\pi = \pi_1 \pi_2 \dots \pi_k.$$

Sei $P(n, k)$ die Anzahl von k -Permutationen einer n -elementigen Menge. Dann gilt rekursiv:

8 J. STIRLING (1692-1770)

- (1) $P(n, k) = 0$, wenn $n < k$;
- (2) $P(n, 0) = 1$, für alle n ;
- (3) $P(n, k) = nP(n-1, k-1)$ für $1 \leq k \leq n$.

Daraus ergibt sich:

LEMMA 1.4. $P(n, k) = n(n-1) \dots (n-k+1)$ gilt für alle $n, k \in \mathbb{N}$. Insbesondere ist

$$P(n, k) = \frac{P(n)}{P(n-k)} = \frac{n!}{(n-k)!}, \quad \text{wenn } k \leq n.$$

EX. 1.2 (Injektionen). Seien K, M Mengen mit $|K| = k$ und $|M| = n$. Wir nehmen $k \leq n$ und $K = \{1, 2, \dots, k\}$ an und betrachten die Menge $\text{Inj}(K, M)$ aller injektiven Abbildungen $\pi : K \rightarrow M$. Mit der Bezeichnung $\pi_i = \pi(i)$ sieht man leicht, dass jedes $\pi \in \text{Inj}(K, M)$ einer k -Permutation entspricht. Also ist die Anzahl der injektiven Abbildungen:

$$|\text{Inj}(K, M)| = P(n, k) = \frac{|M|!}{(|M| - |K|)!}.$$

EX. 1.3. Für jede endliche Menge M ist $\text{Inj}(M, M)$ genau die Menge aller Bijektionen (bzw. Permutationen) von M .



Calling for Berlin

Technology Advisory kennenlernen



Consulting hautnah erleben
 5.-7. November 2015
www.deloitte.com/de/calling-for-berlin

© 2015 Deloitte Consulting GmbH

Faktorielle. Allgemein definiert man zu einer (beliebigen) reellen Zahl $\alpha \in \mathbb{R}$ und natürlichen Zahl $k \in \mathbb{N}$ die fallenden Faktoriellen als

$$(\alpha)_k := \alpha(\alpha - 1) \dots (\alpha - k + 1) \quad (\text{mit } (\alpha)_0 := 1).$$

Bei der Wahl $\alpha \in \mathbb{N}$ erhält man also $(\alpha)_k = P(\alpha, k)$. Analog sind die steigenden Faktoriellen definiert:

$$(\alpha)^k = \alpha(\alpha + 1) \dots (\alpha + k - 1).$$

Zwischen den fallenden und den steigenden Faktoriellen besteht offenbar der folgende Zusammenhang:

$$\boxed{(\alpha)^k = (-1)^k (-\alpha)_k}$$

Teilmengen. Sei $\Pi(n, k)$ die Menge aller (n, k) -Permutationen der n -Menge M und $S \subseteq M$ eine k -elementige Teilmenge.

Mit $\Pi_S(n, k)$ bezeichnen wir die Menge aller (n, k) -Permutationen, die nur Elemente aus S benutzen. Damit erhalten wir $\Pi(n, k)$ als Vereinigung paarweise disjunkter Mengen:

$$\Pi(n, k) = \bigcup_{\substack{S \subseteq M \\ |S|=k}} \Pi_S(n, k).$$

Wegen $|\Pi_S(n, k)| = P(k, k) = k!$, ergibt sich nach dem Zählprinzip (FZP):

$$(9) \quad (n)_k = |\Pi(n, k)| = \sum_{\substack{S \subseteq M \\ |S|=k}} |\Pi_S(n, k)| = \sum_{\substack{S \subseteq M \\ |S|=k}} k! = k! \sum_{\substack{S \subseteq M \\ |S|=k}} 1 = k! C(n, k),$$

wobei der Term

$$(10) \quad C(n, k) = \sum_{\substack{S \subseteq M \\ |S|=k}} 1$$

die k -elementigen Teilmengen von M zählt. Die Gleichung (9) kann man nun auflösen und erkennt die $C(n, k)$ als die Binomialkoeffizienten, die man rekursiv aus dem Pascalschen Dreieck berechnet:

LEMMA 1.5. Die Anzahl aller k -elementigen Teilmengen einer n -elementigen Grundmenge M ist

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

und man hat

$$2^n = \sum_{k=0}^n C(n, k) = \sum_{k=0}^n \binom{n}{k}.$$

Urnenmodelle. Wir nehmen k verschiedene Urnen U_1, \dots, U_k als gegeben an. Über diese seien n Kugeln zu verteilen. Ist u_i die Anzahl der Kugeln in U_i , dann haben wir

$$n = u_1 + u_2 + \dots + u_k.$$

Wieviele Möglichkeiten gibt es, n so in k natürliche Zahlen u_i aufzuteilen?

1. VARIANTE: Alle Urnen enthalten mindestens eine Kugel (d.h. $u_i \geq 1$).

Es muss $n \geq k \geq 1$ gelten. Wir reihen die Kugeln nebeneinander und verteilen $k - 1$ Trennstäbe auf die $n - 1$ Lücken:

$$\circ \circ \dots \circ \mid \circ \dots \circ \circ \mid \dots \mid \circ \circ \dots \circ \circ.$$

Urne U_1 enthält die Kugelmenge bis zum ersten Trennstab. U_2 die Kugeln zwischen dem ersten und dem zweiten Trennstab usw. Also ist die gesuchte Anzahl der Möglichkeiten gleich der, unter den $n - 1$ Lücken eine Teilmenge von $k - 1$ Lücken auszuwählen, d.h.

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

2. VARIANTE: Es darf auch leere Urnen geben (d.h. $u_i \geq 0$).

Wir verteilen $n + k$ Kugeln gemäss Variante 1:

$$n + k = u'_1 + u'_2 + \dots + u'_k \quad (u'_i \geq 1)$$

und setzen $u_i = u'_i - 1$ für $i = 1, \dots, k$. Dann erhalten wir eine Verteilung nach Variante 2:

$$n = u_1 + u_2 + \dots + u_k \quad (u_i \geq 0).$$

Die Zuordnung gilt auch umgekehrt. Also ist die Anzahl der Verteilungen nach Variante 2:

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

Partitionen. Unter einer k -Partition der Menge M versteht man eine Familie $\Pi = \{B_1, \dots, B_k\}$ von k nichtleeren und paarweise disjunkten Mengen B_p , die M überdecken:

- (1) $B_i \neq \emptyset$ für $i = 1, \dots, k$;
- (2) $B_i \cap B_j = \emptyset$ für $i \neq j$;
- (3) $M = B_1 \cup \dots \cup B_k$.

Wird k nicht spezifiziert, so redet man einfach von einer *Partition* Π . Die Mengen B_i sind die *Blöcke* von Π . Zum Beispiel induzieren die Zykeln ζ einer Permutation eine Partition der Grundmenge M in die Blöcke M_ζ .

Stirlingzahlen zweiter Art und Bellzahlen. Die Anzahl aller k -Partitionen einer n -Menge wird mit $S(n; k)$ bezeichnet und heisst *Stirlingzahl 2. Art*. Die Gesamtzahl aller Partitionen ist die sog. *Bellzahl*⁹

$$(11) \quad B(n) = \sum_{k=0}^n S(n, k),$$

9 E.T. BELL (1883-1960)

Mein Wissen rund um Big Data und SAP möchte ich sinnvoll einsetzen. Bin ich bei euch richtig, E.ON?

Lieber Herr Bennett, mit Ihren Fachkenntnissen können Sie bei uns viel bewegen.

Bringen Sie Ihr Know-how in zukunftsweisende Projekte und Applikationen ein: Ob bei der energetischen Vernetzung von Smart Homes, der Steuerung virtueller Kraftwerke oder der Realisierung anspruchsvoller Logistik-Konzepte – der Energiesektor bietet vielfältige Herausforderungen für IT-Consultants, -Architekten und -Projektmanager. Entfalten Sie Ihre Kompetenz und geben Sie Ihrer Karriere neue Impulse.

Ihre Energie gestaltet Zukunft.

top ARBEITGEBER DEUTSCHLAND 2015
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

e.on

www.eon-karriere.com



wobei wir $B(0) = S(0; 0) := 1$ setzen. Rekursiv kann man die Stirlingzahlen 2. Art so berechnen:

- (1) $S(0, 0) := 1$;
- (2) $S(n, 0) = 0$ für $n \geq 1$;
- (3) $S(0, k) = 0$ für $k \geq 1$;
- (4) $S(n, k) = S(n - 1, k - 1) + kS(n - 1, k)$ sonst.

Auf die Gleichung (4) kommt man, wenn man ein festes Element $a \in M$ betrachtet und die k -Partitionen danach unterscheidet, ob $\{a\}$ ein Block ist oder nicht:

Es gibt $S(n - 1, k - 1)$ k -Partitionen, bei denen $\{a\}$ ein Block ist. Die übrigen k -Partitionen ergeben sich, indem man eine k -Partition der $(n - 1)$ -Menge $M' = M \setminus \{a\}$ bildet und dann a in einen der k Blöcke einfügt. Also hat man $kS(n - 1; k)$ solcher k -Partitionen.

Surjektionen. Es seien $K = \{1, \dots, k\}$ und $M = \{1, \dots, n\}$ zwei endliche Mengen und $f: M \rightarrow K$ eine surjektive Abbildung. Dann sind die Urbilder $f^{-1}(i) = \{j \in M \mid f(j) = i\}$ die Blöcke eine k -Partition von M :

Umgekehrt gibt es zu einer gegebenen k -Partition Π von M $k!$ viele Surjektionen $f: M \rightarrow K$ mit $\Pi(f) = \Pi$, da jede Permutation der k Bilder Surjektivität erhält. Also hat die Menge $Surj(M; K)$ aller Surjektionen die Mächtigkeit

$$|Surj(M, K)| = k!S(n, k).$$

Mit $n = |M|$ und $r = |R|$ rechnet man nun allgemein:

$$\begin{aligned} (12) \quad r^n &= |R^M| = \sum_{K \subseteq R} |Surj(M, K)| = \sum_{k=0}^r \sum_{|K|=k} |Surj(M, K)| \\ &= \sum_{k=0}^r \binom{r}{k} k!S(n, k) = \sum_{k=0}^n S(n, k)(r)_k, \end{aligned}$$

da es im Fall $k > n$ sicher keine k -Partition von M gibt.

Harmonische Zahlen. Wir illustrieren das Prinzip des doppelten Zählens anhand der sog. harmonischen Zahlen. Sei t_n die Anzahl der Teiler der natürlichen Zahl $n \geq 1$. Eine einfache Formel für t_n ist schwierig aufzustellen, da t_n sehr vom Typ von n abhängt und z.B. keinesfalls monoton in n ist (vgl. Ex. 1.4).

EX. 1.4. Bekanntlich lässt sich jede natürliche Zahl $n \geq 1$ als ein Produkt paarweise verschiedener Primzahlen p_j mit Potenzen e_j ausdrücken:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}.$$

Man zeige: $t_n = (e_1 + 1)(e_2 + 1) \dots (e_k + 1)$

Insbesondere hat man z.B. $t_8 = 4, t_9 = 3, t_{10} = 4, t_{11} = 2, t_{12} = 6$.

Wir suchen eine Formel für die *durchschnittliche* Anzahl

$$\bar{t}(n) := \frac{t_1 + t_2 + \dots + t_n}{n}$$

der Teiler. Dazu definieren wir für alle $1 \leq i, j \leq n$ die Gewichte

$$w_{ij} := \begin{cases} 1 & i \text{ teilt } j, \\ 0 & i \text{ teilt } j \text{ nicht.} \end{cases}$$

Damit haben wir

$$t_j := \sum_{i=1}^n w_{ij} = \text{Anzahl der Teiler von } j$$

$$v_i := \sum_{j=1}^n w_{ij} = \text{Anzahl der Vielfachen } \leq n \text{ von } i = \lfloor n/i \rfloor,$$

wobei $\lfloor a \rfloor$ die grösste ganze Zahl $\leq a$ bezeichne. Das Prinzip des doppelten Zählens führt auf

$$\sum_{j=1}^n t_j = \sum_{j=1}^n \left(\sum_{i=1}^n w_{ij} \right) = \sum_{i=1}^n \left(\sum_{j=1}^n w_{ij} \right) = \sum_{i=1}^n v_i$$

und somit auf

$$\bar{t}(n) = \frac{v_1 + v_2 + \dots + v_n}{n} = \frac{1}{n} (\lfloor n/1 \rfloor + \lfloor n/2 \rfloor + \dots + \lfloor n/n \rfloor).$$

Wegen $\lfloor n/i \rfloor \leq n/i \leq \lfloor n/i \rfloor + 1$ erhalten wir approximativ

$$(13) \quad \bar{t}(n) \sim H_n \quad \text{bzw.} \quad |\bar{t}(n) - H_n| \leq 1,$$

wobei

$$(14) \quad H_n := 1 + 1/2 + 1/3 + \dots + 1/n$$

die sog. *n*te harmonische Zahl ist. (H_n ist im allgemeinen keine(!) natürliche Zahl.)

BEMERKUNG. Aus der Annäherung des Integrals durch Riemannsche Summen gewinnt man die Approximation

$$H_n \sim \int_1^n \frac{1}{x} dx = \log n .$$

In diesem Sinn sagt man: „Im Durchschnitt“ hat eine natürliche Zahl n etwa $\log n$ viele Teiler.

Ramseyzahlen. Wir beschreiben nun eine Anwendung des Schubfachprinzips. Mit dem kann man zwar keine genauen Anzahlen dingfest machen, weil man die Schubfächer, die viele Elemente enthalten, im allgemeinen im voraus nicht explizit kennt. Dennoch liefert dieses Prinzip oft überraschend einfache Nachweise der Existenz bestimmter kombinatorischer Strukturen. Wir illustrieren dies am Beispiel des Satzes von Ramsey¹⁰.

Dazu betrachten wir eine endliche Menge N mit $n = |N|$ Elementen und schreiben abkürzend für die Menge aller 2-elementigen Teilmengen

$$E_n = \binom{N}{2} := \{e \subseteq N \mid |e| = 2\} .$$

Unter einer (rot / blau)-Färbung der Menge E_n verstehen wir eine Abbildung

10 F.P. RAMSEY (1903-1930)

1 Ziel:
 Du entwickelst unsere Zukunft.
 Wir Deine.

IT-Traineeprogramm

In 18 Monaten durchläufst Du 3 verschiedene Stationen, wirst von einer Führungskraft als Mentor betreut und profitierst von einem breiten Seminarangebot. Anschließend kannst Du eine Fach- oder Führungslaufbahn einschlagen.

www.perspektiven.allianz.de

Allianz Karriere

Allianz



$$c : E_n \rightarrow \{r, b\}.$$

Wir nennen ein $e \in E_n$ rot „bzw. „blau“ je nach dem, ob $c(e) = r$ oder $c(e) = b$ gilt. Wir nennen eine Teilmenge $U \subseteq N$ rot (bzw. blau), wenn jede 2-elementige Teilmenge $e \subseteq U$ rot (bzw. blau) gefärbt ist.

Wir sagen, die natürliche Zahl n habe die *Ramsey-Eigenschaft* $R(p, q)$, falls folgende Aussage richtig ist:

$R(p, q)$: Zu jeder Färbung $c : E_n \rightarrow \{r, b\}$ existiert entweder eine rote Menge $U \subseteq N$ der Mächtigkeit $|U| = p$ oder eine blaue Menge $V \subseteq N$ der Mächtigkeit $|V| = q$ (oder beides).

Wir wollen beweisen:

SATZ 1.1 (Ramsey). Für alle natürlichen Zahlen $p, q \geq 2$ gibt es eine kleinste Zahl $r(p, q) \in \mathbb{N}$ mit der Eigenschaft

$$n \geq r(p, q) \implies n \text{ besitzt die Eigenschaft } R(p, q).$$

Die Zahl $r(p, q)$ des Satzes 1.1 heisst *Ramseyzahl*. Man überzeugt sich leicht:

$$r(p, 2) = p \quad \text{und} \quad r(2, q) = q \quad \text{gilt für alle } p, q \geq 2.$$

Zur Untersuchung des allgemeinen Falls nehmen wir an, dass die Ramseyzahlen $r(p-1, q)$ und $r(p, q-1)$ existieren. Wir wählen

$$n \geq 2 \cdot \max\{r(p-1, q), r(p, q-1)\}$$

und ein Element $a \in N$. Nach dem Schubfachprinzip enthält die Menge

$$E_n^a := \{e \in E_n \mid a \in e\}$$

entweder $n/2$ rote oder $n/2$ blaue Elemente. Nehmen wir an, dass $n/2$ Elemente rot sind (bei blau würden wir analog argumentieren) und setzen

$$N^a := \{u \in N \setminus \{a\} \mid c(\{a, u\}) = r\}.$$

Wegen $|N^a| \geq r(p-1, q)$ gibt es entweder eine blaue Teilmenge $V \subseteq N^a$ mit $|V| = q$ oder eine rote Teilmenge $U' \subseteq N^a$ mit $|U'| = p-1$ (sodass $U = U' \cup \{a\}$ eine rote Teilmenge von N mit $|U| = p$ ist). Auf jeden Fall haben wir somit erkannt:

$$r(p, q) \leq 2 \cdot \max\{r(p-1, q), r(p, q-1)\}$$

BEMERKUNG. Man sieht leicht ein: $r(3; 3) = 6$. Im allgemeinen sind die exakten Werte der Ramseyzahlen $r(p; q)$ nur in wenigen Fällen bekannt. Zum Beispiel kennt man für $r(4; 6)$ und $r(5; 5)$ nur die Schranken

$$35 \leq r(4, 6) \leq 41 \quad \text{bzw.} \quad 43 \leq r(5, 5) \leq 49.$$

EX. 1.5. In einer zufällig ausgewählten Gruppe von $n \geq 6$ Menschen gibt es immer entweder (mindestens) 3 Leute, die sich gegenseitig kennen, oder (mindestens) 3 Leute, die sich gegenseitig unbekannt sind.

Das Spiel Sims. Beim Spiel SIMS auf der Menge $N = \{1; 2; 3; 4; 5; 6\}$ gibt es 2 Spieler ("Rot" und "Blau"), die alternierend die Elemente von E_6 rot bzw. blau färben. Verloren hat der Spieler, der als erster eine 3-elementige Teilmenge $U \subseteq N$ in seiner Farbe produziert. (Wegen $r(3; 3) = 6$ wissen wir, dass das Spiel nicht unentschieden ausgehen kann.)

FRAGE: Würden Sie bei diesem Spiel lieber als anziehender Spieler beginnen oder als zweiter Spieler auftreten?

(Wer diese Frage als zu trivial empfindet, kann SIMS natürlich leicht mit anderen Ramseyparametern verallgemeinern.)

2.3. Die symmetrische Gruppe. Die Menge S_M aller Permutationen (Bijektionen) der endlichen Menge M trägt eine natürliche algebraische Struktur, da Bijektionen umkehrbar sind und Hintereinanderausführungen von Bijektionen wieder Bijektionen ergeben. In diesem Sinn ist S_M eine Gruppe und heisst *symmetrische Gruppe*.

Der *Stabilisator* einer Teilmenge $A \subseteq M$ ist definiert als die Menge aller Bijektionen, die A festhalten (d.h. A auf sich selber abbilden):

$$\mathcal{S}(A) := \{\pi \in S_M \mid \pi(A) = A\}.$$

Wir bezeichnen mit π^{-1} die Umkehrabbildung von π und mit $\sigma \tau$ die Hintereinanderausführung der Bijektionen σ und τ . Dann haben wir

$$\sigma^{-1} \in \mathcal{S}(A) \quad \text{und} \quad \sigma\tau \in \mathcal{S}(A) \quad \text{für alle } \sigma, \tau \in \mathcal{S}(A).$$

In diesem Sinn ist auch $\mathcal{S}(A)$ eine Gruppe. Eine Permutation $\pi \in \mathcal{S}(A)$ entspricht einem Paar (π', π'') von Permutationen $\pi' \in S_A$ und $\pi'' \in S_{M \setminus A}$, die auf A und $M \setminus A$ unabhängig voneinander wirken. Also finden wir gemäss (FZP₂):

$$(15) \quad |\mathcal{S}(A)| = |S_A| \cdot |S_{M \setminus A}| = |A|!(|M| - |A|)!$$

Die Bahn (in S_M) einer Permutation $\zeta \in S_M$ unter $\mathcal{S}(A)$ ist die Menge

$$\zeta\mathcal{S}(A) := \{\zeta\sigma \mid \sigma \in \mathcal{S}(A)\} \subseteq S_M.$$

Die Abbildung $\sigma \mapsto \zeta\sigma$ ist injektiv. Denn:

$$\zeta\sigma = \zeta\tau \iff \sigma = \zeta^{-1}\zeta\sigma = \zeta^{-1}\zeta\tau = \tau.$$

Folglich gilt

$$|\zeta\mathcal{S}(A)| = |\mathcal{S}(A)| = |A|!(|M| - |A|)! \quad \text{für jedes } \zeta \in \mathcal{S}_M.$$

LEMMA 1.6. Für je zwei Permutationen $\zeta, \omega \in \mathcal{S}_M$ gilt

$$\zeta\mathcal{S}(A) = \omega\mathcal{S}(A) \iff \zeta\mathcal{S}(A) \cap \omega\mathcal{S}(A) \neq \emptyset.$$

Beweis. Die Richtung „ \Rightarrow “ ist klar. Umgekehrt schliessen wir im Fall $\zeta\sigma = \omega\tau$ mit $\sigma, \tau \in \mathcal{S}(A)$:

$$\tau\sigma^{-1} \in \mathcal{S}(A) \implies \zeta = \omega\tau\sigma^{-1} \in \omega\mathcal{S}(A)$$

und folglich (wegen der Gleichheit der Mengen $\mathcal{S}(A) = \{\tau\sigma^{-1} \mid \sigma \in \mathcal{S}(A)\}$)

$$\omega\mathcal{S}(A) = \{\omega\tau\sigma^{-1} \mid \tau \in \mathcal{S}(A)\} = \{\zeta\tau \mid \tau \in \mathcal{S}(A)\} = \zeta\mathcal{S}(A).$$

Wegen $\zeta \in \zeta\mathcal{S}(A)$ liefern die Bahnen somit eine Partition von \mathcal{S}_M in





Sind Sie bereit für IBM?

Lieben Sie Herausforderungen?

Möchten Sie innovative Lösungen für führende Unternehmen entwickeln?

Wollen Sie dem weltweit größten Beratungsunternehmen angehören?

Entdecken Sie Ihre vielfältigen Karrieremöglichkeiten. IBM ist auf der Suche nach den besten und hellsten Köpfen. Nach Menschen, die Möglichkeiten entdecken, wo andere nur Probleme sehen. Nach Mitarbeitern, die auch Mitgestalter sein wollen. Wir suchen diese Menschen aus dem Anspruch heraus, die Welt täglich ein bisschen besser zu machen. Sie sind ideengetrieben, zukunftsorientiert und möchten schon heute an den Lösungen von morgen arbeiten? Dann sollten wir uns kennenlernen!

Machen wir den Planeten ein bisschen smarter.
ibm.com/start/de

Alle Bezeichnungen, die in der männlichen Sprachform verwendet werden, schließen sowohl Frauen als auch Männer ein. IBM schafft ein offenes und tolerantes Arbeitsklima und ist stolz darauf, ein Arbeitgeber zu sein, der für Chancengleichheit steht. IBM, das IBM Logo und ibm.com sind Marken oder eingetragte Marken der International Business Machines Corp. in den Vereinigten Staaten und/oder anderen Ländern. Andere Namen von Firmen, Produkten und Dienstleistungen können Marken oder eingetragte Marken ihrer jeweiligen Inhaber sein. © 2010 IBM Corp. Alle Rechte vorbehalten.



$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (\text{mit } n = |M| \text{ und } k = |A|)$$

verschiedene Blöcke der Mächtigkeit $k!(n-k)!$.

EX. 1.6. Sei $M = \{1, \dots, n\}$. Im Fall $A = \emptyset$ oder $A = M$ haben wir $S(A) = S_M$ und erhalten S_M als die einzige Bahn bzgl. $S(A)$. Im Fall $A_1 = \{1\}$ gibt es n Bahnen bzgl. $S(A)$. Wir betrachten die n zyklischen Permutationen

$$\begin{aligned} \rho^0 &= 123 \dots (n-1)n \\ \rho^1 &= 234 \dots (n-1)n1 \\ \rho^2 &= 345 \dots (n-1)n12 \\ &\vdots \\ \rho^{n-1} &= n12 \dots (n-2)(n-1). \end{aligned}$$

Dann sind die n verschiedenen Bahnen:

$$S(A_1) = \rho^0 S(A_1), \rho^1 S(A_1), \dots, \rho^{n-1} S(A_1).$$

Spernertheorie. Sei M eine n -elementige Menge, die wir ohne Beschränkung der Allgemeinheit als $M = \{1, 2, \dots, n\}$ annehmen. \mathcal{F} sei ein System von Teilmengen $F \subseteq M$. Dazu definieren wir die Teilsysteme

$$\mathcal{F}_i := \{F \in \mathcal{F} \mid |F| = i\} \quad (i = 0, 1, \dots, n)$$

und setzen $f_i := |\mathcal{F}_i|$. Das *Profil* von \mathcal{F} ist dann der Kardinalitätenvektor

$$f = (f_0, f_1, \dots, f_n).$$

In der allgemeinen *Spernertheorie*¹¹ interessiert man sich dafür, wie gross eine Mengenfamilie \mathcal{F} sein kann, wenn sie bestimmte Eigenschaften haben muss.

Zum Beispiel nennt man \mathcal{F} eine *Spernerfamilie* (oder *Antikette*), wenn \mathcal{F} die Eigenschaft hat, dass keine Menge eine andere echt enthält, d.h. dass für alle $F, G \in \mathcal{F}$ die folgende Implikation gilt:

$$F \subseteq G \implies F = G.$$

Haben z.B. alle Mengen in \mathcal{F} die gleiche Mächtigkeit, dann ist \mathcal{F} eine Spernerfamilie (s. auch Satz 1.2).

11 E. SPERNER (1905-1980)

Die allgemeine LYM-Ungleichung. Seien die Mengen $A_i \subseteq M$ definiert als

$$A_0 = \emptyset \quad \text{und} \quad A_i := \{1, 2, \dots, i\} \quad (i = 1, \dots, n).$$

Wir schreiben allgemein kurz $S_i = S(A_i)$ und halten nun einen Parameter t mit $0 \leq t \leq n$ fest. Sei i irgendeine natürliche Zahl mit $t \leq i \leq n$. Wir betrachten die Bilder von A_i unter Permutationen, die A_t fixieren, d.h.

$$\mathcal{W}_i^t := \{\sigma(A_i) \mid \sigma \in \mathcal{S}_t\}$$

und ebenso die verschiedenen Bilder von A_i unter Permutationen, die A_t fixieren:

$$\mathcal{A}_i^t := \{\tau(A_i) \mid \tau \in \mathcal{S}_i\}.$$

Wir finden:

$$w_i^t := |\mathcal{W}_i^t| = \binom{n-t}{i-t} \quad \text{und} \quad a_i^t := |\mathcal{A}_i^t| = \binom{i}{t}.$$

Sei $\mathcal{R} \subseteq \mathcal{S}_M$ eine Menge von Permutationen derart, dass

$$\mathcal{S}_M = \bigcup_{\rho \in \mathcal{R}} \rho \mathcal{S}_t.$$

Sei nun \mathcal{F} ein nichtleeres System von Teilmengen von M und (wie oben)

$$\mathcal{F}_i = \{F \in \mathcal{F} \mid |F| = i\} \quad \text{und} \quad f_i := |\mathcal{F}_i|.$$

Für jedes $F \in \mathcal{F}_i$, $\rho \in \mathcal{R}$ und $\pi \in \mathcal{S}_M$ definieren wir den *Inzidenzkoeffizienten*

$$\lambda(F, \rho, \pi) := \begin{cases} 1 & \text{wenn } F = \pi(\rho(A_i)), \\ 0 & \text{sonst.} \end{cases}$$

Sei $t \leq m \leq n$ beliebig (aber fest gewählt). Wir sagen, \mathcal{F} habe die Eigenschaft (Σ_t) , falls für jede Permutation $\pi \in \mathcal{S}_M$ gilt:

$$(\Sigma_t) \quad \sum_{\rho \in \mathcal{R}} \sum_{i=t}^m \sum_{F \in \mathcal{F}_i} \frac{\lambda(F, \rho, \pi)}{a_i^t} \leq 1.$$

Nach dem Prinzip des doppelten Zählens (Summationsvertauschung) beobachten wir:

LEMMA 1.7. Für alle $0 \leq t \leq m \leq n$ gilt:

$$(\Sigma_t) \implies \sum_{i=t}^m \frac{f_i}{w_i^t} \leq 1$$

Beweis. Zu jedem $F \in \mathcal{F}_i$ und $\rho \in \mathcal{R}$ gibt es $(n-i)!$ viele Permutationen $\pi \in \mathcal{S}_M$ derart, dass $\lambda(F, \rho, \pi) = 1$. Da \mathcal{S}_M von Bahnen $\rho \mathcal{S}_t$ mit $\rho \in \mathcal{R}$ überdeckt wird, haben wir

$$|\mathcal{R}| \geq \binom{n}{t}.$$

Wir schliessen somit aus (Σ_t) :

$$\begin{aligned} n! = \sum_{\pi \in \mathcal{S}_M} 1 &\geq \sum_{\pi \in \mathcal{S}_M} \sum_{\rho \in \mathcal{R}} \sum_{i=t}^m \sum_{F \in \mathcal{F}_i} \frac{\lambda(F, \rho, \pi)}{a_i^t} \\ &\geq \sum_{i=t}^m \sum_{F \in \mathcal{F}_i} \sum_{\rho \in \mathcal{R}} \sum_{\pi \in \mathcal{S}_M} \frac{\lambda(F, \rho, \pi)}{a_i^t} \\ &= \sum_{i=t}^m \sum_{F \in \mathcal{F}_i} \sum_{\rho \in \mathcal{R}} \frac{(n-i)!}{a_i^t} \\ &\geq \sum_{i=t}^m \sum_{F \in \mathcal{F}_i} \binom{n}{t} \frac{(n-i)!}{a_i^t} \\ &= \sum_{i=t}^m \binom{n}{t} \frac{f_i (n-i)!}{a_i^t} = n! \sum_{i=t}^m \frac{f_i}{w_i^t}. \end{aligned}$$

Wir betrachten zwei Spezialfälle von Lemma 1.7. Bei $t = 0$ ist

$$w_i^0 = \binom{n}{i} \quad \text{und} \quad a_i^0 = 1.$$

Es gibt nur die eine Bahn $\mathcal{S}_0 = \mathcal{S}_M$ bzgl. $t = 0$ (vgl. Ex. 1.6).

PROPOSITION 1.1 (Lubell/Yamamoto/Meshalkin). Für jede beliebige Spernerfamilie \mathcal{F} gilt die sog. LYM-Ungleichung:

$$(16) \quad \sum_{i=0}^n \frac{f_i}{\binom{n}{i}} \leq 1.$$

Beweis. Wir beobachten, dass es zu jedem $\pi \in \mathcal{S}_M$ höchstens ein $F \in \mathcal{F}$ geben kann mit $\lambda(F, \rho^0, \pi) = 1$. Denn $\lambda(F', \rho, \pi) = 1$ bedeutet

$$F = \pi(A_i) \quad \text{und} \quad F' = \pi(A_j)$$

für geeignete Indices i, j . Denn wäre z.B. $i < j$ und somit $A_i \subset A_j$, dann hätte man auch $F \subset F'$, was bei einer Spernerfamilie aber nicht sein kann! Ebenso schliesst man $j < i$ und folgert $i = j$. Also ist (Σ_t) erfüllt. (16) folgt deshalb direkt aus Lemma 1.7.

SATZ 1.2 (Sperner). Ist \mathcal{F} eine Spernerfamilie mit einer n -elementigen Grundmenge M , dann gilt

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}.$$

Insbesondere bildet die Menge aller Teilmengen $F \subseteq M$ der Kardinalität $|F| = \lfloor n/2 \rfloor$ eine maximale Spernerfamilie.

Beweis. Für alle $0 \leq k \leq n$ gilt

JETZT BEWERBUNG AUFPOLIEREN.

Bereiten Sie sich optimal auf den Bewerbungsprozess vor und geben Sie Ihrem Profil den letzten Schliff. Nutzen Sie unsere Tipps, Persönlichkeitstests und kostenlosen E-Books zu Studium, Business und Karriere.

rwe.com/Bewerberakademie

HIERMIT PRÄSENTIERE ICH:

MICH!

VORWEG GEHEN



$$\frac{\binom{n}{k+1}}{\binom{n}{k}} = \frac{n-k}{k+1} \begin{cases} \geq 1 & \text{falls } k < \lfloor n/2 \rfloor, \\ \leq 1 & \text{falls } k \geq \lfloor n/2 \rfloor. \end{cases}$$

Die Binomialkoeffizienten wachsen also mit k bis $k = \lfloor n/2 \rfloor$ und fallen dann. Also schliessen wir aus der LYM-Ungleichung:

$$|\mathcal{F}| = f_0 + f_1 + \dots + f_n \leq w_{\lfloor n/2 \rfloor} (f_0/w_0 + f_1/w_1 + \dots + f_n/w_n) \leq w_{\lfloor n/2 \rfloor}.$$

$w_{\lfloor n/2 \rfloor}$ ist also eine Obergrenze der Mächtigkeit einer Spernerfamilie. Sie wird von der Familie der Teilmengen $F \subseteq M$ der Kardinalität $|F| = \lfloor n/2 \rfloor$ erreicht.

Der Satz von Erdős, Ko und Rado. Sei \mathcal{F} eine Spernerfamilie mit der zusätzlichen Eigenschaft

$$F, F' \in \mathcal{F} \implies |F \cap F'| \geq 1 \quad \text{und} \quad |F|, |F'| \leq n/2.$$

Wir betrachten $t = 1$ und wählen $m = \lfloor n/2 \rfloor$. Dann ergibt sich

$$w_k^1 = \binom{n-1}{i-1} \quad \text{und} \quad \|a_i^1\| = i.$$

Für ein Repräsentantensystem \mathcal{R} bzgl. der S_1 -Bahnen wählen wir die zyklischen Permutationen ρ^k aus Ex. 1.6.

Wieviele Paare (F, ρ) mit $\lambda(F, \rho, \pi) = 1$ kann es zu einer festen Permutation π geben? Um die Frage zu beantworten, können wir π als die identische Permutation ι annehmen. Denn sonst betrachten wir einfach die äquivalente Spernerfamilie

$$\mathcal{F}_\pi = \{\pi^{-1}(F) \mid F \in \mathcal{F}\}$$

mit der Eigenschaft

$$\lambda(F, \rho, \pi) = 1 \iff \lambda(\pi^{-1}(F), \rho, \iota) = 1.$$

Unter der Annahme $\pi = \iota$ interessieren wir uns für die Mächtigkeit der Menge

$$\begin{aligned} \mathcal{A}^\lambda &:= \{F \in \mathcal{F} \mid \exists \rho \in \mathcal{R} : \lambda(F, \rho, \iota) = 1\} \\ &= \{F \in \mathcal{F} \mid F = \rho(A_i) \text{ für ein } \rho \in \mathcal{R} \text{ und } 1 \leq i \leq \lfloor n/2 \rfloor\}. \end{aligned}$$

Sei $i_\lambda := \min\{|F| \mid F \in \mathcal{A}^\lambda\}$. Wir behaupten

$$(17) \quad |\mathcal{A}^\lambda| \leq i_\lambda .$$

Um dies einzusehen, stelle man sich die Menge $M = \{1, \dots, n\}$ im Kreis angeordnet vor. Die Teilmengen der Form $F = \rho(A_i)$ sind nun Kreisintervalle der Länge $i \leq n/2$. Da $\mathcal{A}^\lambda \subseteq \mathcal{F}$ selber eine Spernerfamilie ist, überlappen sich alle Intervalle in \mathcal{A}^λ und besitzen folglich einen gemeinsamen Punkt

$$a \in \bigcap \{F \in \mathcal{A}^\lambda\}.$$

Ausserdem ist jedes Intervall schon durch seinen linken (und ebenso durch seinen rechten) Endpunkt eindeutig bestimmt (sonst wäre mindestens ein $F \in \mathcal{A}^\lambda$ in einem anderen $F' \in \mathcal{A}^\lambda$ enthalten!).

Sei $\overline{F} \in \mathcal{A}^\lambda$ minimal (d.h. $|\overline{F}| = i_\lambda$). Jedes andere Kreisintervall $F \in \mathcal{A}^\lambda$ hat entweder genau den linken oder genau den rechten Endpunkt in \overline{F} . Dieser liegt entweder links von $a \in \overline{F}$ oder rechts von a . Also gibt es höchstens $|\overline{F}|$ solcher Intervalle, wie in (17) behauptet.

Aus der Eigenschaft (17) folgt nun sofort

$$\sum_{i=1}^m \sum_{F \in \mathcal{F}_i} \frac{\lambda(F, \rho, \pi)}{a_i^t} \leq \sum_{i=1}^n \sum_{F \in \mathcal{F}} \frac{\lambda(F, \rho_j, \sigma)}{i_\lambda} = \frac{|\mathcal{A}^\lambda|}{i_\lambda} \leq 1 .$$

und damit die *Ungleichung von Bollobás*¹²:

$$(18) \quad \boxed{\sum_{i=1}^{\lfloor n/2 \rfloor} \frac{f_i}{\binom{n-1}{i-1}} \leq 1}$$

Der Spezialfall $\mathcal{F} = \mathcal{F}_k$ (d.h. $|\mathcal{F}| = f_k$) liefert daraus:

SATZ 1.3 (Erdős-Ko-Rado¹³). Sei \mathcal{F} eine Familie von k -elementigen Teilmengen der n -elementigen Menge M derart, dass $k \leq n/2$ und

$$F, F' \in \mathcal{F} \implies F \cap F' \neq \emptyset.$$

Dann gilt

12 B. BOLLOBÁS (*1943)

13 P. ERDÖS (1913-1996), CH. KO (1910-2002), R. RADO (1906-1989)

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

Eine im Sinne von Satz 1.3 extremale Mengenfamilie \mathcal{F} kann man leicht angeben: Man halte ein beliebiges Element $a \in M$ fest und wähle \mathcal{F} als die Menge aller Teilmengen $k \leq n/2$, der Kardinalität $k \leq n/2$, die a enthalten. \mathcal{F} ist eine Spernerfamilie von sich paarweise überschneidenden Mengen, deren Kardinalität $|\mathcal{F}|$ die Schranke von Erdős, Ko und Rado erreicht.

BEMERKUNG. Die klassische LYM-Ungleichung (16) lässt sich leicht auf Spernerfamilien \mathcal{F} linearer Unterräume eines endlichen Vektorraums verallgemeinern, wenn man das Profil so definiert:

$$f_i := \text{Anzahl der Teilräume } F \text{ mit } \dim F = i.$$

In wie weit die Bollobás-Ungleichung (18) und Satz 1.3 entsprechend verallgemeinert werden kann, ist eine offene Frage.

© 2013 Accenture. All rights reserved.

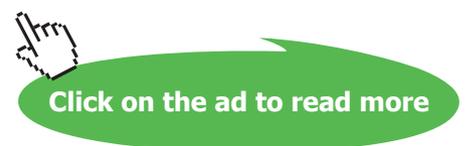
be > your degree

Bring your talent and passion to a global organization at the forefront of business, technology and innovation. Discover how great you can be.

Visit accenture.com/bookboon

Be greater than.
consulting | technology | outsourcing

accenture
High performance. Delivered.



2 Polynomialgebra

Unter einer (reellen) Polynom¹⁴funktion in den Variablen x_1, \dots, x_k versteht man eine Funktion $f : \mathbb{R}^k \rightarrow \mathbb{R}$ der Form

$$(19) \quad f(x_1, \dots, x_k) = \sum_{0 \leq i_1, \dots, i_k \leq n} a_{i_1 \dots i_k} x_1^{i_1} \dots x_k^{i_k}$$

mit $n \in \mathbb{N}$ und den Koeffizienten $a_{i_1 \dots i_k} \in \mathbb{R}$. Polynomfunktionen kann man addieren und miteinander multiplizieren, ohne den Bereich der Polynomfunktionen zu verlassen. In diesem Sinn sind Polynombereiche algebraische Verallgemeinerungen von Zahlbereichen. Zusätzlich können Polynome aber auch als Funktionen gesehen werden, die nach Substitutionen von reellen Zahlenwerten $\xi_i \in \mathbb{R}$ in die Variablen x_i des Polynomns dann konkrete reelle Zahlen

$$f(\xi_1, \dots, \xi_k) = \sum_{0 \leq i_1, \dots, i_k \leq n} a_{i_1 \dots i_k} \xi_1^{i_1} \dots \xi_k^{i_k}$$

produzieren. Ausserdem kann man noch ausnutzen, dass alle Ableitungen von Polynomfunktionen existieren (und selber wieder Polynomfunktionen sind).

Das Zusammenspiel der algebraischen und funktionellen Sichtweise von Polynomen führt oft zu eleganten Ableitungen von kombinatorischen Identitäten, d.h. funktionellen Beziehungen (bzw. "Formeln") für kombinatorische Zählgrößen.

1 Der Binomialsatz

Zu der Menge $M = \{1, \dots, n\}$ gesellen wir (reelle) Polynomfunktionen in den $2n$ Variablen $x_1, \dots, x_n, y_1, \dots, y_n$. Unter einem Binom¹⁵ verstehen wir ein Polynom der speziellen Form $b(x_i, y_i) = x_i + y_i$. Fundamental für die kombinatorische Zähltheorie ist der folgende Binomialsatz, der eigentlich nichts anders tut als das Produkt aller Binome ausmultiplizieren. Dabei benutzen wir die Kurzschreibweise für Produkte von Variablen zu beliebigen Indexteilmengen $S \subseteq M$:

$$x_S := \begin{cases} 1 & (S = \emptyset) \\ \prod_{i \in S} x_i & (S \neq \emptyset) \end{cases}$$

$$y_S := \begin{cases} 1 & (S = \emptyset) \\ \prod_{j \in S} y_j & (S \neq \emptyset). \end{cases}$$

SATZ 2.1 (Binomialsatz). *Es gilt die sog. Binomialidentität*

14 poly (griech.) Vorsilbe für „viele“

15 bi lat. Vorsilbe für „zwei“

$$(20) \quad \prod_{i \in M} (x_i + y_i) = \sum_{S \subseteq M} x_S y_{M \setminus S} .$$

Beweis. Wir argumentieren per Induktion über $n = |M|$ und stellen sofort fest, dass die behauptete Identität für $n = 0$ (d.h. $M = \emptyset$) trivialerweise richtig ist. Für den Induktionsschritt rechnet man:

$$\begin{aligned} (x_n + y_n) \prod_{i=1}^{n-1} (x_i + y_i) &= (x_n + y_n) \sum_{S \not\ni n} x_S y_{M \setminus (S \cup n)} \\ &= \sum_{S \not\ni n} x_n x_S y_{M \setminus (S \cup n)} + \sum_{S \not\ni n} x_S y_{M \setminus (S \cup n)} y_n \\ &= \sum_{S \ni n} x_S y_{M \setminus S} + \sum_{S \not\ni n} x_S y_{M \setminus S} \\ &= \sum_{S \subseteq M} x_S y_{M \setminus S} . \end{aligned}$$

1.1. Kombinatorische Identitäten. Durch Substitution reeller Zahlen in einige der Variablen x_i und y_i ergibt sich eine Fülle kombinatorischer Identitäten.

Beispiele. $y_1 = \dots = y_n = 1, x_1 = \dots = x_n = x$ und somit

$$x_S = x^{|S|} \quad \text{und} \quad y_S = 1 \quad \text{für alle } S \subseteq M .$$

Fasst man nach dieser Substitution in dem Summenausdruck der Binomialidentität (20) die Terme nach Potenzen von x zusammen, so ergibt sich die Identität

$$(x + 1)^n = \sum_{S \subseteq M} x^{|S|} = \sum_{k=0}^n C(n, k) x^k = \sum_{k=0}^n \binom{n}{k} x^k .$$

Daraus gewinnen wir mit $x = 1$ eine uns schon bekannte Identität:

$$2^n = \sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^n C(n, k)$$

Die Wahl $x = -1$ führt auf

$$0 = \sum_{k=0}^n (-1)^k C(n, k) \quad \text{bzw.:} \quad \sum_{k \text{ ungerade}} C(n, k) = \sum_{k \text{ gerade}} C(n, k) .$$

Das heisst:

- Es gibt genausoviele Teilmengen mit ungerader Mächtigkeit wie mit gerader Mächtigkeit.

Durch Ableiten der reellen differenzierbaren Funktion

$$f(x) = (x + 1)^n = \sum_{i=0}^n C(n, i)x^i$$

erhalten wir auch sofort eine explizite Formel für die Binomialkoeffizienten. Die k ten Ableitungen der beiden Seiten

$$\begin{aligned} \left(\frac{d}{dx}\right)^k (x + 1)^n &= n(n - 1) \dots (n - k + 1)(x + 1)^{n-k} \\ \left(\frac{d}{dx}\right)^k \sum_{i=0}^n C(n, i)x^i &= \sum_{i=k}^n i(i - 1) \dots (i - k + 1)C(n, i)x^{i-k} \end{aligned}$$

sind natürlich gleich. Für $x = 0$ bleibt im Summenausdruck der k ten Ableitung nur der Term mit $i = k$ übrig. Das ergibt die Gleichheit



McKinsey & Company

**Start
your
engines.**

McKinsey sucht Ingenieure.
Nutzen Sie Ihr Potenzial
und starten Sie durch.

Mehr auf mckinsey.de/ingenieure

$$n(n-1)\dots(n-k+1) = k(k-1)\dots(k-k+1)C(n, k)$$

und somit

$$C(n, k) = \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}.$$

1.2. Das Cauchy-Produkt. Die Multiplikation zweier Polynomfunktionen in der Variablen x ergibt wieder eine Polynomfunktion in der Variablen x :

$$\begin{aligned} & (p_0 + p_1x + \dots + p_nx^n)(q_0 + q_1x + \dots + q_mx^m) \\ &= p_0q_0 + (p_0q_1 + p_1q_0)x + (p_0q_2 + p_1q_1 + p_2q_0)x^2 + \dots \\ &= r_0 + r_1x + r_2x^2 + \dots + r_{n+m}x^{n+m}. \end{aligned}$$

Das Ausmultiplizieren und Zusammenfassen nach Potenzen von x zeigt sofort:

$$(21) \quad r_j = \sum_{i+k=j} p_i q_k \quad (j = 0, 1, \dots, n+m)$$

Der nach der Polynommultiplikationsregel (21) berechnete Koeffizientenvektor

$$(r_0, r_1, \dots, r_{n+m}) = (p_0, p_1, \dots, p_n) * (q_0, q_1, \dots, q_m)$$

ist als das *Cauchy¹⁶-Produkt* der Vektoren (p_0, \dots, p_n) und (q_0, \dots, q_m) bekannt.

Die Vandermondesche Identität. Aus der Produktregel (21) ergibt sich z.B. die *Vandermonde¹⁷sche Identität* (22). Seien nämlich $a, b \in \mathbb{N}$ beliebige natürliche Zahlen und $n = a + b$. Dann schliessen wir aus dem Binomialsatz:

$$\begin{aligned} \sum_{k=0}^{a+b} \binom{a+b}{k} x^k &= (x+1)^{a+b} = (x+1)^a (x+1)^b \\ &= \left(\sum_{i=0}^a \binom{a}{i} x^i \right) \cdot \left(\sum_{j=0}^b \binom{b}{j} x^j \right). \end{aligned}$$

Das Cauchy-Produkt besagt in diesem Fall:

16 A.L. CAUCHY (1789-1857)

17 A. VANDERMONDE (1735-1796)

$$(22) \quad \boxed{\binom{a+b}{k} = \sum_{i=0}^k \binom{a}{i} \binom{b}{k-i}}$$

BEMERKUNG. Die Vandermondsche Identität (22) kann man kombinatorisch so interpretieren: Man teilt die n -elementige Menge M in disjunkte Teilmengen M_a mit $|M_a| = a$ und M_b mit $|M_b| = b$ auf. Eine k -elementige Teilmenge von M konstruiert man dann, indem man i Elemente aus M_a und $k - i$ Elemente aus M_b wählt.

Die elementarsymmetrischen Funktionen. Der Binomialsatz besagt bei der Variablensubstitution $x_1 = \dots = x_n = x$ und $y_1 = -x_1, \dots, y_n = -x_n$:

$$(x - x_1) \dots (x - x_n) = \sigma_0 x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \dots + (-1)^n \sigma_n$$

mit

$$\begin{aligned} \sigma_0 &:= 1 \\ \sigma_1 &:= x_1 + x_2 + \dots + x_n \\ \sigma_2 &:= x_1 x_2 + \dots + x_2 x_3 + \dots + x_{n-1} x_n \\ \sigma_3 &:= x_1 x_2 x_3 + x_1 x_2 x_4 + \dots \\ &\vdots \\ \sigma_n &:= x_1 x_2 \dots x_n. \end{aligned}$$

Die $\sigma_0, \sigma_1, \dots, \sigma_n$ sind die sog. elementarsymmetrischen Funktionen bzgl. der Unbestimmten x_1, \dots, x_n (und entsprechen einfach einer Auflistung sämtlicher Teilmengen der Indexmenge $\{1, 2, \dots, n\}$ nach ihren Kardinalitäten).

Substituieren wir ferner $x_1 = \xi_1, \dots, x_n = \xi_n$, so berechnet man aus den elementarsymmetrischen Funktionen σ_i per

$$a_{n-i} := (-1)^i \sigma_i(\xi_1, \dots, \xi_n)$$

genau die Koeffizienten a_{n-i} des reellen Polynoms in der Variablen x mit den Nullstellen ξ_1, \dots, ξ_n :

$$(x - \xi_1) \dots (x - \xi_n) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 .$$

1.3. Polynomvektorräume. Sei $\mathbb{R}[x]$ die Menge aller reeller Polynomfunktionen in einer Variablen x . Bzgl. der Addition und Multiplikation mit reellen Skalaren erweist sich $\mathbb{R}[x]$ als Vektorraum über dem Skalarkörper \mathbb{R} . Die sog. *Standardbasis* von $\mathbb{R}[x]$ besteht aus den Elementen

$$1, x, x^2, \dots, x^n, \dots$$

und ist ein Erzeugendensystem, aus dem sich jede Polynomfunktion in $\mathbb{R}[x]$ als (endliche) Linearkombination konstruieren lässt. Aber auch sehr viele andere Erzeugendensysteme existieren.

LEMMA 2.1. Jede beliebige Folge $b^{(0)}(x), b^{(1)}(x), \dots, b^{(n)}(x), \dots$ von reellen Polynomfunktionen $b^{(n)}(x) = \sum_{i=0}^n b_i^{(n)} x^i$ mit $b_n^{(n)} \neq 0$ für alle $n \in \mathbb{N}$ ergibt ein Erzeugendensystem für $\mathbb{R}[x]$.

Beweis. Wir zeigen per Induktion, dass sich jedes x^n als Linearkombination von Funktionen vom Typ $b^{(n)}(x)$ darstellen lässt. Für $n = 0$ ist das klar, da (wegen $b_0^{(0)} \neq 0$) die Polynomfunktion $b^{(0)}(x)$ einen konstanten Wert $b_0 \neq 0$ annimmt und somit

$$x^0 = 1 = b_0^{-1} b^{(0)}(x)$$

ergibt. Sei $n \geq 1$ und $b^{(n)}(x) = \sum_{k=0}^n b_k x^k$. Dann haben wir

$$x^n = b_n^{-1} (b^{(n)}(x) - \sum_{k=0}^{n-1} b_k x^k) = b_n^{-1} b^{(n)}(x) + \sum_{k=0}^{n-1} (-b_n^{-1} b_k) x^k.$$

Nach Induktionsvoraussetzung sind alle x^k mit $k \leq n - 1$ als Linearkombinationen gewisser $b^{(j)}(x)$ darstellbar. Also auch x_n .

IELTS™  UNIVERSITY OF CAMBRIDGE 

**GEWINNE EINEN
SPRACHKURS IN MIAMI MIT
EXAMENSVORBEREITUNG**

Bereite Dich mit EF Sprachreisen auf ein international anerkanntes Sprachzertifikat wie TOEFL, Cambridge oder IELTS vor.

www.ef.com/bookboon

JETZT TEILNEHMEN!


Education First



Binomialkoeffizienten. Vom Standpunkt der Polynomialgebra aus kann man viele kombinatorische Identitäten als Umrechnungsformeln interpretieren, die ein lineares Erzeugendensystem von $\mathbb{R}[x]$ in ein anderes überführen. Zum Beispiel weist die Identität

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

die Binomialkoeffizienten als die Umrechnungskoeffizienten aus, um die Polynomfunktionen

$$1, x + 1, (x + 1)^2, \dots, (x + 1)^n, \dots$$

mittels der Standardbasis auszudrücken.

EX. 2.1. Man bestimme Koeffizienten $a_0, \dots, a_n \in \mathbb{R}$ mit der Eigenschaft

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

(Hinweis: Man wende den Binomialsatz auf $(x - 1)^n$ an.)

Stirlingzahlen. Nach Lemma 2.1 bilden die Polynome

$$(x)_n = x(x - 1) \dots (x - n + 1) \quad (n = 0, 1, 2, \dots)$$

ein Erzeugendensystem von $\mathbb{R}[x]$. Analoges gilt für die Polynome

$$(x)^n = x(x + 1) \dots (x + n - 1) = (-1)^n (-x)_n.$$

LEMMA 2.2. $x^n = \sum_{k=0}^n S(n, k)(x)_k$.

Beweis. Wir erinnern an die Identität (12) bzgl. der Stirlingzahlen zweiter Art:

$$r^n - \sum_{k=0}^n S(n, k)(r)_k = 0 \quad \text{für alle } r \in \mathbb{N}.$$

Das bedeutet, dass das reelle Polynom

$$p(x) = x^n - \sum_{k=0}^n S(n, k)(x)_k$$

unendlich viele Nullstellen besitzt. Also muss $p(x)$ das Nullpolynom sein (vgl. Lemma 2.4 in Abschnitt 2.1).

LEMMA 2.3. $(x)_n = \sum_{k=0}^n (-1)^{n-k} s(n, k)x^k.$

Beweis. Wir beweisen die äquivalente Aussage

$$(x)^n = \sum_{k=0}^n s(n, k)x^k$$

per Induktion. Gemäss der Rekursion der Stirlingzahlen erster Art rechnen wir

$$\begin{aligned} (x)^n &= (x + n - 1)(x)^{n-1} \\ &= \sum_{k=0}^{n-1} s(n - 1, k)x^{k+1} + \sum_{k=0}^{n-1} (n - 1)s(n - 1, k)x^k \\ &= \sum_{k=0}^n s(n - 1, k - 1)x^k + \sum_{k=0}^n (n - 1)s(n - 1, k)x^k \\ &= \sum_{k=0}^n [s(n - 1, k) + (n - 1)s(n - 1, k)]x^k \\ &= \sum_{k=0}^n s(n, k)x^k. \end{aligned}$$

BEMERKUNG. Aufgrund der obigen Lemmata sagt man, die Koeffizienten $S(n, k)$ und $(-1)^{n-k} s(n, k)$ seien zueinander *reziprok*. Die Zahlen $(-1)^{n-k} s(n, k)$ heissen auch *signierte Stirlingzahlen 1. Art*.

2 Division mit Rest

Zu je zwei Zahlen $m, n \in \mathbb{N}$ mit $n \geq 1$, gibt es bekanntlich eindeutig bestimmte Zahlen $d, r \in \mathbb{N}$ mit der Eigenschaft

$$m = dn + r \quad \text{und} \quad r < n.$$

Dabei ist $d = \lfloor m/n \rfloor$ die grösste natürliche Zahl $\leq m/n$. ist der sog. Rest der Division von m durch n .

Eine völlig analoge Eigenschaft beobachtet man in $\mathbb{R}[x]$, wenn man die „Grösse“ eines Polynoms durch seinen *Grad* misst.

BEMERKUNG. Der *Grad* des Polynoms $p(x) = \sum_{i=0}^n a_i x^i$ ist der Parameter

$$(23) \quad G(p) := \begin{cases} -\infty & \text{wenn } a_0 = \dots = a_n = 0; \\ \max\{i \mid a_i \neq 0\} & \text{sonst.} \end{cases}$$

SATZ 2.2. Zu je zwei Polynomen $q(x), p(x) \in \mathbb{R}[x]$ mit $G(q) \geq 1$ gibt es Polynome $d(x), r(x) \in \mathbb{R}[x]$ mit der Eigenschaft

$$q(x) = d(x)p(x) + r(x) \quad \text{und} \quad G(r) < G(p).$$

Die Gültigkeit von Satz 2.2 ist mit der folgenden algorithmischen Konstruktion¹⁸ leicht einzusehen. Sei z.B.

$$q(x) = \sum_{i=0}^m q_i x^i.$$

DIVISIONSALGORITHMUS:

- Im Fall $G(q) < G(p)$ nimmt man $d(x) \equiv 0$ und $r(x) = q(x)$.
- Im Fall $G(q) \geq G(p)$ subtrahiert man ein Vielfaches von $p(x)$, nämlich

18 das Verfahren geht zurück auf EUKLID (ca. 300 v. Chr.)

START UP - MEHR ALS EIN TRAINEE-PROGRAMM. JETZT BEWERBEN!

Die Antwort auf fast alles.
Antworten auf Ihre Karrierefragen finden Sie hier: www.telekom.com/absolventen

Jetzt bewerben!

T . . .

ERLEBEN, WAS VERBINDET.

$$q_m x^{m-n} p(x),$$

von $q(x)$. Ist der Grad danach immer noch $\geq G(p)$, bringt man wieder den höchsten Koeffizienten zum Verschwinden und fährt fort, bis man den Grad des Restes unter $G(p)$ gedrückt hat.

2.1. Nullstellen und Eindeutigkeit. Sei $q(x) = \sum_{k=0}^n q_k x^k \in \mathbb{R}[x]$ ein Polynom und $\xi_0 \in \mathbb{R}$ eine beliebige reelle Zahl. Dann liefert der Divisionsalgorithmus bzgl. $p(x) = x - \xi$ die Darstellung

$$q(x) = d(x)(x - \xi_0) + r(x) \quad \text{mit } G(r) \leq 0.$$

Das Restpolynom $r(x)$ ist also konstant mit Wert $r(\xi_0) = q(\xi_0)$. Im Fall $q(\xi_0) = 0$ ergibt sich somit die Faktordarstellung

$$q(x) = d(x)(x - \xi_0) \iff q(\xi_0) = 0.$$

Sind $\xi_0, \xi_1, \dots, \xi_k$ alle Nullstellen von $q(x)$, dann sind ξ_1, \dots, ξ_k alle Nullstellen von $d(x)$. Wir können also $d(x)$ faktorisieren usw. und erhalten die Darstellung

$$(24) \quad q(x) = \bar{d}(x)(x - \xi_0)(x - \xi_1) \dots (x - \xi_k).$$

Daraus erschliesst man eine wichtige Eigenschaft:

LEMMA 2.4. Sei $q(x) \in \mathbb{R}[x]$ ein Polynom mit $k \geq G(q) + 1$ verschiedenen Nullstellen. Dann ist $q(x)$ das Nullpolynom.

Beweis. Im Fall $k \geq G(q)$ und $G(\bar{d}) \geq 0$, ergäbe sich aus dem Produkt der rechten Seite von (24) ein Polynom vom Grad mindestens $k + 1 > G(q)$ und somit ein Widerspruch zur Annahme. Also gilt $\bar{d}(x) \equiv 0$ und folglich auch $q(x) \equiv 0$.

Aus Lemma 2.4 ergibt sich ausserdem, dass jede Polynomfunktion $p(x) \in \mathbb{R}[x]$ eine *eindeutige* Darstellung hat:

$$(25) \quad \sum_{i=0}^n a_i x^i = p(x) = \sum_{i=0}^n b_i x^i \implies a_i = b_i \quad (i = 0, 1, \dots, n).$$

In der Tat hat das Differenzpolynom $q(x) = \sum_{i=0}^n (a_i - b_i)x^i$ unendlich viele Nullstellen und folglich Grad $G(q) = -\infty$, d.h. $a_i - b_i = 0$ gilt für alle $i = 0, \dots, n$.

BEMERKUNG. Natürlich kann man auch Polynomfunktionen über anderen Zahlbereichen als \mathbb{R} (z.B. Ringe oder endliche Körper) betrachten (s. Kapitel 3). Die Eindeutigkeit der Darstellung ist dann aber nicht unbedingt gewährleistet.

3 Ringe

Bekanntlich erweitert man den Rechenbereich \mathbb{N} der natürlichen Zahlen durch Hinzunahme der negativen Zahlen zum Bereich der *ganzen Zahlen*

$$\mathbb{Z} = \{\dots, -n, \dots, -1, 0, +1, \dots, n, \dots\},$$

aus dem der Bereich $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ der rationalen Zahlen als Brüche ganzer Zahlen entsteht. Durch Limesüberlegungen wird \mathbb{Q} schliesslich zum Bereich \mathbb{R} reellen Zahlen ergänzt. Das Rechnen in diesen Bereichen, die Addition und Multiplikation, kann zu einem noch abstrakteren Rechnen verallgemeinert werden, das zu kombinatorischer Analyse nützlich sein kann, wie wir schon in Kapitel 2 gesehen haben. Wir gehen hier auf diese algebraischen Aspekte nochmals allgemein ein.

1 Halbgruppen und Ringe

Sei G eine Menge mit einer binäre Operation \circ , d.h. einer Abbildung

$$\circ : G \times G \rightarrow G.$$

Der Einfachheit halber schreibt man „ $a \circ b$ “ anstelle des etwas umständlichen (aber eigentlich korrekten) „ $\circ(a, b)$ “. Ein Neutralelement der algebraischen Struktur (G, \circ) ist ein Element $e \in G$ mit der Eigenschaft

$$g \circ e = e \circ g = g \quad \text{für alle } g \in G.$$

$G = (G, \circ)$ ist eine *Halbgruppe*, wenn G ein Neutralelement besitzt und zusätzlich G *assoziativ* ist in dem Sinn

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{für alle } a, b, c \in G.$$

Diese Assoziativitätseigenschaft besagt: Elemente von G dürfen beim Rechnen beliebig „zusammengefasst“ werden. Wir können somit auf das Setzen von Klammern verzichten, ohne Widersprüche befürchten zu müssen. Zum Beispiel:

$$\begin{aligned} a \circ (b \circ c \circ d) &= a \circ ((b \circ c) \circ d) = (a \circ (b \circ c)) \circ d = (a \circ b \circ c) \circ d \\ &= a \circ b \circ c \circ d. \end{aligned}$$

Die Halbgruppe G ist eine *Gruppe*, wenn es zu jedem Element $g \in G$ ein sog. *inverses Element* gibt, d.h. eine Element $f \in G$ mit der Eigenschaft

$$f \circ g = e.$$

Die Halbgruppe $G = (G, \circ)$ ist *kommutativ* (oder *abelsch*), wenn beim Rechnen die Reihenfolge der Elemente unmassgeblich ist, d.h. wenn für alle $a, b \in G$ gilt:

$$a \circ b = b \circ a .$$

BEMERKUNG. Binäre Operationen in Halbgruppen werden auch mit einem Additionssymbol oder mit einem Multiplikationssymbol notiert. Das zu a inverse Element wird bei additiver Schreibweise als „ $-a$ “ und bei multiplikativer Schreibweise als „ a^{-1} “ notiert.

EX. 3.1. Die Menge M^M aller Abbildungen $f : M \rightarrow M$ bildet eine Halbgruppe (M^M, \circ) bzgl. der Operation der Hintereinanderausführung

$$(f \circ g)(m) := g(f(m)) \quad \text{für alle } f, g \in M^M \text{ und } m \in M.$$

Neutralelement ist die identische Abbildung $\iota : M \rightarrow M$ mit $\iota(m) = m$.

EX. 3.2. Die „symmetrische Gruppe“ S_M ist ein Gruppe. Genau im Fall $|M| \leq 2$ ist S_M kommutativ.

EX. 3.3. Die natürlichen Zahlen bilden die kommutative Halbgruppe $(\mathbb{N}, +)$ mit Neutralelement 0 . $(\mathbb{Z}, +)$ ist eine kommutative Gruppe mit $(-n)$ als inverses Element von $n \in \mathbb{Z}$.



Machen Sie die Zukunft sichtbar

Kleine Chips, große Wirkung: Heute schon sorgt in rund der Hälfte aller Pässe und Ausweise weltweit ein Infineon Sicherheitscontroller für den Schutz ihrer Daten. Gleichzeitig sind unsere Halbleiterlösungen der Schlüssel zur Sicherheit von übermorgen. So machen wir die Zukunft sichtbar.

Was wir dafür brauchen? Ihre Leidenschaft, Kompetenz und frische Ideen. Kommen Sie zu uns ins Team! Freuen Sie sich auf Raum für Kreativität und Praxiserfahrung mit neuester Technologie. Egal ob Praktikum, Studienjob oder Abschlussarbeit: Bei uns nehmen Sie Ihre Zukunft in die Hand.

Für Studierende und Absolventen (w/m):

- > Ingenieurwissenschaften
- > Naturwissenschaften
- > Informatik
- > Wirtschaftswissenschaften



www.infineon.com/karriere



charta der vielfalt



$(\mathbb{Z} \setminus \{0\}, \cdot)$ ist eine (abelsche) Halbgruppe bzgl. der Multiplikation mit Neutralelement 1, aber keine Gruppe, da Division (d.h. die inverse Operation) nicht uneingeschränkt durchführbar ist. $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

Division auf $\mathbb{Q} \setminus \{0\}$ ist eine binäre Operation, die weder assoziativ noch kommutativ ist.

Sei nun $\mathcal{R} = (\mathcal{R}, +, \cdot)$ eine Menge, auf der zwei kommutative Operationen definiert sind, die wir als „Addition“ und „Multiplikation“ bezeichnen. Ausserdem gebe es zwei spezielle Elemente $0, 1 \in \mathcal{R}$.

Wir sagen $\mathcal{R} = (\mathcal{R}, +, \cdot)$ ist ein (kommutativer) Halbring, falls

- (R.1) $(\mathcal{R}, +)$ ist eine kommutative Halbgruppe mit Neutralelement 0.
- (R.2) $(\mathcal{R} \setminus \{0\}, \cdot)$ ist eine (kommutative) Halbgruppe mit Neutralelement 1.
- (R.3) Für alle $a, b, c \in \mathcal{R}$ gilt: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

BEMERKUNG. Mit der üblichen Verabredung, dass Multiplikation stärker bindet als Addition, wird das sog. *Distributivgesetz* (R.3) auch einfach so notiert:

$$a(b + c) = ab + ac.$$

Der Halbring R ist ein Ring, wenn $(\mathcal{R}, +)$ eine Gruppe ist, und ein Körper, wenn $(\mathcal{R}, +)$ und $(\mathcal{R} \setminus \{0\}, \cdot)$ Gruppen sind.

EX. 3.4. $(\mathbb{N}, +, \cdot)$ ist ein Halbring aber kein Ring. $(\mathbb{Z}, +, \cdot)$ ist ein Ring aber kein Körper. $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper. $\mathbb{R}[x]$ ist ein Ring.

1.1. Boolesche Algebra. Die Boolesche Algebra $\mathcal{B}_2 = (\{0, 1\}, \oplus, \odot)$ ist ein 2-elementiger Halbring (aber kein Körper) mit Addition und Multiplikation wie folgt:

\oplus	0	1		\odot	0	1
0	0	1		0	0	0
1	1	1		1	0	1

Man denkt sich \mathcal{B}_2 zusätzlich mit der Negationsoperation $x \rightarrow \bar{x}$ ausgestattet, wobei

$$x = 1 \iff \bar{x} = 0.$$

Auf $\mathcal{B}_n = \{0, 1\}^n$ kann man nun komponentenweise gemäss \mathcal{B}_2 rechnen:

$$\begin{aligned} (x_1, \dots, x_n) \oplus (y_1, \dots, y_n) &:= (x_1 \oplus y_1, \dots, x_n \oplus y_n) \\ (x_1, \dots, x_n) \odot (y_1, \dots, y_n) &:= (x_1 \odot y_1, \dots, x_n \odot y_n) \\ \overline{(x_1, \dots, x_n)} &:= (\bar{x}_1, \dots, \bar{x}_n). \end{aligned}$$

EX. 3.5. Interpretiert man einen Vektor $x \in \{0, 1\}^n$ als Indikator einer Teilmenge $X \subseteq N := \{1, \dots, n\}$, so entspricht die Addition in \mathcal{B}_n mengentheoretisch der Vereinigung und die Multiplikation in \mathcal{B}_n dem Durchschnitt. Die Negation entspricht der Komplementbildung:

$$\bar{x} \longleftrightarrow N \setminus X.$$

Also bildet die Potenzmenge (d.h. die Familie aller Teilmengen) von N im Sinne der Booleschen Algebra einen Halbring mit Negationsoperation.

1.2. Binäre Vektorräume. Rechnet man auf der Menge $\{0, 1\}$ additiv und multiplikativ wie folgt:

$$\begin{array}{c|cc}
 + & 0 & 1 \\
 \hline
 0 & 0 & 1 \\
 1 & 1 & 0
 \end{array}
 \qquad
 \begin{array}{c|cc}
 \cdot & 0 & 1 \\
 \hline
 0 & 0 & 0 \\
 1 & 0 & 1
 \end{array},$$

dann erhält man den

$\mathbb{Z}_2 = (\{0, 1\}, +, \cdot)$. Folglich kann man $\{0, 1\}^n$ auch als den n -dimensionalen Vektorraum \mathbb{Z}_2^n über \mathbb{Z}_2 auffassen.

VORSICHT: Addition in \mathcal{B}_n und Addition in \mathbb{Z}_2^n sind verschieden!

EX. 3.6. Sei $n \geq 2$. Definiert man in \mathbb{Z}_2^n eine Multiplikation analog zu \mathcal{B}_n ,

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) := (x_1 \cdot y_1, \dots, x_n \cdot y_n),$$

dann erhält man den Ring $(\mathbb{Z}_2^n, +, \cdot)$ – aber keinen Körper!

EX. 3.7. Man kann das Rechnen in \mathcal{B}_2 durch \mathbb{Z}_2 imitieren:

$$a \oplus b = a + b + (a \cdot b) \quad \text{und} \quad \bar{a} = a + 1.$$

Umgekehrt kann man Rechnungen bzgl. \mathbb{Z}_2 in \mathcal{B}_2 nachbilden:

$$a + b = (\bar{a} \odot b) \oplus (a \odot \bar{b}).$$

1.3. Entfernungen. Sei $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$ der erweiterte reelle Zahlbereich mit der zusätzlichen Rechenregel

$$a + \infty := \infty \quad \text{für alle } a \in \overline{\mathbb{R}}.$$

EX. 3.8. $(\overline{\mathbb{R}}, \oplus, \odot)$ ist ein Halbring mit den algebraischen Operationen

$$a \oplus b := \min\{a, b\} \quad \text{und} \quad a \odot b := a + b.$$

Hier ist ∞ das Nullelement von $(\overline{\mathbb{R}}, \oplus)$. Einselement in $(\overline{\mathbb{R}}, \odot)$ ist die reelle Zahl $0 \in \mathbb{R}$.

Der Halbring $(\overline{\mathbb{R}}, \oplus, \odot)$ tritt z.B. in folgendem Zusammenhang auf:

Sei $S = \{s_1, \dots, s_n\}$ eine Menge von n „Städten“. Eine Distanzmatrix bzgl. S ist eine Matrix $D \in \overline{\mathbb{R}}^{S \times S}$ mit (nichtnegativen) Einträgen $d(s, t) \geq 0$ derart, dass

$$d(s, s) = 0 \quad \text{für alle } s \in S.$$

Der Parameter $d(s, t)$ kann als die „direkte Entfernung“ von s nach t gesehen werden. Ein k -Weg von s nach t ist eine Folge $w = (v_0, \dots, v_k)$ von (nicht notwendigerweise paarweise verschiedenen) „Städten“ $v_j \in S$ mit $s = v_0$ und $t = v_k$. Die Länge des Weges w ist

$$\ell(w) := d(v_0, v_1) + d(v_1, v_2) + \dots + d(v_{k-1}, v_k).$$

SIEMENS

EIGENVERANTWORTUNG
 KREATIVE TEAMPLAYER
 NEUGIERDE
 OFFENHEIT
 INNOVATION ERFINDERGEIST
 ENGAGEMENT
 PERSPEKTIVEN CHANCEN
 ENTSCLOSSENHEIT
 WELTWEITE MÖGLICHKEITEN
 WORK-LIFE-BALANCE

Verwirklichen, worauf es ankommt –
 mit einer Karriere bei Siemens.

siemens.de/karriere



Wir definieren die Entfernungsparameter

$$d^{(k)}(s, t) := \min\{\ell(w) \mid w \text{ ist } k\text{-Weg von } s \text{ nach } t\}.$$

Dann gilt offenbar die *Bellman*¹⁹-Rekursion für alle $s, t \in N$:

$$(26) \quad \boxed{\begin{array}{l} (B_1) \quad d^{(1)}(s, t) = d(s, t) \\ (B_2) \quad d^{(k+1)}(s, t) = \min\{d^{(k)}(s, u) + d(u, t) \mid u \in S\} \end{array}}$$

Denn man gelangt auf einem $(k+1)$ -Weg von s nach t , indem man sich auf einem k -Weg von s zu einem u und dann von u auf einem 1-Weg nach t bewegt.

LEMMA 3.1. $d^{(n)}(s, t)$ ist die Länge eines kürzesten Weges von s nach t bzgl. der Distanzmatrix D .

Beweis. Sei $w = (v_0, v_1, \dots, v_k)$ ein kürzester Weg von $s = v_0$ nach $t = v_k$. Im Fall $k > n$, durchläuft w einen Kreis K . Denn da es ja nur n Städte gibt, muss nach dem Schubfachprinzip mindestens eine Stadt zweimal auftreten. Wir können auf das Durchlaufen von K verzichten und erhalten einen Weg w' von s nach t , der sicherlich nicht länger ist. Also dürfen wir ohne Beschränkung der Allgemeinheit annehmen, dass w kreisfrei ist und folglich $k \leq n$ gilt.

Andererseits können wir im Fall $k < n$, den Weg w „künstlich“ zu einem n -Weg w'' gleicher Länge $\ell(w'') = \ell(w)$ erweitern:

$$w'' = (v_0, \dots, v_k, v_{k+1}, \dots, v_n) \quad \text{mit } v_k = v_{k+1} = \dots = v_n = t.$$

Denn nach Voraussetzung gilt ja $d(v_k, v_{k+1}) = \dots = d(t, t) = 0$. Also dürfen wir auch $k = n$ annehmen. Das Argument zeigt:

Die Länge $d^{(n)}(s, t)$ ist die Länge eines kürzesten n -Weges von s nach t ist auch die Länge eines kürzesten Weges von s nach t schlechthin.

Bzgl. des Halbrings $\overline{\mathbb{R}}$ lässt sich der Rekursionsschritt (B2) algebraisch so ausdrücken:

$$(27) \quad d^{(k+1)}(s, t) = (d^{(k)}(s, s_1) \odot d(s_1, t)) \oplus \dots \oplus (d^{(k)}(s, s_n) \odot d(s_n, t)).$$

Dies bedeutet: Berechnen wir der Reihe nach die Potenzen D^2, D^3, \dots, D^n der Matrix D nach den algebraischen Regeln des Halbrings $\overline{\mathbb{R}}$, d.h.

$$D^{k+1} = D^k \odot D \quad (k = 1, 2, \dots, n - 1),$$

19 R. BELLMAN (1920-1984)

dann folgt aus (27), dass die k -Entfernungen leicht mit Hilfe der Matrixrechnung ermittelt werden können:

Die Elemente der Matrix D^{k+1} sind genau die Entfernungskoeffizienten $d^{(k+1)}(s, t)$.

Insbesondere ist D^n die Matrix der kürzesten Entfernungen.

EX. 3.9. Sei $m \in \mathbb{N}$ so gross, dass $n \leq 2^m$ (d.h. $\log_2 n \leq m$). Dann braucht man nur m Matrixmultiplikationen, um D^n zu ermitteln:

$$D \odot D = D^2, D^2 \odot D^2 = D^4, \dots, D^{2^{m-1}} \odot D^{2^{m-1}} = D^{2^m} = D^n.$$

Also: Zur Berechnung von D_n reichen $\lceil \log_2 n \rceil$ Matrixmultiplikationen aus.

1.4. Kürzeste Wege. D^n ist die Matrix der kürzesten Entfernungen zwischen allen Städtepaaren bzgl. der Distanzmatrix D . Ist D^n bekannt, kann man leicht einen konkreten kürzesten Weg z.B. zwischen den Städten s und t konstruieren:

Wähle ein $t_1 \in S \setminus \{t\}$	mit	$d^{(n)}(s, t) = d^{(n)}(s, t_1) + d(t_1, t).$
Wähle ein $t_2 \in S \setminus \{t, t_1\}$	mit	$d^{(n)}(s, t) = d^{(n)}(s, t_2) + d(t_2, t_1).$
Wähle ein $t_3 \in S \setminus \{t, t_1, t_2\}$	mit	$d^{(n)}(s, t) = d^{(n)}(s, t_3) + d(t_3, t_2).$
		<i>usw.</i>

Ein t_i der geforderten Art muss existieren, da es ja einen kürzesten Weg von s nach t gibt. t_1 ist die Stadt vor dem Erreichen von t . Natürlich muss dann auch der Weg von s nach t_1 minimale Länge haben. t_2 ist die Stadt vor t_1 auf einem kürzesten Weg von s nach t_1 usw. So erhält man schliesslich einen kürzesten Weg:

$$s \rightarrow \dots \rightarrow t_3 \rightarrow t_2 \rightarrow t_1 \rightarrow t.$$

2 Restklassen und endliche Körper

Wir betrachten zuerst \mathbb{N} und halten eine natürliche Zahl $n \geq 1$ fest. Mit \bar{m} bezeichnen wir den Rest von $m \in \mathbb{N}$ nach Division durch n :

$$\bar{m} := m - \lfloor m/n \rfloor \cdot n.$$

Nun kann man leicht nachrechnen, dass die folgenden Operationen wohldefiniert sind (d.h. nur von den jeweiligen Resten abhängen):

$$\begin{aligned} \overline{m_1} + \overline{m_2} &:= \overline{m_1 + m_2} \\ \overline{m_1} \cdot \overline{m_2} &:= \overline{m_1 \cdot m_2} \end{aligned}$$

Die n -elementige Menge $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$ aller möglichen Reste \overline{m} modulo n trägt die algebraische Struktur $(\mathbb{Z}_n, +, \cdot)$. Diese bildet einen Ring, den sog. *Restklassenring*. Zum Beispiel rechnen wir in $(\mathbb{Z}_n, +, \cdot)$ mit $a, b \in \mathbb{Z}_n$:

$$\begin{aligned} a + b &= \overline{a + b} \\ a + (n - a) &= \overline{n} = 0 \\ \text{(d.h. } (n - a) &= -a \text{ (bzgl. der abelschen Gruppe } (\mathbb{Z}_n, +)) \\ a \cdot b &= \overline{ab} \\ &\text{usw.} \end{aligned}$$

LEMMA 3.2. Der Restklassenring $(\mathbb{Z}_n, +, \cdot)$ modulo $n \geq 1$ ist ein Körper genau dann, wenn n eine Primzahl ist.

Beweis. Ist $n = pq$ das Produkt von Zahlen $1 \leq p, q \leq n - 1$, dann finden wir

$$\overline{pq} = \overline{pq} = \overline{n} = 0.$$

Wäre \mathbb{Z}_n ein Körper, so besäßen die Elemente $p, q \in \mathbb{Z}_n \setminus \{0\}$ (multiplikativ) inverse Elemente p^{-1}, q^{-1} , die einen Widerspruch ergäben:

Jonas von Malottki Finance Accounting IT Solutions, Deutschland (Stuttgart)
 Hortense Denise Kirby HR Business Partner, USA (Dallas/Fort Worth)
 Yu Chang Engineering Support Office, China (Peking)

Fünf Kontinente. Jede Menge Platz zur persönlichen Entfaltung. Das sind wir.

Hier geht es für Sie weiter: www.career.daimler.com

DAIMLER

Die Daimler AG ist eines der erfolgreichsten Automobilunternehmen der Welt. Zum Markenportfolio gehören Mercedes-Benz, smart, Freightliner, Western Star, BharatBenz, Fuso, Setra, Thomas Built Buses sowie die Mercedes-Benz Bank, Mercedes-Benz Financial und Truck Financial.



$$1 = \overline{p^{-1}pqq^{-1}} = \overline{p^{-1}q^{-1}} \cdot \overline{pq} = \overline{p^{-1}q^{-1}} \cdot \overline{n} = \overline{p^{-1}q^{-1}} \cdot 0 = 0.$$

Ist umgekehrt n eine Primzahl und $1 \leq p \leq n - 1$, so betrachten wir die Abbildung $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ mit $f(x) = \overline{px}$. f ist injektiv. Denn sonst gäbe es Elemente $1 \leq x < y \leq n - 1$ mit der Eigenschaft

$$f(x) = f(y) \quad \text{und folglich} \quad \overline{(y-x)p} = 0,$$

d.h.: die Primzahl n teilt entweder $(y-x)$ oder p . Das kann aber nicht sein, da beide Zahlen kleiner als n sind.

Da f injektiv (und \mathbb{Z}_n endlich) ist, ist f sogar surjektiv. Also existiert ein $p' \in \mathbb{Z}_n$ mit $f(p') = 1$ und somit der Inverseneigenschaft:

$$\overline{p' \cdot p} = f(p) = 1.$$

2.1. Endliche Körper. Im vorherigen Abschnitt wurde gezeigt, wie man aus dem Ring \mathbb{Z} und einer Primzahl $p \in \mathbb{Z}$ den Körper \mathbb{Z}_p erhält. Genau die gleichen Konstruktionen und Argumente gestatten es, weitere endliche Körper zu gewinnen. Dazu definieren wir (analog zu $\mathbb{R}[x]$) die Menge $\mathbb{K}[x]$ aller Polynome

$$p(x) = a_0 + a_1x + \dots + a_nx^n \quad \text{mit } a_0, \dots, a_n \in \mathbb{K}.$$

Genauso wie bei $\mathbb{R}[x]$ kann man in $\mathbb{K}[x]$ addieren, multiplizieren und Divisionen mit Rest durchführen. Insbesondere ist $\mathbb{K}[x]$ ein Ring.

Analog zum Begriff einer Primzahl nennen wir ein Polynom $p(x) \in \mathbb{K}[x]$ vom Grad $G(p) \geq 1$ *prim*, prim, wenn für alle Polynome $q_1(x), q_2(x) \in \mathbb{K}[x]$ mit $G(q_1) \geq 1$ und $G(q_2) \geq 1$ gilt:

$$p(x) = q_1(x)q_2(x) \quad \implies \quad p(x) = q_1(x) \text{ oder } p(x) = q_2(x).$$

Sei nun $p(x) \in \mathbb{K}[x]$ mit $Gd(p) = n \geq 1$ fest gewählt. Mit $\overline{q(x)}$ bezeichnen wir das Restpolynom, das man nach Division von $q(x)$ durch $p(x)$ erhält. Die möglichen Restpolynome haben die Form

$$r(x) = r_0 + r_1x + \dots + r_{n-1}x^{n-1} \quad \text{mit } r_i \in \mathbb{K} \text{ beliebig.}$$

Der Ring $\mathbb{K}[x]/p(x)$ aller möglichen Reste hat also (nach dem zweiten fundamentalen Zählprinzip) die Kardinalität

$$|\mathbb{K}[x]/p(x)| = |\mathbb{K}| \times |\mathbb{K}| \times \dots \times |\mathbb{K}| = |\mathbb{K}|^n.$$

Ganz genau wie das Lemma 3.2 beweist man nun

LEMMA 3.3. Der Ring $\mathbb{K}[x]/p(x)$ ist ein Körper genau dann, wenn $p(x)$ ein Primpolynom ist.

Damit hat man ein einfaches Rezept zur Konstruktion endlicher Körper:

- (1) Man wählt eine beliebige Primzahl $p \in \mathbb{N}$ und dazu ein beliebiges Primpolynom $p(x) \in \mathbb{Z}_p[x]$ vom Grad $G(p) = n \geq 1$.
- (2) Dann ist $GF(p^n) := \mathbb{Z}_p[x]/p(x)$ ein Körper mit p^n Elementen.

BEMERKUNG. Ein endlicher Körper vom Typ $GF(p^n) := \mathbb{Z}_p[x]/p(x)$ heisst auch *Galois²⁰-Körper*. In der Algebra kann man zeigen:

- Jeder endliche Körper ist isomorph zu einem Galois-Körper.
- Zu jeder Primzahl $p \in \mathbb{N}$ und jedem $n \geq 1$ gibt es ein Primpolynom $p(x) \in \mathbb{Z}_p[x]$ vom Grad $Gd(p) = n$.

Also existiert ein endlicher Körper \mathbb{K} der Kardinalität $|\mathbb{K}| = q$ genau dann, wenn q eine Primzahlpotenz ist.

Als Beispiel konstruieren wir den 4-elementigen Körper $GF(2^2)$ aus $GF(2) = \mathbb{Z}_2$.

Die einzigen Polynome über \mathbb{Z}_2 vom Grad 1 sind x und $x + 1$. Das Polynom $p(x) = x^2 + x + 1$ hat Grad 2 und ist prim in $\mathbb{Z}_2[x]$ (denn $p(x)$ ist weder ein Vielfaches von x noch von $x + 1$).

Also erhalten wir $GF(4) = \mathbb{Z}_2[x]/(x^2 + x + 1)$ als Körper und können (nach den Regeln des Rechnens mit Resten) die Additions- und die Multiplikationstafel aufstellen:

+	0	1	x	$x + 1$
0	0	1	x	$x + 1$
1	1	0	$x + 1$	x
x	x	$x + 1$	1	1
$x + 1$	$x + 1$	x	1	0

·	1	x	$x + 1$
1	1	x	$x + 1$
x	x	$x + 1$	1
$x + 1$	$x + 1$	1	x

Zur Überprüfung der Richtigkeit der Tabellen rechnen wir z.B.

$$\begin{aligned}
 (x + 1)^2 &= x^2 + x + x + 1 \\
 &= x + p(x) \\
 \text{d.h. } (x + 1)^2 &= x \quad (\text{in } \mathbb{Z}_2[x]/p(x)) .
 \end{aligned}$$

Schreiben wir abkürzend $a := x$ und $b := x + 1$, dann erhalten wir die Additions- und Multiplikationstafel des Körpers $GF(4) = \{0, 1, a, b\}$ als

20 É. GALOIS (1811-1832)

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	1	1
b	b	a	1	0

·	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

NOTA BENE: Der 4-elementige Körper $GF(4)$ ist nicht zu verwechseln mit dem 4-elementigen Ring \mathbb{Z}_4 !!!

BEMERKUNG. Es gibt Tabellen, in denen man Primpolynome (bzgl. dem für die Praxis besonders interessanten Körper \mathbb{Z}_2) für alle praktischen Zwecke nachschlagen kann. Beispiele:

$$p_5(x) = x^5 + x^3 + 1 \quad \text{oder} \quad p_{9689}(x) = x^{9689} + x^{84} + 1 \in \mathbb{Z}_2[x].$$

2.2. Lateinische und magische Quadrate. Ein *lateinisches Quadrat* über der n -elementigen Menge M ist eine $(n \times n)$ -Matrix L derart, dass jeder Zeilen- und jeder Spaltenvektor von L eine Permutation der Elemente von M ist. Die Zahl n ist die sog. *Ordnung* von L . Lateinische Quadrate kann man zu jeder Ordnung n leicht konstruieren:

1	2	3	...	$n - 1$	n
2	3	4	...	n	1
3	4	5	...	1	2
⋮	⋮	⋮		⋮	⋮
n	1	2	...	$n - 2$	$n - 1$

Interessanter ist die Frage, zu welcher Ordnung sog. *orthogonale* lateinische Quadrate existieren. Dabei nennt man die lateinischen Quadrate L_1, L_2 *orthogonal*²¹, wenn man sie so erhalten kann: Man ordnet die n^2 verschiedenen Elemente der Menge $M \times M$ aller Paare so zu einer quadratischen Matrix L an, dass L_1 genau aus den ersten Komponenten und L_2 aus den zweiten Komponenten der Elemente von L erwächst. Zum Beispiel:

(0, 0)	(1, 1)	(2, 2)	(3, 3)	(4, 4)
(1, 2)	(2, 3)	(3, 4)	(4, 0)	(0, 1)
(2, 4)	(3, 0)	(4, 1)	(0, 2)	(1, 3)
(3, 1)	(4, 2)	(0, 3)	(1, 4)	(2, 0)
(4, 3)	(0, 4)	(1, 0)	(2, 1)	(3, 2)

Orthogonale lateinische Quadrate kann man z.B. so konstruieren:

Man nehme einen n -elementigen Körper $GF(n) = (M, +, \cdot)$ mit der Grundmenge $M = \{a_0 = 0, a_1, \dots, a_{n-1}\}$ und definiere zu jedem $h \in \{1, \dots, n - 1\}$ das lateinische Quadrat L_h mit den Koeffizienten

21 auch oft *graeco-lateinische Quadrate*, weil man die Elemente von M gerne einmal mit griechischen und einmal mit lateinischen Buchstaben notiert

$$L_h(i, j) := a_h \cdot a_i + a_j \quad (i, j = 0, \dots, n - 1).$$

BEMERKUNG. Die j te Spalte von L_h entspricht genau den Werten der diskreten Geradenfunktion $f : GF(n) \rightarrow GF(n)$ mit $f(x) = a_h x + a_j$.

Man überprüft ohne grosse Mühe, dass L_h tatsächlich ein lateinisches Quadrat ist und dass je zwei dieser $n - 1$ so konstruierten lateinischen Quadrate orthogonal sind.

Anzahl paarweise orthogonaler Quadrate. Es bezeichne $N(n)$ die maximale Anzahl paarweise orthogonaler lateinischer Quadrate der Ordnung n . Da man zu jeder Primzahlpotenz $n = p^k$ den Körper $GF(n)$ mit n Elementen konstruieren kann, finden wir

$$N(n) \geq n - 1, \text{ falls } n \text{ Primzahlpotenz ist.}$$

Andererseits gilt allgemein die obere Schranke:

SATZ 3.1. $N(n) \leq n - 1$.

Beweis. Es seien L_1, L_2, \dots, L_t paarweise orthogonale lateinische Quadrate. Wir beobachten zuerst, dass die Orthogonalität erhalten bleibt, wenn wir die Spalten in jedem Quadrat so permutieren, dass in der ersten Zeile die Elemente in der Reihenfolge

Nehmen Sie die nächsten 50 Stufen Ihrer Karriereleiter doch gleich auf einmal.

Das gibt es nur bei JobStairs: Auf einer Seite alle favorisierten Top Unternehmen sehen und sich bequem bei allen gleichzeitig bewerben. Ideale Bedingungen also, um Ihren persönlichen Karriereaufstieg erfolgreich in Angriff zu nehmen.

Und hier geht's direkt zu Ihren Top Jobs:

JobStairs
The Top Company Portal

Logos of various companies including Allianz, BMW Group, Bosch, Daimler, E.ON, SAP, Siemens, etc.



$$123 \dots n$$

stehen. Wir betrachten nun die Elemente an der Position $(2, 1)$ in L_k , $k = 1, \dots, t$. Keines darf 1 sein, da 1 ja schon in der ersten Spalte an Position $(1, 1)$ vorkommt. Ausserdem muessen alle verschieden sein (sonst wuerde z.B. das Paar (i, i) beim U bereinanderlegen der entsprechenden Quadrate sowohl in der ersten wie in der zweiten Zeile auftreten, was der Orthogonalitaet der Quadrate widerspraechen). Also gilt $t \leq n - 1$.

SATZ 3.2. $N(n_1 n_2) \geq \min\{N(n_1), N(n_2)\}$.

Beweis. Sei $t = N(n_1) \leq N(n_2)$. Wir betrachten die Menge aller $n_1 n_2$ geordneten Paare

$$M = \{ii' \mid 1 \leq i \leq n_1, 1 \leq i' \leq n_2\} .$$

Nach Annahme gibt es jeweils t lateinische Quadrate $L_k^{(1)}$ bzw. $L_k^{(2)}$ auf den Mengen $M_1 = \{1, 2, \dots, n_1\}$ bzw. $M_2 = \{1, 2, \dots, n_2\}$. Wir bilden daraus t lateinische Quadrate L_k auf M :

$$L_k(ii', jj') := (L_k^{(1)}(i, j), L_k^{(2)}(i', j')) , \quad k = 1, \dots, t .$$

Man verifiziert nun, dass die L_k tatsaechlich lateinische Quadrate und paarweise orthogonal sind.

Wir haben oben festgestellt, dass fuer Primzahlpotenzen $n = p^k$ gilt:

$$N(p^k) = p^k - 1 .$$

Ist n eine allgemeine ungerade natuerliche Zahl, so folgern wir aus Satz 3.2:

$$N(n) \geq N(3) = 2 :$$

Da der 4-elementige Koerper $GF(4)$ existiert, finden wir allgemeiner

$$N(n) \geq 2 \quad \text{fuer alle } n \not\equiv 2 \pmod{4} ,$$

da in diesen Faellen n ungerade ist oder 4 als Teiler besitzt. (Fuer den Fall $n \equiv 2 \pmod{4}$ beachte man die folgenden Anmerkungen.) Dabei benutzt man die Notation

$$n \equiv k \pmod{m} \iff n - k \text{ ist durch } m \text{ ohne Rest teilbar.}$$

HISTORISCHE ANMERKUNGEN:

Aus der Relation $6 \equiv 2 \pmod{4}$ ergibt sich das kleinste (interessante) lateinische Quadrat mit $n = 6$. Hier hatte schon Euler²² vermutet, dass kein Paar orthogonaler lateinischer Quadrate existiert, was durch Tarry um 1900 (durch vollständiges Enumerieren aller potentiellen Kandidaten) bestätigt wurde. Euler hatte allerdings die Nichtexistenz auch in allen andern Fällen $n = 10; 14; 18, \dots$ usw. vermutet. Bose, Shrikhande und Parker konnten jedoch 1960 für alle diese Ordnungen paarweise orthogonale Quadrate konstruieren!

Die meisten übrigen konkreten Fragen um orthogonale lateinische Quadrate sind offen. Zum Beispiel konnten bisher noch keine 3 paarweise orthogonale lateinischen Quadrate der Ordnung $n = 10$ konstruiert werden.

Magische Quadrate. Eine mit n^2 verschiedenen natürlichen Zahlen gefüllte $(n \times n)$ -Matrix M ist ein *magisches Quadrat*, wenn alle Zeilen, Spalten und Diagonalen dieselbe Summe ergeben. Das Quadrat ist *halbmagisch*, wenn diese Eigenschaft nur für die Zeilen und Spalten gefordert wird. Zum Beispiel²³:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Wie schon Euler feststellte, kann man halbmagische Quadrate M einfach konstruieren, wenn man von zwei orthogonalen Quadraten L_1 und L_2 mit den jeweiligen Einträgen $0, 1, \dots, n - 1$ ausgeht: Man setzt

$$M(i, j) := 1 + L_1(ij) + n \cdot L_2(ij) \quad (i, j = 1, \dots, n).$$

M ist ein magisches Quadrat, wenn L_1 und L_2 die „lateinische“ Bedingung (alle Elemente sind paarweise verschieden) auch auf den Diagonalen erfüllen.

22 L. EULER (1707-1783)

23 von A. Dürer auf seinem Stich MELENCOLIA im Jahr 1514 festgehalten und z.B. im Kölner Wallraf-Richartz-Museum zu besichtigen

4 Potenzreihen

Potenzreihen sind allgemeiner als Polynome und gestatten dennoch, dass man mit ihnen genauso rechnet: Man addiert koeffizientenweise und multipliziert nach den Regeln der Cauchy-Multiplikation. Ausserdem sind Potenzreihen oft multiplikativ invertierbar (was Polynome ausser in Trivialfällen *nicht(!)* sind). Das lässt sich beim kombinatorischen Zählen vorteilhaft nutzen.

Der Nachteil von Potenzreihen besteht darin, dass sie nicht immer Funktionen definieren, da Substitutionen zu möglicherweise divergenten Reihen führen. Im Fall von Konvergenz kann man mit Potenzreihen allerdings ebenso umgehen wie mit Polynomen.

1 Formale Potenzreihen

Wir betrachten die Menge $\mathcal{R}^{\mathbb{N}}$ aller Abbildungen $a : \mathbb{N} \rightarrow \mathcal{R}$ in den Ring $(\mathcal{R}, +, \cdot)$, die wir auch als unendliche Koeffizientenvektoren auffassen können:

$$a = (a_0, a_1, \dots, a_n, \dots) \quad (a_n \in \mathcal{R}).$$

Um eine algebraische Struktur auf $\mathcal{R}^{\mathbb{N}}$ sichtbar zu machen, ist es praktisch, sich a als den Koeffizientenvektor einer formalen (unendlichen) Summe vom Typ

The advertisement features a cyclist in a red jacket and helmet standing with a bicycle in a field. A large text box on the left reads "ICH BEI ZF. INFORMATIKER UND OUTDOOR-PROFI." with the website "www.ich-bei-zf.com". Below this is the ZF logo and the text "MOTION AND MOBILITY". In the bottom left corner, there is a "100 YEARS MOTION AND MOBILITY" logo and a blue box with a QR code and the text "Scan den Code und erfahre mehr über mich und die Arbeit bei ZF:". In the bottom right corner, there is a business card for "WALTER LAUTER", an IT-Spezialist for Serversysteme at ZF Friedrichshafen AG, with a ZF logo.

$$(28) \quad a(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{n=0}^{\infty} a_n x^n$$

vorzustellen. In diesem Fall nennen wir den Ausdruck (28) eine *formale Potenzreihe* und bezeichnen mit $\mathcal{R}_{\infty}[x]$ die Menge aller formalen Potenzreihen. $\mathcal{R}_{\infty}[x]$ stellt also einfach eine gewisse Sichtweise auf $\mathcal{R}^{\mathbb{N}}$ dar.

Wir rechnen mit (formalen) Potenzreihen *ganz genauso* wie mit Polynomen, nämlich mit der komponentenweise genommenen Addition und dem Cauchy-Produkt:

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &:= \sum_{n=0}^{\infty} (a_n + b_n) x^n \\ \sum_{i=0}^{\infty} a_i x^i * \sum_{j=0}^{\infty} b_j x^j &:= \sum_{n=0}^{\infty} c_n x^n \quad \text{mit} \quad \boxed{c_n = \sum_{i+j=n} a_i b_j}. \end{aligned}$$

Damit ist $(\mathcal{R}_{\infty}[x], +, *)$ ein Ring mit dem multiplikativen Einselement

$$(1, 0, \dots, 0, \dots) \longleftrightarrow 1 + 0x + 0x^2 + \dots + 0x^n + \dots$$

EX. 4.1. *Es gibt noch andere Möglichkeiten, „sinnvoll“ Produkte von Potenzreihen einzuführen. Zum Beispiel:*

$$\sum_{n=0}^{\infty} a_n x^n \circ \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} (a_n \cdot b_n) x^n.$$

Auch $(\mathcal{R}_{\infty}[x], +, \circ)$ ist ein Ring und hat die geometrische Reihe (s. Ex. 4.2) als sein multiplikatives Einselement:

$$1 + x + x^2 + \dots + x^n + \dots \longleftrightarrow \sum_{n=0}^{\infty} x^n.$$

(Für Zählprobleme erweist sich das Cauchy-Produkt jedoch oft als fruchtbarer).

1.1. Skalare und Polynome als Potenzreihen. Wir identifizieren ein Polynom mit einer Potenzreihe,

$$\sum_{i=0}^n p_i x^i \longleftrightarrow \sum_{i=0}^{\infty} p_i x^i \quad \text{wobei} \quad p_{n+1} = p_{n+2} = \dots = 0.$$

Insbesondere können wir Skalare (Ringelemente) $r \in \mathcal{R}$ als Potenzreihen

$$r \longleftrightarrow r + 0x + 0x^2 + \dots + 0x^n + \dots$$

auffassen. Damit ist z.B. das Element $1 \in \mathcal{R}$ auch das multiplikative Einselement von $\mathcal{R}_\infty[x]$.

BEMERKUNG. Während ein Polynom $p(x) = \sum_{i=0}^n p_i x^i$ auch immer eine Funktion $p : \mathcal{R} \rightarrow \mathcal{R}$ definiert vermöge der Substitution

$$\xi \mapsto p(\xi) := \sum_{i=0}^n p_i \xi^i,$$

ist das bei Potenzreihen im allgemeinen *nicht(!)* so, da unendliche Summen in Ringen (oder Körpern) nicht immer sinnvoll definiert sind. Wenn eine Potenzreihe zufällig auch eine Funktion definiert, kann das oft in der kombinatorischen Analyse ausgenutzt werden. (Beispiele dazu finden sich in Abschnitt 2.)

1.2. Potenzreiheninversion. Eine wichtige Eigenschaft, die den Potenzreihenring $\mathcal{R}_\infty[x]$ vor dem Polynomring $\mathcal{R}[x]$ auszeichnet, ist die Tatsache, dass viele Potenzreihen (multiplikativ) invertierbar sind:

PROPOSITION 4.1. Sei $a(x) = \sum_{i=0}^\infty a_i x^i$ mit $a_0 = 1$. Dann existiert eine eindeutig bestimmte Potenzreihe $b(x) = \sum_{j=0}^\infty b_j x^j$ mit der Eigenschaft

$$a(x) * b(x) = 1.$$

Beweis. Wir müssen haben:

$$\begin{array}{rcl} a_0 b_0 & = & 1 \\ a_0 b_1 + a_1 b_0 & = & 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 & = & 0 \\ \vdots & & \vdots \\ \sum_{i=0}^n a_i b_{n-i} & = & 0 \\ \vdots & & \vdots \end{array} \quad \text{bzw.} \quad \begin{array}{rcl} b_0 & = & 1 \\ b_1 & = & -a_1 b_0 \\ b_2 & = & -(a_1 b_1 + a_2 b_0) \\ \vdots & & \vdots \\ b_n & = & -\sum_{i=1}^n a_i b_{n-i} \\ \vdots & & \vdots \end{array}$$

Die Koeffizienten b_n berechnen sich also der Reihe nach aus den zuvor berechneten Koeffizienten b_j mit $j \leq n - 1$ und den (gegebenen) a_i und die so berechnete Reihe $b(x)$ ist invers zu $a(x)$.

Im Fall $a(x) * b(x) = 1$ schreibt man

$$b(x) = a^{-1}(x) \quad \text{oder} \quad b(x) = \frac{1}{a(x)}.$$

EX. 4.2 (Die geometrische Reihe). Das Polynom $p(x) = 1 - x$ ist in $\mathcal{R}_\infty[x]$ invertierbar:

$$(1 - x) * (1 + x + \dots + x^n + \dots) = 1 .$$

Die zu $1 - x$ inverse Reihe ist die sog. geometrische Reihe

$$(29) \quad (1 - x)^{-1} = \frac{1}{1 - x} = 1 + x + \dots + x^n + \dots = \sum_{n=0}^{\infty} x^n .$$

EX. 4.3 (Die geometrische Summe). Das Produkt

$$(1 - x) * (1 + x + \dots + x^n) = 1 - x^{n+1}$$

führt auf die geometrische Summationsformel

$$(30) \quad 1 + x + \dots + x^n = \frac{1 - x^{n+1}}{1 - x} .$$

Ist $\xi \in \mathcal{R} R$ ein Ringelement derart, dass $(1 - \xi)^{-1}$ in R existiert, dann ist die Substitution $\xi \mapsto x$ sinnvoll und ergibt





by BNP PARIBAS

DEINE SCHNITTSTELLE ZUM ERFOLG.
HIER BIST DU RICHTIG VERBUNDEN!

Die Consorsbank ist eine der führenden Direktbanken Europas. Lege jetzt als Werkstudent oder Praktikant bei uns den Grundstein für deine erfolgreiche Karriere.

Einfach online bewerben unter:
www.consorsbank.de/karriere



$$1 + \xi + \dots + \xi^n = \frac{1 - \xi^{n+1}}{1 - \xi} \in \mathcal{R} .$$

2 Erzeugende Funktionen

Im Fall des Skalarbereichs $\mathcal{R} = \mathbb{R}$ (oder auch $\mathcal{R} = \mathbb{C}$ der komplexen Zahlen) ist es sinnvoll, bei einer Potenzreihe $a(x)$ zu fragen, für welche $z \in \mathcal{R}$ die Reihe

$$a(z) = a_0 + a_1z + a_2z^2 + \dots = \sum_{n=0}^{\infty} a_n z^n$$

konvergiert. Wie man aus der Analysis weiss, ist dann die Funktion $z \mapsto a(z)$ im Inneren des Konvergenzkreises K_a wohldefiniert und unendlich oft differenzierbar. An der Stelle $z = 0$ ergeben sich die Ableitungen

$$a^{(n)}(0) = n! a_n \quad \text{bzw.} \quad a_n = \frac{a^{(n)}(0)}{n!} \quad (n = 0, 1, 2, \dots).$$

Liegt z zudem im Inneren des Konvergenzkreises K_b der Potenzreihe $b(x)$, so gilt

$$(a * b)(z) = a(z) \cdot b(z) .$$

NOTA BENE: Die (Cauchy-)Multiplikation von konvergenten Potenzreihen ist mit der Substitution $z \mapsto x$ verträglich.

Erzeugende Funktionen. Man sagt, dass die Funktion $a : K_a \rightarrow \mathcal{R}$ die Koeffizienten a_0, a_1, a_2, \dots erzeugt. In etwas allgemeinerer Sprechweise nennt man jedoch schon die formale Potenzreihe $a(x) \in \mathcal{R}_\infty[x]$ (unabhängig von etwaiger Konvergenz) die erzeugende Funktion für die Koeffizientenfolge a_0, a_1, a_2, \dots und überträgt die für konvergente Potenzreihen bekannten linearen Operatoren der Differentiation und Integration auf allgemeine formale Potenzreihen:

$$a'(x) := a_1 + 2a_2x + 3a_3x^2 + \dots = \sum_{n=1}^{\infty} n a_{n+1} x^{n-1}$$

$$\int a(x) := a_0x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \dots = \sum_{n=0}^{\infty} \frac{a_n}{n+1} x^{n+1} .$$

2.1. Beispiele erzeugender Funktionen. Die Reihenentwicklungen bekannter (reeller oder komplexer) Funktionen geben sofort Beispiele von erzeugenden Funktionen für gewisse Koeffizientenfolgen:

$$\begin{aligned}
 e^x &= 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \dots \\
 \ln\left(\frac{1}{1-x}\right) &= x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + \dots \\
 \cos x &= 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 - \frac{1}{6!}x^6 + \dots \\
 \sin x &= x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7 + \dots \\
 \tan x &= x + \frac{1}{3}x^3 + 16\frac{2}{5}x^5 + \frac{17}{315}x^7 + \dots \\
 &\vdots
 \end{aligned}$$

Es gelten natürlich die bekannten Zusammenhänge wie z.B.

$$\begin{aligned}
 \sin^2 x + \cos^2 x &= 1 \\
 (\tan x) * (\cos x) &= \sin x.
 \end{aligned}$$

Als weiteres Beispiel betrachten wir die differenzierbare reelle Funktion

$$f(z) = (1+z)^a \quad (\text{mit festem } a \in \mathbb{R})$$

und erhalten über

$$\begin{aligned}
 f'(z) &= a(1+z)^{a-1} \\
 f''(z) &= a(a-1)(1+z)^{a-2} \\
 &\vdots \\
 f^{(n)} &= (a)_n(1+z)^{a-n},
 \end{aligned}$$

eine Potenzreihendarstellung von $f(z)$ als Taylorreihe:

$$(1+z)^a = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} z^n = \sum_{n=0}^{\infty} \frac{(a)_n}{n!} z^n.$$

Beispielsweise ergibt sich im Fall $a = -1/2$:

$$\begin{aligned}
 (-1/2)_n &= -\frac{1}{2} \left(-\frac{1}{2} - 1\right) \dots \left(-\frac{1}{2} - (n-1)\right) \\
 &= \frac{(-1)^n}{2^n} 1 \cdot 3 \cdot \dots \cdot (2n-1) = \frac{(-1)^n}{4^n} \cdot \frac{(2n)!}{n!}
 \end{aligned}$$

und deshalb

$$\frac{1}{\sqrt{1+z}} = \sum_{n=0}^{\infty} \frac{(-1)^n (2n)!}{4^n n!n!} z^n = \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n} \binom{2n}{n} z^n.$$

BEMERKUNG. Die sog. *Binomialreihe* ist die (formale) Potenzreihe

$$(31) \quad (1+x)^a = \sum_{n=0}^{\infty} \frac{(a)_n}{n!} x^n = \sum_{n=0}^{\infty} \binom{a}{n} x^n \quad \text{mit} \quad \binom{a}{n} := \frac{(a)_n}{n!}.$$

Ist a eine natürliche Zahl, so ist die Reihe endlich.

3 Rekursionen

In der Kombinatorik werden charakteristische Parameter grundsätzlich rekursiv definiert (vgl. Kapitel 1). Wir untersuchen hier die Frage, wie man nun aus einer gegebenen Rekursion explizite „Formeln“ für die Parameter gewinnen kann. \mathcal{R} bezeichnet immer den zugrunde liegenden Ring.

3.1. Lineare Rekursionen. Man sagt, die Folge $f_0, f_1, \dots, f_n, \dots$ von Koeffizienten $f_n \in \mathcal{R}$ erfüllt eine *lineare Rekursion der Länge k* , wenn es Koeffizienten $a_1, \dots, a_k \in \mathcal{R}$ gibt mit der Eigenschaft



AOK
Die Gesundheitskasse.

AOK-Liveonline – Powerstart für die Zukunft

Entdecken Sie die innovativen LIVEONLINE Vorträge der AOK. Wir bieten drei Themenfelder: Strategische Karriereplanung, Überzeugen im Auswahlverfahren sowie Study-Life-Balance. Jetzt schnell anmelden unter:

Gesundheit in besten Händen aok-on.de/nordost/studierende

AOK Studenten-Service

$$(32) \quad f_n = a_1 f_{n-1} + a_2 f_{n-2} + \dots + a_k f_{n-k}$$

für alle $n = k, k + 1, k + 2, \dots$. In diesem Fall ist f durch seine Anfangsglieder f_0, f_1, \dots, f_{k-1} und die Rekursion (32) festgelegt und die Koeffizienten f_n können iterativ berechnet werden.

Für die zugeordnete Potenzreihe $f(x) = \sum_{n=0}^{\infty} f_n x^n$ bedeutet die Rekursion:

$$\sum_{n=k}^{\infty} f_n x^n = a_1 x \sum_{n=k}^{\infty} f_{n-1} x^{n-1} + a_2 x^2 \sum_{n=k}^{\infty} f_{n-2} x^{n-2} + \dots + a_k x^k \sum_{n=k}^{\infty} f_{n-k} x^{n-k}.$$

Mit den Polynomen $p_j(x) = \sum_{i=0}^j f_i x^i$ für $j \geq 0$, hat man somit:

$$f(x) - p_{k-1}(x) = a_k x^k f(x) + \sum_{j=1}^{k-1} a_j x^j [f(x) - p_{k-1-j}(x)]$$

bzw.

$$f(x) - a_k x^k f(x) - \sum_{j=1}^{k-1} a_j x^j f(x) = p_{k-1}(x) - \sum_{j=1}^{k-1} a_j x^j p_{k-1-j}(x).$$

Daraus ergibt sich

$$(1 - a_1 x - \dots - a_k x^k) * f(x) = p_{k-1}(x) - a_1 x p_{k-2}(x) - \dots - a_{k-1} x^{k-1} p_0(x).$$

Das Polynom $1 - a_1 x - \dots - a_k x^k$ ist (als formale Potenzreihe betrachtet) invertierbar. Also erhalten wir eine Darstellung von $f(x)$ als Quotient zweier Polynome:

$$(33) \quad \boxed{f(x) = \frac{p_{k-1}(x) - a_1 x p_{k-2}(x) - \dots - a_{k-1} p_0 x^{k-1}}{1 - a_1 x - \dots - a_k x^k}}$$

Wir betrachten einige Beispiele.

Fibonacci-Zahlen. Die *Fibonacci*²⁴-Zahlen F_0, F_1, F_2, \dots sind rekursiv so definiert:

$$F_0 = F_1 = 1 \quad \text{und} \quad F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

24 L. FIBONACCI (ca. 1170-1250)

Die Rekursion ist linear von Länge $k = 2$ mit $a_1 = a_2 = 1$. Damit ist

$$p_{k-1}(x) - \dots - a_{k-1}x^{k-1}p_0(x) = 1 + x - x = 1$$

und folglich

$$F(x) = \sum_{n=0}^{\infty} F_n x^n = \frac{1}{1 - x - x^2}.$$

Im Fall $\mathcal{R} = \mathbb{R}$ zerfällt das Polynom im Nenner in ein Produkt:

$$x^2 + x - 1 = (x - \tau_1) * (x - \tau_2) \quad \text{mit} \quad \tau_1 = \frac{1}{2}(-1 + \sqrt{5}), \tau_2 = \frac{1}{2}(-1 - \sqrt{5}).$$

Mit $\tau_1 \tau_2 = -1$ berechnet man nun

$$\begin{aligned} \frac{\sqrt{5}}{1 - x - x^2} &= \frac{1}{\tau_1 - x} - \frac{1}{\tau_2 - x} \\ &= \frac{-\tau_2}{1 - (-\tau_2 x)} - \frac{-\tau_1}{1 - (-\tau_1 x)} \\ &= -\tau_2 \sum_{n=0}^{\infty} (-\tau_2)^n x^n - (-\tau_1) \sum_{n=0}^{\infty} (-\tau_1)^n x^n \\ &= \sum_{n=0}^{\infty} [(-\tau_2)^{n+1} - (-\tau_1)^{n+1}] x^n. \end{aligned}$$

Also:

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

Der zweite Term des Ausdrucks für F_n ist im Absolutbetrag immer echt kleiner als $1/2$. Bezeichnen wir mit $[r]$ die der reellen Zahl $r \in \mathbb{R}$ nächstgelegene ganze Zahl, so finden wir im Fall $\mathcal{R} = \mathbb{R}$:

PROPOSITION 4.2. $F_n = \left[\frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} \right]$ für alle $n = 0, 1, \dots$

BEMERKUNG. Unter dem sog. *goldenen Schnitt* versteht man die reelle Zahl

$$\tau^* = \frac{1 + \sqrt{5}}{2} \quad (= -\tau_2).$$

BEMERKUNG. Die explizite Darstellung von F_n gemäss Proposition 4.2 ist theoretisch befriedigend. In der rechnerischen Praxis wird man aber z.B. F_{100} lieber rekursiv ausrechnen als nach dieser Formel, um Rundungsfehlern des Computers besser zu begegnen. (Der Leser möchte das vielleicht selber überprüfen?)

Catalan-Zahlen. Die *Catalan*²⁵-Zahlen C_n sind definiert über eine nichtlineare(!) Rekursion

- (1) $C_0 = 0$ und $C_1 = 1$;
- (2) $C_n = C_1C_{n-1} + C_2C_{n-2} + \dots + C_{n-1}C_1 = \sum_{k=1}^{n-1} C_kC_{n-k} \quad (n \geq 2)$

Eine explizite Formel für C_n kann man über die Potenzreihen

$$C(x) = \sum_{n=1}^{\infty} C_n x^n \quad \text{bzw.} \quad C(x) - x = \sum_{n=2}^{\infty} C_n x^n$$

gewinnen. Aus der Rekursion sehen wir im Fall $\mathcal{R} = \mathbb{R}$ sofort

25 É. CATALAN (1814-1894)

Gemeinsam nachhaltig zum Erfolg.

Denn bei der REWE Group, einem der führenden Handels- und Touristikkonzerne Europas, ist Bewegung drin. Dafür sorgen unsere ca. 330.000 Mitarbeiter Tag für Tag: Sie liefern Tonnen von Waren, schicken Urlauber zu fernen Zielen oder verhandeln die günstigsten Preise. Sie halten die Welt am Laufen. Werden Sie Teil einer großen Gemeinschaft, die Großes bewirkt. Freuen Sie sich auf die Zusammenarbeit mit sympathischen Kollegen auf internationaler Ebene und erleben Sie, was Sie in unserer vielfältigen Marken- und Arbeitswelt bewegen können. Und durch individuelle Förderung bewegt sich auch Ihre Karriere, wohin immer Sie wollen.

Was bewegen Sie?

www.rewe-group.com/karriere
www.facebook.com/REWEGroupKarriere

Du bewegst.

330.000 **Mitarbeiter**
 523 **Berufe**
 1 **Zukunft**

REWE GROUP

REWE

nahkauf

PENNY

toom!
DER BAUMARKT

BILLA

MERKUR

BIPA

D&R
Touristik



LEMMA 4.1. Die Catalan-Zahl C_{n+1} ist die Anzahl der regulären Klammerungen, die man aus n Paaren von Klammern () konstruieren kann.

Dyck-Pfade. Ein Dyck-Pfad P durchläuft nichtnegative ganzzahlige Gitterpunkte $(x, y) \in \mathbb{N} \times \mathbb{N}$ der euklidischen Ebene \mathbb{R}^2 vom Ursprung $(0, 0)$ zu einem Punkt $(x_P, 0) \in \mathbb{N} \times \mathbb{N}$ auf der x -Achse nach der folgenden Regel:

$$(DP) \quad (x, y) \in P \implies (x + 1, y + 1) \in P \text{ oder } (x + 1, y - 1) \in P.$$

Der Parameter $|P| = x_P$ ist die Länge des Dyckpfads P .

LEMMA 4.2. Die Länge $|P|$ des Dyckpfades P ist eine gerade Zahl. Die Anzahl der Dyckpfade der Länge $2n$ ist durch die Catalanzahl C_{n+1} gegeben.

Beweis. P macht den Schritt $y \rightarrow (y + 1)$ genau so oft wie den Schritt $y \rightarrow (y - 1)$. $|P|$ ist Summe dieser Zahlen, also eine gerade Zahl. Man macht sich ausserdem leicht klar, dass Dyckpfade die gleiche rekursive Konstruktionseigenschaft aufweisen wie reguläre Klammerungen.

3.2. Urnenbelegungen. Wählen wir in der binomischen Reihe den Parameter a als negative ganze Zahl, d.h. als $a = -k$ mit $k \in \mathbb{N}$, so ergibt sich

$$\begin{aligned} \frac{1}{(1-x)^k} &= (1+(-x))^{-k} = \sum_{n=0}^{\infty} \frac{(-k)_n}{n!} (-1)^n x^n = \sum_{n=0}^{\infty} \frac{(k)_n}{n!} x^n \\ &= \sum_{n=0}^{\infty} \binom{k+n-1}{n} x^n. \end{aligned}$$

Andererseits gilt nach der Cauchyschen Multiplikationsregel

$$\frac{1}{(1-x)^k} = (1+x+x^2+\dots)^k = \sum_{n=0}^{\infty} c_n x^n \text{ mit } c_n := \sum_{\substack{0 \leq i_1, \dots, i_k \leq n \\ i_1 + \dots + i_k = n}} 1.$$

c_n ist genau die Anzahl der Möglichkeiten, n Kugeln über k Urnen zu verteilen. Per Koeffizientenvergleich erhalten wir aus den Reihen die (uns schon bekannte) Formel:

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

Weiterhin rechnen wir:

$$\frac{x^k}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} x^{n+k} = \sum_{n=k}^{\infty} \binom{n-1}{k-1} x^n = \sum_{n=k}^{\infty} \bar{c} x^n.$$

Multiplikation und Koeffizientenvergleich führt nun aus der Produktdarstellung

$$\begin{aligned} \frac{x^k}{(1-x)^k} &= \frac{x}{1-x} * \frac{x}{1-x} * \dots * \frac{x}{1-x} \\ &= (x + x^2 + \dots) * (x + x^2 + \dots) * \dots * (x + x^2 + \dots) \end{aligned}$$

direkt zu der Formel für die Anzahl der Möglichkeiten, n Kugeln so über k Urnen zu verteilen, dass keine Urne leer bleibt:

$$\binom{n-1}{k-1} = \bar{c}_n = \sum_{\substack{1 \leq i_1, \dots, i_k \leq n \\ i_1 + \dots + i_k = n}} 1.$$

EX. 4.4. *Wieviele verschiedene ganzzahlige Lösungen hat*



Bundesnachrichtendienst

einzigartige **Lösungen** einzigartigere **Ideen** einzigartige **Vielfalt**

Sie sind einzigartig? Wir auch!

einzigartiger **Auftrag** einzigartiger **Arbeitgeber**

Wir suchen

Ingenieure/innen der Elektro- und Informationstechnik

Informatiker/innen

mit den Abschlüssen **FH/Bachelor**

Mehr Informationen zum Thema Karriere beim BND unter www.bundesnachrichtendienst.de (Karriere)



$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = n$$

$$2 \leq x_1, x_2, x_3, x_4, x_5, x_6, x_7 \leq 6 ?$$

Sei a_n diese Anzahl und $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Dann haben wir

$$f(x) = (x^2 + x^3 + x^4 + x^5 + x^6)^7 = x^{14}(1 + x + x^2 + x^3 + x^4)^7$$

$$= x^{14} \left(\frac{1 - x^5}{1 - x}\right)^7 = x^{14}(1 - x^5)^7 \frac{1}{(1 - x)^7} (1 - x^5)^7$$

$$= x^{14} \sum_{i=0}^7 (-1)^i \binom{7}{i} x^{5i} \sum_{k=0}^{\infty} \binom{k+6}{k} x^k.$$

Daraus erhalten wir zum Beispiel für $n = 25$:

$$a_{25} = (-1)^0 \binom{7}{0} \binom{11+6}{11} + (-1)^1 \binom{7}{1} \binom{6+6}{6} (-1)^2 \binom{7}{2} \binom{1+6}{1}$$

$$= \binom{17}{11} - 7 \cdot 7 + \binom{7}{2} \cdot 7 = 12.474.$$

3.3. Summationsformeln. Sei $A(x) = \sum_{i=0}^{\infty} a_i x^i$ die erzeugende Funktion für die Koeffizientenfolge a_0, a_1, \dots : und

$$S(x) = \sum_{n=0}^{\infty} s_n x^n = \left(\sum_{i=0}^{\infty} a_i x^i\right) * \left(\sum_{j=0}^{\infty} x^j\right) = \frac{A(x)}{1 - x}.$$

Nach der Multiplikationsregel haben wir:

$$s_n = a_0 + a_1 + \dots + a_n \quad (n = 0, 1, \dots)$$

Mit anderen Worten:

- $S(x)$ ist die erzeugende Funktion für die Partialsummen s_n der Koeffizienten a_i .

Betrachten wir z.B. die Funktion

$$f(x) = (1 - x)^{-1} = \sum_{k=0}^{\infty} x^k$$

mit den Ableitungen

$$\begin{aligned}(1-x)^{-2} &= f'(x) = \sum_{k=0}^{\infty} (k+1)x^k \\ 2(1-x)^{-3} &= f''(x) = \sum_{k=0}^{\infty} (k+1)(k+2)x^k \\ 6(1-x)^{-4} &= f'''(x) = \sum_{k=0}^{\infty} (k+1)(k+2)(k+3)x^k \\ &\vdots\end{aligned}$$

Im Fall

$$\sum_{n=0}^{\infty} s_n^{(1)} x^n = S^{(1)}(x) = \frac{f'(x)}{1-x} = (1-x)^{-3}$$

ergibt sich dann die Summationsformel

$$1 + 2 + \dots + n = s_{n-1}^{(1)} = \frac{(n+1)n}{2}$$

Im Fall

$$\sum_{n=0}^{\infty} s_n^{(2)} x^n = S^{(2)}(x) = \frac{f''(x)}{1-x} = 2(1-x)^{-4}$$

finden wir

$$\sum_{n=0}^{\infty} s_n^{(2)} x^n = S^{(2)}(x) = \frac{f''(x)}{1-x} = 2(1-x)^{-4}$$

usw.

Daraus kann man neue Formeln gewinnen. Zum Beispiel so:

$$\sum_{k=1}^n k^2 = \sum_{k=1}^n k(k+1) - \sum_{k=1}^n k = s_{n-1}^{(2)} - s_{n-1}^{(1)}$$

ergibt:

$$1 + 2^2 + 3^2 + \dots + n^2 = n(n + 1)(n/3 + 1/6)$$

usw.

3.4. Typen erzeugender Funktionen. Sei f_0, f_1, \dots eine Folge von Koeffizienten. Dann ist

$$f(z) = \sum_{n=0}^{\infty} f_n z^n$$

eine erzeugende Funktion vom sog. *Standardtyp*. Eine Funktion der Form

$$\bar{f}(z) = \sum_{n=0}^{\infty} \frac{f_n}{n!} z^n$$

ist eine erzeugende Funktion vom *exponentiellen Typ*. Eine erzeugende Funktion vom *Dirichlet*²⁶ schen Typ für die Koeffizienten a_1, a_2, \dots ist

26 P.G. LEJEUNE DIRICHLET (1805-1859)



$$\tilde{f}(z) = \frac{a_1}{1^z} + \frac{a_2}{2^z} + \frac{a_3}{3^z} + \dots = \sum_{n=1}^{\infty} \frac{a_n}{z^n}.$$

Zum Beispiel ist die Riemann²⁷sche ζ -Funktion

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$$

eine erzeugende Funktion vom Dirichletschen Typ für die Koeffizienten $a_n = 1$ ($n \geq 1$).

Die verschiedenen Darstellungstypen sind deshalb von Interesse, weil sie zu verschiedenen Produktdarstellungen führen. Sei z.B.

$$\left(\sum_{i=0}^{\infty} \frac{f_i}{i!} z^i \right) * \left(\sum_{j=0}^{\infty} \frac{g_j}{j!} z^j \right) = \sum_{n=0}^{\infty} \frac{h_n}{n!} z^n$$

Dann gilt

$$\frac{h_n}{n!} = \sum_{i=0}^n \frac{f_i}{i!} \cdot \frac{g_{n-i}}{(n-i)!} \quad \text{d.h.} \quad h_n = \sum_{i=0}^n \binom{n}{i} f_i g_{n-i}.$$

Beim Dirichletschen Typ führt die Multiplikation

$$\left(\sum_{i=1}^{\infty} \frac{a_i}{i^z} \right) * \left(\sum_{j=1}^{\infty} \frac{b_j}{j^z} \right) = \sum_{n=1}^{\infty} \frac{c_n}{n^z}$$

auf das Ergebnis

$$\frac{c_n}{n^z} = \sum_{i \cdot j = n} \frac{a_i}{i^z} \cdot \frac{b_j}{j^z} \quad \text{d.h.} \quad c_n = \sum_{d|n} a_d b_{n/d},$$

wobei „ $d|n$ “ bedeutet, dass $d \in \mathbb{N}$ ein Teiler von $n \in \mathbb{N}$ ist.

27 B. RIEMANN (1826-1866)

Dérangements. Als Anwendung betrachten wir folgende Situation: Wir haben Strukturtypen A und B , die auf Mengen gegeben sein können. Mit a_n bzw. b_n bezeichnen wir die Anzahl aller Konfigurationen vom Typ A bzw. vom Typ B auf einer n -Menge. Dann ist

$$\binom{n}{k} a_k b_{n-k}$$

die Anzahl aller zusammengesetzten Konfigurationen auf einer n -Menge derart, dass eine k -elementige Teilmenge eine Konfiguration vom Typ A und deren Komplement eine $(n - k)$ -elementige Konfiguration vom Typ B darstellt. Die Anzahl aller zusammengesetzten Konfigurationen ist folglich

$$(36) \quad c_n = \sum_{k=0}^n \binom{n}{k} a_k b_{n-k} = n! \sum_{k=0}^n \frac{a_k}{k!} \cdot \frac{b_{n-k}}{(n-k)!}.$$

Die Beziehung (36) drückt aber gerade die Multiplikation der entsprechenden erzeugenden Funktionen vom exponentiellen Typ aus:

$$\sum_{n=0}^{\infty} \frac{c_n}{n!} x^n = \left(\sum_{k=0}^{\infty} \frac{a_k}{k!} x^k \right) \cdot \left(\sum_{j=0}^{\infty} \frac{b_j}{j!} x^j \right).$$

Wir illustrieren diese Situation konkret anhand von Permutationen:

Sei $M = \{1, \dots, n\}$ eine Menge und Potenzreihe eine Permutation von M . $i \in M$ ist ein Fixpunkt von Potenzreihen, wenn $i = \pi(i)$ gilt. Hat π genau k Fixpunkte, so bewirkt π auf den übrigen $n - k$ Elementen ein sog. *Dérangement*, d.h. eine fixpunktfreie Permutation. Für die Anzahl d_n aller Dérangements einer n -Menge gilt offenbar

Gemäss (36) bedeutet dies für die entsprechenden Potenzreihen:

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = \left(\sum_{k=0}^{\infty} \frac{1}{k!} x^k \right) * \left(\sum_{j=0}^{\infty} \frac{d_j}{j!} x^j \right) = e^x * D(x).$$

Da die Potenzreihe e^x die Inverse e^{-x} besitzt, können wir nach $D(x)$ auflösen und erhalten

$$D(x) = \sum_{n=0}^{\infty} \frac{d_n}{n!} x^n = \frac{e^{-x}}{1-x} = \left(\sum_{k=0}^{\infty} \frac{(-1)^k}{k!} x^k \right) * \left(\sum_{j=0}^{\infty} x^j \right)$$

und somit (mit $\mathcal{R} = \mathbb{R}$ und e als der Eulerschen Zahl) eine explizite Formel für die Dérangementanzahlen d_n :

$$\boxed{d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}} \quad \text{d.h.} \quad \left| d_n - \frac{n!}{e} \right| \leq \frac{1}{(n+1)!} .$$

4 Asymptotische Eigenschaften

Man nennt zwei Funktionen $f, g \in \mathbb{R}^{\mathbb{N}}$ asymptotisch gleich, wenn der folgende Limes existiert:

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1 .$$

Man notiert asymptotische Gleichheit auch mit $f(n) \sim g(n)$ und sagt, dass f und g die gleiche *Wachstumsrate* haben. Man sagt, dass f *langsamer wächst als* g , wenn



SEW-EURODRIVE — Driving the world



Gestalten Sie die Technologien der Zukunft!

Clevere Köpfe mit Lust auf Neues gesucht.
Wir sind einer der Innovationsführer weltweit im Bereich Antriebstechnologie und bieten Studierenden der Fachrichtungen Elektrotechnik, Maschinenbau, Mechatronik, (Wirtschafts-) Informatik oder auch Wirtschaftsingenieurwesen zahlreiche attraktive Einsatzgebiete. Sie möchten uns zeigen, was in Ihnen steckt? Dann herzlich willkommen bei SEW-EURODRIVE!

Jährlich 120 Praktika und Abschlussarbeiten

www.karriere.sew-eurodrive.de



$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0.$$

EX. 4.5 (Fibonaccizahlen). Für $F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^{n+1}$ findet man sofort

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

EX. 4.6 (Dérangements). Bei den Dérangementanzahlen d_n hat man

$$\lim_{n \rightarrow \infty} \frac{d_n}{n!/e} = \frac{1}{e} \left(\lim_{n \rightarrow \infty} \sum_{k=0}^n \frac{(-1)^k}{k!} \right) = 1$$

und somit $d_n \sim n!/e$.

4.1 Asymptotik der Binomialkoeffizienten.

LEMMA 4.3. Seien a_0, a_1, \dots positive reelle Zahlen $a_n > 0$ derart, dass es Konstanten α, β gibt mit der Eigenschaft

$$\frac{a_{n+1}}{a_n} = \frac{n + \alpha}{n + \beta} = \frac{1 + \alpha/n}{1 + \beta/n} \quad (n = 0, 1, 2, \dots).$$

Dann existiert eine Konstante c mit der Eigenschaft

$$a_n \sim c \cdot n^{\alpha-\beta}.$$

Beweis. Wir setzen zur Abkürzung $\gamma = \alpha - \beta$. Wir zeigen, dass der folgende Limes existiert:

$$K = \lim_{n \rightarrow \infty} \ln \frac{a_n}{n^\gamma} = \lim_{n \rightarrow \infty} (\ln a_n - \gamma \ln n).$$

(Die Konstante $c = e^K$ hat dann die gewünschte Eigenschaft.) Wir wollen mit dem Cauchy-Kriterium zeigen, dass die Folge

$$\tilde{a}_n = \ln a_n - \gamma \ln n$$

konvergiert. Dazu betrachten wir die in einer Umgebung von $t_0 = 0$ zweimal stetig differenzierbare Funktion

$$f(t) = \ln \left(\frac{1 + \alpha t}{1 + \beta t} \right).$$

Zu f existiert eine Konstante F derart, dass bei genügend kleinem $|t|$ gilt:

$$|f(t) - f(0) - f'(0)t| \leq Ft^2.$$

Wegen $f(0) = 0$ und $f'(0) = \alpha - \beta = \gamma$ gibt es somit ein $N \in \mathbb{N}$ derart, dass für alle $n \geq N$ (bzw. $t = 1/n$) gilt:

$$|\ln a_{n+1} - \ln a_n - \gamma/n| = |\ln(a_{n+1}/a_n) - \gamma/n| \leq F/n^2.$$

Nach der Dreiecksungleichung ergibt sich daraus für alle $m > 0$:

$$\begin{aligned} \left| \ln a_{n+m} - \ln a_n - \gamma \sum_{k=0}^{m-1} \frac{1}{n+k} \right| &\leq \sum_{k=0}^{m-1} |\ln a_{n+(k+1)} - \ln a_{n+k} - \gamma/(n+k)| \\ &\leq F \sum_{k=0}^{m-1} \frac{1}{(n+k)^2} \leq F \sum_{j=N}^{\infty} \frac{1}{j^2} < \infty. \end{aligned}$$

Da $\sum_{j=1}^{\infty} 1/j^2$ konvergiert, kann zu jedem vorgegebenen $\varepsilon > 0$ das N so gross gewählt werden, dass

$$\left| \ln a_{n+m} - \ln a_n - \gamma \sum_{k=0}^{m-1} \frac{1}{n+k} \right| < \varepsilon/2 \quad \text{für alle } n+m \geq n \geq N.$$

Folglich finden wir (wieder mit der Dreiecksungleichung)

$$\begin{aligned} &|\tilde{a}_{n+m} - \tilde{a}_n| \\ &= \left| \ln a_{n+m} - \ln a_n - \gamma \ln \frac{n+m}{n} \right| \\ &\leq \left| \ln a_{n+m} - \ln a_n - \gamma \sum_{k=0}^{m-1} \frac{1}{n+k} \right| + |\gamma| \cdot \left| \sum_{k=0}^{m-1} \frac{1}{n+k} - \ln \frac{n+m}{n} \right| \\ &< \varepsilon/2 + |\gamma| \cdot \left| \sum_{j=n}^{n+m-1} \frac{1}{j} - \ln(n+m) + \ln n \right|. \end{aligned}$$

Nun muss man sich noch davon überzeugen, dass der letztere Ausdruck beliebig klein (d.h. $< \varepsilon/2$) gemacht werden kann. Das ist aber klar, wenn man sich an die harmonischen Zahlen

$$H_n = \sum_{j=1}^n \frac{1}{j} \sim \ln n$$

erinnert. Denn wir haben

$$\begin{aligned} \left| \sum_{j=n}^{n+m-1} \frac{1}{j} - \ln(n+m) + \ln n \right| &= |H_{n+m-1} - \ln(n+m) + (\ln n - H_{n-1})| \\ &\leq |H_{m+n} - \ln(n+m)| + |\ln n - H_{n-1}|. \end{aligned}$$

(Die Details der letzten Behauptung seien dem Leser überlassen!)

Betrachten wir nun (zu einem gegebenen $r \in \mathbb{R}$) die Binomialkoeffizienten

$$b_n = \binom{r}{n} = \frac{(r)_n}{n!} = \frac{r(r-1)\dots(r-n+1)}{n!} \quad (n = 0, 1, \dots).$$

Gilt $r \in \mathbb{N}$, dann ist die Folge der b_n endlich (und hat deshalb keine interessante asymptotische Eigenschaft). Sei z.B. $r > 0$ eine nicht-natürliche reelle Zahl. Dann hat man

> Apply now

REDEFINE YOUR FUTURE
AXA GLOBAL GRADUATE PROGRAM 2015

redefining / standards 

agence c&is - © Photonistop



$$a_n = (-1)^{n-\lfloor r+1 \rfloor} b_n > 0 \quad \text{für grosse } n$$

und

$$\frac{a_{n+1}}{a_n} = \frac{n-r}{n+1}.$$

Lemma 4.3 garantiert somit die Existenz einer Konstanten c mit der Eigenschaft $a_n \sim cn^{-(r+1)}$. Daraus ergibt sich

$$\binom{r}{n} \sim (-1)^{n-\lfloor r+1 \rfloor} cn^{-(r+1)}$$

EX. 4.7 (Catalanzahlen). Für die Zahlen $a_n = C_{n+1}/4^n$ gilt

$$\frac{a_{n+1}}{a_n} = \frac{C_{n+2}}{4C_{n+1}} = 1 - \frac{6}{4(n+2)} = \frac{n+1/2}{n+2}$$

und somit $\gamma = 1/2 - 2 = -3/2$. Also hat man

$$a_n \sim cn^{-3/2} \quad \text{bzw.} \quad C_{n+1} \sim c \frac{4^n}{\sqrt{n^3}}.$$

Das heisst: Die f_n wachsen langsamer als n .

4.2. Langsames Wachstum. Sei $f(x) = \sum_{n=0}^{\infty} f_n x^n$ eine Potenzreihe mit Konvergenzradius ρ und reellen Koeffizienten $f_n \geq 0$ und $\varepsilon > 0$ beliebig. Dann ergibt sich im Fall $0 < 1/\varepsilon < \rho$ die konvergente Reihe

$$f(1/\varepsilon) = \sum_{n=0}^{\infty} \frac{f_n}{\varepsilon^n} \quad \text{und folglich} \quad \lim_{n \rightarrow \infty} \frac{f_n}{\varepsilon^n} = 0.$$

Das heisst: Die f_n wachsen langsamer als ε^n .

Zum Beispiel wachsen im Fall $\rho = \infty$ die Koeffizienten f_n langsamer als jede beliebige Folge der Form ε^n mit $\varepsilon > 0$.

5 Inzidenzalgebra

Man kann das Modell (formaler) Potenzreihen verallgemeinern, indem man eine zusätzliche „azyklische“ Grundstruktur, die gewisse Ordnungsbeziehungen zwischen Elementen der Grundmenge festhält, in die Betrachtungen mit einbezieht. Dadurch ist man in der Lage, mit Potenzreihentechniken auch ordnungstheoretische Strukturaspekte kombinatorisch zu erfassen. Diese Idee wurde zuerst von Rota²⁸ klar formuliert. Wir beschreiben zunächst das allgemeine algebraische Modell.

Sei $P = (M, \prec)$ eine (nicht notwendigerweise endliche) Menge mit einer binären Relation „ \prec “. Wir nehmen an, dass \prec *azyklisch* ist, d.h. es gibt keine Elemente $x_0, x_1, \dots, x_k \in M$ derart, dass

$$(AZ) \quad x_0 \prec x_1 \prec \dots \prec x_k \prec x_0.$$

Wir schreiben $x \preceq y$ für den Fall $x \prec y$ oder $x = y$. Unter einem *Intervall* (bzgl. P) verstehen wir eine Teilmenge vom Typ

$$[x, y] := \{z \in M \mid x \preceq z \preceq y\}.$$

Um Summation (und insbesondere das Faltungsprodukt (37) unten) im Kontext $P = (M, \prec)$ als wohldefiniert zu garantieren, setzen wir zusätzlich voraus, dass P *lokal endlich* ist, d.h. dass alle Intervalle endlich sind:

$$(LE) \quad |[x, y]| < \infty \text{ für alle } x, y \in M.$$

BEMERKUNG (Transitivität). $P = (M, \prec)$ ist transitiv ist, falls für alle $x, y, z \in M$ gilt:

$$(T) \quad \text{Wenn } x \prec y \text{ und } y \prec z, \text{ dann auch } x \prec z.$$

Sehr viele azyklische Relationen von kombinatorischem Interesse sind auch transitiv. Für die allgemeine Theorie der Inzidenzalgebra genügt jedoch die Voraussetzung einer azyklischen Grundstruktur.

Die *Inzidenzalgebra* ist die $P = (M, \prec)$ zugeordnete Menge von Funktionen

$$\mathcal{A}(P) := \{f : M \times M \rightarrow \mathbb{R} \mid f(x, y) = 0 \text{ falls } x \not\preceq y\}.$$

$\mathcal{A}(P)$ ist offenbar ein Vektorraum über dem Körper \mathbb{R} der reellen Zahlen. Ausserdem ist auf $\mathcal{A}(P)$ das sog. Faltungsprodukt $h = f * g$ definiert, wobei

$$(37) \quad h(x, y) := \begin{cases} \sum_{x \preceq z \preceq y} f(x, z)g(z, y), & \text{wenn } x \preceq y \\ 0 & \text{sonst.} \end{cases}$$

MAN BEACHTE: Das Faltungsprodukt in $\mathcal{A}(P)$ ist nicht notwendigerweise kommutativ (s. Ex. 5.3).

EX. 5.1 (Dirac-Funktion). Die Dirac²⁹-Funktion $\delta \in \mathcal{A}(P)$ ist definiert als

$$\delta(x, y) := \begin{cases} 1 & \text{wenn } x = y \\ 0 & \text{wenn } x \neq y. \end{cases}$$

Es gilt: $\delta * f = f * \delta$ für alle $f \in \mathcal{A}(P)$ für alle $f \in \mathcal{A}(P)$ (d.h. δ ist das multiplikative Neutralelement).

EX. 5.2. Alle beliebigen $f, g, h \in \mathcal{A}(P)$ erfüllen das Assoziativgesetz

$$f * (g * h) = (f * g) * h$$

und die Distributivgesetze:

$$f * (g + h) = f * g + f * h \quad \text{und} \quad (f + g) * h = f * h + g * h.$$

EX. 5.3 (Matrixmultiplikation). Sei $M = \{1, \dots, n\}$ und $P = (M, <)$ die natürliche Ordnung $1 < 2 < \dots < n$ auf M . Die reelle Funktion $f : M \times M \rightarrow \mathbb{R}$ entspricht dann der $(n \times n)$ -Matrix F mit den Koeffizienten $f_{ij} := f(i, j)$. Im Fall $f \in \mathcal{A}(P)$ besteht die zusätzliche Eigenschaft

29 P. DIRAC (1902-1984)



» Ich habe den Weg zur KfW-Förderung verkürzt: von drei Wochen auf fünf Minuten.

Wir suchen kluge Köpfe, die nachhaltig etwas bewegen und verändern wollen. So wie Kerstin Kronenberger: Als IT-Projektmanagerin bei der KfW hat sie in einem interdisziplinären Team erreicht, dass Bauherren schon während des Beratungsgesprächs erfahren, ob die Wärmendämmung ihres Eigenheims gefördert werden kann. Damit leistet sie täglich einen innovativen Beitrag für mehr Kundennähe und den Klimaschutz. Und wann fangen Sie an?

Jetzt informieren auf www.kfw.de/karriere

Bank aus Verantwortung **KfW**

$$f(i, j) = 0 \quad \text{wenn } i \not\leq j,$$

welche bedeutet, dass F eine (obere) Dreiecksmatrix ist. Das Faltungsprodukt $f * g$ entspricht dem Produkt FG der zugeordneten Matrizen. Insbesondere ist $f \in \mathcal{A}(P)$ genau dann invertierbar, wenn $f(i, i) \neq 0$ für alle $i \in M$ gilt.

EX. 5.4 (Cauchyprodukt und Faltung). Sei $P = (\mathbb{N}, <)$ die natürlich geordnete Menge der nichtnegativen ganzen Zahlen. Jeder Funktion (bzw. formalen Potenzreihe) $f : \mathbb{N} \rightarrow \mathbb{R}$ ordnen wir eine Funktion $\tilde{f} \in \mathcal{A}(P)$ zu mit der Eigenschaft $\tilde{f}(x, y) := 0$, wenn $x > y$, und

$$\tilde{f}(x, y) := f(y - x), \quad \text{wenn } x \leq y.$$

Insbesondere hat man $f(x) = \tilde{f}(0, x)$ für alle $x \in \mathbb{N}$ und es gilt:

- Dem Cauchyprodukt $f * g$ zweier Funktionen $f, g : \mathbb{N} \rightarrow \mathbb{R}$ ist die Faltung $\tilde{f} * \tilde{g}$ zugeordnet.

1 Möbiusfunktion und -Funktion

Eine Kette der Länge k von x nach y in $P = (M, <)$ ist eine $(k + 1)$ -Permutation $\pi = x_0 x_1 \dots x_{k-1} x_k$ von M mit der Eigenschaft

$$x = x_0 < x_1 < \dots < x_{k-1} < x_k = y.$$

Wir betrachten nun die Indikatorfunktion $\kappa \in \mathcal{A}(P)$ mit der Eigenschaft

$$\kappa(x, y) = 1 \quad :\iff \quad x < y$$

und deren rekursiv definierte Potenzen

$$\kappa^0 := \delta, \kappa^1 := \kappa, \dots \quad \text{und allgemein} \quad \kappa^k := \kappa^{k-1} * \kappa.$$

Nach Definition der Faltung hat man

$$\kappa^k(x, y) = \sum_{x \preceq z \preceq y} \kappa^{k-1}(x, z) \kappa(z, y)$$

und sieht somit (per Induktion) sofort:

- $\kappa^k(x, y) = \text{Anzahl der Ketten der Länge } k \text{ von } x \text{ nach } y.$

Im Fall $x \preceq y$ ist die alternierende Summe

$$\mu(x, y) := \kappa^0(x, y) - \kappa^1(x, y) + \kappa^2(x, y) - \dots = \sum_{k=0}^{\infty} (-1)^k \kappa^k(x, y)$$

wohldefiniert, da (wegen der Endlichkeit des Intervalls $[x, y]$) ja nur endlich viele Summanden von 0 verschieden sind. Damit ergibt sich die sog. *Möbius*³⁰-Funktion der Inzidenzalgebra $\mathcal{A}(P)$ als

$$(38) \quad \mu := \kappa^0 - \kappa^1 + \kappa^2 - \dots = \sum_{k=0}^{\infty} (-1)^k \kappa^k.$$

Die Funktion $\zeta := \delta + \kappa \in \mathcal{A}(P)$ ist die sog. ζ -Funktion. Sie ist die Indikatorfunktion der binären Relation \preceq :

$$\zeta(x, y) = 1 \iff x \preceq y.$$

Wir finden:

$$\zeta * \mu = \delta * \mu + \kappa * \mu = \sum_{k=0}^{\infty} (-1)^k \kappa^k + \sum_{k=0}^{\infty} (-1)^k \kappa^{k+1} = \kappa^0 = \delta.$$

Mit anderen Worten:

$$(39) \quad \boxed{\text{Die Möbiusfunktion } \mu \text{ und die } \zeta\text{-Funktion } \zeta \text{ sind zueinander inverse Funktionen in } \mathcal{A}(P). \text{ D.h. } \mu = \zeta^{-1} \text{ und } \zeta = \mu^{-1}.}$$

1.1. Der Gitterverband. Als Beispiel betrachten wir die Menge $M = \mathbb{Z}^n$ aller n-dimensionalen Vektoren $\mathbf{x} = (x_1, \dots, x_n)$ mit ganzzahligen Komponenten x_i . Sei $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{Z}^n$ ein weiterer solcher Vektor. Dann setzen wir

$$\mathbf{x} \prec \mathbf{y} \iff \mathbf{x} \neq \mathbf{y} \text{ und } y_i - x_i \geq 0 \forall i = 1, \dots, n.$$

$P = (\mathbb{Z}^n, \prec)$ ist der n-dimensionale Gitterverband. Offenbar gilt dann in der Inzidenzalgebra $\mathcal{A}(P)$ mit $\mathbf{0} := (0, 0, \dots, 0)$:

$$\kappa(\mathbf{x}, \mathbf{y}) = \kappa(\mathbf{0}, \mathbf{y} - \mathbf{x})$$

und folglich

30 A.F. MÖBIUS (1790-1868)

$$\mu(\mathbf{x}, \mathbf{y}) = \mu(\mathbf{0}, \mathbf{y} - \mathbf{x}) \quad \text{und} \quad \zeta(\mathbf{x}, \mathbf{y}) = \zeta(\mathbf{0}, \mathbf{y} - \mathbf{x}).$$

Wir beschränken uns deshalb auf die Menge $\mathbb{Z}_+^n \subseteq \mathbb{Z}^n$ aller nichtnegativer Vektoren und schreiben die Möbiusfunktion und die ζ -Funktion abkürzend als

$$\mu(\mathbf{d}) := \mu(\mathbf{0}, \mathbf{d}) \quad (\mathbf{d} \in \mathbb{Z}_+^n).$$

Wir betrachten zuerst den Fall $n = 1$ und behaupten, dass für jedes $d \in \mathbb{Z}_+$ gilt:

$$(40) \quad \mu(d) = \begin{cases} +1 & \text{falls } d = 0 \\ -1 & \text{falls } d = 1 \\ 0 & \text{falls } d \geq 2. \end{cases}$$

Das folgt aber sofort aus Ex. 5.5 (was nachzurechnen dem Leser überlassen sei).

EX. 5.5. Es gilt $\zeta(0, d) = 1$ für alle $d \in \mathbb{Z}_+$. Für die zu ζ inverse Funktion μ muss gelten:



**Karriere als IT-Experte.
Hier ist Ihre Chance.**

Karriere gestalten als Praktikant, Trainee m/w oder per Direkteinstieg.
Ohne Jungheinrich bliebe Ihr Einkaufswagen vermutlich leer. Und nicht nur der. Täglich bewegen unsere Geräte Millionen von Waren in Logistikzentren auf der ganzen Welt.

Unter den Flurförderzeugherstellern zählen wir zu den Top 3 weltweit, sind in über 30 Ländern mit Direktvertrieb vertreten – und sehr neugierig auf Ihre Bewerbung.



www.jungheinrich.de/karriere

JUNGHEINRICH
Machines. Ideas. Solutions.



$$\delta(0, d) = \sum_{k=0}^d \zeta(0, k) \mu(k, d) = \sum_{k=0}^d \mu(d - k) = \sum_{k=0}^d \mu(k).$$

Die durch (40) definierte Funktion hat offenbar genau diese Eigenschaft. Also ist sie die Möbiusfunktion.

Die Möbiusfunktion ist nun auch im allgemeinen Fall $n \geq 2$ mit Hilfe von (40) leicht zu bestimmen:

PROPOSITION 5.1. Sei $\mathbf{d} = (d_1, d_2, \dots, d_n) \in \mathbb{Z}_+^n$ beliebig. Dann gilt die Produktformel

$$(41) \quad \boxed{\mu(\mathbf{d}) = \mu(d_1) \cdot \mu(d_2) \cdots \mu(d_n)}.$$

Beweis. Wir argumentieren mit Hilfe von Ex. 5.5 bzgl. der Produktformel:

$$\begin{aligned} \sum_{\mathbf{0} \preceq \mathbf{k} \prec \mathbf{d}} \mu(\mathbf{k}) &= \sum_{k_1=0}^{d_1} \sum_{k_2=0}^{d_2} \cdots \sum_{k_n=0}^{d_n} \mu(k_1) \mu(k_2) \cdots \mu(k_n) \\ &= \left(\sum_{k_1=0}^{d_1} \mu(k_1) \right) \cdot \left(\sum_{k_2=0}^{d_2} \cdots \sum_{k_n=0}^{d_n} \mu(k_2) \cdots \mu(k_n) \right) \\ &= \left(\sum_{k_1=0}^{d_1} \mu(k_1) \right) \cdot \left(\sum_{k_2=0}^{d_2} \mu(k_2) \right) \cdots \left(\sum_{k_n=0}^{d_n} \mu(k_n) \right) \\ &= \delta(0, d_1) \cdots \delta(0, d_{n-1}) \cdot \delta(0, d_n) \\ &= \delta(\mathbf{0}, \mathbf{d}). \end{aligned}$$

Das bedeutet $\zeta * \mu = \delta$ und folglich $\mu = \zeta^{-1}$, wie behauptet.

BEMERKUNG. Unter einem Verband versteht man in der diskreten Mathematik generell eine azyklische und transitive Struktur (V, \prec) derart, dass es zu je zwei Elementen $x, y \in V$ eindeutig bestimmte Elemente $x \wedge y, x \vee y \in V$ gibt mit der Eigenschaft:

- (1) $z \not\prec x \wedge y \implies z \not\prec x \text{ oder } z \not\prec y$ (für alle $z \in V$).
- (2) $z \not\prec x \vee y \implies z \not\prec x \text{ oder } z \not\prec y$ (für alle $z \in V$).

$x \wedge y$ ist das Infimum und $x \vee y$ das Supremum von x und y .

1.2. Der Teilverband. Wir betrachten nun die Menge $\mathbb{N}_1 = \mathbb{N} \setminus \{0\}$ aller positiven natürlichen Zahlen unter der binären und offenbar azyklischen Relation

$$m \prec n : \iff m \text{ ist ein echter Teiler von } n.$$

In diesem Kontext schreibt man oft $m \mid n$ anstelle von $m \preceq n$ und bezeichnet die Struktur $\mathcal{T} = (\mathbb{N}_1, \mid)$ als den *Teilverband*.

Bekanntlich können beliebige Zahlen $m, n \in \mathbb{N}_1$ als Produkte von Primzahlpotenzen ausgedrückt werden. Das heisst: Es gibt paarweise verschiedene Primzahlen p_1, \dots, p_k und Vektoren $\mathbf{x} = (x_1, \dots, x_k), \mathbf{y} = (y_1, \dots, y_k) \in \mathbb{Z}^k$ derart, dass

$$m = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k} \quad \text{und} \quad n = p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k},$$

und es gilt

$$m \mid n \quad :\iff \quad x_i \leq y_i \quad \forall i = 1, \dots, k.$$

Das Intervall $[m, n]$ hat folglich bzgl. \mathcal{T} die gleiche Kettenstruktur wie das Intervall $[x, y]$ im Gitterverband \mathbb{Z}^k und somit auch den gleichen Möbiusfunktionswert. Damit erhalten wir die klassische Möbiusfunktion μ der Zahlentheorie und schliessen aus (40) und (41):

$$(42) \quad \mu(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \begin{cases} 0 & \text{wenn ein } e_i \geq 2 \text{ existiert} \\ (-1)^{\sum_{i=1}^k e_i} & \text{sonst.} \end{cases}$$

EX. 5.6 (Riemanns ζ -Funktion). Die klassische ζ -Funktion der Zahlentheorie ist definiert für komplexe Zahlen z als

$$\zeta(z) := \sum_{n=1}^{\infty} \frac{1}{n^z}$$

Da die Möbiusfunktion des Teilverbandes zur Inzidenzfunktion des Teilverbandes invers ist, ergeben die Rechenregeln (Cauchy-Multiplikation) formaler Potenzreihen:

$$\frac{1}{\zeta(z)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^z}.$$

1.3. Potenzmengenverbände. Sei $N = \{1, 2, \dots, n\}$ und M die Menge aller Teilmengen $S \subseteq N$. Wir setzen

$$S \prec T \quad :\iff \quad S \subset T \quad (S, T \subseteq N).$$

Dann ist $P = (M, \subset)$ der *Potenzmengenverband* von N . Stellen wir die Teilmengen $S \subseteq N$ durch ihre Indikatorvektoren in $\{0, 1\}^n \subseteq \mathbb{Z}^n$ dar, so finden wir, dass die Möbiusfunktion auf P der Möbiusfunktion ihres Indikators im Gitterverband entspricht. Also gilt nach (40) und (41):

$$(43) \quad \mu(S) = (-1)^{|S|} \quad \text{für alle } S \subseteq N.$$

2 Möbiusinversion und Siebformel

Sei nun $\mathcal{A} = \mathcal{A}(M, \prec)$ eine beliebige Inzidenzalgebra bzgl. der azyklischen Binärrelation \prec auf M . Eine Funktion $\varphi \in \mathcal{A}$ induziert auf \mathcal{A} die Transformation

$$f \mapsto f^\varphi := \varphi * f.$$

Ist $\psi \in \mathcal{A}$ eine weitere Funktion der Inzidenzalgebra, so gilt wegen der Assoziativität der Faltung:

$$(f^\varphi)^\psi = \psi * (\varphi * f) = (\psi * \varphi) * f = f^{\psi * \varphi}.$$

Der Spezialfall der Wahl $\varphi = \zeta$ und $\psi = \mu$ führt deshalb sofort auf die folgende, als Möbiusinversion bekannte, Identität für beliebige Funktionen $f \in \mathcal{A}$:

$$(44) \quad \boxed{(f^\zeta)^\mu = f}$$

2.1. Diskrete Integrale. Einer beliebigen Funktion $f : M \rightarrow \mathbb{R}$ können wir eine Art Integral in der Inzidenzalgebra $\mathcal{A}(M, \prec)$ zuordnen, indem wir definieren

Die Antwort ist 42.

Oder Baden-Württemberg.







Baden-Württemberg
Wir können alles. Außer Hochdeutsch.



$$F(x, y) := \sum_{x \preceq z \preceq y} f(z).$$

Interpretieren wir $f \in \mathbb{R}^M$ als eine Funktion $\bar{f} \in \mathcal{A}$ der Inzidenzalgebra mit den Werten

$$\bar{f}(x, y) := \begin{cases} f(x) & \text{falls } x \preceq y \\ 0 & \text{falls } x \not\preceq y, \end{cases}$$

so finden wir

$$F(x, y) = \sum_{x \preceq z \preceq y} \zeta(x, z) \bar{f}(z, y) = \bar{f}^\zeta(x, y).$$

Möbiusinversion ergibt somit

$$(45) \quad \boxed{f(x) = \bar{f}(x, y) = F^\mu(x, y) = \sum_{x \preceq z \preceq y} \mu(x, z) F(z, y) .}$$

BEMERKUNG. (45) kann man so interpretieren: Die Anwendung der Möbiusfunktion μ auf das Integral F ergibt den Integranden f als "Ableitung" zurück.

2.2. Die Siebformel. Sei M die Potenzmenge der endlichen Menge N und $\mathcal{A} = \mathcal{A}(M, \subseteq)$ die Inzidenzalgebra der Enthaltenseinsrelation. Ausserdem ordnen wir einer Funktion $f : M \rightarrow \mathbb{R}$ ihre summatorische Funktion $F : M \rightarrow \mathbb{R}$ zu mit den Werten

$$F(S) := \sum_{T \supseteq S} f(T) \quad (S \subseteq N).$$

Aus der Möbiusinversionsformel (45) ergibt sich nun die sog. *Siebformel*

$$(46) \quad \boxed{f(S) = \sum_{T \supseteq S} \mu(S, T) F(T) = \sum_{T \supseteq S} (-1)^{|T|-|S|} F(T) \quad (S \subseteq N) .}$$

Der Spezialfall $S = \emptyset$ liefert

$$\begin{aligned}
 f(\emptyset) &= \sum_{T \subseteq N} (-1)^{|T|} F(T) \\
 &= F(\emptyset) - \sum_{i \in N} F(\{i\}) + \sum_{\{i,j\} \subseteq N} F(\{i,j\}) - \dots
 \end{aligned}$$

BEMERKUNG. Die Siebformel ist auch als *Prinzip von Inklusion-Exklusion* bekannt.

Das Sieb des Eratosthenes. Sei \mathcal{G} eine endliche Menge von Gegenständen und $\mathcal{E} = \{E_1, \dots, E_n\}$ Eng eine Menge von Eigenschaften, die die Gegenstände aufweisen können. Wir definieren für $i = 1, \dots, n$:

$$A_i := \{G \in \mathcal{G} \mid G \text{ besitzt die Eigenschaft } E_i\}.$$

Für jede Teilmenge $S \subseteq \{1, \dots, n\}$ ng sei

$$f(S) := |\{G \in \mathcal{G} \mid G \text{ hat genau die Eigenschaften } E_i \text{ mit } i \in S\}|.$$

Die summatorische Funktion von f ist die Funktion

$$F(S) = |\{G \in \mathcal{G} \mid G \in A_i \forall i \in S\}|.$$

Also ergibt sich die Anzahl der Gegenstände, die *keine* der Eigenschaften in ϵ aufweisen nach der Siebformel (46) als

$$(47) \quad f(\emptyset) = |\mathcal{G}| - \sum_i |A_i| + \sum_{i < j} |A_i \cap A_j| - \sum_{i < j < k} |A_i \cap A_j \cap A_k| + \dots$$

BEMERKUNG. Die Zählmethode gemäss (47) ist das sog. *Sieb des Eratosthenes*³¹.

EX. 5.7. In einer Gruppe von 73 Leuten spielen 52 Klavier, 25 Geige, 20 Flöte, 17 Klavier und Geige, 12 Klavier und Flöte, 7 Geige und Flöte. Genau eine Person beherrscht alle 3 Instrumente. Wieviel Personen spielen kein Instrument?

Um diese Frage zu beantworten, betrachten wir die Menge $\mathcal{G} = \{kl, ge, fl\}$ und definieren für jedes $T \subseteq \mathcal{G}$ den Wert $F(T)$ als die Anzahl der Leute, die (mindestens) die Instrumente in T spielen. Dann haben wir

$$\begin{array}{llll}
 F(\emptyset) &= 73, & F(kl) &= 52, & F(ge) &= 25 \\
 F(fl) &= 20, & F(kl, ge) &= 17, & F(kl, fl) &= 12 \\
 F(ge, fl) &= 7, & F(kl, ge, fl) &= 1 & &
 \end{array}$$

und berechnen die gesuchte Zahl nach der Siebformel als

31 ERATOSTHENES (276-195 v.Chr.)

$$f(\emptyset) = 73 - (52 + 25 + 20) + (17 + 12 + 7) - 1 = 11 .$$

Urnenbelegungen. Es werden n Kugeln über die r verschiedenen Urnen U_1, U_2, \dots, U_r „zufällig“ verteilt. Für jedes $\bar{S} \subseteq R = \{1, \dots, r\}$ sei $P(S)$ die Wahrscheinlichkeit dafür, dass die Urnen U_i mit Index $i \in S$ (und möglicherweise andere) leer bleiben. $p(S)$ bezeichne dagegen die Wahrscheinlichkeit, dass *genau* die Urnen U_i mit Index $i \in S$ leer (und die übrigen nichtleer) sind. Dann ist P die summatorische Funktion von p :

$$P(S) = \sum_{T \supseteq S} p(T).$$

Folglich ergibt sich die Wahrscheinlichkeit dafür, dass keine Urne leer bleibt, nach der Siebformel als

$$p(\emptyset) = \sum_{S \subseteq R} (-1)^{|S|} P(S).$$

Zum Beispiel gilt im Spezialfall, wo alle r^n möglichen Verteilungen der Kugeln auf die Urnen gleichwahrscheinlich sind

MASTER OF SCIENCE IN MANAGEMENT



BUSINESS GAME

23 & 24 May 2014

- Work on a business case
- Interact with students & alumni
- Stay a night at our campus

www.nyenrode.nl/businessgame





The Master of Science in Management has been voted the Best Master 2014 in the Netherlands for the fifth time running. This could only be achieved because of our remarkable students. Our students distinguish themselves by having the courage to take on challenges and through the development of the leadership, entrepreneurship and stewardship skills. This makes the

Master program at Nyenrode an achievement, from which you can benefit for the rest of your life. During this program you will not only learn in class, you will also develop your soft skills by living on campus and by working together in the student association. Do you think this program is something for you? Then it is our pleasure to invite you to Nyenrode. Go to www.nyenrode.nl/msc or call +31 346 291 291.



NYENRODE. A REWARD FOR LIFE



$$P(S) = \frac{(r - |S|)^n}{r^n} \quad \left(= \frac{\text{Anz. günstige Fälle}}{\text{Anz. mögliche Fälle}} \right)$$

und folglich

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

Dérangements. Werfen wir nochmals einen Blick auf Dérangements (s. Abschnitt 3.4) von der Warte der Siebformel. $p(S)$ bezeichne die Wahrscheinlichkeit dafür, dass bei einer zufälligen Permutation π der Menge $N = \{1, \dots, n\}$ genau S als die Menge der Fixpunkte auftritt. Dann ergibt sich als zugehörige summatorische Funktion

$$\sum_{T \supseteq S} p(T) =: P(S) = \frac{|N \setminus S|!}{n!}$$

und folglich die Wahrscheinlichkeit dafür, dass eine zufällig gewählte Permutation fixpunktfrei ist, als

$$p(\emptyset) = \sum_{S \subseteq N} (-1)^{|S|} P(S) = \sum_{k=0}^n \binom{n}{k} (-1)^k \frac{(n - k)!}{n!} = \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

Die Eulersche Φ -Funktion. Sei $n \geq 2$ eine natürliche Zahl mit den k verschiedenen Primfaktoren p_1, p_2, \dots, p_k . Die *Eulersche Φ -Funktion* ist definiert über die Anzahl

$$\Phi(n) := |\{m \mid 1 \leq m \leq n, \text{ggT}(m, n) = 1\}|$$

der zu n teilerfremden kleineren Zahlen m (d.h. die Zahlen $m \leq n$, die 1 als grössten gemeinsamen Teiler mit n haben). Zur Untersuchung von $\Phi(n)$ betrachten wir die Menge

$$P = \{p_1, p_2, \dots, p_k\}$$

und definieren für alle Teilmengen $S \subseteq P$ den Wert $f(S)$ als die Anzahl der Zahlen $m \leq n$, die genau die Zahlen in S als Teiler haben. Die summatorische Funktion

$$F(S) = \sum_{S \subseteq T} f(T)$$

zählt dann die Anzahl der Vielfachen des Produktes, die kleiner oder gleich n sind. D.h.:

$$F(\emptyset) = n \quad \text{und} \quad F(p_{i_1}, \dots, p_{i_s}) = \frac{n}{p_{i_1} \cdots p_{i_s}}$$

Daraus ergibt sich die Darstellung

$$\begin{aligned} \Phi(n) = f(\emptyset) &= n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_k}\right) + n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \dots\right) - \\ &\quad - n\left(\frac{1}{p_1 p_2 p_3} + \frac{1}{p_1 p_2 p_4} + \dots\right) + n\left(\frac{1}{p_1 p_2 p_3 p_4} + \dots\right) - \dots \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Ist $d \geq 1$ ein Teiler von n mit einem (mindestens) quadratisch auftretenden Primfaktor, so verschwindet die Möbiusfunktion der Teilbarkeitsrelation: $\mu(d) = 0$ (s. Abschnitt 1.2). Deshalb können wir die obige Darstellung auch so schreiben:

$$\Phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{m|n} m \mu\left(\frac{n}{m}\right)$$

Dies bedeutet, dass die Eulersche Funktion $\Phi(n)$ per Möbiusinversion aus der Funktion $F(m, n) = n$ gewonnen wird. Folglich ist F die summatorische Funktion von Φ und es gilt

$$\sum_{d|n} \phi(d) = n.$$

3 Eulercharakteristik und Kettenkomplexe

Sei X eine beliebige Menge. Unter einem *Komplex* verstehen wir eine endliche Familie \mathcal{F} endlicher Teilmengen $F \subseteq X$ mit $\emptyset \in \mathcal{F}$. Die Mengen $F \in \mathcal{F}$ gewichten wir mit

$$e(F) := \begin{cases} (-1)^{|F|-1} & \text{im Fall } F \neq \emptyset \\ 0 & \text{im Fall } F = \emptyset. \end{cases}$$

und definieren dann die *Eulercharakteristik* des Komplexes \mathcal{F} als den Parameter

$$(48) \quad \chi(\mathcal{F}) := \sum_{F \in \mathcal{F}} e(F) = \sum_{F \in \mathcal{F} \setminus \{\emptyset\}} (-1)^{|F|-1}.$$

$\chi(\mathcal{F})$ misst also im nichttrivialen Fall die Diskrepanz zwischen der Anzahl der nichtleeren Mengen $F \in \mathcal{F}$ ungerader Kardinalität $|F|$ und der Anzahl der nichtleeren Mengen $F' \in \mathcal{F}$ gerader Kardinalität $|F'|$:

$$\chi(\mathcal{F}) = \sum_{|F| \text{ ungerade}} (+1) + \sum_{|F'| \text{ gerade}} (-1) = \sum_{|F| \text{ ungerade}} 1 - \sum_{|F'| \text{ gerade}} 1.$$

EX. 5.8. Sei X endlich mit Potenzmenge \mathcal{F} . Dann haben wir

$$\sum_{F \in \mathcal{F}} (-1)^{|F|} = \sum_{k=0}^{|X|} (-1)^k \binom{|X|}{k} = 0$$

und folglich

$$\chi(\mathcal{F}) = \sum_{k=1}^{|X|} (-1)^{k-1} \binom{|X|}{k} = 1.$$

Vereinigung und Durchschnitt zweier Komplexe \mathcal{F}_1 und \mathcal{F}_2 sind wieder Komplexe. Ausserdem macht man leicht sich das sog. modulare Gesetz klar:

Think Umeå. Get a Master's degree!

- modern campus • world class research • international atmosphere
- 36 000 students • top class teachers • no tuition fees

Master's programmes:

- Architecture • Industrial Design • Science • Engineering

Umeå University
Sweden
www.umu.se

APPLY NOW!



$$(49) \quad \chi(\mathcal{F}_1) + \chi(\mathcal{F}_2) = \chi(\mathcal{F}_1 \cup \mathcal{F}_2) + \chi(\mathcal{F}_1 \cap \mathcal{F}_2).$$

Denn eine Teilmenge F trägt zur linken Seite von (49) denselben Wert bei wie zur rechten.

Sei nun $P = (M, \prec)$ eine transitive und azyklische Struktur und $x, y, z \in M$ Elemente mit $x \prec y$. Wir ordnen dem offenen Intervall

$$(x, y) := \{z \in M \mid x \prec z \prec y\}$$

die Menge $\mathcal{C} = \mathcal{C}(x, y)$ aller Ketten $C \subseteq (x, y)$ als seinen Kettenkomplex zu. Dann erhalten wir

$$f_i := |\{C \in \mathcal{C}(x, y) \mid |C| = i\}| = \kappa^{i+1}(x, y) \quad (i = 1, 2, \dots)$$

und können somit die Eulercharakteristik des Kettenkomplexes \mathcal{C} mittels der Möbiusfunktion μ von P ausdrücken:

$$\chi(\mathcal{C}) = f_1 - f_2 + f_3 \pm \dots = \sum_{i=1}^{\infty} (-1)^{i+1} \kappa^{i+1}(x, y) = \mu(x, y) + 1.$$

4 Planare Graphen

In diesem Abschnitt illustrieren wir Anwendungen der Eulercharakteristik auf planare Graphen. Der Einfachheit halber behandeln wir dabei die geometrisch-topologischen Aspekte von in der Ebene \mathbb{R}^2 gezeichneten Graphen etwas informell.

4.1. Kanten, Pfade und plane Graphen. Sei $e : (0, 1) \rightarrow \mathbb{R}^2$ eine stetige injektive Abbildung vom offenen Einheitsintervall $(0, 1) \subseteq \mathbb{R}$ in die euklidische Ebene \mathbb{R}^2 . Wir identifizieren e mit seinem Bild $e(0, 1) \subseteq \mathbb{R}^2$ und nennen e eine (geometrische) Kante, wenn es Punkte $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2 \setminus e$ gibt mit der Eigenschaft

$$\mathbf{x} = \lim_{t \rightarrow 0} e(t) \quad \text{und} \quad \mathbf{y} = \lim_{t \rightarrow 1} e(t).$$

x und y sind dann die Endpunkte der Kante e . Ein Pfad von x nach y ist eine Folge

$$P = \mathbf{x}_1 e_1 \mathbf{x}_2 e_2 \mathbf{x}_3 \dots \mathbf{x}_\ell e_\ell \mathbf{x}_{\ell+1}$$

von endlich vielen paarweise disjunkten Kanten e_i mit Endpunkten \mathbf{x}_i und \mathbf{x}_{i+1} derart, dass $\mathbf{x} = \mathbf{x}_1$ und $\mathbf{x}_{\ell+1} = \mathbf{y}$. Im Fall $\mathbf{x} = \mathbf{y}$ ist P geschlossen. Ein geschlossener Pfad mit mindestens einer Kante ist ein Kreis, wenn kein Endpunkt einer Kante mehr als einmal auftritt. Ein Kreis mit genau einer Kante ist eine Schlinge.

EX. 5.9 (Schlichter Pfad). Der Pfad $P = \mathbf{x}_1 e_1 \mathbf{x}_2 e_2 \mathbf{x}_3 \dots \mathbf{x}_\ell e_\ell \mathbf{x}_{\ell+1}$ von x nach y heißt schlicht, wenn die Knoten $\mathbf{x}_2, \dots, \mathbf{x}_\ell$ paarweise verschieden sind. In diesem Fall ist

$$e = e_1 \cup \{\mathbf{x}_2\} \cup e_2 \cup \{\mathbf{x}_3\} \cup \dots \cup \{\mathbf{x}_{\ell-1}\} \cup e_\ell$$

eine Kante mit den Endpunkten \mathbf{x} und \mathbf{y} . Ein Kreis ist ein geschlossener schlichter Pfad.

Ein *planer Graph* ist ein Paar $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, wobei \mathcal{E} eine endliche Menge von paarweise disjunkten Kanten und $\mathcal{V} \subseteq \mathbb{R}^2$ eine endliche Menge von Punkten ist, welche alle Endpunkte der Kanten $e \in \mathcal{E}$ enthält. Die Punkte $\mathbf{v} \in \mathcal{V}$ sind die sog. Knoten des Graphen \mathcal{G} . Wir benutzen die Notation

$$\bar{\mathcal{G}} := \mathcal{V} \cup \mathcal{E} \subseteq \mathbb{R}^2.$$

4.2. Zusammenhangskomponenten und Flächen. Bzgl. des planen Graphen $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ nennen wir zwei Punkte $\mathbf{x}, \mathbf{y} \in \bar{\mathcal{G}}$ *äquivalent*, wenn es einen Pfad $P \subseteq \bar{\mathcal{G}}$ von \mathbf{x} nach \mathbf{y} gibt. Man macht sich leicht klar, dass hier wirklich eine Äquivalenzrelation vorliegt. Die verschiedenen Klassen $\bar{\mathcal{G}}_i$ äquivalenter Punkte von \mathcal{G} sind die *Zusammenhangskomponenten* von \mathcal{G} . Also ergibt sich die Dekomposition

$$\bar{\mathcal{G}} = \bar{\mathcal{G}}_1 \cup \bar{\mathcal{G}}_2 \cup \dots \quad \text{mit } \bar{\mathcal{G}}_i \cap \bar{\mathcal{G}}_j = \emptyset \text{ wenn } i \neq j.$$

Im Fall $\bar{\mathcal{G}} = \bar{\mathcal{G}}_1$ gibt es genau eine Zusammenhangskomponente. \mathcal{G} wird dann *zusammenhängend* genannt.

Analog nennen wir zwei Punkte $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2 \setminus \bar{\mathcal{G}}$ *äquivalent*, wenn es eine Kante $e \subseteq \mathbb{R}^2 \setminus \bar{\mathcal{G}}$ mit den Endpunkten \mathbf{x} und \mathbf{y} gibt. Wieder erkennt man leicht, dass auch hier eine Äquivalenzrelation vorliegt. Die Äquivalenzklassen \mathcal{F}_s bzgl. dieser Relation sind die *Flächen* von \mathcal{G} und ergeben die Dekomposition

$$\mathbb{R}^2 \setminus \bar{\mathcal{G}} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots \quad \text{mit } \mathcal{F}_s \cap \mathcal{F}_t = \emptyset \text{ wenn } i \neq j.$$

Insgesamt liefert \mathcal{G} eine eindeutige Zerlegung der Ebene \mathbb{R}^2 in paarweise disjunkte Zusammenhangskomponenten und Flächen von \mathcal{G} :

$$\mathbb{R}^2 = \bar{\mathcal{G}}_1 \cup \bar{\mathcal{G}}_2 \cup \dots \cup \mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots$$

Ist z.B. $\bar{\mathcal{G}}$ ein Kreis, dann hat \mathcal{G} genau 2 Flächen, nämlich die von $\bar{\mathcal{G}}$ umgrenzte *Innenfläche* \mathcal{F}_1 und die (unendliche) *Außenfläche*

$$\mathcal{F}_2 = \mathbb{R}^2 \setminus (\bar{\mathcal{G}} \cup \mathcal{F}_1).$$

4.3. Eulersche Formel und Eulercharakteristik. Sei $f_1 = |\mathcal{V}|$ die Anzahl der Knoten, $f_2 = |\mathcal{E}|$ die Anzahl der Kanten, f_3 die Anzahl der Flächen und k die Anzahl der Zusammenhangskomponenten des planen Graphen $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.

Wenn man sich vorstellt, dass $\overline{\mathcal{G}}$ aufgebaut wird, indem man Schritt für Schritt Kanten aus ε der Punktmenge \mathcal{V} hinzufügt, so hat man am Anfang der Prozedur $f_2 = 0, f_3 = 1$, und $k = |\mathcal{V}|$.

Wird dann eine Kante e mit zwei Endpunkten $x, y \in \mathcal{V}$ zugefügt, so hat man $f_2 = 1, f_3 = 1$ und $k = |\mathcal{V}| - 1$. Bildet e jedoch einen Schlinge, so ergibt sich $f_2 = 1, k = |\mathcal{V}|$ und $f_3 = 2$, da nun die Punkte im Inneren der Schlinge von den Punkten ausserhalb getrennt sind.

Für $|\mathcal{E}| \leq 1$ erkennen wir also die Gültigkeit der Eulerschen Formel

$$(50) \quad \boxed{f_1 - f_2 + f_3 = 1 + k .}$$

SATZ 5.1. Die Eulersche Formel (50) gilt für jeden planen Graphen.

Beweis. Wir nehmen an, (50) gelte für den planen Graphen $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Wir fügen nun eine Kante e derart hinzu, dass der erweiterte Graph $\mathcal{G}' = (\mathcal{V}, \mathcal{E} \cup e)$ auch plan ist.

Ergibt e mit schon vorhandenen Kanten einen Kreis, so wird e einer Zusammenhangskomponente von \mathcal{G} zugefügt. Die Anzahl der Komponenten bleibt also gleich. Allerdings erhöht sich die Anzahl der Flächen um 1, da nun die Punkte innerhalb des neuen Kreises von den Punkten ausserhalb nicht mehr über Pfade $P \subseteq \mathbb{R}^2 \setminus \overline{\mathcal{G}'}$ erreichbar sind. Schliesst e keinen Kreis, so verbindet e zwei Zusammenhangskomponenten von \mathcal{G} . Die Anzahl der Komponenten sinkt also um 1, während die Anzahl der Flächen gleich bleibt. Auf jeden Fall gilt die Eulersche Formel auch \mathcal{G}' .

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

Jetzt **bewerben** und jederzeit einsteigen!

FastTrack
IT-Einsteigerprogramm für Bachelor- und Masterabsolventen

Durchstarten in Ihre IT-Karriere

Unser 18-monatiges Programm bildet die perfekte Grundlage für Ihren beruflichen Erfolg: Arbeit in Top-Projekten, Ausbildung in fachlichen und Soft-Skill-Trainings, Betreuung durch einen persönlichen Mentor und Austausch mit Kollegen aus aller Welt. Ihren Schwerpunkt wählen Sie selbst:

- **Business Technology Consulting**
- **Individuelle Softwarelösungen**
- **Lösungen auf Basis von Standardsoftware**
- **Business Information Management**
- **Application Lifecycle Services**

Mehr Informationen auf www.capgemini.de/karriere

f XING

People matter, results count.



BEMERKUNG. Das induktive Argument im vorangehenden Beweis zeigt insbesondere, dass ein planer Graph genau eine unbegrenzte Fläche hat, die sog. *Aussenfläche*. Die übrigen Flächen sind von Kreisen begrenzt.

Triangulierte Graphen. Der plane Graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ heisst *trianguliert*, wenn jede begrenzte Fläche von einem Kreis mit genau 3 Kanten begrenzt ist, d.h. ein „Dreieck“ darstellt.

Man kann \mathcal{G} z.B. folgendermassen triangulieren:

- 1) Man unterteilt jede Kante $e \in \mathcal{E}$ in drei neue Kanten e', e'' und e''' , indem man 2 Punkte $\mathbf{x}', \mathbf{x}'' \in e$ wählt, die bisher noch nicht als Knoten auftreten, und als neue Knoten behandelt. So erhält man einen Graphen $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ mit $\overline{\mathcal{G}'} = \overline{\mathcal{G}}$. Insbesondere ändern sich die Flächen nicht. Es ist jedoch sichergestellt, dass jede begrenzte Fläche \mathcal{F} bzgl. \mathcal{G}' von einem Kreis mit mindestens 3 Kanten begrenzt ist.
- 2) Jede Fläche \mathcal{F} , die von einem Kreis mit $c \geq 4$ Knoten umschlossen wird, kann nun durch eine durch \mathcal{F} verlaufende neue Kante in zwei neue Flächen unterteilt werden, deren umschliessenden Kreise mindestens 3, aber weniger als c , Knoten haben. Diese Unterteilung führt man fort, bis ein triangulierter Graph vorliegt.

EX. 5.10. Sei $\tilde{\mathcal{G}} = (\tilde{\mathcal{V}}, \tilde{\mathcal{E}})$ der nach dem obigen Verfahren aus $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ erhaltene triangulierte Graph. Dann hat $\tilde{\mathcal{G}}$ dieselbe Anzahl k von Zusammenhangskomponenten wie \mathcal{G} .

Sei $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ ein triangulierter Graph und Δ die Familie aller Teilmengen von Knoten, die entweder als Einzelknoten oder als Endknotenpaar einer Kante oder als Knotentripel eines eine Fläche begrenzenden Kreises auftreten, dann gilt nach der Eulerformel:

$$k = f_1 - f_2 + (f_3 - 1) = \chi(\Delta)$$

Denn bei $\chi(\Delta)$ wird die Aussenfläche von \mathcal{G} nicht mitgezählt. Somit finden wir:

PROPOSITION 5.2. Die Zusammenhangszahl k eines planen Graphen ist genau die Eulercharakteristik seiner Triangulierung.

4.4 Die Knoten-Kanten-Ungleichung.

PROPOSITION 5.3. Sei $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ ein planer Graph mit mindestens 3 Knoten derart, dass jeder Kreis mindestens 3 Kanten umfasst. Dann gilt die Knoten-Kanten- Ungleichung

$$(51) \quad |\mathcal{E}| \leq 3|\mathcal{V}| - 6.$$

Beweis. Wir dürfen annehmen, dass die Knoten, die auf dem Rand einer Fläche \mathcal{F} liegen, einen Kreis bilden. Sonst fügen wir zwischen zwei nicht benachbarten solchen Knoten x und y eine Kante $e \subseteq \mathcal{F}$ mit den Endpunkten x und y ein. Dadurch entsteht wieder ein planarer Graph \mathcal{G}' mit derselben Knotenzahl und einer sogar noch höheren Kantenzahl. Ausserdem hat auch jeder Kreis von \mathcal{G}' mindestens 3 Kanten. Nun wiederholen wir diese Operation solange, bis diese Annahme erfüllt ist und weisen dann die Knoten-Kanten- Ungleichung für den Endgraphen nach.

Ist unsere Annahme erfüllt, zählen wir die Kanten der Kreise, die Flächen beranden und erhalten die Ungleichung

$$3f_3 \leq 2f_2,$$

weil eine Kante im Rand von höchstens 2 Flächen auftreten kann und deshalb höchstens doppelt gezählt wird. Wir schliessen darum aus der Eulerschen Formel (50):

$$6 \leq 3(k+1) = 3f_1 - 3f_2 + 3f_3 \leq 3f_1 - f_2$$

und somit $|\mathcal{E}| = f_2 \leq 3f_1 - 6 = 3|\mathcal{V}| - 6$.

Als Folgerung der Knoten-Kanten-Ungleichung finden wir:

PROPOSITION 5.4. *Sei $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ ein planer Graph, bei dem jeder Kreis mindestens 3 Kanten umfasst. Dann existiert ein Knoten $v \in \mathcal{V}$, der Endpunkt von höchstens 5 Kanten ist.*

Beweis. Hat \mathcal{G} weniger als 2 Knoten, ist die Behauptung trivialerweise richtig. Nehmen wir also an, \mathcal{G} habe mindestens 3 Knoten, die Behauptung sei aber falsch und jeder Knoten sei Endpunkt von mindestens 6 Kanten.

Zählen wir nun die Kanten gemäss ihren Endpunkten, dann ergibt sich

$$6|\mathcal{V}| \leq 2|\mathcal{E}|,$$

da jede Kante auf diese Weise doppelt gezählt wird. Das steht jedoch im Widerspruch zur Knoten-Kanten-Ungleichung, wonach gilt:

$$2|\mathcal{E}| \leq 2 \cdot (3|\mathcal{V}| - 6) = 6|\mathcal{V}| - 12.$$

Damit ist die Annahme, die Behauptung sei falsch, ad absurdum geführt.

4.5. Färbungen. Unter einer p -Färbung des Graphen $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ versteht man eine Abbildung

$$c : \mathcal{V} \rightarrow \{1, 2, \dots, p\}$$

derart, dass es keine Kante gibt, deren Endpunkte x dieselbe „Farbe“ $c(x)$ tragen.

PROPOSITION 5.5. *Sei $\mathcal{G} = (V, E)$ ein beliebiger planer Graph ohne Schlingen. Dann gestattet \mathcal{G} eine 5-Färbung.*

Beweis. Wir argumentieren per Induktion über die Grösse von \mathcal{G} . Ohne Beschränkung der Allgemeinheit dürfen wir dabei annehmen, dass \mathcal{G} keine „parallelen“ Kanten (d.h. Kreise mit 2 Kanten) hat. Denn sonst kann man eine Kante weglassen, ohne die Färbungseigenschaft zu verändern. Also können wir davon ausgehen, dass jeder Kreis in \mathcal{G} mindesten 3 Kanten umfasst.

Folglich gibt es einen Knoten v , der Endpunkt von höchstens 5 Kanten ist (Proposition 5.4). Wir entfernen nun v und die Kanten, die v als Endpunkt haben. Per Induktion nehmen wir an, dass der Restgraph \mathcal{G}' 5-färbbar ist. Treten nun unter den Kantennachbarn von v höchstens 4 verschiedene Farben auf, so geben wir v eine noch verfügbare Farbe und haben dann auch \mathcal{G} zulässig gefärbt.

Es bleibt also noch die folgende Situation zu analysieren: v hat Kantennachbarn v_1, \dots, v_5 (die wir uns im Kreis angeordnet denken), die sämtliche 5 Farben repräsentieren. Wir betrachten die Knoten v_1 und v_3 . U bezeichne die Menge aller Knoten, die von v_1 über Kantennpfade in \mathcal{G}' erreicht werden können die nur Knoten der Farben „1“ und „3“ durchlaufen. Wir unterscheiden nun zwei Fälle.

1. FALL: $v_3 \notin U$. Wir vertauschen dann die Farben 1 und 3 auf der Knotenmenge U . Daraus resultiert offenbar eine zulässige 5-Färbung von \mathcal{G}' , in der v_1 aber nun die Farbe 3 trägt! Also steht nun die Farbe 1 nun zur Färbung von v zur Verfügung.
2. FALL: $v_3 \in U$. Es gibt also einen Pfad P von v_1 nach v_3 in \mathcal{G}' , mit ausschliesslich den Farben 1 und 3. Dieser bildet mit dem Knoten v einen Kreis K in G und es gilt:

- v_2 liegt im Inneren des Kreises K und v_4 liegt im A"usseren von K .

Daraus folgt:

- *Es kann in \mathcal{G}' keinen Pfad von v_2 nach v_4 geben, der nur die Farben 2 und 4 benutzt.*

Wir können deshalb mit den Knoten v_2 und v_4 genauso wie zuvor mit v_1 und v_3 argumentieren – und sind dann aber mit dem FALL 1 schon fertig.

Deutsche Bank
db.com/careers

Können Banktechnologien die Welt verändern?

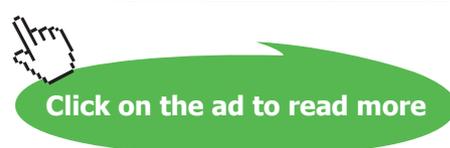
Ein wacher Verstand weiß, dass dies längst Alltag ist

Ihr Weg zu Group Technology & Operations (GTO)

Technologie ist der Motor der Finanzindustrie. Sie ermöglicht Geschäfte über Zeitzonen hinweg, liefert wichtige Entscheidungshilfen und schafft die Verbindung zu anderen Banken und unseren Kunden. Ohne Technologie – und damit bald ohne Sie – wäre die Welt eine andere. Ob als Praktikant oder Trainee: Sie erschließen mit uns neue technische Einsatzfelder, lösen komplexe Aufgaben und überschreiten die Grenzen des technisch Möglichen: ob Sie Ihre Zukunft in der Entwicklung, Analyse oder im Management sehen.

Entdecken Sie den Unterschied auf db.com/careers/jobs

Leistung aus Leidenschaft



BEMERKUNG. Tatsächlich sind plane Graphen sogar 4-färbbar (wenn man einem entsprechenden mit langen Computerberechnungen geführten Beweis glaubt). Ein elementarer Beweis für die 4-Färbbarkeit planer Graphen ist bisher jedoch noch nicht gelungen.

4.6. Planare Graphen. Ein *abstrakter (kombinatorischer) Graph* ist ein Tripel $G = (V, E, I)$, wobei V und E endliche Mengen sind und I eine Abbildung

$$I : E \rightarrow 2^V \quad \text{so, dass} \quad 1 \leq |I(e)| \leq 2 \quad \forall e \in E$$

ist. Wir nennen die Elemente von V *Knoten* und die Elemente von E *Kanten* von G . Die Menge $I(e)$ enthält die *Endpunkte* der Kante e . Im Fall $|I(e)| = 1$ ist die Kante $e \in E$ vom Typ $I(e) = \{v\}$ und heisst *Schlinge* von G .

BEMERKUNG. Wenn die Funktion I aus dem Kontext klar ist, notiert man den kombinatorischen Graphen $G = (V, E, I)$ oft auch einfach als Paar $G = (V, E)$ und identifiziert eine Kante e mit der Menge $I(e)$ ihrer Endpunkte.

Der Graph $G = (V, E, I)$ heisst *planar* (oder *plättbar*), wenn es einen planen Graphen $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ gibt, dessen Inzidenzstruktur bzgl. der Knoten und Kanten zu der von G *isomorph* ist. Das soll heissen:

- Es gibt Bijektionen $\varphi : \mathcal{V} \rightarrow V$ und $\psi : \mathcal{E} \rightarrow E$ so, dass für jede Kante $e \in \mathcal{E}$ mit den Endpunkten x und y gilt: $I(\psi(e)) = \{\varphi(x), \varphi(y)\}$.

Man sagt dann auch, \mathcal{G} sei eine *Einbettung* von G in \mathbb{R}^2 . Natürlich muss ein planarer Graph z.B. ebenso die Knoten-Kanten-Ungleichung erfüllen wie ein planer Graph. Damit kann man oft kombinatorisch beweisen, dass ein abstrakter Graph G *nicht* plättbar ist.

EX. 5.11 (Kuratowski-Graphen). Mit K_5 bezeichnet man den abstrakten Graphen auf $V = \{1, 2, 3, 4, 5\}$, bei dem jedem Paar von Knoten genau eine Kante entspricht. $K_{3,3}$ ist der Graph auf $V = \{1, 2, 3, 4, 5\}, 6g$, wobei genau die Paarmengen $\{v, v'\}$ mit $v \in \{1, 2, 3\}$ und $v' \in \{4, 5, 6\}$ Kanten repräsentieren.

K_5 kann wegen $3|\mathcal{V}| - 6 = 9 < 10 = |\mathcal{E}|$ nicht planar sein. In $K_{3,3}$ besteht jeder Kreis aus mindestens 4 Kanten. Gäbe es eine plane Einbettung $K_{3,3}$, so hätte man $4f_3 \leq 2f_2$ und folglich $2f_3 \leq 9$. Nach der Eulerformel muss aber gelten:

$$f_3 = 2 - f_1 + f_2 = 5.$$

Also sind weder K_5 noch $K_{3,3}$ planar.

BEMERKUNG. Kuratowski³² hat gezeigt, dass jeder nichtplanare Graph entweder K_5 oder $K_{3,3}$ enthält. Diese Graphen sind also die „minimalen“ nichtplanaren Graphen.

32 K. KURATOWSKI (1902-1980)

6 Netzwerke

Das Modell abstrakter Graphen wird erweitert, wenn man mögliche Orientierungen der Kanten mitberücksichtigt. Damit erhält man nicht nur ein mathematisches Modell, das viele kombinatorische Strukturen „intuitiv“ sichtbar macht, sondern auch eine Grundlage zum praktischen Berechnen von Strukturen mit gewissen Optimalitätseigenschaften.

Orientierungen. Sei $G = (V, E, I)$ ein abstrakter Graph. Unter einer *Orientierung* einer Kante $e \in E$ mit zwei Endknoten versteht man einfach eine Anordnung (v, w) der Endknotenmenge $I(e) = \{v, w\}$, die einen „Durchlaufsinne“ der Kante festlegt. Wir schreiben dann $e^- = v$ und $e^+ = w$ und können uns e intuitiv als einen von $v = e^-$ nach $w = e^+$ gerichteten Pfeil vorstellen:

$$v \xrightarrow{e} w \quad \text{bzw.} \quad e^- \xrightarrow{e} e^+.$$

G heisst *orientiert* (oder *gerichtet*), wenn jede Kante mit zwei Endpunkten orientiert ist³³.

Inzidenzmatrix. Die *Inzidenzmatrix* des gerichteten Graphen $G = (V, E, I)$ ist die Matrix $A = [a_{ve}] \in \mathbb{R}^{V \times E}$, deren Zeilen den Knoten $v \in V$ und deren Spalten den Kanten $e \in E$ entsprechen, mit den Einträgen

$$a_{ve} := \begin{cases} +1 & \text{wenn } e \text{ keine Schlinge und } v = e^+, \\ -1 & \text{wenn } e \text{ keine Schlinge und } v = e^-, \\ 0 & \text{sonst.} \end{cases}$$

Jede Spalte von A hat also entweder alle Koeffizienten „0“ oder genau einen Koeffizienten „+1“ und einen Koeffizienten „-1“ (und die übrigen „0“).

EX. 6.1 (Umorientierungen). *Wird die Orientierung (v, w) der Kante e in (w, v) umgekehrt, dann erhält man die neue Inzidenzmatrix dadurch, dass man die e -Spalte der alten Inzidenzmatrix mit (-1) multipliziert.*

Pfade und Kreise. Analog zur Begriffsbildung bei planen Graphen sprechen wir im (abstrakten) Graphen $G = (V, E, I)$ von einem Pfad vom Knoten $s \in V$ zum Knoten $t \in V$ als einer alternierenden Folge von Knoten $x_i \in V$ und Kanten $e_j \in E$,

$$(52) \quad P = x_0 e_1 x_1 e_2 x_2 \dots x_{k-1} e_k x_k,$$

wobei $x_0 = s, x_k = t$ und $I(e_j) = \{x_{j-1}, x_j\}$ für alle $j = 1, \dots, k$. Ein *Teilpfad* von P ist ein Pfad vom Typ

$$P' = x_i e_{i+1} x_{i+1} e_{i+2} x_{i+2} \dots x_{j-1} e_j x_j.$$

33 bei Schlingen interessieren mögliche Orientierungen im Kontext dieses Kapitels nicht

Bzgl. einer gegebenen Orientierung heisst P *gerichtet*, wenn zusätzlich gilt

$$e_j^- = x_{j-1} \quad \text{und} \quad e_j^+ = x_j \quad \forall j = 1, \dots, k.$$

Im Fall $s = t$ ist der Pfad P *geschlossen*. P heisst *schlicht*, wenn P keinen geschlossenen echten Teilpfad enthält. Ein schlichter geschlossener Pfad ist ein *Kreis*.

Bezüglich einer gegebenen Orientierung des Graphen G können wir den (gerichteten oder ungerichteten) schlichten Pfad P durch seinen (*Kanten-*)*Inzidenzvektor* (oder *Indikator*) darstellen, den wir der Einfachheit halber selber auch mit „ P “ bezeichnen. Der Pfad (52) entspricht dann dem Vektor $P \in \mathbb{R}^E$ mit den Komponenten

$$P_e := \begin{cases} +1 & \text{wenn } e = e_j \text{ und } e^+ = x_j \\ -1 & \text{wenn } e = e_j \text{ und } e^- = x_j \\ 0 & \text{sonst.} \end{cases}$$

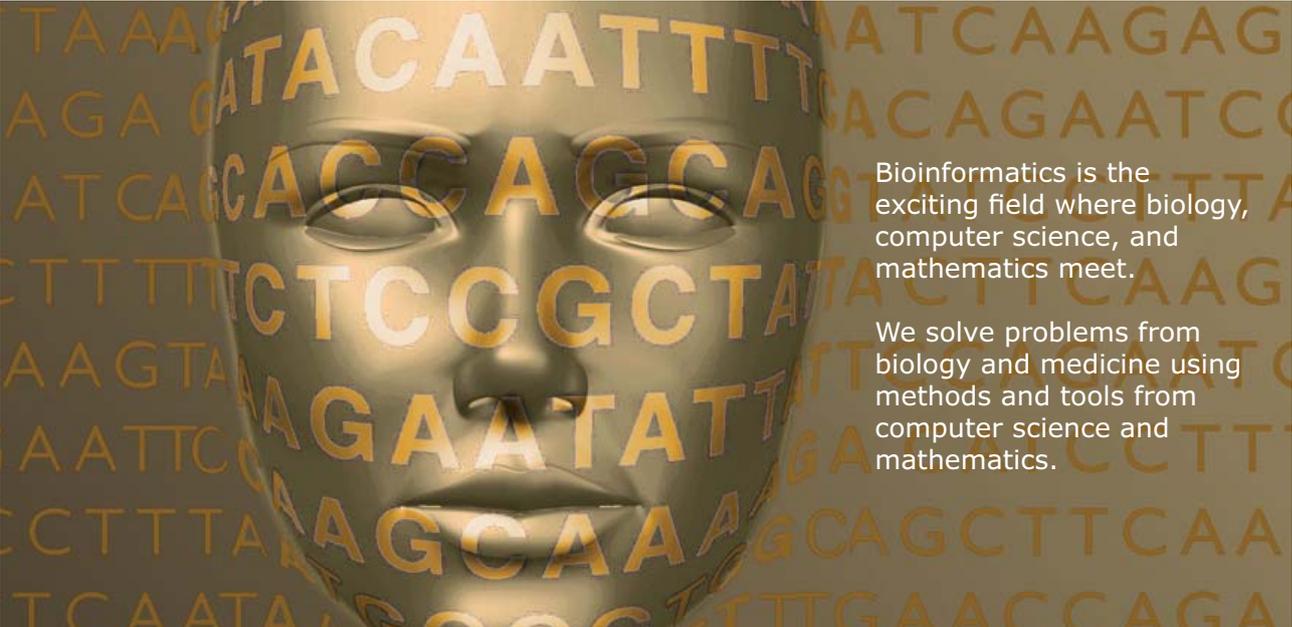
Im Fall $P_e = +1$ ist e eine sog. *Vorwärtskante* und im Fall $P_e = -1$ eine *Rückwärtskante* des Pfades P (bzgl. der gewählten Orientierung von G). Ein gerichteter schlichter Pfad umfasst also ausschliesslich Vorwärtskanten.

EX. 6.2. Sei P ein schlichter Pfad, der nur die Kante e enthält. Ist e eine Schlinge, so ist $P = e$ (als Inzidenzvektor) der Nullvektor. Andernfalls ist $P = e$ in Abhängigkeit von der Orientierung von e entweder ein positiver oder ein negativer Einheitsvektor in \mathbb{R}^E .



UPPSALA
UNIVERSITET

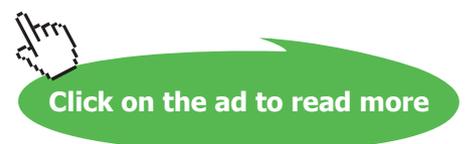
Develop the tools we need for Life Science Masters Degree in Bioinformatics



Bioinformatics is the exciting field where biology, computer science, and mathematics meet.

We solve problems from biology and medicine using methods and tools from computer science and mathematics.

Read more about this and our other international masters degree programmes at www.uu.se/master



Zirkulationen. Wir betrachten G mit einer festen Orientierung und der zugehörigen Inzidenzmatrix $A = [a_{ve}]$. Ein (allgemeiner) Fluss auf G ist aus mathematischer Sicht nichts anderes als eine Abbildung $x : E \rightarrow \mathbb{R}$, die jeder Kante e einen Flusswert $x_e \in \mathbb{R}$ zuweist. Der Träger von x ist definiert als die Menge

$$\text{tr}(x) := \{e \in E \mid x_e \neq 0\}.$$

Der Durchfluss von x im Knoten v ist die Differenz zwischen dem Zufluss und Abfluss bzgl. x , d.h. der Parameter

$$(53) \quad \delta_v(x) := \sum_{e^+=v} x_e - \sum_{e^-=v} x_e = \sum_{e \in E} a_{ve} x_e.$$

In Matrixnotation ergibt sich der Vektor $\delta(x) \in \mathbb{R}^V$ aller Durchflüsse somit als

$$\delta(x) = Ax.$$

Wir nennen den Fluss x eine *Zirkulation*, wenn bei keinem Knoten etwas hinzugewonnen wird oder verloren geht, d.h. wenn für jedes $v \in V$ gilt

$$\delta_v(x) = 0 \quad \text{bzw.} \quad \sum_{e^+=v} x_e = \sum_{e^-=v} x_e.$$

In der Sprache der linearen Algebra ist eine Zirkulation ein Vektor im Kern der Inzidenzmatrix A :

$$x \in \mathbb{R}^E \text{ ist Zirkulation} \iff Ax = \mathbf{0} \quad (\text{d.h. } x \in \ker A).$$

EX. 6.3. Sei x der Inzidenzvektor eines Kreises K im Graphen G . Dann ist x eine Zirkulation. Folglich ergibt auch jede Linearkombination von Kreisen eine Zirkulation.

LEMMA 6.1 (Zirkulationslemma). Ein Fluss $x \in \mathbb{R}^E$ mit $\text{tr}(x) \neq \emptyset$ ist eine Zirkulation genau dann, wenn x eine Linearkombination von (Inzidenzvektoren von) Kreisen ist.

Beweis. In Anbetracht von Ex. 6.3 bleibt zu zeigen, dass sich eine Zirkulation x mit $\text{tr}(x) \neq \emptyset$ als Linearkombination von Kreisen darstellen lässt. Wir argumentieren per Induktion über die Mächtigkeit $|\text{tr}(x)|$ des Trägers.

Sei $e_1 \in \text{tr}(x)$ und v_1 und v_2 ein Endpunkt von e_1 . Ist e_1 eine Schlinge, so ist $x_{e_1} \cdot e_1$ und folglich auch $x' = x - x_{e_1} e_1$ eine Zirkulation. Wegen $|\text{tr}(x')| \leq |\text{tr}(x)| - 1$ dürfen wir per Induktion annehmen, dass x' entweder der Nullvektor ist oder sich als Linearkombination von Kreisen schreiben lässt. Also ist auch $x = x' + x_{e_1} e_1$ eine Linearkombination von Kreisen. Wir dürfen also im Weiteren ohne Beschränkung der Allgemeinheit annehmen, dass $\text{tr}(x)$ keine Schlingen enthält.

Die Kante $e_1 \in \text{tr}(x)$ besitzt also einen weiteren Endpunkt v_2 . v_2 muss Endpunkt einer weiteren Kante $e_2 \in \text{tr}(x)$ sein (denn sonst wäre $\delta_{v_2}(x) \neq 0$!). e_2 ist nach unserer jetzigen Annahme keine Schlinge und besitzt somit einen weiteren Endpunkt x_3 . Auf diese Weise konstruieren wir schrittweise einen Pfad

$$v_1 e_1 v_2 e_2 v_3 \dots$$

Da G nur endlich viele Knoten hat, wird nach endlich vielen Schritten ein Knoten durchlaufen werden, der schon vorher besucht worden war. Damit ist ein geschlossener Pfad P mit $\text{tr}(P) \subseteq \text{tr}(x)$ gefunden. Der geschlossener Pfad P enthält (mindestens) einen Kreis K . Für diesen gilt $\text{tr}(K) \subseteq \text{tr}(x)$.

Sei $e \in \text{tr}(K)$ eine beliebige Kante. Dann ist $x_e \neq 0$ und $x_e K$ eine Zirkulation. Folglich ist $x' = x - x_e K$ eine Zirkulation mit $|\text{tr}(x')| \leq |\text{tr}(x)| - 1$. Damit können wir mit der analogen Argumentation wie zuvor den Beweis per Induktion zu Ende führen.

Auf die folgende wichtige Folgerung des Kreislemmas werden wir später noch wiederholt zurückkommen.

SATZ 6.1. Sei $G = (V, E)$ ein beliebig orientierter Graph mit Inzidenzmatrix $A \in \mathbb{R}^{V \times E}$. Dann sind für jede Kantenmenge $S \subseteq E$ die folgenden Aussagen äquivalent:

- 1) S ist kreisfrei (d.h. Die Kantenmenge keines Kreises K von G ist ganz in S enthalten).
- 2) Die der Kantenmenge S entsprechende Spaltenteilmatrix A^S von A hat Rang $\text{rg}(A^S) = |S|$ (d.h. die Spalten sind linear unabhängig).

Beweis. Seien die Spaltenvektoren in A^S linear abhängig. Dann kann der Nullvektor $\mathbf{0} \in \mathbb{R}^E$ als nichttriviale Linearkombination der Spaltenvektoren A^e in A^S geschrieben werden, d.h.

$$\mathbf{0} = \sum_{e \in S} x_e A^e$$

mit mindestens einem $x_e \neq 0$. x ergibt somit eine Zirkulation of G mit $\text{tr}(x) \subseteq S$. Also existiert nach dem Zirkulationslemma ein Kreis $K \subseteq \text{tr}(x) \subseteq S$. Gibt es umgekehrt einen Kreis $C \subseteq S$, dann gilt nach Ex. 6.3:

$$\sum_{e \in C} A^e = \mathbf{0}.$$

Also ist A^C und somit auch die Obermenge $A^S \supseteq A^C$ linear abhängig.

1 Der Algorithmus von Ford und Fulkerson

Wir nehmen an, dass auf dem (orientierten) Graphen $G = (V, E)$ jeder Kante e eine (nichtnegative) Kapazität $c_e \in \mathbb{R}_+ \cup \{+\infty\}$ zugeordnet ist.

BEMERKUNG (Netzwerke). Ein orientierter Graph G , bezüglich welchem weitere Strukturparameter (wie z.B. Kantenkapazitäten) definiert sind, wird oft als *Netzwerk* bezeichnet.

Wir nennen eine Zirkulation $x \in \mathbb{R}^E$ zulässig, wenn gilt

$$0 \leq x_e \leq c_e \quad \text{für alle } e \in E.$$

Man bemerke, dass zulässige Zirkulationen immer existieren (Beispiel: die triviale Nullzirkulation $x = 0$).

Das Fluss-Modell von Ford-Fulkerson. Sei $f \in E$ eine ausgezeichnete Kante mit $c_f = \infty$ im orientierten Graphen $G = (V, E)$ mit der Kapazität c . Eine zulässige Zirkulation x^* heisst *f-optimal*, wenn gilt:

$$(54) \quad x_f^* = \max\{x_f \mid x \text{ ist zulässige Zirkulation auf } G\}$$

Das *Flussproblem* von Ford und Fulkerson³⁴ besteht darin, eine *f*-optimale zulässige Zirkulation zu konstruieren.

1.1. Schnitte und Augmentierungen. Wie erkennt man, ob eine gegebene zulässige Zirkulation *f*-optimal ist? Zur Untersuchung dieser Frage betrachten wir zu jeder Knotenmenge $S \subseteq V$ die Menge

34 L.R. FORD (1927), R.D. FULKERSON (1924-1976)



A NEW FUTURE
IS WAITING FOR
YOU AT ERICSSON.

Look up for our continuous offers of graduate positions at our various locations within Germany (Backnang, Duesseldorf, Frankfurt, Herzogenrath/Aachen). We are looking forward to getting to know you! Apply via the internet: www.ericsson.com/careers

ERICSSON

$$S^- := \{e \in E \mid e^- \in S, e^+ \in V \setminus S\}$$

derjenigen Kanten, die von S in das Komplement $V \setminus S$ führen. Eine Kantenmenge vom Typ S^- ist ein sog. Schnitt im Graphen $G = (V, E)$. Wir nennen S^- einen f -Schnitt, wenn $f \in (V \setminus S)^-$ gilt (d.h. wenn die Kante f von $V \setminus S$ zurück nach S weist).

Bzgl. eines beliebigen Vektors $x \in \mathbb{R}^E$ benutzen wir die Kurzschreibweise

$$x(S^-) := \sum_{e \in S^-} x_e.$$

LEMMA 6.2. Sei $x \in \mathbb{R}^E$ eine beliebige Zirkulation auf dem orientierten Graphen $G = (V, E)$. Dann gilt

$$(55) \quad x(S^-) = x(V \setminus S)^- \quad \text{für alle } S \subseteq V.$$

Beweis. Es genügt, die Behauptung für Kreise zu beweisen. Denn dann gilt sie offenbar auch für alle Linearkombinationen von Kreisen, d.h. alle Zirkulationen. Sei also x der Inzidenzvektor des Kreises K . Wenn wir nun K einmal durchlaufen, ist klar, dass wir genauso oft einen Schritt von S nach $V \setminus S$ machen wie von $V \setminus S$ nach S . Mit anderen Worten: K enthält genauso viele von S nach $V \setminus S$ gerichtete Kanten wie von $V \setminus S$ nach S . Das ist genau die Aussage von (55).

Wir nehmen nun die Kantenkapazität $c : E \rightarrow \mathbb{R}_+ \cup \{\infty\}$ als gegeben an und definieren die *Kapazität* eines Schnittes S^- als den aggregierten Kapazitätswert

$$(56) \quad c(S^-) := \sum_{e \in S^-} c_e.$$

LEMMA 6.3 (Schnittlemma). Sei x eine beliebige zulässige Zirkulation auf dem Netzwerk $G = (V, E)$ mit Kapazität c . $S \subseteq V$ sei eine beliebige Knotenmenge. Dann gilt für jede Kante $f \in (V \setminus S)^-$:

$$x_f \leq c(S^-).$$

Insbesondere ist x im Fall $x_f = c(S^-)$ garantiert f -optimal.

Beweis. Da x zulässig und deshalb nichtnegativ ist, folgert man aus Lemma 6.2:

$$x_f \leq x((V \setminus S)^-) = x(S^-) \leq c(S^-).$$

1.2. Augmentierende Pfade. Wir wollen einsehen, dass die hinreichende Bedingung für f -Optimalität im Schnittlemma 6.3 auch notwendig ist und folglich generell f -Optimalität charakterisiert. Dabei gehen wir von einer gegebenen zulässigen Zirkulation x und einer Kante $f \in E$ aus und nennen einen schlichten Pfad

$$P = se_1v_1e_2 \dots e_kv_k \quad \text{mit} \quad s = f^+$$

augmentierend (bzgl. x und f), wenn für jede Kante $e_j \in P$ folgende Aussage zutrifft:

- (0) $e_j \neq f$.
- (i) Ist e_j eine Vorwärtskante in P , dann gilt $x_{e_j} < c_{e_j}$.
- (ii) Ist e_j eine Rückwärtskante in P , dann gilt $x_{e_j} > 0$.

SATZ 6.2 (Ford-Fulkerson). Sei x eine zulässige Zirkulation auf dem orientierten Graphen $G = (V, E)$ und $f \in E$ eine Kante mit den beiden Endknoten $s := f^+$ und $t := f^-$. Dann sind die folgenden Aussagen äquivalent:

- 1) x ist nicht f -optimal.
- 2) x gestattet einen augmentierenden Pfad P von s nach t .

Beweis. Wir nehmen zuerst an, dass es keinen augmentierenden Pfad von s nach t gibt, und betrachten die Menge S aller Knoten v , die von s über einen augmentierenden Pfad erreicht werden können. Dann gilt trivialerweise $s \in S$ und $t \in V \setminus S$ (nach Annahme). Folglich ist S^- ein f -Schnitt.

Sei $e \in S^-$ eine beliebige Schnittkante mit dem Endpunkt $e^- \in S$ und dem andern Endpunkt $e^+ \in V \setminus S$. Dann muss $x_e = c_e$ gelten, da sonst ein augmentierender Pfad von s nach e^- mit e als Vorwärtskante nach $e^+ \notin S$ fortgesetzt werden können, was aber der Definition von S widerspricht.

Genauso muss $x_e = 0$ für jede Kante $e \neq f$ mit Endpunkten $e^+ \in S$ und $e^- \notin S$ gelten. Denn sonst könnte man einen augmentierenden Pfad von s nach e^+ mit e als Rückwärtskante zum Knoten e^- fortsetzen. Also ergibt sich insgesamt

$$x_f = x((V \setminus S)^-) = x(S^-) = c(S^-),$$

was nach dem Schnittemma 6.3 die Zirkulation x als f -optimal erweist.

Wir nehmen jetzt umgekehrt an, dass x einen augmentierenden Pfad

$$P = se_1v_1e_2 \dots e_kv_k t$$

von s nach t gestattet, und setzen $\varepsilon := \min\{\varepsilon^+, \varepsilon^-\} > 0$, wobei

$$\begin{aligned} \varepsilon^+ &:= \min\{c_e - x_e \mid e \text{ ist Vorwärtskante in } P\} > 0 \\ \varepsilon^- &:= \min\{x_e \mid e \text{ ist Rückwärtskante in } P\} > 0. \end{aligned}$$

Wir modifizieren nun x zu einem neuen Fluss x' mit den Kantenflusswerten

$$(57) \quad x'_e := \begin{cases} x_e + \varepsilon & \text{wenn } e = f \text{ oder } e \text{ Vorwärtskante in } P. \\ x_e - \varepsilon & \text{wenn } e \text{ Rückwärtskante in } P. \\ x_e & \text{sonst.} \end{cases}$$

Da f den Pfad P zu einem Kreis schliesst, ersieht man aus der Konstruktion leicht, dass x' eine zulässige Zirkulation ist. Wegen $x'_f = x_f + \varepsilon > x_f$ erkennt man, dass x nicht f -optimal war.

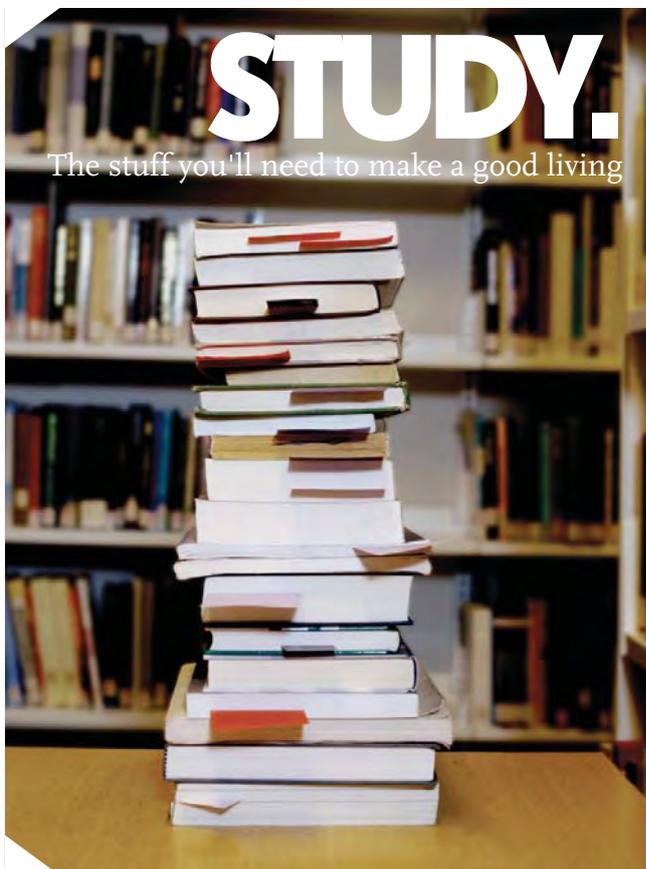
1.3. Der FF-Algorithmus. Man bemerke, dass der Beweis des Satzes 6.2 von Ford und Fulkerson im Prinzip algorithmisch konstruktiv ist. Um nach einer f -optimale Zirkulation zu suchen, kann man nach dem sog. *Ford-Fulkerson-Algorithmus* („FF-Algorithmus“) vorgehen.

FF-ALGORITHMUS:

(FF₀) Beginne mit der trivialen zulässigen Zirkulation $x = 0$ und iteriere dann den folgenden Schritt (FF₁) bis eine f -optimale Zirkulation vorliegt.

(FF₁) Ist die zulässige Zirkulation x schon konstruiert, nimm einen augmentierenden Pfad und modifiziere x zu einer zulässigen Zirkulation x' mit $x'_f > x_f$ gemäss der Vorschrift (57).

Die Frage erhebt sich allerdings, ob der FF-Algorithmus überhaupt nach endlich vielen Iterationsschritten zu einem Ende kommt. Wir betrachten zuerst einen Spezialfall und verschieben die Diskussion des Allgemeinfalles auf Abschnitt 2.4 und den dortigen Satz 6.5.



Download free eBooks at bookboon.com



KOROLLAR 6.1. Sei $G = (V, E)$ ein Netzwerk mit der ausgezeichneten Kante f und ganzzahliger Kantenkapazität $c : E \setminus \{f\} \rightarrow \mathbb{Z}_+$. Dann konstruiert der FF-Algorithmus in endlich vielen Iterationsschritten eine ganzzahlige zulässige Zirkulation x^* und einen f -Schnitt S mit der Eigenschaft

$$x_f^* = c(S^-).$$

Insbesondere ist x^* eine f -optimale zulässige Zirkulation.

Beweis. Wegen der Ganzzahligkeit von c konstruiert der FF-Algorithmus in jedem Stadium einen ganzzahligen Fluss x . Der Zielfunktionswert x_f steigt bei jeder Augmentierung um mindestens $+1$. Andererseits sind auch alle Schnittkapazitäten ganze Zahlen. Also muss nach endlich vielen Schritten x_f seine Obergrenze erreicht haben.

2 Anwendungen

Wir wollen ein paar kombinatorische Anwendungen der Theorie von Ford und Fulkerson geben.

BEMERKUNG. Interessanterweise wurden die Sachverhalte dieser Anwendungen unabhängig von und z.T. lange vor der Netzwerkflusstheorie entdeckt. Sie lassen sich aber in diesem Rahmen besonders bequem ableiten.

2.1. Kantenüberdeckungen und Matchings. Der Graph $G = (V, E)$ wird *bipartit* genannt, wenn V eine Partition $V = V_1 \cup V_2$ in disjunkte Mengen V_1 und V_2 gestattet derart, dass jede Kante einen Endknoten in V_1 und einen Endknoten in V_2 hat.

Der Einfachheit halber stellen wir uns in diesem Abschnitt die Kanten des bipartiten Graphen $G = (V_1 \cup V_2, E)$ als Paare $e = (v_1, v_2)$ mit $v_1 \in V_1$ und $v_2 \in V_2$ vor, jeweils per $(v_1, v_2)^- := v_1$ und $(v_1, v_2)^+ := v_2$ orientiert.

Eine *Kantenüberdeckung* von G ist eine Knotenteilmenge $C \subseteq V$ derart, dass jede Kante (mindestens) einen Endpunkt in C besitzt. Wir suchen eine Kantenüberdeckung mit *möglichst wenigen* Knoten.

Ein *Matching* M in G ist eine Menge von Kanten, von denen keine zwei einen Endknoten gemeinsam haben. Wir suchen ein Matching mit *möglichst vielen* Kanten. Man beobachtet sofort:

- Für jede Kantenüberdeckung C und jedes Matching M gilt:

$$|M| \leq |C|.$$

Denn C muss ja insbesondere die Kanten in M abdecken. Folglich liegt im Gleichheitsfall $|M| = |C|$ einerseits ein maximales Matching und andererseits eine minimale Kantenüberdeckung vor.

Um Matchings und Kantenüberdeckungen zu untersuchen, erweitern wir G zum Graphen \overline{G} mit den zusätzlichen Knoten s und t , der Kante $f = (t, s)$ und den Kanten vom Typ

$$(s, v_1) \quad \text{und} \quad (v_2, t) \quad (v_1 \in V_1, v_2 \in V_2).$$

Als Kapazitäten auf \overline{G} wählen wir $c_f = +\infty$ und $c_e = 1$ in allen anderen Fällen.

KOROLLAR 6.2 (König-Egerváry³⁵). *In jedem bipartiten Graphen G gilt:*

$$\max\{|M| \mid M \text{ Matching}\} = \min\{|C| \mid C \text{ Kantenüberdeckung}\}$$

Beweis. Sei $G = (V_1 \cup V_2, E)$. Nach unseren Vorbemerkungen genügt es, ein Matching M und eine Kantenüberdeckung C mit $|M| \geq |C|$ zu konstruieren. Denn da $|M| \leq |C|$ ohnehin gilt, ergibt sich dann die Gleichheit $|M| = |C|$.

Dazu berechnen wir im zugeordneten Netzwerk \overline{G} eine f -optimale zulässige Zirkulation x nach dem FF-Algorithmus. Dann ist die Kantenmenge

$$M = \{(v, w) \in E \mid v_1 \in V_1, v_2 \in V_2, x(v_1, v_2) = 1\}$$

ein Matching und wir haben $x_f = |M|$. Denn x ist gemäss Ford-Fulkerson konstruiert und hat deshalb einen ganzzahligen Flusswert $x_e \in \{0, 1\}$ auf jeder Kante $e \neq f$. Hätten zwei Kanten aus M z.B. den Endknoten $v_2 \in V_2$ gemeinsam, dann würde x mindestens 2 Flusseinheiten nach v_2 schicken. Es kann aber aus Kapazitätsgründen maximal nur eine Einheit aus v_2 abfließen. x wäre somit keine Zirkulation.

Es gibt also einen f -Schnitt S^- in \overline{G} der Kapazität $c(S^-) = |M|$. Wir setzen

$$C := \{e^+ \mid e \in S^-\}$$

und beobachten $|C| = |S^-| = |M|$. Es bleibt jetzt nur noch einzusehen, dass C eine Kantenüberdeckung ist. Das ist aber klar. Denn gäbe es eine Kante (v', w') , die von C nicht abgedeckt ist, dann wäre ja $s \rightarrow v' \rightarrow w' \rightarrow t$ ein x augmentierender Pfad und x somit nicht f -optimal.

2.2. Der Heiratssatz. Wir betrachten ein System $\mathcal{A} = (A_1, \dots, A_n)$ von (nicht notwendigerweise paarweise verschiedenen) endlichen Mengen A_i . Wir suchen ein *Repräsentantensystem*, d.h. eine Menge

$$R = \{r_1, \dots, r_n\} \quad \text{so, dass} \quad r_i \in A_i \quad \forall i = 1, \dots, n.$$

Unser Problem kann leicht als das Matchingproblem in dem bipartiten Graphen $G = (V_1 \cup V_2, E)$ erkannt werden, wobei

35 D. KÖNIG (1884-1944), J. EGERVÁRY (1891-1958)

$$\begin{aligned} V_1 &= A_1 \cup A_2 \cup \dots \cup A_n \\ V_2 &= \mathcal{A} \\ (v, A_i) \in E &\iff v \in A_i. \end{aligned}$$

Ein Matching M in G entspricht offensichtlich einem Repräsentantensystem für ein Teilsystem \mathcal{A}' von \mathcal{A} (und umgekehrt!):

$$(r_i, A_i) \in M \iff r_i \text{ repräsentiert } A_i.$$

Wir brauchen also einfach in G ein maximales Matching $|M|$ konstruieren. Dann ist im Fall $|M| = n$ ein (volles) Repräsentantensystem gefunden. Im Fall $|M| < n$ existiert kein volles Repräsentantensystem.

Eine abstrakte Charakterisierung der Existenz voller Repräsentantensystem gibt der folgende Satz.

SATZ 6.3 („Heiratssatz“ von Hall³⁶). *Genau dann gestattet $\mathcal{A} = \{A_1, \dots, A_n\}$ ein Repräsentantensystem, wenn für alle $J \subseteq \{1, \dots, n\}$ gilt:*

$$(58) \quad \left| \bigcup_{j \in J} A_j \right| \geq |J|.$$

36 PH. HALL (1904-1982)



Beweis. Die Hallsche Bedingung (58) ist sicherlich notwendig für die Existenz eines Repräsentantensystem, da eine Vereinigung von k Mengen A_j ja mindestens k Elemente zu Repräsentationszwecken enthalten muss. Wir zeigen umgekehrt, dass im zugeordneten bipartiten Graphen G ein Matching M mit $|M| \geq n$ existiert, wenn Halls Bedingung erfüllt ist. Das beweisen wir mit dem Argument, dass jede Kantenüberdeckung $|C|$ mindestens n Knoten enthält, und setzen dazu

$$J = \{j \mid A_j \notin C\} \quad \text{und} \quad C_2 = \{A_i \in \mathcal{A} \mid A_i \in C\}.$$

Wegen $|\bigcup_{j \in J} A_j| \geq |J|$ muss C noch mindestens $|J| = n - |C_2|$ weitere Knoten aus V_1 umfassen, um die von C_2 noch nicht erfassten Kanten abzudecken. Folglich finden wir in der Tat

$$|C| \geq |C_2| + |J| = n.$$

BEMERKUNG. Die Bezeichnung *Heiratssatz* leitet sich aus der Vorstellung ab, dass n Männer jeweils eine Frau suchen und dabei für Herrn i nur eine Dame aus der Menge A_i von Kandidatinnen in Frage kommt. Die Männer können unter diesen Umständen genau dann „verheiratet“ werden, wenn es ein Repräsentant(inn)ensystem für (A_1, \dots, A_n) gibt.

Hinreichende Bedingungen. Oft kann man schon aus einfacheren Bedingungen ersehen, dass ein System $\mathcal{A} = (A_1, \dots, A_n)$ von Mengen $A_i \subseteq X$ ein Repräsentantensystem gestattet. Nennen wir z.B. \mathcal{A} ρ -regulär, wenn es eine Zahl $\rho \geq 1$ gibt mit der Eigenschaft

- 1) Jedes A_i enthält mindestens ρ Elemente $x \in X$.
- 2) (2) Jedes $x \in X$ liegt in höchstens ρ vielen Mengen A_i .

KOROLLAR 6.3. Ein ρ -reguläres Mengensystem $\mathcal{A} = (A_1, \dots, A_n)$ besitzt ein Repräsentantensystem.

Beweis. Wir zeigen, dass \mathcal{A} die Hallsche Bedingung (58) erfüllt. Dazu betrachten wir z.B.

$$A = A_1 \cup \dots \cup A_k.$$

Zum Nachweis von $|A| \geq k$ wenden wir das Prinzip des doppelten Zählens auf die Menge

$$\mathbf{A} = \{(x, A_i) \mid x \in A_i, 1 \leq i \leq k\}$$

an. Unter Berücksichtigung der Regularitätseigenschaften (1) und (2) finden wir

$$k\rho \leq \sum_{i=1}^k |A_i| = |\mathbf{A}| \leq \sum_{m \in A} \rho = |A|\rho.$$

Division durch ρ ergibt nun $k \leq |A|$, wie gewünscht.

EX. 6.4 (Lateinische Rechtecke). Es sei A eine Matrix mit m Zeilen und n Spalten derart, dass jedes der n Symbole eines Alphabets Σ in jeder Zeile genau einmal, in jeder Spalte jedoch höchstens einmal auftritt. Eine solche Matrix A ist ein lateinisches Rechteck.

BEHAUPTUNG: Im Fall $m < n$ kann man die Matrix A zu einem lateinischen Rechteck mit $m+1$ Zeilen erweitern. (Man erhält also nach $n-m$ solchen Erweiterungen ein lateinisches Quadrat).

Zum Beweis ordnen wir jeder Spalte i genau die Menge A_i der Symbole zu, die in der bisherigen i -ten Spalte von A nicht(!) auftreten. Das System (A_1, \dots, A_n) ist ρ -regulär mit $\rho = n-m$. Also existiert ein Repräsentantensystem $R = (r_1, \dots, r_n)$, welches als neue Zeile das bisherige lateinische Rechteck A in zulässiger Weise erweitert.

2.3. Ketten und Antiketten. Wir gehen hier von einer sog. Halbordnung $P = (V, \prec)$ aus (d.h.: die Relation \prec ist azyklisch und transitiv auf V). Zusätzlich zum schon eingeführten Kettenbegriff definieren wir nun eine Antikette in P als eine Menge $A = \{a_1, \dots, a_k\} \subseteq V$ derart, dass gilt:

$$a_i \not\prec a_j \quad \text{für alle } i \neq j.$$

Anders gesagt ist eine Antikette eine Menge, die aus jeder Kette höchstens 1 Element enthält. Die Weite $w(P)$ von P ist die maximal mögliche Mächtigkeit einer Antikette:

$$w(P) := \max\{|A| \mid A \subseteq M \text{ Antikette in } P\}.$$

Zum Beispiel hat eine Kette $K \neq \emptyset$ die Weite $w(K) = 1$.

EX. 6.5. Sei $V = 2^N$ die Potenzmenge einer n -elementigen Menge N unter der Enthaltenseinsrelation $P = (2^N, \subset)$. Dann folgt aus dem Spernerschen Satz 1.2:

$$w(P) = \binom{n}{\lfloor n/2 \rfloor}.$$

Eine Kettenüberdeckung von P ist eine Menge $\mathcal{K} = \{K_1, \dots, K_\ell\}$ von Ketten in P mit der Eigenschaft

$$V = \bigcup_{i=1}^{\ell} K_i.$$

Dann gilt sicherlich $\ell \geq w(P)$, da K ja insbesondere die Elemente einer maximalen Antikette überdecken muss. Wir suchen eine sog. Dilworthzerlegung von P , d.h. eine Kettenüberdeckung $\mathcal{K} = \{K_1, \dots, K_\ell\}$ mit möglichst wenig Ketten. Sicherlich dürfen wir die Ketten in \mathcal{K} als paarweise disjunkt annehmen, da das Entfernen eines redundanten Elementes aus einer Kette ja die Anzahl der Ketten nicht vergrößern würde.

Um die Beziehung zum Matchingproblem deutlich zu machen, nehmen wir eine Menge $\mathcal{K} = \{K_1, \dots, K_\ell\}$ paarweise disjunkter Ketten als gegeben an und betrachten den P zugeordneten bipartiten Graphen $G = (V \cup V', E)$, wobei V' eine disjunkte Kopie von V ist und die Kanten in E die Relation P wiedergeben:

$$(v, w') \in E \iff v \prec w \text{ in } P.$$

Eine Kette $K = \{v_0 \prec v_1 \dots \prec v_h\} \in \mathcal{K}$ entspricht nun den h paarweise disjunkten Kanten

$$(v_0, v'_1), (v_1, v'_2), \dots, (v_{h-1}, v'_h)$$

in G . Folglich lässt sich aus den ℓ Ketten von \mathcal{K} auf diese Weise ein Matching M in G konstruieren. Man macht sich leicht klar:

$$|V| = |K_1 \cup \dots \cup K_\ell| = \ell + |M|.$$

Umgekehrt gehen wir von einem Matching M in G aus und konstruieren daraus eine Kettenüberdeckung von P auf folgende Weise:

Die Matchingkanten $(v, w') \in M$ ergeben $|M|$ viele 2-elementige Ketten $v \prec w$, von denen keine zwei denselben Anfangs- oder denselben Endpunkt haben. Diese Ketten setzen wir nun zusammen, um möglichst lange Ketten zu bauen:



WAGENINGEN UNIVERSITY
WAGENINGEN UR

WILLST DU EINFLUSS AUF EINEN GESUNDEN LEBENSRAUM HABEN?

DANN DENKE AN DIE WAGENINGEN UNIVERSITY IN DEN NIEDERLANDEN

Bist du an einem Master auf dem Gebiet der innovativen Methoden und nachhaltigen Lösungen interessiert, um die Qualität unseres Lebensraumes zu verbessern? Dann denke an die Wageningen University. Hier findest du besondere Umweltstudien wie **Nachhaltiger Tourismus, Sozialökonomische Entwicklung, Umwelt und Innovative Technologien**. Diese multidisziplinäre Herangehensweise macht diese Masterstudiengänge einzigartig!



Um mehr Information zu erhalten, gehe zu www.wageningenuniversity.eu







$$(59) \quad v_0 \prec v_1 \prec \dots \prec v_h \iff (v_{j-1}, v'_j) \in M \text{ für } j = 1, \dots, h.$$

Sei $\tilde{\ell}$ die Anzahl der Ketten, die man so am Ende erhält. Wir überlassen es dem Leser sich klarzumachen, dass diese paarweise disjunkt sind und zusammen

$$\tilde{\ell} + |M|$$

Elemente der Grundmenge V überdecken. Diesen Ketten fügen wir noch alle 1- elementigen Ketten $\{v\}$ der Elemente $v \in V$ hinzu, die in den bisherigen Ketten noch nicht vorkommen. So erhalten wir insgesamt eine Kettenüberdeckung $\mathcal{K} = \{K_1, \dots, K_\ell\}$, für welche gilt:

$$|V| = \ell + |M| \quad \text{bzw.} \quad \ell = |V| - |M|.$$

Sei ℓ^* die Anzahl von Ketten einer minimalen U'' berdeckung \mathcal{K} von P . Dann zeigen unsere bisherigen U'' berlegungen:

$$(60) \quad |V| - \max\{|M| \mid M \text{ Matching in } G\} = \ell^* \geq w(P),$$

da eine Antikette aus jeder Kette ja höchstens 1 Element enthalten darf. Tatsächlich gilt in (60) sogar durchweg Gleichheit:

SATZ 6.4 (Dilworth³⁷). P gestattet eine U'' berdeckung mit $w(P)$ paarweise disjunkten Ketten.

Beweis. Sei $|M|$ ein maximales Matching im P zugeordneten bipartiten Graphen $G = (V \cup V', E)$. Unter Berücksichtigung von (60) bleibt noch zu zeigen, dass P eine Antikette A mit $|A| \geq |V| - |M|$ Elementen besitzt. Das ist aber leicht:

Denn Korollar 6.2 garantiert ja eine Kantenüberdeckung $C_1 \cup C'_2 \subseteq V \cup V'$ in G mit $|C_1 \cup C'_2| = |M|$ Knoten. Wir beobachten:

$$A := V \setminus (C_1 \cup C'_2) \text{ ist eine Antikette in } P.$$

Gäbe es nämlich Elemente $v, w \in A$ mit $v \prec w$, dann wäre (v, w') eine Kante in G , die durch $C_1 \cup C'_2$ nicht abgedeckt wäre! Diese Antikette A leistet das Gewünschte:

$$|A| \geq |V| - |C_1 \cup C'_2| = |V| - |M|.$$

2.4. Konformität. Sei $G = (V, E)$ ein orientierter Graph mit Inzidenzmatrix $A = [a_{ve}] \in \mathbb{R}^{V \times E}$. Wir bewerten die Länge eines Flusses $x : E \rightarrow \mathbb{R}$ durch die Betragsnorm

37 R.P. DILWORTH (1912-1993)

$$|x| := \sum_{e \in E} |x_e|.$$

Die folgende einfache Beobachtung sei dem Leser überlassen:

LEMMA 6.4. Für alle Flüsse $x, y \in \mathbb{R}^E$ gilt die Dreiecksungleichung

$$|x + y| \leq |x| + |y|.$$

Ausserdem hat man

$$|x + y| = |x| + |y| \iff x_e \cdot y_e \geq 0 \forall e \in E.$$

Im Fall $|x + y| = |x| + |y|$ (bzw. $x_e y_e \geq 0$ für alle $e \in E$) nennen wir die Flüsse x und y *konform*. Wir konzentrieren uns nun vor allem auf Zirkulationen und erinnern daran, dass wir einen Kreis

$$K \iff v_0 e_1 v_e e_2 \dots e_k v_0,$$

mit seinem (Kanten-)Inzidenzvektor identifizieren, wobei die Komponenten gegeben sind als

$$K_e = \begin{cases} +1 & \text{wenn } e \text{ Vorwärtskante} \\ -1 & \text{wenn } e \text{ Rückwärtskante} \\ 0 & \text{sonst.} \end{cases}$$

Ganzzahlige Zirkulationen. Mit der Argumentation wie im Beweis des Zirkulationslemmas 6.1 kommen wir zu speziellen ganzzahligen Aussagen.

LEMMA 6.5. Sei $E \rightarrow \mathbb{Z}$ eine ganzzahlige Zirkulation mit $\text{tr}(x) \neq \emptyset$. Dann existiert ein zu x konformer Kreis K mit $\text{tr}(K) \subseteq \text{tr}(x)$.

Beweis. Wir wählen eine Kante $e_0 \in \text{tr}(x)$. Ist e_0 eine Schlinge, dann ist ein Kreis der gesuchten Art schon gefunden. Ist e_0 keine Schlinge, setzen wir

$$\begin{aligned} v_0 &:= e_0^+ \text{ und } v_1 := e_0^-, & \text{wenn } x_{e_0} > 0 \\ v_0 &:= e_0^- \text{ und } v_1 := e_0^+, & \text{wenn } x_{e_0} < 0 \end{aligned}$$

und beginnen einen Pfad $v_0 e_0 v_1$, bei dem e_0 konform mit x_{e_0} ist. Da x eine Zirkulation ist, muss v_1 Endknoten einer Kante $e_1 \in \text{tr}(x)$ sein, bei der gilt

entweder $v_1 = e_1^-$ und $x_{e_1} > 0$ oder $v_1 = e_1^+$ und $x_{e_1} < 0$.

Wir können also den Pfad über eine x -konforme Kante fortsetzen:

$$v_0 e_0 v_1 e_1 v_2 \dots \text{ usw.}$$

Nach endlich vielen Schritten wird so ein Knoten erreicht werden, der schon zuvor besucht wurde. Damit ist ein geschlossener Pfad P mit $\text{tr}(P) \subseteq \text{tr}(x)$ gefunden, dessen Kanten konform mit x sind. P enthält (mindestens) einen Kreis K , der natürlich auch konform mit x ist.

LEMMA 6.6 (Tutte³⁸). Sei $x : E \rightarrow \mathbb{R}$ eine Zirkulation mit $\text{tr}(x) \neq \emptyset$. Genau dann ist x ganzzahlig, wenn es konforme Kreise $K^{(1)}, \dots, K^{(\ell)}$ gibt derart, dass

$$x = \sum_{i=1}^{\ell} K^{(i)} \quad \text{und} \quad |x| = \sum_{i=1}^{\ell} |K^{(i)}|.$$

Beweis. Eine Summe von Kreisen ergibt immer eine Zirkulation mit ganzzahligen Flusswerten auf den Kanten. Also ist die Bedingung hinreichend. Um die umgekehrte Richtung einzusehen, nehmen wir an, dass eine Zirkulation $x : E \rightarrow \mathbb{Z}$ mit $\text{tr}(x) \neq \emptyset$ existiert, die sich nicht in der behaupteten Art darstellen lässt. Sei x ein Gegenbeispiel mit Betragsnorm $|x|$ so klein wie möglich.

38 W.T. TUTTE (1917-2002)

LOCATION: ZÜRICH



ONE YOU
One Credit Suisse

ROMY WOLLTE UNSERE IT-STRATEGIE MITGESTALTEN. WIR GABEN IHR DIE MÖGLICHKEIT DAZU. Im Frühling 2009 wurde Romy mit dem Aufbau einer IT-Management-Schulung betraut, um die Implementierung eines neuen Betriebsmodells zu begleiten. Heute ist diese Ausbildung ein strategisches Programm zur Prozessoptimierung. Die daraus resultierenden Impulse bedeuten für uns einen grossen Schritt – die Erfahrungen und Kontakte zum Top-Management für sie einen Karrieresprung. Lesen Sie Romys Geschichte unter credit-suisse.com/careers

CREDIT SUISSE

Download free eBooks at bookboon.com



Nach Lemma 6.5 existiert ein zu x konformer Kreis K mit $\text{tr}(K) \subseteq \text{tr}(x)$. Dann ist $x' := x - K$ eine ganzzahlige Zirkulation mit kleinerer Betragsnorm

$$|x'| < |x|.$$

Im Fall $\text{tr}(x') = \emptyset$ haben wir $x = K$ und erkennen, dass x kein Gegenbeispiel ist. Im Fall $\text{tr}(x') = \emptyset$ gibt es (wegen der Betragsminimalität des Gegenbeispiels x) Kreise $K^{(1)}, \dots, K^{(\ell-1)}$ derart, dass

$$x' = \sum_{i=1}^{\ell-1} K^{(i)} \quad \text{und} \quad |x'| = \sum_{i=1}^{\ell-1} |K^{(i)}|.$$

Aber dann ergibt sich mit $K^\ell = K$ auch eine Darstellung von x der gesuchten Art:

$$|x| = |x' + K| = |x'| + |K| = \sum_{i=1}^{\ell} |K^{(i)}|.$$

Die Annahme der Existenz eines Gegenbeispiels ist damit ad absurdum geführt. Dass die behaupteten Kreise $K^{(i)}$ paarweise konform sind folgt aus der Betragsgleichheit in der Summendarstellung.

Pfadssysteme. Wir halten im orientierten Graphen $G = (V, E)$ eine Kante f mit den zwei Endknoten $s := f^+$ und $t := f^-$ fest und betrachten die Menge \mathcal{P} aller schlichten Pfade von s nach t , welche die Kante f nicht benutzen. Jeder solche Pfad P wird deshalb mit der Kante f von t zurück nach s zu einem Kreis \overline{P} ergänzt:

$$\overline{P} \longleftrightarrow se_0v_1e_2v_3 \dots v_{k-1}e_k t f s.$$

LEMMA 6.7. Zu beliebigen nonkonformen Pfaden $P, Q \in \mathcal{P}$ existieren konforme Pfade $P \wedge Q, P \vee Q \in \mathcal{P}$ mit den folgenden Eigenschaften:

- (1) $\text{tr}(P \wedge Q) \cup \text{tr}(P \vee Q) \subseteq \text{tr}(P + Q)$.
- (2a) Für alle $e \in E$ mit $(P \wedge Q)_e + (P \vee Q)_e \geq 0$ gilt $(P \wedge Q)_e + (P \vee Q)_e \leq P_e + Q_e$.
- (2b) Für alle $e \in E$ mit $(P \wedge Q)_e + (P \vee Q)_e \leq 0$ gilt $(P \wedge Q)_e + (P \vee Q)_e \geq P_e + Q_e$.
- (3) $|P \wedge Q| + |P \vee Q| < |P| + |Q|$.

Die Summe $x = \overline{P} + \overline{Q}$ der von P und Q induzierten Kreise ist eine ganzzahlige Zirkulation mit $x_f = 2$. Zudem haben wir

$$x_e = (P + Q)_e \quad \text{für alle Kanten } e \neq f.$$

Nach dem Tutte-Lemma 6.6 lässt sich x als Summe von konformen Kreisen ausdrücken. Zwei dieser Kreise, etwa K und K' , müssen wegen $x_f = 2$ die Kante f enthalten. Weil \overline{P} und \overline{Q} nicht konform sind, haben wir

$$|K| + |K'| \leq |x| < |\overline{P}| + |\overline{Q}|.$$

Sei $P \wedge Q$ der (schlichte) Weg von s nach t entlang K und $P \vee Q$ der Weg von s nach t entlang K' (d.h. wir entfernen die Kante f aus den beiden Kreisen). Es ist nun leicht zu sehen, dass $P \wedge Q$ und $P \vee Q$ die geforderten Eigenschaften haben.

BEMERKUNG. Mit den partiell erklärten binären Operationen \wedge und \vee hat \mathcal{P} eine algebraische Struktur. Auf Ungleichungen vom Typ (2) in Lemma 6.7 kommen wir im Rahmen des Diskussion von Sub- und Supermodularität im nächsten Kapitel zurück.

Die Regel von Edmonds und Karp. Wir lassen nun zu, dass der orientierte Graph $G = (V, E)$ mit der ausgezeichneten Kante f und den Knoten $s = f^+$ und $t = f^-$ eine nicht notwendig ganzzahlige Kantenkapazität $c : E \rightarrow \mathbb{R}_+$ hat. Wir wollen zeigen, dass der FF-Algorithmus nach endlich vielen Schritten ein Optimum erreicht, wenn wir Augmentierungen nach der verschärften Zusatzregel von Edmonds und Karp durchführen:

(EK) Unter den möglichen augmentierenden Pfaden wähle man immer einen Pfad P mit möglichst kleiner Betragslänge $|P|$.

Zur Analyse dieser Regel bezeichnen wir zu jeder zulässigen Zirkulation x mit \mathcal{P}^x die Menge der x augmentierenden Pfade $P \in \mathcal{P}$ von s nach t mit minimal möglichen Betrag $|P|$.

LEMMA 6.8. Die Pfade in \mathcal{P}^x sind paarweise konform.

Beweis. Angenommen, es gäbe nicht konforme Pfade $P, Q \in \mathcal{P}^x$ und folglich Pfade $P \wedge Q$ und $P \vee Q$ wie in Lemma 6.7. Wir behaupten, dass diese Pfade notwendigerweise auch augmentieren.

Denn wäre z.B. $P \wedge Q$ nicht x augmentierend, dann gäbe es eine Kante e mit $(P \wedge Q)_e = +1$ und $x_e = c_e$ oder $(P \wedge Q)_e = -1$ und $x_e = 0$. Wir untersuchen beispielsweise den ersten Fall (der zweite Fall kann völlig analog abgehandelt werden). Da $P \vee Q$ konform zu $P \wedge Q$ ist, muss auch $(P \vee Q)_e \leq 0$ gelten und deshalb (Eigenschaft (2b) in Lemma 6.7):

$$1 \leq (P \wedge Q)_e + (P \vee Q)_e \leq P_e + Q_e \quad \text{d.h. } P_e = +1 \text{ oder } Q_e = +1.$$

Dann wäre aber (wegen $x_e = c_e$) entweder P oder Q nicht x -augmentierend!

Da \mathcal{P}^x nur betragsminimale augmentierende Pfade enthält, ergibt sich nun der Widerspruch

$$|P| + |Q| \leq |P \wedge Q| + |P \vee Q| < |P| + |Q|,$$

der die Annahme, P und Q seien nicht konform, ad absurdum führt.

LEMMA 6.9. Sei $P \in \mathcal{P}^x$ und y die aus x gemäss P erhaltende zulässige Zirkulation. Dann gilt für jedes $Q \in \mathcal{P}^y$:

- (i) $|Q| \geq |P|$.
- (ii) $|Q| = |P| \iff Q \in \mathcal{P}^x$.

Beweis. Wir nehmen $Q \notin \mathcal{P}^x$ an und müssen dann $|Q| > |P|$ nachweisen. Dazu beobachten wir, dass P und Q nicht konform sein können, da nach unserer Annahme ja erst eine Augmentierung entlang P eine weitere Augmentierung entlang Q ermöglicht.

Die Pfade $P \wedge Q$ und $P \vee Q$ existieren somit und erweisen sich mit den analogen Argumenten wie im Beweis von Lemma 6.8 als x -augmentierend. Folglich ergibt die Betragsminimalität der Pfade in \mathcal{P}^x die Ungleichungen

$$|P| + |P| \leq |P \wedge Q| + |P \vee Q| < |P| + |Q| \quad \text{und damit} \quad |P| > |Q|.$$

SATZ 6.5 (Edmonds-Karp³⁹). *Wird der FF-Algorithmus von Ford und Fulkerson unter der Regel (EK) ausgeführt, dann werden weniger als $|V| \cdot |E|$ Augmentierungsschritte benötigt.*

Beweis. Wir betrachten ein Stadium des Algorithmus, wo eben ein Augmentierungspfad $P \in \mathcal{P}^x$ mit Betrag $k := |P|$ benutzt wurde. Nach Lemma 6.9 nehmen die Beträge der im weiteren Verlauf des FF-Algorithmus verwendeten Augmentierungspfade nicht ab. Sei m die Anzahl der nächsten Augmentierungen mit Pfaden Q vom Betrag $|Q| = k$. Dann muss $m < |E|$ gelten. Denn diese Pfade liegen alle in \mathcal{P}^x und sind folglich konform. Bei jedem Augmentierungsschritt erreicht mindestens eine Kante ihre Kapazitätsgrenze und kann deshalb bei späteren konformen Augmentierungspfaden nicht mehr auftreten.

Nach weniger als $|E|$ Schritten wird deshalb der Augmentierungspfad Q mindestens Betrag $k + 1$ haben. Andererseits gilt immer $|Q| > |V|$, da Q kreisfrei ist. Also stoppt das Iterationsverfahren nach weniger als $|V| \cdot |E|$ Schritten.

Konstruktion k" urzester augmentierender Pfade. Einen kürzesten augmentierenden Pfad zu einer gegebenen zulässigen Zirkulation x kann man z.B. mit der Methode kürzester Wege (s. Kapitel 3) berechnen. Dazu interpretieren wir die Knoten $i \in V$ als „Städte“, zwischen denen Distanzen $d(i, j)$ folgendermassen erklärt sind:

$$d(i, j) = \begin{cases} 1 & \text{es gibt } e \in E \text{ mit } e^- = i, e^+ = j \text{ und } x_e < c_e \\ 1 & \text{es gibt } e \in E \text{ mit } e^- = i, e^+ = j \text{ und } x_e > 0 \\ \infty & \text{sonst.} \end{cases}$$

Ein kürzester x augmentierender Pfad von s nach t endlicher Länge entspricht einem kürzesten Weg bzgl. der oben gegebenen Distanzen, die ja genau bei den Vorwärts- und den Rückwärtskanten den Zählwert 1 ergeben.

39 J. EDMONDS (*1943), R.M. KARP (*1935)

7 Der Greedy-Algorithmus

Die in diesem Kapitel untersuchten Packungs- und U^* -berdeckungsprobleme sind kombinatorische Grundprobleme, für die im allgemeinen keine effizienten Lösungsverfahren bekannt sind. Sind zusätzlich jedoch sub- und supermodulare Eigenschaften vorhanden, so können sie analog zu den Flussproblemen im Ford-Fulkersonschen Modell angegangen werden.

1 Packungs- und U^* -berdeckungsprobleme

Sei $\mathcal{F} = [f_{ij}] \in \mathbb{R}^{m \times n}$ eine $(m \times n)$ -Matrix mit Koeffizienten $f_{ij} \in \{0, 1\}$ und ohne Nullspalten. Wir fassen die n Spaltenvektoren F^j von \mathcal{F} als die Indikatorfunktionen von n nichtleeren Teilmengen einer m -elementigen Grundmenge $Z = \{z_1, \dots, z_m\}$ zmg auf und identifizieren die Matrix \mathcal{F} mit dem entsprechenden Mengensystem $\mathcal{F} = (F^1, \dots, F^n)$.

Ein ganzzahliger nichtnegativer Vektor $x \in \mathbb{Z}_+^n$ definiert eine *Packung* der Grundmenge Z mit Mengen aus \mathcal{F} dadurch, dass die Mengen F^j jeweils mit der Vielfachheit x^j auszuwählen sind. Die Zahl

$$f_{i1}x_1 + \dots + f_{in}x_n = \sum_{j=1}^n f_{ij}x_j$$

Realise your dreams and ambitions

Mid Sweden University offers a wide range of international programmes in English. This way, you can study, meet new, inspiring people and experience a different culture and environment at the same time. Invest in a first-class education which you will benefit from in years to come – an education that makes a difference.

Apply today!

Learn more at www.miun.se/eng



Mittuniversitetet

MID SWEDEN UNIVERSITY

Discover your opportunities



ist dann genau die Vielfachheit, mit der das Element $z_i \in Z$ durch x insgesamt ausgewählt wird. Bzgl. einer gegebenen Kapazität $c \in \mathbb{Z}_+^m$ nennen wir x zulässig, wenn gilt

$$f_{i1}x_1 + \dots + f_{in}x_n \leq c_i \quad \forall i = 1, \dots, m.$$

Wir suchen eine optimale zulässige Packung x und messen dabei die Qualität von x mit Hilfe einer gegebenen Zielfunktion vom Typ

$$v^T x = v_1x_1 + \dots + v_nx_n \quad \text{mit } v = (v_1, \dots, v_n) \in \mathbb{Z}_+^n.$$

In kompakter Vektor- und Matrixschreibweise ergibt sich das Problem, eine optimale Packung zu bestimmen, als

$$(61) \quad \max_{x \in \mathbb{Z}_+^n} v^T x \quad \text{so, dass } \mathcal{F}x \leq c.$$

Das Problem (61) hat nur endlich viele zulässige Lösungen. Also ist die Existenz von (mindestens) einer Optimallösung garantiert. Trotzdem sind Packungsprobleme im allgemeinen schwer⁴⁰. Wir geben im Folgenden ein paar Struktureigenschaften an, deren Vorliegen den Erfolg eines einfachen Lösungsverfahrens garantiert.

Eine wichtige Argumentationstechnik, um Optimalität einer zulässigen Packung zu beweisen, kommt aus der Dualitätstheorie der linearen Programmierung. Dazu betrachten wir mit der transponierten Matrix $\mathcal{F}^T = [f_{ji}] \in \mathbb{R}^{n \times m}$ Rnm das zu (61) *duale Problem*:

$$(62) \quad \min_{y \in \mathbb{Z}_+^m} c^T y \quad \text{so, dass } \mathcal{F}^T y \geq v.$$

(62) kann als *U^{''} berdeckungsproblem* im folgenden Sinn verstanden werden: Wir fassen die n Zeilenvektoren F_i von F (d.h. die Spaltenvektoren der transponierten Matrix \mathcal{F}^T) als die Indikatorvektoren einer n -elementigen Grundmenge $S = \{s_1, \dots, s_n\}$ auf. Wir suchen eine Packung y der m Mengen F_i derart, dass jedes $s_j \in S$ mindestens mit der Vielfachheit v_j überdeckt wird. Die Qualität von y bewerten wir mit der Zielfunktion

$$c^T y = c_1y_1 + \dots + c_my_m.$$

LEMMA 7.1 (Dualitätslemma). Sei $x \in \mathbb{Z}_+^n$ eine beliebige zulässige Packung bzgl. c und $y \in \mathbb{Z}_+^m$ eine beliebige zulässige *U^{''} berdeckung* bzgl. v . Dann gilt

$$v^T x \leq c^T y.$$

Also ist im Fall $v^T x = c^T y$ die Packung x optimal bzgl. (61) und die *U^{''} berdeckung* y optimal bzgl. (62).

40 In der Sprechweise der Informatik sind allgemeine Packungsprobleme NP-schwer.

Beweis. Nach Annahme sind die Vektoren $x, y, c - \mathcal{F}x$ und $\mathcal{F}^T y - v$ nichtnegativ. Folglich erhalten wir nichtnegative innere Produkte

$$0 \leq y^T (c - \mathcal{F}x) = y^T c - y^T \mathcal{F}x \quad \text{und} \quad 0 \leq x^T (\mathcal{F}^T y - v) = x^T \mathcal{F}^T y - x^T v.$$

Das innere Produkt ändert sich unter Transposition nicht. Somit finden wir

$$c^T y = y^T c \geq y^T \mathcal{F}x = x^T \mathcal{F}^T y \geq x^T v = v^T x.$$

Da nun $c^T y$ als eine allgemeine Obergrenze für die Zielfunktion zulässiger Packungen erkannt ist, muss ein x , welches Gleichheit erreicht, optimal sein. Die Optimalität von y sieht man analog ein.

2. Sub- und Supermodularität

Wir kehren zum Mengensystem $F = (F^1, \dots, F^m)$ und dem Packungsproblem (61) zurück und nennen F *submodular*, wenn es für alle $F^i \neq F^j$ mit nichtleerem Schnitt $F^{i \wedge j}$ und $F^{i \vee j}$ in \mathcal{F} gibt mit den Eigenschaften

- (1) $i \wedge j < i, j$ oder $i \vee j < i, j$.
- (2) $F^{i \wedge j} \cup F^{i \vee j} \subseteq F^i \cup F^j$ und $F^{i \wedge j} \cap F^{i \vee j} \subseteq F^i \cap F^j$.

In intuitiver Notation schreiben wir dann

$$F^i \wedge F^j := F^{i \wedge j} \quad \text{und} \quad F^i \vee F^j := F^{i \vee j}.$$

EX. 7.1. Die Eigenschaft (2) der Submodularität von F bedeutet aus der Sicht der Zeilen-Inzidenzvektoren, dass für jeden Zeilenindex k der Matrix $\mathcal{F} = [f_{k\ell}]$ gilt:

$$f_{k, i \wedge j} + f_{k, i \vee j} \leq f_{ki} + f_{kj}.$$

Der Vektor $v \in \mathbb{Z}_+^n$ heisst *supermodular* bzgl. des submodularen Systems F , wenn für alle $F^i \neq F^j$ mit $F^i \cap F^j \neq \emptyset$ gilt

$$v_{i \wedge j} + v_{i \vee j} \geq v_i + v_j.$$

v heisst *fallend* (bzgl. der Anordnung von F), wenn $v_1 \geq v_2 \dots \geq v_n$ gilt.

3. Das lexikographische Optimum

Ein Vektor $x \in \mathbb{Z}^n$ wird *lexikographisch positiv* genannt, wenn es einen Komponentenindex j gibt derart, dass

$$x_j > 0 \quad \text{und} \quad x_i = 0 \quad \forall i < j.$$

Seien $x, y \in \mathbb{Z}^n$ beliebig. Wir nennen x *lexikographisch grösser* als y und notieren dies mit $x \sqsupset y$, wenn der Differenzvektor $x - y$ lexikographisch positiv ist.

EX. 7.2 (Lexikographische Ordnung). Die Relation \sqsupseteq ist azyklisch und transitiv auf \mathbb{Z}^n und für beliebige $x, y \in \mathbb{Z}^n$ gilt genau eine der drei Relationen

$$x = y \quad \text{oder} \quad x \sqsupseteq y \quad \text{oder} \quad y \sqsupseteq x.$$

Insbesondere gibt es unter den zulässigen Packungsvektoren x des Problems (61) einen eindeutig bestimmten lexikographisch maximalen Vektor x^* .

Die lexikographisch maximale Packungslösung x^* für (61) kann man leicht konstruieren: Man beginnt mit der ersten Komponente und macht x_1^* so gross wie möglich, ohne die Kapazitätsbedingung zu verletzen. Dann macht man x_2^* so gross wie noch möglich usw. Diese Vorgehensweise ist als *Greedy¹¹-Algorithmus* bekannt und kann bzgl. der Matrix $\mathcal{F} = [f_{ij}]$ und dem Kapazitätsvektor $c \in \mathbb{Z}_+^m$ mit $c^{(0)} := c$ so formalisiert werden:

GREEDY-ALGORITHMUS:

- (1) Setze $x_1^* = \min\{c_i^{(0)} \mid f_{i1} = 1\}$ und $c^{(1)} := c^{(0)} - x_1^*F^1$.
- (2) Setze $x_2^* = \min\{c_i^{(1)} \mid f_{i2} = 1\}$ und $c^{(2)} := c^{(1)} - x_2^*F^2$.
- (3) Setze $x_3^* = \min\{c_i^{(2)} \mid f_{i3} = 1\}$ und $c^{(3)} := c^{(2)} - x_3^*F^3$.
- (4) usw.

41 greedy (engl.) = gierig

Economy – Business – First
Ermitteln Sie Ihren Marktwert

Einfach einchecken unter www.alma-mater.de und Gehaltsstudie kostenlos downloaden!

Damit Sie beim Verhandeln festen Boden unter den Füßen behalten.

Nutzen Sie Deutschlands großes Akademiker-Netzwerk für Praktika, Diplomarbeiten sowie Jobs für Absolventen und junge Berufserfahrene.

Welcome on Board: www.alma-mater.de

alma mater



Denn die Minima der c_i^k beschreiben ja immer die von der Kapazität implizierte Obergrenze für die Komponentenwahlen x_{k+1}^* .

SATZ 7.1. Sei $F = (F^1, \dots, F^n)$ submodular und im zugehörigen Packungsproblem (61) der Zielfunktionsvektor v supermodular und fallend. Dann ist die lexikographisch maximale zulässige Packungslösung x^* optimal.

Beweis. Sei \hat{x} die lexikographisch maximale unter den optimalen Lösungen. Wir wollen die Annahme, dass x^* nicht optimal sei, zum Widerspruch führen. Dazu dürfen wir $x^* \neq \hat{x}$ unterstellen. Denn sonst wäre $x^* = \hat{x}$ ja optimal.

Sei i der kleinste Index, wo sich \hat{x} und x^* unterscheiden. Dann muss $x_i^* > \hat{x}_i$ gelten, da x^* lexikographisch maximal und damit insbesondere grösser als \hat{x} ist. Folglich gilt

$$\sum_{\ell=1}^i v_\ell \hat{x}_\ell < \sum_{\ell=1}^i v_\ell x_\ell^* \leq \sum_{\ell=1}^n v_\ell x_\ell^* < \sum_{\ell=1}^n v_\ell \hat{x}_\ell.$$

Es gibt deshalb mindestens einen Index $j > i$ mit $\hat{x}_j > x_j^*$. Im Fall $F^i \cap F^j = \emptyset$ könnten wir \hat{x}_i um +1 erhöhen und gleichzeitig \hat{x}_j um +1 erniedrigen, um so eine zulässige Lösung x' zu erhalten, die lexikographisch grösser als \hat{x} ist. Andererseits ist v fallend. Das impliziert aber, dass x' auch optimal sein müsste:

$$v^T x' - v^T \hat{x} = v_i - v_j \geq 0.$$

Damit wäre, im Gegensatz zu unserer Wahl, \hat{x} nicht die lexikographisch optimale Lösung. Wir finden somit, dass $F^i \cap F^j \neq \emptyset$ gelten muss und $F^{i \wedge j}$ und $F^{i \vee j}$ existieren. Wir erhöhen nun die Komponenten $\hat{x}_{i \wedge j}$ und $\hat{x}_{i \vee j}$ um jeweils +1 und erniedrigen gleichzeitig \hat{x}_i und \hat{x}_j um jeweils -1. Da F submodular ist, ergibt der resultierende Vektor x'' eine zulässige Lösung, die lexikographisch grösser als \hat{x} ist. Andererseits erweist die Supermodularität von v auch x'' als optimal:

$$v^T x'' - v^T \hat{x} = v_{i \wedge j} + v_{i \vee j} - (v_i + v_j) \geq 0.$$

Dieser Widerspruch zur Wahl von \hat{x} führt die Annahme, dass x^* nicht optimal sei, ad absurdum.

KOROLLAR 7.1. Ist F submodular und v supermodular und fallend, dann kann das Packungsproblem (61) mit dem Greedy-Algorithmus optimal gelöst werden.

4. Potenzmengensysteme

Wir illustrieren den Greedyalgorithmus bei einem kombinatorischen Standardmodell mit einer Grundmenge E der Mächtigkeit $m = |E|$. \mathcal{F} sei die Familie aller nichtleeren Teilmengen $S \subseteq E$ und $n = |\mathcal{F}| = 2^m - 1$. Gegeben sei eine monotone Funktion $v : \mathcal{F} \rightarrow \mathbb{Z}_+$, d.h. für alle $S, T \in \mathcal{F}$ gilt:

$$S \subseteq T \implies v(S) \leq v(T).$$

Nun ordnen wir F nach dem folgenden Schema an:

- 1) $F^1 := E$.
2. (2) Sind F^1, F^2, \dots, F^j schon definiert, so sei F^{j+1} eine Menge $F \in \mathcal{F} \setminus \{F^1, \dots, F^j\}$ mit möglichst grossem Wert $v(F)$. Gibt es davon mehrere Kandidaten, nehme man einen möglichst grosser Mächtigkeit $|F|$.

EX. 7.3. Man zeige: Das nach dem vorangehenden Schema angeordnete System $F = (F^1, \dots, F^n)$ ist submodular bzgl.

$$F^i \wedge F^j := F^i \cap F^j \quad \text{und} \quad F^i \vee F^j := F^i \cup F^j$$

und der Vektor $v \in \mathbb{R}^n$ mit den Komponenten $v_j := v(F^j)$ ist fallend.

Zu einer gegebenen Kapazität $c : E \rightarrow \mathbb{Z}_+$ ordnen wir die Grundmenge $E = \{e_1, \dots, e_m\}$ emg nach steigenden Kapazitätswerten an, d.h.

$$c(e_1) \leq c(e_2) \leq \dots \leq c(e_m),$$

und definieren dazu die Kette $\mathcal{E} = \{E_1 \supset E_2 \supset \dots \supset E_m\}$ der m nichtleeren Teilmengen

$$E_1 := E \quad \text{und} \quad E_i := E_i \setminus \{e_{i-1}\} \quad \forall i = 2, \dots, m.$$

Die Menge der bzgl. c zulässigen Packungen ist

$$\mathbb{P}(c) = \{x : \mathcal{F} \rightarrow \mathbb{Z}_+ \mid \sum_{F \ni e} x(F) \leq c_e \quad \forall e \in E\}.$$

LEMMA 7.2 (Greedy-Algorithmus). *Im obigen Potenzmengenmodell ist die lexikographisch maximale Packung x^* gegeben durch*

- (1) $x^*(E_1) = c(e_1)$ und $x^*(E_i) = c(e_i) - c(e_{i-1})$ für $i = 2, \dots, m$.
- (2) $x^*(F) = 0$ für alle $F \notin \mathcal{E}$.

Bzgl. der Funktion $\mathcal{F} \rightarrow \mathbb{Z}$ hat x^* deshalb den Zielfunktionswert

$$(63) \quad \boxed{v^T x^* = v(E_1)c(e_1) + \sum_{i=2}^m v(E_i)[c(e_i) - c(e_{i-1})].}$$

Beweis. Wir haben $E = E_1$ und deshalb $x^*(E_1) = c(e_1)$, da e_1 minimale Kapazität hat. Deshalb haben in der Folge alle $F \in \mathcal{F}$ mit $e_i \in F$ den Wert $x^*(F) = 0$. Der nächste Kandidat für einen nichttrivialen x^* -Wert ist $E_2 = E_1 \setminus \{e_1\}$ mit dem Wert

$$x^*(E_2) = c(e_2) - c(e_1).$$

Alle übrigen $F \in \mathcal{F}$ mit $e_2 \in F$ erhalten den Wert $x^*(F) = 0$ usw.

4.1. Rang und Ko-Rang in Graphen. Sei $G = (V, E)$ ein (irgendwie) orientierter Graph und A die zugehörige Inzidenzmatrix. A^S bezeichne die Spaltenteilmatrix von A , die den Kanten der Teilmenge $S \subseteq E$ entspricht. Dadurch ist der Rang einer Kantenmenge als der Rang der entsprechenden Teilmatrix wohldefiniert:

$$(64) \quad r(S) := \text{rg}(A^S) \quad (S \subseteq E).$$

Aus der elementaren linearen Algebra ergeben sich sofort für alle Elemente $e \in E$ und Mengen $S, T \subseteq E$ die folgenden Eigenschaften:

- (M₀) $r(\emptyset) = 0$;
- (M₁) $0 \leq r(S) \leq r(S \cup e) \leq r(S) + 1$;
- (M₂) $r(S \cap T) + r(S \cup T) \leq r(S) + r(T)$ (Submodularität).

Für unser Greedymodell wichtig ist auch die sog. *Korang-Funktion* v , wobei

$$v(S) := r(E) - r(E \setminus S) \quad (S \subseteq E).$$

EX. 7.4. Die Korangfunktion v hat die Eigenschaften

- (1) $v(E) = r(E)$.
- (2) $0 \leq v(S) \leq v(S \cup e) \leq v(S) + 1$.
- (3) $v(S \cap T) + v(S \cup T) \geq v(S) + v(T)$ (Supermodularität).



Für Ihren
Karrierestart
unbezahlbar.
Für Sie kostenlos.




Karriere zum Download
Jetzt dem kostenlosen Staufenbiel Career Club beitreten und die aktuellste Ausgabe als eBook sichern: staufenbiel.de/ebooks

>>> Jetzt downloaden: staufenbiel.de/ebooks



Sei nun $c : E \rightarrow \mathbb{Z}_+$ eine Kantengewichtung. Gemäss Ex. 7.4 und Korollar 7.1 ist bei der Wahl von F als Familie aller nichtleeren Teilmengen $S \subseteq E$ und v als Korangfunktion die Optimalität des Greedy-Algorithmus für das zugehörige Packungsproblem garantiert. Die optimale Lösung x^* produziert nach Lemma 7.2 den Zielfunktionswert

$$\begin{aligned} v^T x^* &= v(E_1)c(e_1) + \sum_{i=2}^m v(E_i)[c(e_i) - c(e_{i-1})] \\ &= r(E_1)c(e_1) + \sum_{i=2}^m [r(E_1) - r(E_1 \setminus E_i)](c(e_i) - c(e_{i-1})) \\ &= c(e_1)r(e_1) + \sum_{i=2}^m c(e_i)[r(E'_i) - r(E'_{i-1})], \end{aligned}$$

mit den komplementären Mengen $E'_i := \{1, \dots, i\}$, d.h.

$$E'_1 = \{e_1\} \quad \text{und} \quad E'_i = E'_{i-1} \cup \{e_i\} \quad (i = 2, \dots, m).$$

4.2. Kruskals Algorithmus. Aus der Sicht der dritten (letzten) Gleichung im vorherigen Abschnitt wird der Greedyalgorithmus bei Graphen zu einem Konstruktionsverfahren für eine gewisse Kantenmenge $T^* \subseteq E$. In dieser Form ist der Greedyalgorithmus auf einem Graphen als Algorithmus von Kruskal⁴² bekannt⁴³.

ALGORITHMUS:

- (1) Ordne $E = \{e_1, \dots, e_m\}$ derart, dass $c(e_1) \leq \dots \leq c(e_m)$.
- (2) Setze $T_0 := \emptyset$ und konstruiere T_1, \dots, T_m iterativ gemäss

$$T_i := \begin{cases} T_{i-1} \cup \{e_i\} & \text{im Fall } r(E'_i) = r(E'_{i-1}) + 1. \\ T_{i-1} & \text{im Fall } r(E'_i) = r(E'_{i-1}). \end{cases}$$
- (3) Gib $T^* = T_n$ aus.

SATZ 7.2. Sei $c : E \rightarrow \mathbb{Z}_+$ eine beliebige Kantengewichtung des Graphen G . Dann gilt:

- 1) Kruskals Algorithmus konstruiert eine kreisfreie Kantenmenge T^* maximaler Kardinalität $|T^*| = r(E)$.
- 2) Für jede Kantenmenge D maximalen Ranges $r(D) = r(E)$ gilt

$$c(D) := \sum_{e \in D} c(e) \geq \sum_{e \in T^*} c(e) = c(T^*).$$

Beweis. Kruskals Algorithmus garantiert

$$|T_i| = r(E'_i) \quad \text{für } i = 1, \dots, m.$$

Also hat man $|T^*| = r(E) = \text{rg}(A)$. Die T^* entsprechende Spaltenteilmatrix A^{T^*} von A ist somit maximal linear

42 J.B. KRUSKAL (1928-2010)

43 tatsächlich wurde der Algorithmus zuerst von O. BORUVKA (1899-1995) entdeckt

unabhängig. Insbesondere ist T^* kreisfrei.

Sei $D \subseteq E$ eine Kantenmenge mit vollem Rang $r(D) = r(E)$. Dann enthält D eine kreisfreie Kantenmenge T maximaler Kardinalität $|T| = r(E)$. Wegen $c(D) \geq c(T)$ dürfen wir also ohne Beschränkung der Allgemeinheit annehmen, dass D selber schon kreisfrei ist (d.h. $D = T$).

Sei $F \in \mathcal{F}$ eine beliebige Kantenteilmenge. Da Teilmengen kreisfreier Mengen natürlich selber kreisfrei sind, haben wir

$$r(D \cap F) + r(D \setminus F) = |D \cap F| + |D \setminus F| = |D| = r(E)$$

und erhalten daraus die Korang-Ungleichung

$$|D \cap F| = r(E) - r(D \setminus F) \geq r(E) - r(E \setminus F) = v(F).$$

Sei $y^D \in \{0, 1\}^E$ der Indikatorvektor von D und F^j ein beliebiger Spaltenvektor von $\mathcal{F} = [f_{ij}]$ (bzw. Zeilenvektor der transponierten Matrix F^T). Dann ergibt sich für das innere Produkt die Korang-Ungleichung

$$\sum_{i=1} f_{ij} y_i^D = |D \cap F^j| \geq v(F^j).$$

Das bedeutet aber, dass y^D eine zulässige Lösung des dem Packungsproblem zugeordneten dualen U[“] berdeckungsproblems (62) ist! Aus dem Dualitätsslemma 7.1 folgt somit die behauptete Ungleichung

$$c(D) = c^T y^D \geq v^T x^* = c(T^*).$$

BEMERKUNG. Eine kreisfreie Kantenmenge T im Graphen $G = (V, E)$ ist in der Sprache der Graphentheorie ein Wald. Ein maximaler Wald ist ein sog. *aufspannender* Wald. Satz 7.2 besagt, dass Kruskals Algorithmus (bzw. der Greedy-Algorithmus) einen aufspannenden Wald minimalen Gewichtes konstruiert. Ein zusammenhängender Wald ist ein sog. *Baum*. Bei einem zusammenhängenden Graphen ergibt der Algorithmus also einen aufspannenden Baum.

BEMERKUNG. Ein Paar $M = (E, r)$ heisst *Matroid*⁴⁴, wenn r eine auf der Potenzmenge von E definierte ganzzahlige Funktion mit den Eigenschaften (M_0) - (M_2) ist. Im Fall der Rangfunktion eines Graphen spricht man von einem *graphischen* Matroid. Man kann leicht einsehen, dass Kruskals Algorithmus in analoger Weise bei jedem Matroid eine Teilmenge $T \subseteq E$ mit $|T| = r(E)$ minimal möglichen Gewichtes konstruiert.

Eine tiefere Einführung in die Theorie der Matroide geht im Rahmen dieses Textes zu weit. Der Leser sei deshalb auf die (umfangreiche) Fachliteratur (z.B. [10] oder [12]) verwiesen.

44 auf deutsch: *das* Matroid

Literaturverzeichnis

- [1] M. Aigner, *Kombinatorik I: Grundlagen der Zähltheorie*, Springer-Verlag, 1975.
- [2] M. Aigner, *Graphentheorie - eine Entwicklung aus dem 4-Farben Problem*, Teubner, 1984.
- [3] M. Aigner, *Diskrete Mathematik*, vieweg studium 68, 2004.
- [4] W.J Cook, W.H. Cunningham, W.R. Pulleyblank und A. Schrijver, *Combinatorial Optimization*, Wiley-Interscience, 1998.
- [5] R. Diestel, *Graphentheorie*, Springer-Verlag, 2010.
- [6] U. Faigle, W. Kern und G. Still, *Algorithmic Principles of Mathematical Programming*, Springer, Texts in the Mathematical Sciences 24, 2002.
- [7] S. Fujishige, *Submodular Functions and Optimization*, Elsevier, 2005.
- [8] L. Lovász, *Combinatorial Problems and Exercises*, North Holland, 1993.
- [9] L. Lovász und M.D. Plummer, *Matching Theory*, North Holland, 1986.
- [10] J.G. Oxley, *Matroid Theory*, Oxford University Press, 2011.
- [11] R.P. Stanley: *Enumerative Combinatorics I, II*, Cambridge University Press, 1997.
- [12] W.T. Tutte, *Introduction to the Theory of Matroids*. Elsevier, 1971.



AUBI-plus

Mit AUBI-plus findest Du Deinen Platz!
Praktika · Trainees · Jobs

Das Karriereportal
www.aubi-plus.de

place for talents

